UCAM

UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Programa de Doctorado Social Science

"A Generic Approach for the Automated Notarization of Cloud Configurations Using Blockchain-Based Trust"

Autor:

Thorsten Weber

Directores:

Prof. Dr. Rüdiger Buchkremer

Prof. Dr. Eva López González

Murcia, Septiembre de 2022

EIDUCAM
Escuela Internacional
de Doctorado

UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

AUTHORIZATION OF THE DIRECTORS OF THE THESIS FOR SUBMISSION

Prof. Dr. Rüdiger Buchkremer and Prof. Dr. Eva López González as Directors[1] of the Doctoral Thesis "A Generic Approach for the Automated Notarization of Cloud Configurations Using Blockchain-Based Trust" by Mr. Thorsten Weber in the Programa de Doctorado en Ciencias Sociales, **authorizes for submission** since it has the conditions necessary for his defense.

Sign to comply with the Royal Decree 99/2011, in Murcia, February 10, 2021.

LOPEZ GONZALEZ EVA - 23312868E
Firmado digitalmente por LOPEZ GONZALEZ EVA - 23312868E
Fecha: 2022.10.25 16:56:39 +02'00'

Rüdiger Buchkremer

Prof. Dr. Rüdiger Buchkremer

Prof. Dr. Eva López González

[1] If the Thesis is directed by more than one Director, both of them must sign this document.

UCAM
EIDUCAM
Escuela Internacional
de Doctorado

ABSTRACT

Due to their scalability, cloud applications have a significant cost advantage for businesses. As a result, companies want both to outsource their data to, and obtain services from, the cloud. However, because most companies have internal policies and compliance requirements for operating and using software applications, the use of cloud applications creates a new challenge for enterprises. Adopting cloud applications is equivalent to outsourcing services in that companies must trust that the cloud application provider will implement internal compliance requirements in the adopted cloud applications. Research has shown that trust and security are key factors that influence the adoption of cloud applications. This dissertation aims to develop a cloud architecture that addresses this challenge by shifting the trust for compliance-driven configurations of cloud applications from the cloud application provider to the blockchain. This work thus seeks to reduce the adoption risk of cloud applications due to compliance requirements. This dissertation uses design science research to create the architecture for shifting trust to the blockchain. A focus group discussion determined the scope of the work. The knowledge base of this work was built using artificial intelligence and a systematic literature review, and the architecture presented was developed and prototyped using the rapid application development method. Mixed-method semi-structured guided interviews were used to evaluate the presented architecture approach and assess the adoption risk reduction qualities. The dissertation showed that the developed software architecture could shift the trust from the cloud provider to the blockchain. The evaluation of the proposed software architecture further demonstrated that the adoption risk due to compliance-driven cloud application configurations could be reduced from "high" to "low" using blockchain technology. This dissertation presents an architecture that shifts the trust for implementing compliance-driven configurations from the cloud provider to the blockchain. Furthermore, it shows that the trust shift can significantly reduce cloud applications' adoption risk.

Keywords: Blockchain, Business Administration, Cloud Computing, Compliance, Risk Management, Software Architecture, Software Engineering, Trust Management

RESUMEN

Debido a su escalabilidad, las aplicaciones en la nube tienen una importante ventaja de costes para las empresas. En consecuencia, las empresas quieren tanto externalizar sus datos como obtener servicios de la nube. Sin embargo, dado que la mayoría de las empresas tienen políticas internas y requisitos de cumplimiento para operar y utilizar aplicaciones de software, el uso de aplicaciones en la nube crea un nuevo desafío para las empresas. La inclusión de aplicaciones en la nube equivale a la subcontratación de servicios en el sentido de que las empresas deben confiar en que el proveedor de aplicaciones en la nube aplicará los requisitos de cumplimiento interno en las aplicaciones adoptadas. La investigación ha demostrado que la confianza y el riesgo están estrechamente relacionados y son factores clave que influyen en la utilización de aplicaciones en la nube. Esta tesis pretende desarrollar una arquitectura en la nube que aborde este reto, trasladando la confianza en las configuraciones de cumplimiento del proveedor de aplicaciones en la nube a la cadena de bloques. Así, este trabajo pretende reducir el riesgo de adopción de las aplicaciones en la nube debido a los requisitos de cumplimiento. En esta tesis, la investigación de la ciencia del diseño se utiliza para crear la arquitectura para trasladar la confianza mencionada a la cadena de bloques. Un grupo de discusión determinó el alcance del trabajo. La base de conocimientos de este trabajo se construyó utilizando inteligencia artificial y una revisión sistemática de la literatura, y la arquitectura presentada se desarrolló y prototipó utilizando el método de desarrollo rápido de aplicaciones. Se utilizaron entrevistas guiadas semiestructuradas de método mixto para evaluar el enfoque de la arquitectura presentada y valorar las cualidades de reducción del riesgo de adopción. La tesis demostró que la arquitectura de software desarrollada podía trasladar la confianza del proveedor de la nube a la cadena de bloques. La evaluación de la arquitectura de software propuesta demostró además que el riesgo de adopción debido a las configuraciones de la nube basadas en el cumplimiento podía reducirse de "alto" a "bajo" utilizando la tecnología blockchain. Esta tesis presenta una arquitectura que desplaza la confianza para la implementación de configuraciones basadas en el cumplimiento de la normativa desde el proveedor de la nube a la cadena de bloques. Además, muestra que el cambio de confianza puede reducir significativamente el riesgo de adopción de las aplicaciones en la nube.

Palabras clave: blockchain, administración de empresas, informática en la nube, cumplimiento, gestión de riesgos, arquitectura de software, ingeniería de software, gestión de confianza

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABI	Application Binary Interface
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AIDS	Anomaly-based Intrusion Detection System
ALMA	Architecture-level Modifiability Analysis
API	Application Programming Interfaces
CA	Certification Authority
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CERN	Conseil Européen pour la Recherche Nucléaire
CIA	Confidentiality, Integrity, and Availability
CLI	Command Line Interface
CMI	Cloud Management Interface
CSF	Critical Success Factors
dApp	Decentralized Application
DevOps	Development and Operations
DSR	Design Science Research
EA	Existing Architecture
ECDSA	Elliptic Curve Digital Signing Schema
EVM	Ethereum Virtual Machine
EU	European Union
FGQ	Focus Group Question
GCM	Galois/Counter Mode
HF	Hyperledger Fabric
HIDS	Host-based Intrusion Detection Systems
HTTP	Hypertext Transfer Protocol

HTTPS	Secure Hypertext Transfer Protocol
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoD	Internet of Drones
IoMT	Internet of Mobile Things
IoT	Internet of Things
IS	Information Systems
ISMS	Information Security Management System
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
kWH	Kilowatt-hours
LDA	Latent Dirichlet Allocation
LRC-DB	Literature Review Collection Database
MDPI	Multidisciplinary Digital Publishing Institute
MITM	Man-In-The-Middle
MRQ	Main Research Question
NIDS	Network-based Intrusion Detection Systems
NIST	National Institute of Standards and Technology
nltk	Natural Language Toolkit
P2P	Peer-to-Peer
PA	Proposed Architecture
PaaS	Platform-as-a-Service
PC	Personal Computer
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PoC	Proof of Concept

PoS	Proof of Stake
PoW	Proof of Work
RAD	Rapid Application Development
REST	Representational State Transfer
RPC	Remote Procedure Call
RQ	Research Question
SaaS	Software-as-a-Service
ScDi	Science Direct
SD	Standard Deviation
SIDS	Signature-based Intrusion Detection System
SLA	Service Level Agreement
SSI	Semi-structured Interviews
STIRL	Systemic Taxonomy for Information Retrieval from Literature
UML	Unified Modeling Language
UTF-8	8-Bit Universal Coded Character Set Transformation Format
VANET	Vehicular Ad-hoc Network
VM	Virtual Machine
Web PKI	Web Public Key Infrastructure
WoS	Web of Science
WWW	World Wide Web
XML	Extensible Markup Language

1 INTRODUCTION

Economists generally consider the world to be in the midst of a fourth industrial revolution characterized by increased interconnectivity, computerization, and artificial intelligence (M. Xu et al., 2018). Today, the economy stands on the brink of a technological revolution that will fundamentally alter the way of living and working. In its scale, scope, and complexity, the fourth industrial revolution will be unlike anything humankind has experienced before (Schwab, 2017). With the fourth industrial revolution, digital technologies have reformed how companies do business (Ritter & Pedersen, 2020). Following advancements in the digital economy (like the internet, e-mail, digital automation, digital payments, social media), the emergence of big data, and the on-demand availability of computing resources (like data storage, or computing power), without direct management (cloud computing) has become a popular technology for reducing burdens on users. Cloud computing's broadband network access and on-demand services provide many advantages over other computing and data storage technologies. These advantages include scalability, availability, and reduced hardware and maintenance expenses (Mell & Grance, 2017; Murthy et al., 2020).

Moreover, cloud computing allows enterprises to pay on demand instead of maintaining in-house data centers (D. Ma, 2007). As a result of these benefits, cloud computing has grown significantly in recent years and may generate additional investments, employment opportunities, and revenues in the future (Etro, 2015). In particular, the provision of software via cloud infrastructure (*cloud applications*) has gained significant economic importance in recent years (Abuhussein et al., 2020). The economic advantages of cloud infrastructure have led application developers to increasingly deploy their applications on cloud infrastructure (Leymann, 2009). Examples of famous cloud applications include "Dropbox", "Microsoft Office 365", or video conferencing software like "Zoom" (Weber & Buchkremer, 2021a).

Despite the considerable benefits and opportunities associated with cloud computing and, more precisely, cloud applications, security risk, and trust concerns have hindered the technology's utilization and mass deployment potential (Lynn et al., 2021; D. Ma, 2007; A. Singh & Chatterjee, 2017). Trust is critical for adopting cloud applications (Cayirci & de Oliveira, 2018). Research reveals that trust barriers in cloud computing arise because data are no longer regulated by the data-owning companies; instead, data are managed by second or third parties (Lynn et al., 2021; A. Singh & Chatterjee, 2017). So that customers must hand over control of their data to others and trust that cloud application providers will process and use the data as promised. Adopting cloud applications is, therefore, a risk for customers (Lynn et al., 2021). Trust between customers and cloud application providers must be established to realize cloud businesses and benefit from the immense advantages of cloud computing (Mayer et al., 1995).

In the light of adopting cloud applications, this dissertation aims to reduce the risk of adopting them. Specifically, this thesis examines the extent to which risks arising from the lack of data control can be reduced. Today, trusting cloud application providers to implement requirements is necessary. This dissertation will change this by introducing a trusted third party – the blockchain.

1.1 MOTIVATION

The world was forever changed when Tim Berners-Lee introduced the idea of the World Wide Web (WWW) at the Conseil Européen pour la Recherche Nucléaire (CERN) research facility in 1989 (Aghaei et al., 2012; Berners-Lee et al., 1994). The Internet subsequently began in the military and quickly achieved its worldwide breakthrough (Abbate, 1994). With the introduction of the Hypertext Transfer Protocol (HTTP), information could be transferred to and from anywhere in the world and consumed using a personal computer (PC) and a web browser. The foundation for online shopping, games, banking, and social media was set.

However, it turned out that something was missing in these early days of the Internet. HTTP was not secure from attackers; information transmitted over the Internet could be intercepted and manipulated (Naylor et al., 2014). Confidential services were thus not possible. To combat this, an extension of the protocol with a security mechanism—HTTPS—was quickly introduced (Rescorla, 2000). HTTPS is a secure version of HTTP that authenticates the communicating endpoints and provides confidentiality for further communication (Naylor et al., 2014). HTTPS has made possible confidential and integrity-protected communications between the server and browser (client) on the WWW. Authentication during the establishment of communication is supposed to ensure that both communication partners (server and client) prove to each other that they are the entity they claim to be (Callegati et al., 2009). This proof of identity helps prevent attacks such as Man-In-The-Middle (MITM). A MITM attack is a special type of eavesdropping attack. In a MITM attack, an attacker interrupts an existing conversation or data link. After inserting themselves in the "middle" of the conversation, the attackers pretend to be both legitimate participants. Placing themselves in the middle enables attackers to intercept and manipulate information and data from both parties in a way that might not be detected.

MITM protection comes with a price — the price of accepting risk and trusting another party involved in the communication to behave as expected. In HTTPS, at least the server must send some proof that it is the server it claims to be (Naylor et al., 2014). The proof of identity has been conventionally realized through the independent confirmation of the identity by a third party using certificates (Naylor et al., 2014). If a trusted third party certifies that the server with which the client wants to communicate is the one it claims to be, then the client trusts this server if the client trusts the presented certificate. As a result, the client no longer has to trust the server but the party that certified the identity of a server. This is known as a chain of trust. In short, a chain of trust describes a relationship — like that between client, third party certifier, and server — in which trust in one partner is replaced by trust for another partner, the latter vouching for the former's trustworthiness. In this way, trust shifts down the chain of communication partners. Since the '90s, the trust shift from web servers to trusted certificate authorities has been integral to Internet communication (Braun et al., 2014).

Today, we see the need for another shift of trust. The processing of growing data has become an essential part of companies' daily business (Noraziah et al., 2017). Digital technologies have reformed companies' business models and practices (Ritter & Pedersen, 2020). In the 1960s, large rooms with heavy and expensive so-called "mainframe" computers marked the beginning of the large-scale data processing era (Tabrizchi & Kuchaki Rafsanjani, 2020). Because the acquisition, operation, and renewal of such self-managed hardware is expensive, in the late '90s, many organizations formed the approach of distributed resource utilization (Tabrizchi & Kuchaki Rafsanjani, 2020). Instead of running a mainframe computer in-house, distributed computing over the Internet allowed computing loads to be shared across multiple computers.

Grid computing developed from distributed computing in the early 2000s (Tabrizchi & Kuchaki Rafsanjani, 2020). Grid computing combines separate computing units into a large infrastructure. Using this method, various computing resources can be available as required (Sadashiv & Kumar, 2011). However, one thing that has not changed with the shift from distributed computing to grid computing is that computing power and monitoring services must be paid for even when not being used (Tabrizchi & Kuchaki Rafsanjani, 2020). For example, the computing infrastructure must keep running after work or on weekends. In an effort to mitigate these costs, the idea of grid computing is, for many companies, subsequently being replaced by a new approach: *cloud computing* (Tabrizchi & Kuchaki Rafsanjani, 2020). As Shuai Zhang et al. (2010) explains,

> With grid computing, you can provide computing resources as a utility that can be used or not. Cloud computing moves forward one step further with on-demand resource provisioning. This eliminates over-provisioning when used with utility pricing. It also removes the need to over-provision in order to meet the demands of millions of users. (Shuai Zhang et al., 2010, p. 3)

In other words, cloud computing provides companies with a flexible computing infrastructure such that they can use the computing power they need when they need it. Unlike grid computing, though, when cloud computing is used, the company only pays for the computing it needs — computing power is treated as a utility, paid for as used and provided by a second or third party. Thus, cloud computing enables a paradigm shift (Bello et al., 2021).

The idea of cloud computing is to share resources among parties and distribute the costs for computing power among the sharing parties according to consumption (Avram, 2014). In recent years, advancements in the digital economy—such as e-business, digital payment, or social media—as well as the emergence of Big Data analytics— analyzing data sets that are too large or complex to be processed by traditional data-processing applications and algorithms—have been characterized by the massive generation and consumption of data. As a result of these greatly increased data demands, cloud computing has become a popular technology for software providers to reduce the infrastructure costs of application hosting, and many software applications are nowadays hosted in the cloud (Abuhussein et al., 2020).

However, the increasing reliance on cloud resources has placed cloud customers in a special dependency (Bomhard & Daum, 2021). Customers entrust their data to cloud application providers just as they placed their trust in HTTP in the earlier days of the Internet. In both cases, clients are obliged to trust the providers' assurance. In the case of HTTP, clients trust that the server is actually the server it claims to be. In cloud computing, clients trust that cloud application providers deliver on their service promises and that data will not fall into the wrong hands. Today, customers must trust cloud application providers to ensure data security (confidentiality, integrity, and availability [CIA]) against threats like MITM, malware, phishing, and data theft (Shaikh & Iyer, 2019). For companies, it is risky to outsource their data to a cloud application; for this reason, trust in the cloud application provider is essential (Lynn et al., 2021; Michael, 2009).

From the large field of outsourcing services (such as the protection of data from third-party access, the physical protection of cloud infrastructures, the monitoring of network infrastructures, or the training and education of administrators with critical system access), this dissertation deals with the topic of compliance requirements. More precisely, this dissertation addresses the existing risk in dealing with *compliance-driven cloud configuration* and *compliance-driven configuration changes*.

Compliance-driven cloud application configurations (short: compliance-driven configurations) are guidelines, policies, or laws issued by an authority (such as a government or company) whose compliance is in the interest of the cloud application user. Examples of compliance-driven configurations are the definition of the data storage location, the backup policy of the cloud application, the firewall settings, the intrusion detection system signatures, or even the appearance of a cloud application. For example, in the case of data storage location, European Union (EU) regulations require that data be stored within the EU or in a jurisdiction where a country outside the EU offers an adequate level of data protection (Voigt & Von dem Bussche, 2017).

To comply with this regulation, a cloud application customer (that operates in the EU) must ensure that its data is stored in a location in the EU or a country that offers adequate data protection. Adjusting the data storage location of a cloud application to the EU regulation is a *compliance-driven configuration change*. Similarly, in the case of firewall settings, compliance-driven configuration changes might include blocking undesirable websites that trivialize violence or extremist views or blocking network access to services such as file sharing or the darknet. In this case, it is in the interest of the cloud service customer that the cloud application provider adjusts the firewall to the service user's specifications. Customers must trust the cloud application provider to ensure this for them.

One case involving a compliance-driven configuration incident occurred at Capital One Bank in 2019. During this incident, a vulnerability allowed hackers the opportunity to steal account and credit card information from millions of customers of Capital One Bank (PRNewswire, 2019). As can be seen from later court records (Department of Justice, 2019), a programmer allegedly bragged about the crime online and posted relevant files on GitHub, a source code hosting website. After investigations by the US police, the guilty person was identified and arrested. In the Capital One Bank case, a police employee involved in the investigation confirmed that “a firewall misconfiguration permitted commands to reach and be executed by that server,” which in turn enabled the intrusion (Department of Justice, 2019). The case of Capital One Bank is neither new nor unique. Table 1 below shows four similar cases recorded in recent years. All cases can be traced to not correct or not sufficient implementing compliance-driven configurations, resulting in an incident.

Table 1: Collection of Data Breaches Due to Configuration Errors

Company	Year	Description
National Electoral Institute of Mexico	2016	Data is stored on an insecure and illegally hosted cloud server situated outside of Mexico (Chris Baraniuk, 2016)
Microsoft	2010	A breach due to a configuration issue in the Business Productivity Online Suite resulted in unauthorized access to employee contact information (de Haes, 2010)
Uber	2016	The data breach occurred due to accidentally placing secret keys on a public website (Choi, 2021)
Adult Friend Finder	2016	Configured to use weak security enhancing algorithms (Alsubhi et al., 2021)

In the case of HTTP, the risks of eavesdropping and receiving manipulated data could be reduced by providing a certificate from a trusted third party. Today, there are two leading trust management systems for securing encryption keys: Web Public Key Infrastructure (Web PKI) and the Pretty Good Privacy (PGP) approach of the Web of Trust (see 3.1.9 for details). Although these trust management systems provide trust, both systems have real-world issues (Bright, 2011; Goodin, 2016). Within the internet, several hundred Web PKI authorities issue certificates trusted by web browsers (Goodin, 2016). Some of these authorities even have sub-authorities that sign certificates in their name. All of these authorities can issue a certificate for any valid domain name.

Consequently, any authority could issue a certificate for a specific domain. This certificate could be used for MITM attacks on the specific domain for which it was issued. The relying party would trust this certificate since a trusted authority signed it. For example, in 2015, some unauthorized certificates issued by the Chinese Certificate Authority were used to decrypt traffic passing through the Great Firewall (Brychta & Hagara, 2017).

The emerging blockchain-based trust management system can overcome the known problems of the existing systems (Alexopoulos et al., 2017; Hawlitschek et al., 2018).

As the case of HTTPS has already shown, a shift in trust (from the server with which communication takes place to certificates and their issuers) can lead to implementing new security mechanisms and finally reduce risks. This dissertation investigates how trust can be shifted from the cloud application provider to the blockchain and how this shift might affect the risk of adopting cloud applications from a compliance-driven configuration perspective.

1.2 RISKS IN ADOPTING CLOUD COMPUTING

In 2009 Bret Michael observed that trust plays an essential role in cloud computing (Michael, 2009). Nowadays, trust in the cloud and cloud application providers is a main limiting factor for cloud service adoption in enterprises (J. Huang & Nicol, 2013; Lyons, 2021; Moreno-Vozmediano et al., 2013; Takabi et al., 2010). Adopting cloud services includes four main risks for an organization (Lyons, 2021). These are *relational, performance, technological, compliance and regulatory risks*.

Relational risks were defined by Das and Teng (1996) and address the risk of inter-firm alliances. According to Das and Teng, in a relational risk scenario, firms do not cooperate in the agreed or expected manner; moreover, they do not cooperate in pursuit of jointly set goals or cooperate differently than expected by the partners. Relational risk arises, for example, when a financial company lends money to another company. The financial company must trust that the lent company will follow the agreed goals using the money. There is a risk that the lent company will not do so.

Performance risks arise when a customer cannot use its cloud service because it is unavailable or does not perform as expected (Lyons, 2021). In the financial example, performance risk refers to a financial company investing in a company. After the investment, the financial company has the risk that the invested company does not perform as expected. On the other hand, the invested company has the risk that the financial company exits early to prevent/minimize possible financial losses due to the poor performance of the invested company.

Technological risks are related to the information technology (IT) security and quality of cloud providers' service, as addressed by Ackermann et al. (2011). The security challenges in cloud computing involve potential threats to objectives of IT security, such as CIA, performance risks (network or scaling issues), accountability (poor identity management), reliability risks (provider quality issues), maintainability risks due to lack of innovation and investment (leading to cloud service obsolescence), and regulatory risks (intellectual property theft or data disclosure) (Ackermann et al., 2011).

Compliance and regulatory risks arise from the risk that a company may be subject to sanctions from third parties because it has not complied with applicable policies or laws (Anderson et al., 2014). Compliance risks involve illegal practices, including fraud, scamming, data theft, bribery, money laundering, and embezzlement. A common compliance risk in cloud computing is the violation of privacy laws. To be more precise, the 2022 Cloud Security Report shows that, for one out of three companies (33%), legal and regulatory compliance are the biggest barriers preventing cloud adoption (ISC2 Foundation & Cybersecurity Insiders, 2022). Various other studies have made similar observations regarding the significance of compliance and the associated adoption of cloud services in different sectors and countries (M. A. Khan & Salah, 2020; Phaphoom et al., 2015; Swanson, 2010; Tweneboah-Koduah et al., 2014).

In the broad area of cloud computing adoption risks, this dissertation places itself in the topic area of compliance and regulatory risks.

1.3 FACTORS INFLUENCING COMPLIANCE-BASED RISKS

This dissertation deals with risks that arise for a company due to the need to fulfill compliance requirements. By outsourcing services, companies have to transfer control over them (at least partially). To understand which compliance-related cloud application adoption risks (In the following, also abbreviated as *adoption risks*) exist, one must understand both compliance-based risks and whether or how the adoption risk of compliance-based requirements can be reduced. Research shows significant compliance and regulatory risks of adopting cloud applications (Lynn et al., 2021). Research also shows which factors influence the risk of non-compliance (Alali & Yeh, 2012). The following section briefly discusses these factors and explains how compliance-related risks can influence the adoption of cloud applications. When considering compliance risks, it is important to note that they are not standardized. Various authors have identified different risks related to cloud adoption (Ali & Osmanaj, 2020; Brandis et al., 2019; Rakesh Kumar & Goyal, 2019; Yimam & Fernandez, 2016). Thus, there is no standardized list of compliance-related risks. This dissertation summarizes various identified risks into three overall compliance-related risks. Summarizing the risks has the advantage that the broadest possible spectrum of risks can be examined during the dissertation. At the same time, however, abstraction has the disadvantage of losing details. For example, very specific risks (e.g., for certain industries or professional groups) may be lost due to the generalization. This is a limitation that the author of the thesis is aware of. However, the dissertation aims to show whether a shift of trust to the blockchain for the configuration of cloud applications is possible in principle and to what extent this reduces compliance-related cloud adoption risks. If the dissertation can show that a reduction of risks is possible in general, then in the further course, it can also be investigated whether a reduction is possible for a specific use case/profession. Therefore, the abstraction of risks is accepted for the course of this dissertation.

1.3.1 Transparency Risk

The Cambridge dictionary defines transparency as "the quality of being done in an open way without secrets" (Cambridge Dictionary, 2022). For this dissertation, transparency is seen as the open availability of information. As stated by Yimam and Fernandez (2016), "In the case of [cloud applications], consumers are responsible to secure data; service providers are responsible to secure services, platforms and infrastructures. In general, the lack of full control and transparency creates compliance challenges in the cloud." Transparency is an important mechanism that removes the trust barrier between enterprises and cloud services (van der Werff et al., 2019).

Trust in business partners is essential whenever information is not openly accessible to all parties, as is necessarily the case when using cloud services to store sensitive data. Hence, transparency is key in building trust and reducing business risk through adopting cloud applications.

Beserra et al. (Beserra et al., 2012) describe the cloud migration process. First, the potential cloud customer researches a possible cloud service provider or cloud services. For example, this research can be done via the cloud provider's web presence. The information researched may include the configuration of backups, the storage duration of access data, the storage location, or the security mechanisms used by the cloud service provider. For example, one customer may be attracted by a cloud service that stores data indefinitely for a one-time fee, while another may be interested in a yearly subscription service.

Once a customer decides on a cloud service provider, the data must be moved to the cloud. This is the second step. To begin moving the data, cloud customer A (trustor) makes their data available to cloud service provider B (trustee). In other words, A makes the first step in moving the data by providing it to B. In the next step, it is B's turn. B must prove that the trustee processes, stores, and secures the data and configurations as promised. In other words, until B's assurance, it is uncertain whether the trustee will return the advance made in expectation of a benefit for the trustor. This state of affairs is referred to by Coleman as the trust problem (Gibbs & Coleman, 1990). That is, there is a problem of trust between A (trustor) and B (trustee) because A must take the initial risk of sharing data before knowing whether B will keep the data secure.

Business risks now arise for A. If B does not act as agreed, A may incur a monetary loss due to non-compliance with government, customer, or the trustee's own requirements, including insolvency. To name just a few standards to which companies may have to adhere (Susanto et al., 2011):

- International Standards Organization (ISO) 27000-series,
- British Standard (BS) 7799,
- Payment Card Industry Data Security Standard (PCI-DSS),
- Information Technology Infrastructure Library (ITIL),
- Control Objectives for Information and related Technology (COBIT).

For example, a customer may choose to process credit card payment data. In that case, the PCI-DSS standard must be followed (Susanto et al., 2011). PCI-DSS stood for Payment Card Industry Data Security Standard and was developed by the PCI Security Standards Council to reduce fraud in credit card payments on the Internet (Susanto et al., 2011). All companies that process cardholder data must be PCI DSS compliant (Susanto et al., 2011). Complying with PCI-DSS means that a company takes appropriate measures to protect the data in question from cyber theft and fraudulent use. For example, the 2020 Cyber Security Breaches Survey (Johns, 2020) found that 28% of all businesses adhere to the PCI-DSS standard, rising to four in ten large businesses (42%). A quarter of large businesses (24%) adhere to ISO 27001. Moreover, the 2020 Cyber Security Breaches Survey revealed that four in ten businesses (39%) reported any kind of cyber security breach or attack in the last 12 months. With this in mind, it is more important than ever to take responsibility for this customer data and ensure it is protected through compliance.

After the contracts have been concluded, both parties must implement the agreed requirements. E.g., the agreed-upon agreement may require the cloud application provider to implement data storage location or backup policy specifications. The cloud customer (A) must trust that the service provider (B) will implement this as promised. For example, suppose that application provider B agrees to backup the information on the cloud at a regular interval (e.g., every six months). Cloud customer A depends on the cloud application provider implementing the backup frequency as contractually agreed. Customer A must rely on the cloud provider that the provider follows the contractually agreed backup frequency – the schedule for how often data should be backed up – and therefore runs the risk that their requirements will not be implemented as stipulated.

Enterprises must trust application providers to ensure that agreements are fulfilled as negotiated and that the provided data will not fall into the wrong hands. Multiple approaches—like reputation systems, service level agreements (SLAs), transparency mechanisms, or external audits—have been presented as avenues for increasing trust in cloud service adoption (J. Huang & Nicol, 2013; K. M. Khan & Malluhi, 2010). Hence, the shift of trust to third parties is already taking place.

However, existing approaches have a critical weakness: they all rely on the customer trusting another company. In the case of reputation systems – like Google or Amazon ratings – the customer must trust that each rating is independently conducted and the ratings received are genuine. In the case of SLAs, the customer must trust that the provider will deliver on the agreements. SLAs can be seen as client and service provider agreements for recurring services. SLAs provide a monitoring possibility to make it transparent for the client by precisely describing promised service characteristics such as the scope of service, response time, and processing speed (J. Huang & Nicol, 2013). Finally, in the case of transparency mechanisms, such as service certification, the customer must trust that the certifier is working according to the guidelines set by the accreditation body (J. Huang & Nicol, 2013). For external audits, the customer must trust the external auditor.

One way to overcome the trust problem of external audits would be by conducting vendor audits. A vendor audit is an instrument for selecting and evaluating new or existing suppliers. In this process, the supplier's current performance is determined based on an as-is analysis and compared with the target state contractually agreed between the two parties. By taking a detailed look at the supplier's value creation processes, gaps and potential for improvement can be discovered. However, conducting vendor-party audits comes with additional expenditures: increased expenses for communication, planning, and travel costs are just a few (Razaque et al., 2021). Hence, existing transparency-aiming trust-enhancing mechanisms have limitations.

1.3.2 Process Automation Risk

Process automation risks are part of operational risks (Jarrow, 2008). A process automation risk exists when the process that supports a business activity lacks both efficiency and effectiveness, leading to financial, customer, and reputational loss. The reasons for process automation risks are error-prone manual processes or a lack of process automation. For this reason, process risks are also referred to as automation risks in the remainder of this dissertation. In the area of cloud compliance, automation risks may occur due to manual adaptation processes.

Today, compliance-driven cloud application changes are typically commissioned by consultants (Martens et al., 2012). Enterprises communicate their changes to the cloud application consultants, who in turn pass on these change requests internally or implement them on behalf of the customer. Cloud application adaptations are routinely associated with costs for the consultant service and a time delay (Makhlouf, 2020). A 2015 survey of 250 IT managers revealed that over 70% of companies that relied on additional cloud services were confronted with unforeseen or unexpected costs (McCafferty, 2015). Unexpected expenses can easily double the initial budget and play a crucial role in adopting risk (Zimmerman, 2014). Moreover, even if compliance-driven configurations can be implemented transparently, the time factor can still be essential in mitigating risks. Thus, the extra costs and the extra time associated with compliance-driven cloud application changes present significant barriers to adoption.

1.3.3 Repudiation Risk

Today, delays in court cases are common worldwide (Velde et al., 2022). Reports have shown that delaying court cases has led to evidence being destroyed, missed, or lost (Velde et al., 2022). Thus, important evidence will likely be destroyed or lost if a dispute arises between two parties. The loss of evidence inevitably leads to the risk that one of the parties involved in the dispute will take advantage of this situation and repudiate any - now unverifiable - misconduct. Hence, there is a need for technology usage to protect court proceedings, making them accessible with ease and ensuring that there is non-repudiation and data integrity (Velde et al., 2022). In the dissertation’s context, non-repudiation means something cannot be denied. Notaries reach non-repudiation (J. Zhou & Gollmann, 1996). A notary is a trusted entity (like Web PKI, PGP, or blockchain) that provides evidence of a message exchanged between entities (such as its origin and integrity) (J. Zhou & Gollmann, 1996). Notarization is provided via a notarization mechanism like digital signatures (see 3.1.7). In other words, non-repudiation is the certainty that a signature under a document or the sending of a message comes from a certain originator. A notarized message is, therefore, a message that cannot be denied and has been digitally signed by a digital notary (such as Web PKI, PGP, or blockchain).

For this reason, cloud application providers must not only safeguard transparency but also ensure that any changes to data or configuration decisions are clearly documented. In case of doubt about a cloud service's transparency (e.g., due to data breach, audit requirements, or legal requirements), which party made which changes must be traceable. Dykstra and Sherman have described the traceability requirement as follows:

> When brought to court, the judge or jury must ultimately decide if they believe and trust the evidence presented to them. This choice embodies a specific confidence about whether the result is accurate and reliable.[…]. Consider an example where a single desktop computer has been used to plan a murder. If law enforcement removes the hard drive for imaging, they must trust their hard drive hardware to read the disk correctly. If they run forensic tools on the live computer, they may have to trust the integrity of the host operating system in addition to the hardware. If the suspect computer was hosted in the cloud, new layers of trust are inherently introduced. (Dykstra & Sherman, 2012, p. 92)

This example from Dykstra and Sherman demonstrates a chain of trust in the case of a murder investigation. Law enforcement must trust their hardware and multiple third-party software providers, like the host operating system and cloud application provider. While this example concerns a murder investigation, the same chain of trust is involved in data breaches. Later in this dissertation, it will be shown how blockchain technology can be used to build a chain of trust for compliance-driven configuration changes digitally.

As the case of Capital One Bank shows (see 1.1), when data stored on the cloud is compromised, an investigative authority must investigate the case and bring it to court. The court must then clarify which party is responsible for the incident and who may be held liable. If a party denies an action, or if an action cannot be definitively assigned to a party, a repudiation risk arises for one of the two parties involved. This could include risk of increased cost or time spent in litigation, risk to the party’s professional reputation, or risk of another data breach if the liable party is not identified (or misidentified). Similarly, incorrect or insufficient evidence can increase costs and the likelihood of adverse court decisions (Brown, 2016).

Therefore, the traceability of decisions, compliance-driven configurations, and settings, as well as their clear assignment via non-repudiable evidence to individual parties, is decisive in criminal investigations (Brown, 2016; Velde et al., 2022). The clear assignment of actions is in the interest of both the plaintiff and the defendant. Using tamper-proof ways to execute and document configuration decisions is thus advantageous for both the cloud application provider and the customer. It is important to underline that transparency applies to a cloud application provider and its customers. Ultimately, in the event of a dispute, both parties must be able to prove guilt or innocence.

1.4 RESEARCH OBJECTIVE

In section 1.3, three major compliance-based risks to cloud application adoption were identified and discussed: transparency, process automation, and repudiation. It could be shown that those risks present significant barriers to cloud application adoption from the point of view of potential customers. This is because adopting a cloud application or using cloud services is similar to outsourcing a service to a third party (Lynn et al., 2021). Mayer et al. (1995) have shown that risks largely depend on the entity where trust must be placed. Specifically, when adopting cloud applications, it is necessary to trust that the application provider will implement compliance requirements as promised. Today, there is a lack of trust in cloud providers, leading to the fact that missing trust in the cloud provider is one of the main reasons cloud applications are not adopted (van der Werff et al., 2019). There is an increased perceived risk if there is a low level of trust in this entity. Following the theory of Mayer et al. (1995), this dissertation's objective is to shift the trust in implementing compliance requirements from the cloud application provider to a third (independent) party – the blockchain. By utilizing blockchain-based trust and the possibility to configure cloud applications transparent, automatic, and non-repudiable via the blockchain, the adoption risk for cloud applications is to be reduced. In the following, this dissertation explores to which extent blockchain technology could be used to mitigate the named compliance-based risks and to which extent it might reduce them.

1.5 RESEARCH DESCRIPTION

As shown in previous sections, transparency, process automation, and repudiation play important roles in the compliance-driven configuration of cloud services and the reduction of adoption risks. Even after intensive literature research, no solution has yet been identified that allows both the customer and the cloud application provider to configure cloud applications to be (1) transparent, (2) fully automatic, and (3) non-repudiable via the blockchain. This work investigates to what extent the emerging blockchain technology can be used to mitigate the identified risks. This dissertation proposes a solution on how blockchain technology can serve as a trusted third party to provide a software architecture that reduces the three described risks of cloud adoption and allows decision makers to implement compliance-driven configurations transparently, automated and non-repudiable. The research presented in this dissertation addresses one main research question (MRQ) and seven supporting research questions (RQ1-RQ7). The content of this dissertation, the methodology to answer the research questions, and in which chapter of this dissertation the results for each question can be found are listed in Figure 1.

1.5.1 Main Research Question

The MRQ of this dissertation is:

To what extent can adoption risks arising from compliance-driven cloud application configurations be reduced by moving the trust to configure the cloud application to the blockchain?

The underlying assumption of this research question is that either the provider of a cloud application or its customer (or both) cannot or does not want to act completely transparently and openly. In other words, it is assumed that at least one party will behave opportunistically in resolving a dispute. Past research has shown that such opportunistic behavior can be assumed (Muris, 1981). Therefore, it is assumed that when data is compromised, one party accuses the other party of misconduct and wishes to prove or deny this misconduct with legal certainty. As (Brown, 2016) has noted, missing or false evidence in such a case can lead to high costs and adverse civil court decisions.

This dissertation applies a structured approach to answering the MRQ. As will be explained in detail in chapter 2, this dissertation follows the approach presented by Hevner et al. (2004) for the scientific development of software solutions. To be more precise, Design Science Research (DSR). DSR aims to generate prescriptive knowledge about the design of *artifacts*, such as software, methods, models, architectures, or concepts (Hevner et al., 2004). In this context, four factors, namely *the environment*, *the knowledge base, the developed artifact,* and *the evaluation of the artifact*, play an essential role from which the further research questions necessary to answer the MRQ are derived.

1.5.2 Research Questions One and Two (Environment)

According to Hevner et al. (2004), the first relevant factor for developing a solution approach is the environment in which the described problem occurs. This includes the question of for which persons, organizations, and technologies the problem to be solved occurs. For this dissertation, two research questions are derived from this question.

The first research question (RQ1) asks:

In which environments do compliance-driven cloud application adoption risks mainly arise?

The second research question (RQ2) follows from RQ1 and asks:

How do experts rate the trust shift from the cloud application provider to a trusted third party for overcoming compliance-driven adoption risks in cloud environments?

RQ1 and RQ2 will be answered by conducting a focus group discussion, as described by Krueger (2014).

1.5.3 Research Questions Three and Four (Knowledge Base)

According to Hevner et al. (2004), the second factor in the scientific development of software is the knowledge base. The knowledge base provides the necessary foundations and methodologies for developing the software approach. The knowledge base contains, among other things, theories, frameworks, related work, methods, techniques, and formalisms that reflect the current state of science and are relevant for the development of the software approach. The third research question (RQ3) supports the systematic creation of a knowledge base. RQ3 is:

What relevant blockchain-based software approaches exist to increase trust in cloud applications or reduce adoption risks?

Building on RQ3, RQ4 asks:

To what extent can this dissertation connect to existing blockchain-based software approaches for reducing adoption risks in the compliance-driven configuration of cloud applications?

RQ3 and RQ4 are answered using a systematic literature review, as described by Buchkremer et al. (2019) and vom Brocke et al. (2009). RQ3 aims to identify the research gap. RQ4 aims to identify existing approaches and explain how this dissertation can address these approaches. There are two primary reasons for developing the knowledge base. First, existing knowledge can be built upon and continued. Second, the precise and rigorous development of a complete knowledge base ensures that no duplicate work is conducted and that existing resources for applying for the MRQ can be identified and used.

If the environment in which the described problem occurs is determined and the necessary knowledge base is created, the development of an artifact for solving the identified problem follows (Hevner et al., 2004).

Artifacts can take the form of mathematical models, software, or even informal descriptions (Hevner et al., 2004). This dissertation aims to shift trust from cloud application providers to the blockchain and mitigate the three identified risks (see 1.3). To achieve this, the traditional configuration of cloud applications must be adapted to enable configuration using blockchain. Consequently, the artifact of this dissertation is a *software architecture* that enables the transparent, automated, and non-repudiable configuration of cloud applications via the blockchain. A software architecture of a cloud application can be understood as "the structure or structures of the system, which comprise software elements, the externally visible properties of those elements, and the relationships among them." (Bass et al., 2003, p. 21). The development of the artifact takes place with the help of the knowledge base. In the context of this dissertation, developing an artifact means first designing software architecture, then showing its feasibility by implementing and deploying it into a test setting (proof of concept). The terms software architecture and artifact are used similarly in this dissertation.

1.5.4 Research Questions Five and Six (Implementation)

Before the development of the software architecture can occur, this dissertation must formally define configurations. Or in other words, it must be defined how compliance-driven cloud configurations can be formally represented for implementing them in software. Therefore, RQ5 asks:

How can compliance-based cloud application configurations mathematically be described?

After clarifying RQ5, the realization of the software approach can start. The sixth research question (RQ6) is, therefore:

What can a prototype implementation look like that utilizes blockchain-based trust for configuring cloud applications?

To answer RQ5 and RQ6, the knowledge base and Rapid Application Development (RAD) are used (Daud et al., 2010; Nalendra, 2021). RAD aims to develop a software architecture methodically in a prototyped way. As shown later, cloud applications can occur in various scenarios. In order to develop a generic approach rather than a concrete implementation, this dissertation focuses on developing an architecture prototype, not on transforming a specific cloud application use case. Generic can be understood as technology independent in the context of this dissertation. Technology independent means that the architecture developed in this dissertation is neither based on specific blockchain technology nor a specific programming language or cloud application.

It is not intended to show how a specific cloud application can be configured using blockchain. Rather, this dissertation aims to develop a prototypical general architecture that can be used to configure various cloud applications via blockchain. The development of a prototypical architecture has the advantage that it can be used in future projects to configure specific cloud applications using blockchain technology. This dissertation thus presents the blueprint to configure cloud applications via blockchain. Moreover, in future work, the developed prototype architecture can be reused by a developer or a researcher for more mature projects.

1.5.5 Research Question Seven (Evaluation)

Research question seven (RQ7) follows from RQ6. After a prototype has been created to implement the research project, it must be clarified whether this prototype is a solution to the MRQ. RQ7 is, therefore:

To what extent can the developed software architecture reduce adoption risks arising from compliance-driven cloud application configurations?

The answer to RQ7 must provide an evaluation of the developed architecture and hence an answer to whether the developed architecture can reduce adoption risks. RQ7 is addressed via evaluating the developed architecture against existing cloud adoption architectures. This evaluation will utilize architecture-level modifiability analysis (Bengtsson et al., 2004). Architecture-level modifiability analysis examines to what extent the three adoption risks can be reduced with the architecture presented in this dissertation. The MRQ can finally be answered, and it can be shown that the output from RQ7 answers MRQ.

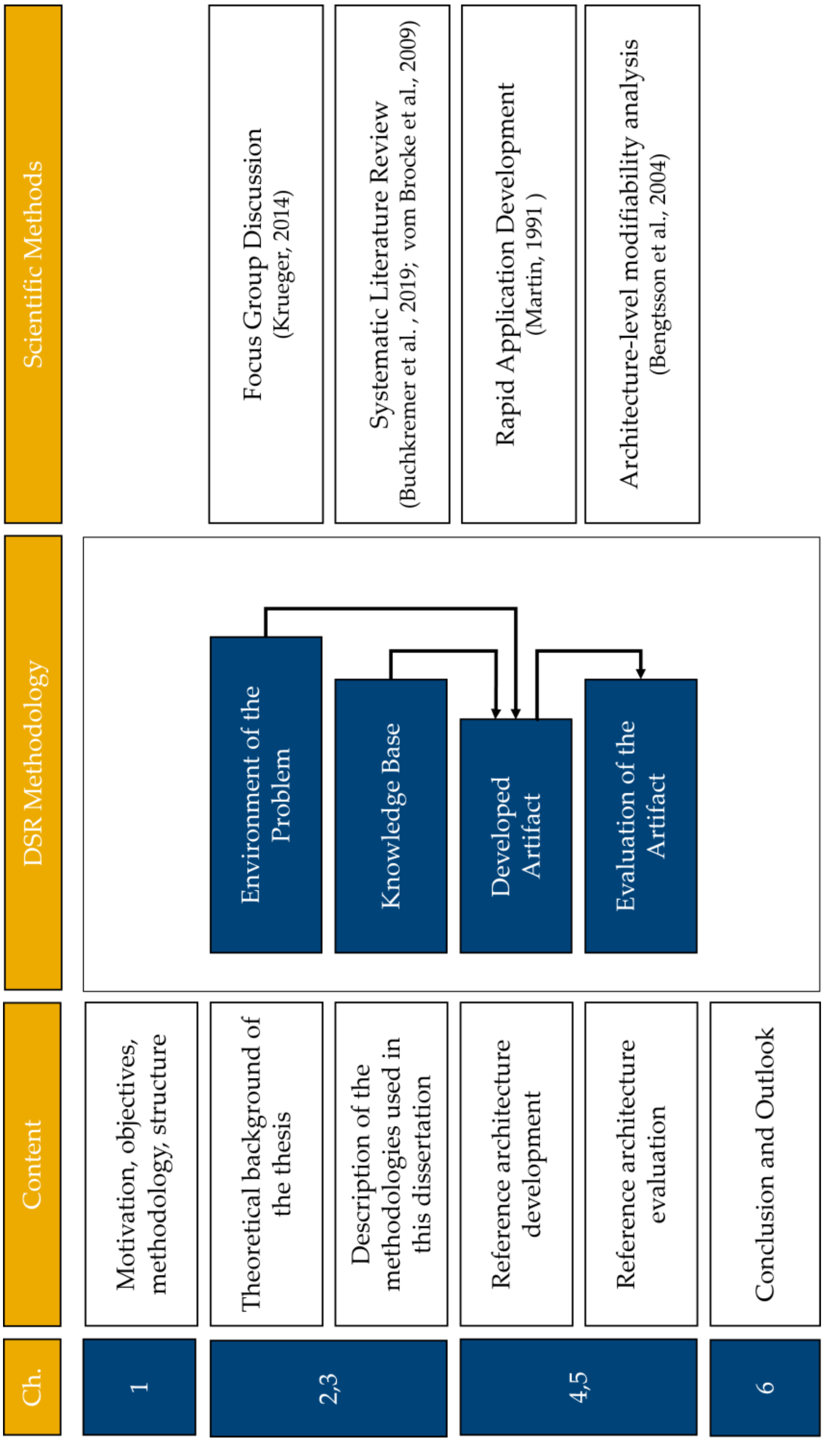

Ch.
Content
DSR Methodology
Scientific Methods
1
Motivation, objectives, methodology, structure
2,3
Theoretical background of the thesis
Description of the methodologies used in this dissertation
4,5
Reference architecture development
Reference architecture evaluation
6
Conclusion and Outlook
Environment of the Problem
Knowledge Base
Developed Artifact
Evaluation of the Artifact
Focus Group Discussion (Krueger, 2014)
Systematic Literature Review (Buchkremer et al. , 2019; vom Brocke et al., 2009)
Rapid Application Development (Martin, 1991)
Architecture-level modifiability analysis (Bengtsson et al., 2004)

Figure 1: Research Structure

1.6 STRUCTURE OF THE DISSERTATION

The remainder of this research is structured as follows: Chapter 2 describes the research methodology of this dissertation. In particular, the research framework and the scientific methods used to answer the research questions are discussed. Chapter 3 presents the theoretical framework of this thesis. This chapter is divided into four parts. The first part (3.1) provides the necessary definitions and foundations for this dissertation. The second (3.2) sets the scope of this dissertation via a focus group discussion. In the third part (3.3), the research gap of this thesis is presented based on the scope identified in 3.2. Based on the definitions and the identified research gap, related work to this thesis is then presented in 3.4. After presenting the methodology and connected science, chapter 4 shows the development of the artifact, including the development of a prototype and proof of concept. The evaluation of the thesis, and thus the answer to RQ7, is then presented in chapter 5. Finally, chapter 6 provides this research's conclusion, limitations, and outlook.

2 METHODOLOGY

This study aims to develop novel software, including methods and architecture, to address the compliance-related adoption risks of cloud applications by utilizing blockchain-based trust. A company's technical departments usually decide to adopt cloud applications (Khajeh-Hosseini et al., 2012). Consequently, a corporate decision is made by a unit within the company for the company. The decision-making unit can be as small as an individual, e.g., a manager, or as large as the entire organizational membership. The conduction of corporate decisions at the unit level is also described as an organizational decision (Huber & McDaniel, 1986). Thus, the presented work aims to solve an organizational problem. With the Design Science Research (DSR) Framework, Hevner et al. (2004) introduced a methodology to solve an organizational problem from information technology in a problem-oriented way. The authors describe how *qualitative* and *quantitative* methods can solve a real-world problem under scientific conditions.

In empirical research, a general distinction can be made between two research approaches: namely, quantitative and qualitative research (Kothari, 2004; Tashakkori et al., 1998). Quantitative research is about facts and numbers, and quantitative methods are used to investigate phenomena that numbers and data can substantiate. In contrast, qualitative research helps understand why and how phenomena come about. Qualitative research can be used to investigate and determine phenomena that numbers cannot capture, like an individual's motivations.

Following the DSR methodology, an artifact based on an existing problem is created. According to Hevner et al. (2004), an IT artifact includes the instantiations, constructs, models, and methods applied in developing and using information systems (IS). The advantage of using this methodology is that it will answer the MRQ in any case. This is because the DSR methodology not only produces an artifact, if possible, it also provides a scientifically based output on whether the development of an artifact is possible. To be more precise, the output of the DSR methodology will either be an artifact built based on scientific methods or scientific evidence that building the artifact is not possible. Either way, consistent application of the methodology will provide an answer to the MRQ.

2.1 INFORMATION SYSTEMS RESEARCH FRAMEWORK

Figure 2 describes the conceptual DSR framework proposed by Hevner et al. (2004) and used in this dissertation. This framework supports understanding, executing, and evaluating IS. The framework is divided into three pillars containing three cycles (Hevner et al., 2004). These three pillars—*Environment, Knowledge Base, and Implementation*—build the basis of DSR. Three individual cycles are performed within the three pillars to develop an artifact that solves the identified problem. These cycles are the *relevance cycle* (see 2.1.1 for details on the method used in this cycle), the *rigor cycle* (see 2.1.2 and 2.1.3 for details on the methods used in this cycle), and the *design cycle* (see 2.1.4 for details on the method used in this cycle),. The cycles are conducted using scientific methods to solve a described problem, as shown in Figure 2 below.

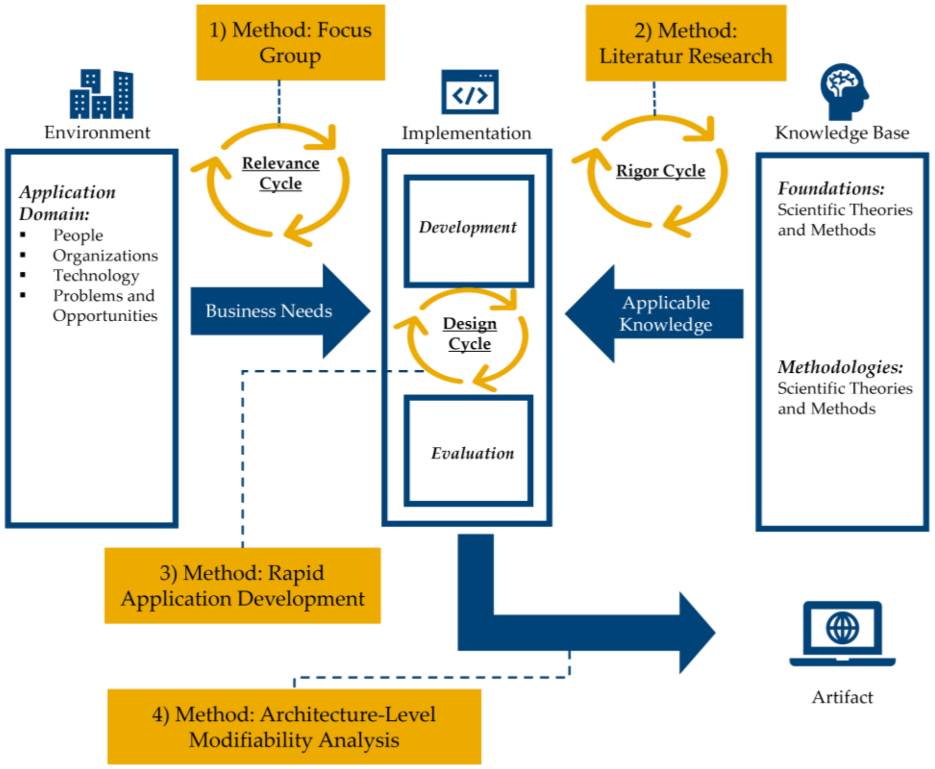

1) Method: Focus Group
2) Method: Literatur Research
Environment
Implementation
Knowledge Base
Relevance Cycle
Rigor Cycle
Application Domain:
People
Organizations
Technology
Problems and Opportunities
Development
Design Cycle
Evaluation
Business Needs
Applicable Knowledge
Foundations: Scientific Theories and Methods
Methodologies: Scientific Theories and Methods
3) Method: Rapid Application Development
4) Method: Architecture-Level Modifiability Analysis
Artifact

Figure 2: DSR Framework. (Adapted from Hevner et al., 2004)

DSR starts from a problem, e.g., the described problem of this dissertation (see 1.5). According to Hevner et al. (2004) it is important to understand the problem space in which the problem occurs.

The *Environment* represents the problem space—the scope of the work. The challenges that are to be solved by DSR arise from the environment. Actors within the environment can be people, companies, organizations, and existing or planned technologies. The environment also contains the goals, tasks, problems, and opportunities that define the company's objectives. Business needs or "problems" develop from this environment. DSR then addresses these business needs. The *relevance cycle* ensures that emerging business needs and their developed artifacts are regularly aligned with the environment. It also ensures artifacts are evaluated to determine whether the development contributes to the solution of the identified problem. RQ1 and RQ2 are addressed in this section of the framework. This dissertation uses qualitative research to address the question raised by RQ1 and RQ2 and to provide answers in the relevance cycle. These results can be found in section 3.2.

After the problem space is identified using scientific methods, the theoretical knowledge of the work must be built. The theoretical knowledge for implementing an artifact comes from the *Knowledge Base* (Hevner et al., 2004). The knowledge base collects existing knowledge, fundamentals, and methodologies. This theoretical knowledge is collected to influence the later artifact design process. The *rigor cycle* ensures that existing knowledge flows into the development of the artifact and that knowledge gained from the artifact development flows back into the knowledge base. The information flow back to the knowledge base differs from regular software development. While regular software development aims to develop a market-ready product, the goal of DSR is to create knowledge during the development of the artifact (Hevner et al., 2004). DSR requires researchers to abstract from learned knowledge, draw principles or theoretical conclusions, and feed knowledge back into the knowledge base. To form a literature foundation of the environment—and, subsequently, to answer RQ3 and RQ4—this dissertation follows a systematic literature review as the scientific method for building a knowledge base. This literature review can be found in section 3.3.

Once the environment—or scope—of this dissertation has been explored and the knowledge base has been built, the development of the artifact starts. Findings related to the environment and knowledge base can be used to develop a scientifically grounded artifact in the *Implementation* pillar. The implementation is performed cyclically in two complementary phases (Hevner et al., 2004). The cycle of these phases is called the *design cycle*. The phases consist of *behavioral science* and *design science*.

Behavioral science addresses the justification of theories and explains behavior connected with the business need. Behavioral science aims to understand why individuals engage in specific behaviors. This understanding is gained by experimentally examining the impact of factors such as conscious thoughts, motivation, social influences, contextual effects, and habits. Behavioral science thus ensures an evaluation of the development. It also helps to incorporate existing theories into the development of the artifact within this dissertation.

Furthermore, behavioral science ensures that scientific standards and methods are used during the artifact's implementation. Behavioral science thus forms the scientific basis for understanding the approach to be developed. The business-driven needs to understand the problem to be overcome in this dissertation comes from both the environment (see 3.2) and the related work (see 3.4).

In contrast, design science adds to the business need by developing an artifact. Therefore, while behavioral science forms the theoretical basis of the approach, design science shapes the practical implementation of the artifact. The scientific method of RAD is used for performing the design cycle (Martin, 1991). RAD is a concept described by James Martin for software development with a prototypical procedure model. RAD makes software development more flexible than classic process models such as the waterfall model and adapts quickly to changing requirements. The environment and the knowledge base provide the input for the RAD method. The output of RAD is a software architecture (including a prototype) that solves the identified research problem. Thus, RAD can provide an answer to RQ5 and RQ6. A full discussion of the RAD process can be found in section 2.1.4. The results of the implementation can be found in 4.2.

Whether and to what extent the developed software architecture approach reduces the named adoption risks must still be investigated. Hevner et al. (2004) point out that: "[t]he utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well executed evaluation methods." (Hevner et al., 2004, p. 83). Therefore, the artifact developed in this dissertation must be evaluated. The evaluation's results will provide an answer to RQ7.

The evaluation of the artifact will be done using architecture-level modifiability analysis (ALMA), combined with case studies and qualitative and quantitative (i.e., mixed) methods (Tashakkori et al., 1998). Using a mixed-methods approach, experts are asked to rate the adoption risk for compliance-driven configuring cloud applications for several use cases (in the case of this dissertation, three are used). Experts rate the adoption risk of a cloud architecture currently used by cloud application providers and the architecture newly developed in this dissertation. The experts are asked to select the architecture that (according to the experts' assessments) causes less transparency, process automation, and repudiation risk during the adoption of cloud applications. Using this expert evaluation, this dissertation will investigate to what extent the developed software approach can reduce the adoption risk of cloud applications. The evaluation provides an answer for RQ7 and the MRQ and can be found in Chapter 5.

The following subsections will present the scientific methods used to answer the research questions. These methods are then applied in the respective chapters.

2.1.1 Focus Group Discussions Based on Krueger

Identifying the environment helps illuminate if, where, and why the problem described in this dissertation occurs in practice (Hevner et al., 2004). Recall that this problem, as articulated by the MRQ, is: *to what extent can adoption risks arising from compliance-driven cloud application configurations be reduced by moving the trust to configure the cloud application to the blockchain?* The subsequent research questions, RQ1–RQ7, all aim to help provide an answer to this question by identifying the environment in which the problem occurs, creating an artifact to help solve the problem, and evaluating the efficacy of the created artifact.

Returning to the two research types discussed in the introduction of this section (qualitative and quantitative research), RQ1 and RQ2 can be identified as qualitative questions that, therefore, qualitative methods must answer. This finding is supported by Hevner et al. (2004), who recommend group discussions for setting the environment of a detected problem. For answering RQ1 and RQ2, this dissertation will focus on a qualitative research method and conduct a group discussion. To be more precise, a focus group discussion based on Krueger (2014) will be conducted.

A focus group discussion is a special group discussion, not just randomly selected people (Krueger, 2014). Focus group interviews collect qualitative data from a focused conversation among a homogeneous group of experts in the field under study. However, some variation among participants is also necessary to allow for opposing opinions. Group interaction and group dynamics can lead to deeper information eliciting group members' other opinions and ideas (Krueger, 2014). A focus group aims to understand an issue, idea, product, or service. Focus groups are about five to ten people who participate in a discussion about the issue, idea, product, or service led by a moderator. Conversations are held in a relaxed environment without time pressure. This enables an open exchange and the development of creative ideas. Because this research aims to evaluate whether blockchain-based software approaches can increase customer trust in cloud applications, it is important to determine potential customers' understanding of the existing trust chain problem first. Due to its open character and aim of creating innovative ideas, focus group discussions will support this dissertation in identifying its relevance.

At the same time, however, focus group discussions are not without disadvantages; research shows that focus groups are not as in-depth as, for example, interviews (A. Adams & Cox, 2008). Since focus group discussions are used in this dissertation to scope out initial opinions and feasibilities, this limitation is acceptable. Another disadvantage of focus groups is that they are very planning intensive (Krueger, 2014). A date must be found on which many experts are available. Additionally, experts who are willing to exchange their opinions in the context of a focus group discussion must be found. However, in the context of this dissertation, this effort is justified. Focus group discussions allow a topic to be assessed from different perspectives and views (Krueger, 2014). Despite the high effort, multiple opinions and experiences from experts offer an ideal opportunity to justify this thesis's environment and scope scientifically.

2.1.2 The STIRL Process Based on Buchkremer et al.

Various approaches to conducting a systematic literature review exist today (Bandara et al., 2015; Levy & J. Ellis, 2006; Linnenluecke et al., 2020; Okoli & Schabram, 2010; Sylvester et al., 2013; Tranfield et al., 2003; vom Brocke et al., 2015; Vom Brocke et al., 2009; Webster & Watson, 2002; Wolfswinkel et al., 2013).

It is important to note, however, that many of the existing approaches are not well suited for this dissertation. The approach described by Tranfield et al. (2003) is an example of an inadequate approach for the purposes of the current research. Tranfield et al. (2003) divide the research process into three stages. The first stage of the literature search consists of planning. In the second stage, the literature search is conducted. During this stage, appropriate literature is identified, evaluated, and analyzed. The last stage is the documentation of step two (Tranfield et al., 2003). Although the steps described by Tranfield et al. (2003) provide a systematic approach, this type of literature review requires the involvement of a panel of experts to guide the literature search. Since this setup is not feasible within the scope of the current research, this dissertation employs a different approach. Other approaches, such as that of Webster and Watson (2002), are manually driven and allow the review of large amounts of literature only at the expense of time.

To overcome the named limitations, this dissertation adopts the two-fold literature review approach proposed by Buchkremer et al. (2019), as this approach is described as suitable for analyzing a large amount of literature. First, a systemic taxonomy for information retrieval from literature (STIRL) is performed. This approach allows for a machine learning-supported systematic literature review. The machine learning-supported approach suggested by Buchkremer et al. (2019) is well suited to the current research because it enables an automatic and human error-free analysis of large literature sets. Thus, it can be applied to examine large volumes of research articles. Following the STIRL approach, a search string suitable for the topic is first defined. Using the defined search string, online scientific databases are searched. The search hits, namely scientific articles matching the search string, are exported. The export contains the following details of the search hit:

- Title
- Author(s)

- Type of paper (journal article, conference paper, review paper, book, etc.)
- The year of publication
- Name of the publisher (journal name, conference name, etc.)
- Abstract of the paper

This search export forms the literature corpus. The literature corpus is subsequently analyzed with artificial intelligence (AI) methods. Specifically, the first step in the analysis is to remove stop words from the corpus. Removing stop words means removing words that are not considered in a full-text analysis. Stop words are the most commonly used words in a language. These extremely common words can be excluded from a sentence without changing the meaning of that sentence and have no relevance for the analysis of the literature corpus. Examples include "the, a, an, another, for, an, nor, but, or, yet, so, in, under, toward, before".

Next, stemming is applied to the remaining words in the literature corpus. Stemming involves tracing the remaining words in the text corpus to their respective common root forms. For example, the different word variants "waits," "waited," and "waiting" would all be traced back to the root form "wait". This allows for a more accurate classification of the papers from the text corpus and reduces the chance of distortion in the analysis due to varying word variants. After the stop words have been removed and the remaining words have been traced back to their root forms, the actual analysis using artificial intelligence starts.

Computers usually cannot recognize the context in text documents per se and, therefore, cannot sort texts by topics. For this, Latent Dirichlet Allocation (LDA) is required (Blei et al., 2002). Utilizing LDA, texts can be assigned to a topic. The basic assumption of LDA is that documents are nothing more than a probability distribution of topics. Complementary to this is the assumption that topics are nothing other than probability distributions of words. In principle, LDA calculates the likelihood, based on words used, that an article is about a given topic. It then assigns the article to that topic. The LDA assumes that documents with similar topics are more likely to use the same word groups. Hence, LDA is a method for the unsupervised classification of documents (Blei et al., 2002). LDA tries to find natural groups of elements (topics) even if they are not known in advance. Here, a document can be a part of several topics. LDA provides methods for automatically organizing, understanding, searching, and summarizing large amounts of literature (Buchkremer et al., 2019).

Suppose we have two topics that can be classified as Cow_related and Penguin_related. A topic has probabilities for each word, so words like "milk", "pasture", and "grass" have higher probabilities in the Cow topic than in the Penguin topic. The Penguin_related topic also has high probabilities for words like "ice", "water", and "fish." Suppose we have a document with the following sentences.

- "Penguins like to eat raw fish and dive quickly in water."
- "Cows on pasture do not eat fish but grass."

Although the second document contains fish and thus may also belong in the penguin category, it is clear that this document belongs to the Cow-related documents as more words fit. This idea is also used for LDA.

2.1.3 Systematic Literature Review Based on vom Brocke et al.

After using the STIRL approach (Buchkremer et al., 2019) and LDA (Blei et al., 2002) to create an AI-supported corpus of relevant literature, a systematic review of the identified literature will be done. The manual review of relevant work ensures that the relevant articles detected automatically by the STIRL process are actually relevant to this work. For example, papers may contain keywords such as cloud computing or blockchain, but the content indicates that these are explicitly excluded. When using LDA, these semantic may be not recognized and the work is wrongly classified as relevant. This dissertation adopts the systematic literature review methods and process steps described by vom Brocke et al. (2009). The approach presented by vom Brocke et al. is ideal for this dissertation since it specifies clear process steps and methods for executing a systematic literature research. Moreover, utilizing the presented steps, a comprehensive literature research's quality, validity, and reliability can be increased (Fischl et al., 2014).

The systematic literature review of vom Brocke et al. (2015) is based on the approach of Webster and Watson (2002). Vom Brocke et al. (2015) adopted the idea of Webster and Watson (2002) and included it in a five phases systematic literature review process. The individual phases are shown in Figure 3, below.

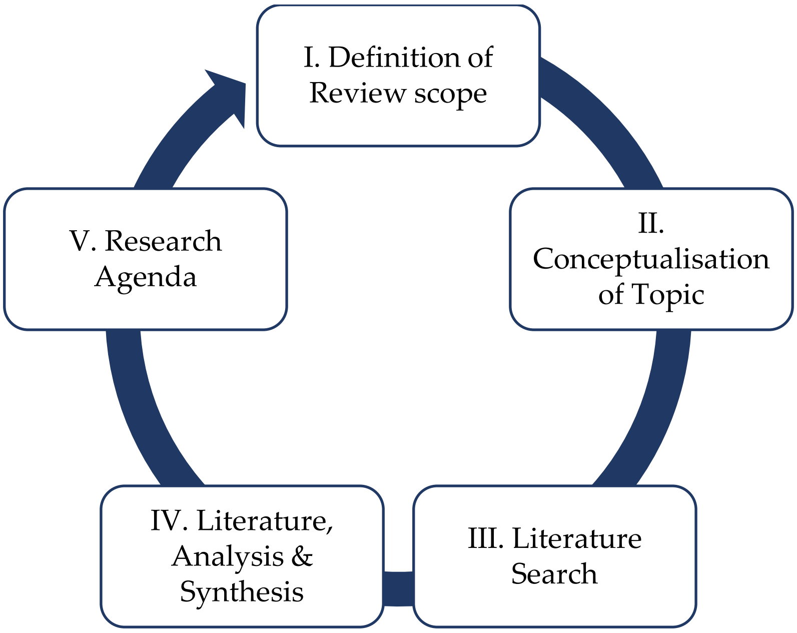

I. Definition of Review scope
II. Conceptualisation of Topic
III. Literature Search
IV. Literature, Analysis & Synthesis
V. Research Agenda

Figure 3: Five Steps of Systematic Literature Review According to vom Brocke et al. (Source: Following: vom Brocke et al. 2009, Figure 3)

During Phase I, the research question or the research object is defined. For a clear definition of the scope of the work, vom Brocke et al. (2009) suggest the use of Cooper's "Taxonomy of Literature Reviews" (Cooper, 1988). The scope of Cooper's Taxonomy is divided into six subcategories (see Table 5, in section 3.3.2). The different subcategories deal with the following characteristics:

a. *Focus* defines the central area of interest for the reviewer. These areas could be research outcomes, methods, theories, or applications.

b. *Goal* describes the objective of the view. These objectives could be, e.g., to bridge the gap between existing research and to integrate existing approaches; to criticize existing approaches; or, to identify central issues from the past and investigate how they have developed.

c. *Organization* describes how the systematic literature review will be shown. This could be in chronological order, grouped by similar concepts, or by the same work methods.

d. *Perspective* indicates how the reviewer will present the literature. This could be that of a neutral judge, i.e., from a neutral position, or from the position of a prejudiced lawyer.

e. *Audience* describes the target group of the review. This could be everything from very specialized researchers to general researchers and practitioners, politicians, or the general public.

f. *Coverage* describes how the literature will be searched and analyzed. This could be exhaustive, with selective criteria, representative, or central/pivotal.

Phase II involves organizing the analysis. The search string and databases for the systematic literature reviews are defined in this phase. Since this dissertation combines the literature review proposed by Buchkremer et al. and vom Brocke et al., the described Phases I and II are replaced by the output of the STIRL approach (see 2.1.2).

In Phase III, the actual literature search occurs. In particular, vom Brocke et al. (2015) suggest that "backward" and "forward" searches can assist. A backward search is performed when starting from a known literature source and searching for further relevant work in the past. This can be done, for example, via the related work part of a paper. A forward search is the counterpart to the backward search and is therefore used to search for more recent articles on a known reference source. The source directories of articles serve as the data basis for this. For this purpose, for example, the "Cited by" function can be accessed via online databases in order to see by which authors the described document was cited. Vom Brocke et al.'s (2009) Phase IV involves the analysis of the literature searched.

In the final phase, Phase V, the research results are documented. For this purpose, the *concept matrix*, as shown in Figure 4, is used. This concept matrix divides the literature searched into the concepts it contains. The researched article names appear on the y-axis of the concept matrix. On the x-axis, concepts described in the researched articles are mapped. If an x-axis article now contains a y-axis concept, this is indicated in the concept matrix.

Consequently, a concept matrix is created from which a connection between articles and their concepts can be deducted. By mapping the articles and their concepts in this way, common themes can be recognized, patterns between the researched articles begin to emerge, and research gaps can be detected. The next step is to identify articles in the concept matrix that contain no or only a few concepts. From this investigation, research gaps can be derived.

Article	Concepts				
	A	B	C	D	…
1	X				
2		X	X		
…	X		X		

Figure 4: Concept Matrix based on Webster and Watson. (Adapted from Webster and Watson, 2002)

2.1.4 Rapid Application Development Based on Martin

RAD was introduced in 1991 by James Martin as a method for rapid software development. As Martin (1991) explains,

> Rapid Application Development (RAD) is a development lifecycle designed to give much faster development and higher-quality results than those achieved with the traditional lifecycle. It is designed to take the maximum advantage of powerful development software that has evolved recently.

In other words, due to its ease of implementation, the RAD method enables the quick creation and adaption of software architectures based on an identified environment. RAD has been shown to be useful for scientific projects and the development of business solutions (Daud et al., 2010; McFarlane, 2004; Nalendra, 2021). This method requires implementing the four process steps shown in Figure 5, below. In what follows, each of these steps is also described in detail.

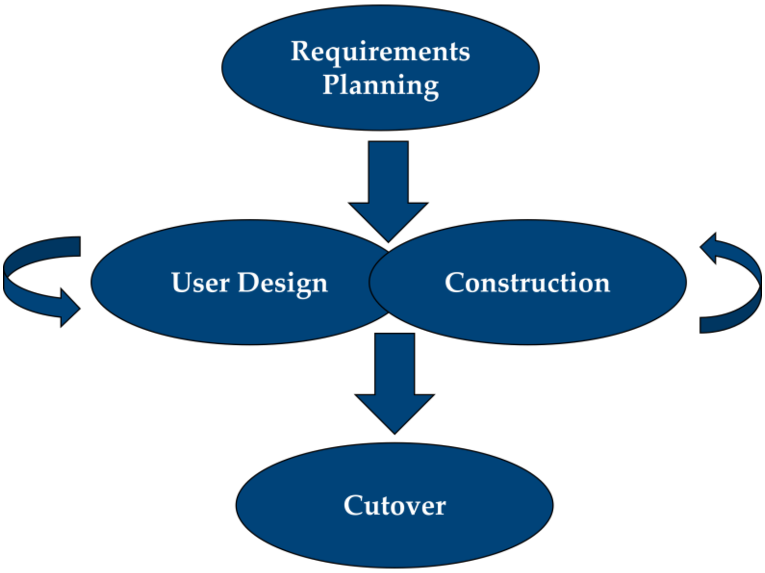


Figure 5: Rapid Application Development Phases. (Adapted from Martin, 1991)

Requirements planning phase. First, a general plan is made regarding the project's scope. For this purpose, the researchers involved in the project define the software requirements and how these requirements should be prioritized in the course of development. The software is then developed based on the prioritization. The goal is to create an executable prototype as quickly as possible. Mandatory software requirements are documented in the form of use case diagrams.

User design phase. The requirements defined in Phase One are transferred to the software architecture. In other words, the identified user requirements are first modeled by using a high-level software diagram (use case diagram). Subsequently, the use case requirements are mapped to the structure of the software. The use case diagram is therefore used to determine the required software elements and their interaction with each other. This is then used to create the architecture of the software. In this phase, the software's system architecture and interfaces are defined. This step is repeated until all the requirements from the previous planning phase have been implemented in the software design.

Construction phase. When the software's basic design is ready, the next step is setting it into software. The requirements from the planning phase (Phase One) and the software design from Phase Two are combined into a first software prototype. This step is repeated until the defined requirements and the planned software architecture are transferred into a running software prototype. It should be noted that this is not a contradiction to the actual goal of the dissertation. As explained in detail, this dissertation aims to develop software architecture for shifting trust to the blockchain. Developing a software prototype – i.e., the concrete implementation of a use case – seems contradictory. That this is not a contradiction, but a necessary step becomes clear in the following. Software architecture is only a blueprint.

Transferred to the building of a house, the software architecture is nothing else than the blueprint of a house. So, the theoretical basis for the construction of a building. In principle, a blueprint can initially contain many things. For example, a construction plan can show that the house's walls must only be a few millimeters thick. Of course, the builder is happy about this because it makes house construction cheaper. However, the construction plan does not clarify that this does not work in practice (due to the high weight of the roof) or only to a limited extent. This is similar to software architecture. Software architecture components may be linked together quickly and sufficiently in theory, but in practice, they have major problems due to a lack of computing power or non-existent data, for example. The supply of a Proof of concept - thus the concrete implementation of the software architecture - strengthens this thesis and the developed architecture and offers no contradiction to the goal of this thesis.

Cutover phase. The last phase allows the developer to test the prototype in a live environment and receive user feedback on the prototype's performance. The next section will provide more details on how the software architecture evaluation will be done.

2.1.5 ALMA Based on Bengtsson et al.

ALMA, developed by Bengtsson et al. (2004), is used to evaluate this dissertation's proposed software architecture. An ALMA evaluation is carried out in five steps. First, a goal of the scenario-based evaluation must be selected. In general, the goal is to evaluate a system's maintenance costs for future requirements, identify risks of a software architecture change, or compare two architectures to select the best alternative for a given scenario. Of these, the third goal—comparing two software architectures—is used to evaluate the artifact developed in this dissertation. Step two is the description of the software architecture(s). Step three is the creation of scenarios based on which software architecture(s) will be evaluated. For this research, the method presented by Yin is used (Yin, 2017). Step four evaluates the architecture(s) based on the set goal and the defined scenarios. For this purpose, this dissertation utilizes the method of interviews, according to W.C. Adams (2015; see 2.1.5.2), and qualitative content analysis based on Mayring (2000; see 2.1.5.3). The final step is the interpretation of the evaluation results. This dissertation's interpretation is done through a detailed discussion of the data obtained in the interviews.

2.1.5.1 Case Study Based on Yin

The artifact developed in this dissertation is generic (technology independent) in that this dissertation presents a general software architecture for configuring cloud applications via blockchain technology. There are a variety of possible application scenarios in which cloud adoption risks can be reduced. However, as mentioned earlier, the adoption risk depends on the environment of the developed software approach. Hence, for a general question of whether experts would say that the developed approach reduces the adoption risk of cloud applications, the answer would strongly depend on the environment in which the experts evaluate the developed approach.

To answer RQ7, this dissertation needs to overcome this limitation. Therefore, experts are presented with concrete environments (scenarios). Based on the scenarios, experts will be asked to evaluate the developed software prototype. The use of concrete case studies ensures that expert opinions can be compared with each other. Using case studies thus makes it possible to evaluate the general approach in concrete environments. Particular importance is attached to selecting multiple scenarios. In this way, it can be ensured that the developed approach is evaluated in a complete application environment.

The literature currently offers three prominent representatives of the creation of case studies, namely Robert Yin, Sharan Merriam, and Robert Stake (Yazan, 2015). Due to its frequent use in past studies, the case study method described by Robert Yin has been well-tested (Yin, 2017). For this reason, this dissertation follows Yin’s method. Within the scope of this dissertation, a multiple case study is used.

More specifically, embedded multiple case studies are used to standardize the evaluation of the developed software approach.

2.1.5.2 *Semi-Structured Expert Interviews Based on W.C. Adams*

As seen above, expert opinions are needed for the dissertation's evaluation design. Qualitative methods are recommended for this case (Kothari, 2004). More precisely, as this dissertation moves on new and unknown terrain, using semi-structured interviews (SSI) is an appropriate research method (W. C. Adams, 2015). SSIs are relatively structured and only slightly standardized. In other words, in SSIs, there is a predefined framework of questions and a guideline, but it is also possible to ask follow-up questions and jump to previous questions. Expert Interviews are a specific form of SSIs.

In contrast to biographical interviews, in Expert Interviews, the interviewees are of less interest as a (whole) person than their capacities as experts for a certain field of activity (Meuser & Nagel, 2009). They are integrated into the study not as a single case but as representing a group of specific experts. For answering RQ7, semi-structured expert interviews are conducted as described by W.C. Adams (2015).

2.1.5.3 *Qualitative Content Analysis Based on Mayring*

The qualitative content analysis method presented by Mayring (2000) was chosen for the data analysis. The overall goal of this analysis is to analyze qualitative content systematically in categories. Mayring's qualitative content analysis can be divided into five phases. The material appropriate to the research question must be selected first. Since the master research question is highly technical and, due to its complexity, divided into several research questions, the use of additional data collection methods is required. In software engineering, qualitative methods have shown their value in collecting data where complex topics require additional user input (Seaman, 2008). In the context of this dissertation, two qualitative methods are used. Identification of the environment in which the problem described in this dissertation occurs is yet unknown and must – based on RQ1 and RQ2 – be identified. In other words, existing knowledge on how to shift compliance-driven configurations to the blockchain is inadequate, and the elaboration of pertinent issues is necessary. In such cases, focus group discussions are a recommended qualitative method for obtaining the missing knowledge (Powell & Single, 1996). In addition, based on RQ7, it must be determined to what extent the approach developed in this dissertation can reduce the three described adoption risks. In the past, expert interviews have proven to be an effective method of software evaluation (Bengtsson et al., 2004).

Thus, semi-structured expert interviews are the second qualitative method used in this dissertation. As described in more detail later (see chapter 5), the software evaluation will require the assessment of the adoption risk. However, in order to be able to compare and evaluate assessed risks between the individual interview participants, the assessment of the risk within the expert interview will be done using quantitative methods. Finally, this can be referred to as a qualitative expert interview with quantitative elements. According to the literature, mixing qualitative and quantitative methods is also referred to as a mixed-methods approach (Tashakkori et al., 1998).

In summary, for answering RQ1, RQ2, and RQ7 qualitative methods (with quantitative content), to be more precise, focus group discussions, and SSI interviews will be conducted. In the second phase, the goal of the analysis must be defined. That is, the researcher must identify what, precisely, is to be investigated with the help of qualitative content analysis.

Based on the identified goal of the content analysis, within the third phase, the form of the analysis must be selected. Mayring (2000) describes the following content analyses used in this dissertation:

- *Summary content analysis*: In the curse of this dissertation, also referred to as *inductive* category creation. Inductive category creation is a technique of summarization. It is, therefore, a matter of reducing the entire material, i.e., for this dissertation, inductive evaluation means that recurring expert statements are summarized in one category. The inductive procedure allows forming new categories. In this way, the inductive procedure enables the derivation of individual theories.
- *Structural content analysis*: With the help of a coding guide, the material is assessed according to predefined criteria. This is also called a *deductive* approach. The analysis of interview data is deductive, i.e., based on the previously defined theoretical framework, if it follows a scientific basis.

> As an example, consider the quantitative analysis of machine operators. Assume that the machine operators with heavy machines have a probably high cognitive load. In this case, the "Cognitive Load Theory" can be used to design interview questions and to guide the analysis. In this regard, the theory now offers certain dimensions according to which a guide for the interviews can be created. The transcripts can be classified based on the categories already provided by the theory.

In the fourth phase, the results must be interpreted. According to Mayring (2000), the interpretation of the results depends on the form of the selected content analysis. In any case, a category system is created in which the transcribed content is assigned. Both approaches (inductive and deductive building of categories) are used for qualitative analysis in this dissertation. The categories are formed during the qualitative analysis by deriving categories from the observed content (inductive) and using categories established in advance through existing literature (deductive).

In the last (fifth) step, the quality criteria of qualitative research must be ensured. Specifically, these are:

- *Transparency*: Are results presented transparently? Is what was intended to be measured really measured?
- *Coverage*: Refers to the reproducibility of the content. Is the qualitative content analysis reproducible when the research is conducted again?
- *Intersubjectivity*: refers to shared understanding. In other words, do two individuals have the same meaning and understanding of an object? A basic human example of intersubjectivity is having a shared, common agreement in defining an object. Most people would experience intersubjectivity when asked to picture an apple- the definition of an apple would be the same.

2.2 GUIDELINES FOR DESIGN SCIENCE IN IS RESEARCH

The previous subsection discussed the research framework and the research methods intended to answer the research questions of this dissertation. In this section, the guidelines for applying these methods are presented. Hevner et al.

(2004) describe DSR as a problem-solving process that follows clear guidelines. Hevner et al. (2004) named seven guidelines for design science in information systems. They further claim that these guidelines serve one underlying principle:

> The fundamental principle of design-science research from which our seven guidelines are derived is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact. (Hevner et al., 2004, p. 82)

In other words, applying the seven fundamental DSR guideline steps is good research practice. These guidelines aim to assist researchers, reviewers, editors, and readers in understanding the requirements of DSR (Hevner et al., 2004). To provide the assistance described by Hevner et al. (2004), this dissertation follows the seven proposed guidelines and implements them in developing the artifact. However, it is important to note that Hevner et al. (2004) presented a methodology for developing artifacts, not a method. In other words, the guidelines should not be understood as an inflexible set of step-by-step instructions but as what they are, namely, a guideline. They should be applied to a given DSR work using the individual's creativity and judgment. To assist the reader of this dissertation, Table 2 (below) shows how the DSR guidelines can be applied to this work.

Table 2: Design Science Research Guidelines and their Application in this Dissertation. (Adapted from Hevner et al., 2004)

Guideline	Description	Implementation
1. Design as an Artifact	Design science must produce an artifact	This dissertation expects to develop an innovative software approach, including methods and architecture, to reduce the adoption risk of cloud applications by shifting trust to the blockchain. Thus, this dissertation aims to produce an artifact in design science research
2. Problem Relevance	The developed solution must solve a relevant business problem	As section 1.1 has shown, the relevance of increasing trust in cloud applications is given.
3. Design Evaluation	Scientific methods must be used to evaluate the utility, quality, and efficacy of a design artifact	Section 2 extensively describes the scientific methods used in this dissertation for designing and evaluating an artifact.
4. Research contributions	Design science research must contribute to the scientific community	This dissertation will be made publicly available. This includes the architecture and prototype developed within the IS Research. A contribution to the scientific community is therefore provided. Furthermore, the findings of this dissertation were published by Weber & Buchkremer (2022b, 2021b)
5. Research Rigor	During the design artifact construction and evaluation phases, rigorous methods must be applied	Section 2 extensively describes the scientific methods used in this dissertation for designing and evaluating an artifact. This demonstrates scientific rigor.
6. Design as a Search Process	Design science research is an iterative process that needs a clear stopping criterion	The acceptance criteria for the design artifact will be an architecture plus running prototype software that enables the shift of trust from cloud providers to the blockchain. The developed artifact should reduce the risk of adopting a cloud application.
7. Communication of Research	Design science research must be communicated well to the technical-oriented and management-oriented audience	This dissertation will provide the source code of the developed design artifact for addressing the technical-oriented audience. Moreover, the dissertation will also explain and architect the design artifact for the management-oriented audience to estimate the implementation effort and costs.

2.3 DISCUSSION

This chapter presents the methods used in this dissertation. Overall, the MRQ of this dissertation is answered scientifically based on the DSR methodology presented by Hevner et al. (2004). For DSR, Hevner et al. (2004) provide seven guidelines that should be followed in the context of good DSR. This chapter has shown in detail how this dissertation follows these guidelines. Furthermore, chapter 2 has shown which methods are used to answer the research questions. Specifically, focus group discussions will be used to answer RQ1 and RQ2. RQ3 and RQ4 are conducted utilizing AI-supported systematic literature. Based on the work identified in RQ4, RQ5 will be answered based on the identified literature. RQ6 will be answered using the RAD method. The evaluation of the dissertation and, thus, the answer to RQ7 is based on the ALMA approach. For the evaluation of the dissertation, three scenarios are developed in which the presented architecture approach is applied. Based on qualitative interviews and a quantitative risk assessment during the interviews, the extent to which the presented architecture can reduce the adoption risk in different scenarios will be examined.

The next chapter now focuses on building the scientific foundation of this dissertation. Specifically, the next chapter will first present this dissertation's main definitions and background. Afterward, the scope of the thesis will be defined using focus group discussions. Based on the defined scope, the systematic literature analysis will be conducted before the last part of the next chapter shows how this dissertation connects to other already published works.

3 THEORETICAL FRAMEWORK

This chapter discusses the theoretical framework used to identify the basic theories and methods for solving the problem described in this dissertation. Figure 6, below, shows that the knowledge base is structured in four main areas. Each of the areas represents a subsection of this chapter. The first section provides the definitions and foundations of this dissertation. Next, based on the methodology described in 2.1, the scope of this dissertation gets defined. The third section contains a systematic literature review. The fourth section uses the systematic literature review results to identify the dissertation's research gap and related work. Identifying related work supports and aligns this dissertation with existing research and helps avoid duplication of effort. The chapter concludes with a discussion.

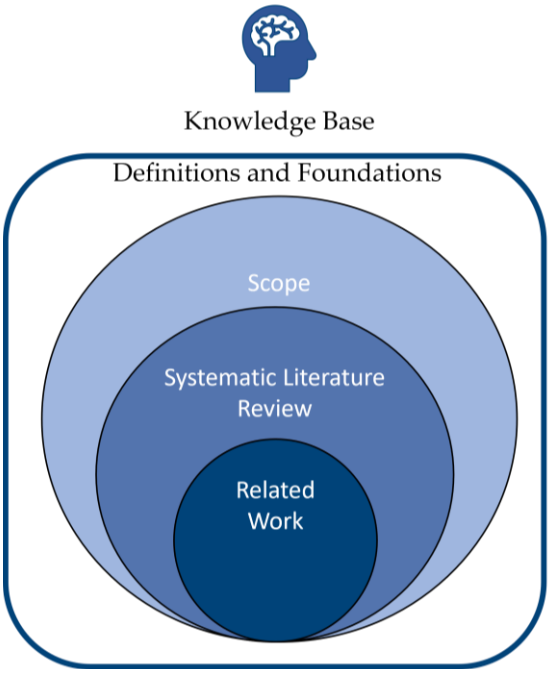


Figure 6: Structure of the Knowledge Base

3.1 DEFINITIONS AND FOUNDATIONS

This subsection provides a brief overview of the dissertation's foundational concepts and fundamental definitions. Concepts such as trust and the relationship of risk, cloud computing, blockchain, and smart contracts are addressed.

3.1.1 Cloud Computing Fundamentals

Although cloud applications are widely used, no universally accepted framework identifies the applications' basic components. This is further complicated by the fact that the terms "cloud computing," "cloud service," "cloud," and "cloud application" are sometimes used interchangeably in the literature (Giurgiu et al., 2009) (see 3.3.1). For a clear definition of terms, this dissertation uses the standard set by the "National Institute of Standards and Technology (NIST)". The NIST provides the most comprehensive and widely used definition of terms (Celar et al., 2011).

> [...] a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Mell & Grance, 2017, p. 2)

As the quote shows, NIST describes *cloud computing (or short cloud)* based on five essential characteristics (Mell & Grance, 2017). These characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Mell & Grance, 2017). Figure 7, below, illustrates these five characteristics, four deployment models, and three service models. Putting together these essential characteristics, a picture of cloud computing begins to form. Cloud computing and storage capacities can be adopted as required by customers through an on-demand self-service without any human involvement from the service ("on-demand self-service"). Services offered are available through a heterogeneous customer base via network access ("broad network access"). Existing computing resources are pooled and made available to customers through the virtualization of resources and multitenant architectures ("resource pooling"). Rapid elasticity allows for an automatic allocation of resources such that no bottlenecks arise, and thus the impression of almost endless computing power is created ("rapid elasticity"). Finally, the NIST standard defines that measured services should ensure that cost-of-service performance can be monitored and automatically optimized as needed ("measured service").

As illustrated in Figure 7, the cloud infrastructure could be deployed as a *private, community, public*, or *hybrid cloud*. A community cloud is exclusively provided to a predefined community of users. The hybrid cloud comprises two or more deployment models (private, community, and public). While community clouds are rarely used, public and private clouds are most common (RightScale, 2019). A private cloud is a cloud service that is not shared with any other entity. The users of a private cloud use this cloud exclusively.

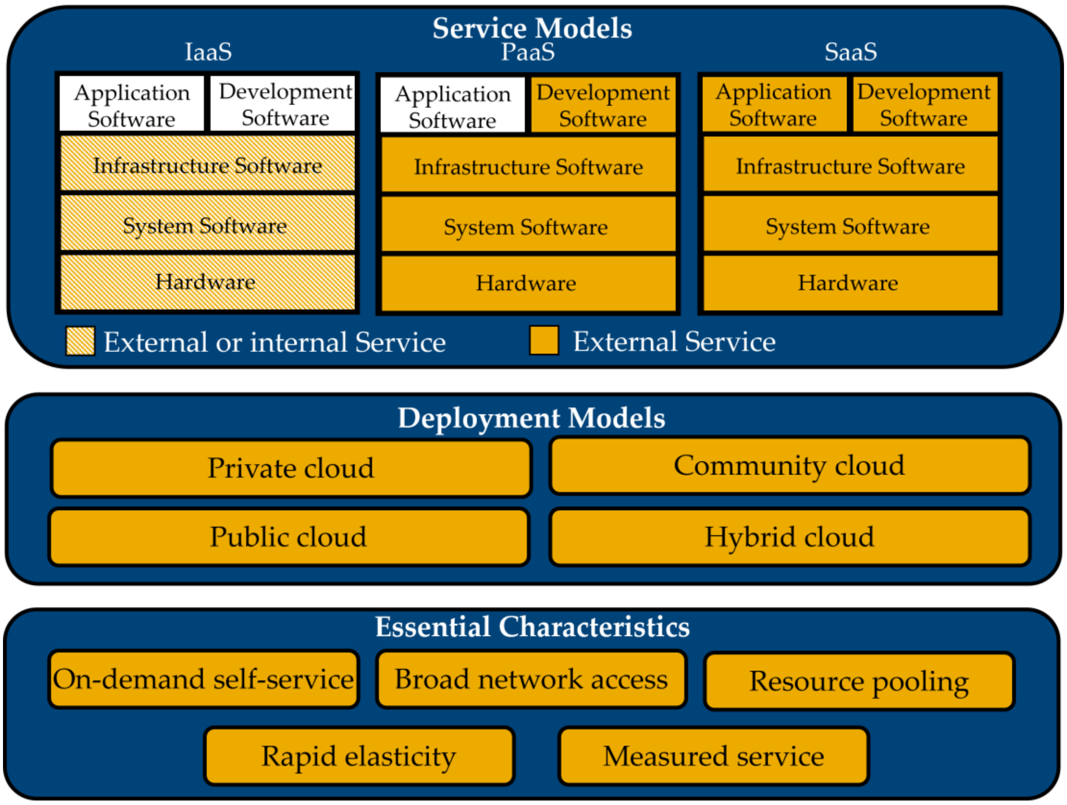


Figure 7: NIST Definition of Cloud Computing. (Adapted from Bohn et al., 2011)

In contrast, a public cloud is a cloud service where different customers share computing services. However, the data and applications of each customer in the cloud are not visible to the other customers. The two cloud models can be seen as analogous to renting apartments. The private cloud is similar to renting a house, whereas the public cloud can be seen as renting an apartment in an apartment building. In both models, a tenant does not have to worry about the substance and renovation of the property and can only use the living space. However, the extent to which the property is used exclusively differs in both cases. There are hosted private clouds offered by an external cloud provider and internal private clouds managed and maintained internally by the organization. While public cloud services are usually significantly cheaper than private cloud services, private cloud services have the advantage that they can be used exclusively without having to share data with others (Goyal, 2014). Public cloud solutions comprise most of the segments that make up the cloud market. This observation closely aligns with the RightScale 2019 State of Cloud report (RightScale, 2019). According to this report, 91% of enterprises reported using a public cloud service, 72% opted for a private cloud solution, and 69% used a hybrid solution. Due to the limited possibilities of operating a private cloud and the fact that public clouds offer the majority of cloud solutions, this dissertation focuses on overcoming the three mentioned adoption risks in public cloud scenarios.

According to the NIST Definition of cloud computing (Mell & Grance, 2017), *cloud services* can be provided using three different service models (see Figure 7). In the *Infrastructure-as-a-Service* (IaaS) model, an external service provider partly provides the infrastructure (e.g., processing capacity, storage, and network). In this service model, cloud service customers may configure network resources (i.e., firewall, ports, and load balancing) and freely install operating systems and application software. *Platform–as–a–Service* (PaaS) aims to provide a development environment that is easy to install and readily available. A PaaS user is provided with a ready-made development platform; therefore, users need not worry about configurations of development environments for the correct integration of libraries. In the *Software–as–a–Service model* (SaaS) model, the cloud infrastructure is used to deliver an application to customers that can be accessed easily via a web connection (e.g., via a web browser). SaaS products are among enterprises' most common cloud computing services to build and grow their businesses (RightScale, 2019). In the context of this dissertation, SaaS products are also referred to as *cloud applications*. A cloud application is highly scalable and easy to use and manage because it doesn't need to be downloaded and installed on individual devices to deploy to an entire team or company. This is especially advantageous for globally distributed teams.

To summarize, cloud (computing) can be described in five essential characteristics. A cloud can be deployed as a private, public, community, or hybrid. The extent to which computing services are shared with other cloud participants depends on the deployment model. Regardless of the deployment model, cloud services can be provided as IaaS, PaaS, or SaaS (cloud application), depending on how much a customer wants to manage their responsibility. In the context of this dissertation, the three described adoption risks are investigated based on cloud applications provided via a public cloud. These cloud applications have, by far, the highest market share. Examples of cloud applications include consumer-facing services like Google Docs and Microsoft Office 365 and the widely used business cloud application SAP S/4HANA Cloud.

3.1.2 The Reference Architecture of Cloud Computing

Shortly after the emergence of the cloud computing idea, it became clear that a standardized meaning of terms and communication relationships was needed so that companies, government agencies, and researchers could work on cloud solutions and projects worldwide (Bohn et al., 2011). The NIST took over this role in 2011 and standardized the cloud architecture that will accurately communicate the components and offerings of cloud computing.

The NIST cloud computing reference architecture consists of a generic high-level conceptual model describing the cloud's requirements, structures, and operations (Bohn et al., 2011). The cloud architecture has two fundamental parts: the front end, consisting of client-side applications and interfaces for accessing cloud computing platforms, and the back end, which the service provider uses to manage computing resources like security functions and data storage.

Besides activities and functions, the reference architecture also defines actors. The parties or actors involved in the developed architecture include *cloud providers, consumers, auditors, brokers,* and *carriers*. Cloud providers are persons or organizations that provide cloud services and enable interested parties to join cloud computing. Cloud consumers are participants in cloud computing and use services from providers. Cloud auditors can independently monitor services and information system operators' performance and security findings. Cloud brokers are independent instances that negotiate relationships between cloud providers and consumers. Lastly, a cloud carrier provides connectivity and transport services from cloud providers to consumers. Together, these parties constitute a developed architecture in the form of a network: cloud providers offer services to consumers, and cloud carriers and brokers mediate this relationship between providers and consumers.

In this dissertation, the term *cloud application provider* refers to a person, organization, or entity that provides the cloud application to be configured based on compliance requirements. A *cloud application consumer* is a person or organization that uses the application provided by the cloud provider and may wish to configure it based on their compliance requirements. *Cloud application* refers to an application hosted and made available in the cloud to a consumer based on the SaaS model.

3.1.3 The Meaning of Trust in Multiple Disciplines

This dissertation aims to utilize the blockchain as a *trusted anchor* for configuring cloud applications based on compliance requirements. For this purpose, the dissertation aims to make the *trust* regarding implementing a compliance requirement dependent on blockchain technology – not on the cloud application provider. Many studies have defined "trust" (Cho et al., 2015; Cristina Costa & Bijlsma-Frankema, 2007). Generally, trust refers to believing that something promised will occur or will be provided (Cristina Costa & Bijlsma-Frankema, 2007). Various researchers have studied trust in the cloud (Cho et al., 2015; C. Huang et al., 2021; Michael, 2009). A survey on trust modeling conducted by Cho et al. (2015) revealed the different meanings of trust in research. The findings of the survey can be seen in Table 3. The context of this dissertation is organizational management (see chapter 2). Hence, this work aims to support an organizational decision and follows the widely used definition of trust set forth by Mayer et al. (1995). These authors define trust as the willingness to take risk and being vulnerable to the relationship based on ability, integrity and benevolence (Mayer et al., 1995). As indicated in the introduction, this definition considers risks as an influencing factor of trust (see 1.2).

Table 3: Multidisciplinary Definitions of Trust. (Adapted from Cho et al., 2015)

Discipline	Meaning of Trust	Source
Sociology	Subjective probability that another party will perform an action that will not hurt my interest under uncertainty and ignorance	(Gambetta, 2000)
Philosophy	Risky action deriving from personal moral relationships between two entities	(Lagerspetz, 1998)
Economics	Expectation upon a risky action under uncertainty and ignorance based on the calculated incentives for the action	(James Jr., 2002)
Psychology	Cognitive learning process obtained from social experiences based on the consequences of trusting behaviors	(Rotter, 1980)
Organizational Management	Willingness to take risk and being vulnerable to the relationship based on ability, integrity, and benevolence	(Mayer et al., 1995)
International Relations	Belief that the other party is trustworthy with the willingness to reciprocate cooperation	(Kydd, 2018)
Automation	Attitude that one agent will achieve another agent's goal in a situation where imperfect knowledge is given with uncertainty and vulnerability	(J. D. Lee & See, 2004)
Computer and Networking	Estimated subjective probability that an entity exhibits reliable behavior for particular operation(s) under a situation with potential risks	(Cho et al., 2011)

3.1.4 Risk and Risk Assessment

Although there is no universally accepted definition of risk and its assessment, the definition adopted by the National Institute of Standards and Technology Special Publication 800-30 Revision 1 (NIST SP 800-30 R1) (N. NIST, 2012) is widely applicable in the enterprise environment, as it provides a standardized way of assessing business risks from a financial point of view. Thus, it allows organizations and governments to decide individually whether they want to adopt a cloud application from a financial risk perspective (Fikri et al., 2019).

Based on NIST SP 800-30 R1 (N. NIST, 2012, p. 12), risk can be defined as "a function of the likelihood of a threat event's occurrence, and potential adverse financial impact should the event occur." This function can be seen as the product of probability and impact for this dissertation. Thus, risk can be represented by the following equation:

$$\text{RISK} = \text{PROBABILITY X IMPACT}$$

An organization can determine the risk of an event by relating the occurrence probability of the event and the impact (e.g., monetary loss) on the organization. For example, an event with a low probability of occurrence and a low financial loss has a lower risk for an organization than an event with a low probability and a high financial loss. It is now common to break down probability into vulnerabilities and threats (N. NIST, 2012). Thus, risk can more specifically be seen as:

$$\text{RISK} = (\text{VULNERABILITY X THREATS}) \text{ X IMPACT}$$

Vulnerabilities can be further divided into three types (Ani et al., 2017). *Technical* vulnerabilities are weaknesses in software that an attacker can exploit. *Process* vulnerabilities are weaknesses in processes (rather than software). For example, assume a company has defined that as soon as an employee forgets their password, it is reset to a company-wide password (known to all employees) by calling customer service. If an employee is now in a position to overhear that another employee has just called customer service and asked for their password to be reset, the eavesdropping employee (if quick enough) can log into the calling employee's account. The password reset process thus offers a vulnerability. Last, *people* can also be a vulnerability. For example, incorrect entries or inadequate configuration of security systems can provide opportunities for attackers to steal data or take over systems. In short, this last type of vulnerability is due to human error. For example, the 2019 Capital One Bank case discussed in the introduction resulted from the exploitation of a people vulnerability: a firewall misconfiguration (Department of Justice, 2019; PRNewswire, 2019).

Threats are factors that exploit vulnerabilities. Like vulnerabilities, threats can be divided into three types (ISO 27005, 2018). *Environmental* threats are threats that arise due to environmental conditions. These can be earthquakes, floods, lightning strikes, or avalanches. *Accidental* threats can happen due to accidental misconduct, such as losing cell phones or sharing data. *Deliberate* threats are events that are intentionally executed by an entity. This can be the deliberate attacking of a server system or the deliberate sending of spam messages.

In combination with an attack's impact on a company, vulnerabilities and threats determine a company's financial risk. It is the task of risk management in an organization to identify all risks and, if possible, mitigate them, monitor their mitigation, and identify emerging risks (Merna & Al-Thani, 2008). This thesis assumes that the change in the cloud adoption architecture has a low impact on an enterprise's threat as the application and associated threat scenarios remain the same. At the same time, it is also assumed that the potential impact from a threat remains more or less the same when changing the configuration architectures. This dissertation assumes that the architecture change ensures an enterprise's vulnerability is lowered. The assumption is that attacks on an enterprise mostly depend on the information obtained by attacking the enterprise rather than the underlying architecture of enterprise software. Impact assumes that it depends on the type of information leaked rather than the architecture over which the attack could have taken place. This thesis assumes that a change in architecture changes an enterprise's vulnerability. Therefore, this dissertation aims to reduce the vulnerability factor in the equation:

$$\text{RISK} = (\text{VULNERABILITY X THREAT}) \text{ X IMPACT}$$

Therefore, the hypothesis for the MRQ is: If the THREAT and the IMPACT of adopting cloud computing remain constant, reducing VULNERABILITY leads to a reduction in risk. The evaluation of the work must later show whether the assumption was correct and to what extent the RISK of cloud adoption might thus be reduced.

3.1.5 The Relation Between Trust and Risk

Understanding why shifting trust from the cloud application provider to the blockchain may reduce (adoption) risks becomes clear when considering the relationship between trust and risk. The relationship between trust and risk is part of many research publications (Cho et al., 2015; Jøsang & Presti, 2004; Luhmann, 2017; Mayer et al., 1995; Pearson & Benameur, 2010; Povey, 1999; Solhaug et al., 2007; Sun, 2019). There is yet no uniformly recognized model of how trust and risk interact, and it is unclear whether such a model can be designed (Jøsang & Presti, 2004). Creating a universally accepted model is difficult in large part because the concepts of trust and risk are influenced by many subjective factors (Jøsang & Presti, 2004). However, the consensus among researchers is that there is an inescapable link between trust and risk. Without risk, it makes no sense to talk about trust (Cho et al., 2015; Solhaug et al., 2007). Thus, a relationship between trust and risk is widely accepted in the scientific community, and it is likewise widely accepted that risk critically affects trust (Benlian & Hess, 2011; Cayirci & de Oliveira, 2018; Cho et al., 2015).

While some authors argue that trust and risk have an inversely proportional relation (Sun, 2019), others claim that trust is not proportional to risk (Solhaug et al., 2007). An understanding of the exact relationship is not necessary for the course of this dissertation. Rather, all that is necessary for this research is the understanding that risk and trust have some inverse relationship, i.e., that increased risk correlates with decreased trust. Thus, this dissertation follows the general assumption that a reduction in risk increases adoption probability (Mayer et al., 1995). For the rest of the dissertation, the relationship between trust and risk is assumed to be that described by Solhaug et al. (2007):

> we have defined trust in terms of the probability that the trustee will not act deceitfully and then associated the trust value with the probability element of a risk. The decision as to whether or not to cooperate with the trustee is then not primarily determined by the estimated trustworthiness. The decisive element is the level of risk the trustor willing to accept as balanced against the prospects involved. (Solhaug et al., 2007, p. 7)

Hence, this dissertation follows the findings of Solhaug et al. (2007) and argues that the perceived risk impacts the adoption decision. Reducing perceived risk (depending on the decision maker's risk perception) can, therefore, positively affect the adoption decision for cloud services. For example, suppose a team lead must decide daily whether to accept projects and to whom on the team to assign them. The team lead must trust that the employee will complete the project. If the project fails, the team lead must justify this to the management. By handing over a project, the team leads risk damaging their reputation. How much a team lead trusts their employee influences how much risk the team lead takes. Therefore, the level of trust influences the perceived risk (Mayer et al., 1995). If the perceived risk is higher than the level of trust, risk-taking in relationships will not occur (Mayer et al., 1995). In other words, if the team lead's perceived risk of transferring a project is higher than the level of trust in the employees, then the project (and the associated risk) will not be transferred to the employee.

Applied to this dissertation, this implies that the same user will evaluate the perceived adoption risk arising from the compliance-driven configuration of cloud applications based on the entity on which the implementation of the compliance requirement depends. Today, this is the cloud application provider. The objective of this dissertation is that it becomes the blockchain. If blockchain technology can achieve a higher level of trust in the compliance-driven configuration of cloud applications than the cloud application provider, then according to the theory of Mayer et al. (1995), the three perceived adoption risks must also be reduced. The evaluation of this work aims to determine whether the adoption risk of cloud applications could be reduced. All other things constant, reducing compliance-based adoption risks would suggest that users trust the blockchain more than cloud application providers. More importantly, it shows that a trust shift towards blockchain is possible.

3.1.6 Cloud Adoption Risks

As shown in the introduction (see 1.3), this dissertation assumes three areas from which adoption risks for cloud applications can arise in compliance and regulation. The risk areas assumed in this dissertation are:

1) *Transparency Risk*: The risk is that a cloud application provider may not implement a contractually, mutually agreed, compliance-driven configuration. As discussed (see 1.3.1), a cloud application's customer depends on the cloud services provider implementing configurations

(such as backup frequencies) as contractually agreed. If an incident occurs and the customer must resort to a backup, the customer must rely on the cloud provider to provide this backup as contractually agreed. Customers, therefore, risk that their requirements will not be implemented as agreed. Based on the risk model described in 3.1.4, this is a people's vulnerability. Human error leads to this risk.

2) *(Process) Automation Risk*: The risk of delaying compliance-driven configuration changes due to slow or untransparent configuration update processes. In addition to the challenges experienced in compliance, there are planning challenges—especially in terms of planning costs (see 1.3.2). Hidden costs can also negatively impact the adoption of cloud services (Al-Marsy et al., 2021). If, for example, enterprises' compliance requirements require changes (i.e., the data storage location must be re-selected, the backup frequency is changed, or design adaptations must be made), this will incur costs. Changes in cloud applications are typically commissioned via consultants for the application (Martens et al., 2012). Enterprises communicate their changes to the cloud service consultants. The consultants consequently pass on these change requests internally or implement them on behalf of the customer. Adaptations are routinely associated with costs for the consultant service and a time delay (Makhlouf, 2020). The delaying of a configuration is a process vulnerability based on the risk model described in 3.1.4. Weak or slow processes create a cloud adoption risk for cloud customers. Based on the risk model described in 3.1.4, this is a process vulnerability.

3) *Repudiation Risk*: The risk of denying the configuration implementation in case of a dispute. There is the risk that one of the two contracting parties denies its responsibility to implement contractual agreements (see 1.3.2). The burden of proof usually falls on the aggrieved party. The risk of denying the configuration implementation is also a people's vulnerability based on the risk model described in 3.1.4.

3.1.7 The Elliptic Curve Digital Signing Schema

This dissertation aims to utilize the blockchain for compliance-driven configuring cloud applications. Hence, it aims to shift the trust for configuring cloud applications to the blockchain, thereby reducing the adoption risk for cloud applications. It is essential to understand the fundamentals of cloud computing and blockchain technology to understand how the blockchain works, why digital signatures are used to notarize transactions, why moving configurations to the blockchain may mitigate risk, and why the blockchain can be trusted. Besides understanding the basic definitions of cloud computing, trust, and risk, this dissertation also requires a basic knowledge of blockchain technology. To be more precise, basic mathematics, cryptography, and computer science knowledge of blockchain technology. To begin, two key cryptographic concepts are discussed: cryptographic hash functions and digital signature schemes.

A *hash function* is a mathematical function that converts an arbitrary length numerical input value into a fixed numerical output value (Damgård, 1990). Values returned by a hash function are called the message *digest* or *hash values*.

For example, a hash function could always truncate an input to the last three digits of the input. The hash function fills the remaining digits with zeros if the input is shorter than three digits. For example, this hash function would map 11815 to 815, 4646034 to 034, and 34 to 034. Thus, the values 4646034 and 034 would produce the same output, called a *collision* (Damgård, 1988). If it is easy (later, the mathematical definition is given here) to find an input for a given hash value (say 034) that produces this hash value (say 34), the hash function is described as not *preimage resistant*.

Furthermore, it would be quite easy to find two input values to produce the hash value 034. 34 and 4646034 are such inputs. If it is easy to find two different input values for a given hash value, the hash function is said to be not *second preimage resistant*.

Passwords are usually not stored in plain text in databases but as hash values. This has the advantage that they can neither be read by a database administrator nor by data theft. Suppose it was easy for an attacker to find a hash collision, the preimage or second preimage to a hash value; storing the passwords as hash values would be unnecessary since these could be guessed easily. Therefore, hash values that may only be traced back to their original input with extreme difficulty are stored using a hash function with special characteristics. Hash functions preimage resistant, second preimage resistant, and collision resistant are called *cryptographic hash functions* (Damgård, 1988, 1990). Formally, a cryptographic hash function is a function $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ and $n \epsilon \mathbb{N} \setminus 0$ that satisfies the following security requirements (Damgård, 1988, 1990):

1) Preimage resistance: Given a hash value h, computing x, such that $H(x) = h$ should be in $\mathcal{O}(2^n)$
2) Second preimage resistance: Given a value x and its corresponding hash value $h = H(x)$, computing a value x' such that $x \neq x'$ and $H(x') = h$ should be in $\mathcal{O}(2^n)$
3) Collision resistance: Computing any two arbitrary values x and x' $s$uch that $x \neq x'$ and $H(x) = H(x')$ should be in $\mathcal{O}(2^{n/2})$

This dissertation often refers simply to a hash function for easier readability, but it always means a cryptographic hash function.

Digital signature schemes are one way that hash functions are commonly used. A digital signature scheme consists of three main components and can be seen as a triple (G, S, V) of algorithms (C. NIST, 1992). These three algorithms are a *key generator (G)*, a *signing algorithm (S)*, and a *verification algorithm (V)*.

Two basic methods can be used for encrypting and signing data: Symmetric and asymmetric (Yassein et al., 2017). The first method will be discussed later (see 4.2.3.3). The second method requires combining a private key with a public key. For encrypting messages with asymmetric methods, the public key is communicated to everyone who wants to encrypt a message. The public key can be used to encrypt a message. It can only be decrypted again using the private key. In the case of asymmetric digital signatures, the private key is used to confirm a message's origin uniquely. Utilizing the public key, potentially known to everyone, the signature created with the private key can be checked for authenticity by anyone. Consequently, the private key must, neither in the case of encryption nor during the digital signing case, be disclosed by the owner.

The algorithm G generates a public key key_{pub} and a private key key_{priv} . The signing algorithm S takes the key_{priv} and a message m as input. In an intermediate step, the algorithm S utilizes a cryptography hash function h to create a digest *h(m)*. S provides $h(m)_{key\_priv}$ a digital signature on $h(m)$ as output. Using the public key key_{pub}, the verification algorithm V verifies whether a received digitally signed message $h(m)_{key\_priv}$ is genuinely signed by the owner of the private key corresponding to key_{pub}. Digital signatures are used to prove the authenticity of a message sender and the integrity of a message (C. NIST, 1992). Thus, provide a possibility of notarizing messages.

Blockchain technology uses digital signatures to notarize transactions (Buterin, 2014; Park & Park, 2017). More precisely, blockchains usually use the elliptic curve digital signing schema (ECDSA), as stated in the Request for Comments (RFC) 6979 (Pornin, 2013). The RFC 6979 defines an ECDSA in the following way:

Let $\mathbb{F}_q$ be a finite field with a characteristic greater than three and $\overline{\mathbb{F}_q} = \bigcup_{k\geq 1} \mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_q$. An elliptic curve E over the Field $\mathbb{F}_q$ is the set of all solutions $(x, y) \in \overline{\mathbb{F}_q}\ x\ \overline{\mathbb{F}_q}$ to the equation

$$y^2 = x^3 + ax + b$$

Where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$, and ∞ a particular point at infinity (the identity at the abelian group E).

3.1.7.1 Generator Algorithm G

ECDSA utilizes an asymmetric digital signing schema. To be more precise, let $(g_x, g_y) = P_0$ with $(g_x, g_y) \in E$ a point called the generator point. The private key key_{priv} is a random integer in the range of [0, q−1]. The public key key_{pub} is calculated as a product of key_{priv} and G.

$$key_{priv} = i \in [0, q-1]$$

$$key_{pub} = key_{priv}.*\ P_0$$

3.1.7.2 Signing Algorithm S

Based on RFC 6979, the ECDSA signing algorithm takes two input values: the message to be signed, *m*, and a private Key, key_{priv}, for signing *m*. As an output, S provides the tuple (*r*, *s*), where *r* and *s* are created as follows:

1) Due to performance reasons, S does not sign *m* directly, but instead, the hash value of *m*: *h = H(m).*
2) Next, S creates a secret number $k \in [0, q-1]$. RFC 6979 describes a deterministic and random method of creating *k*. The following steps are independent of how *k* was generated.
3) Then, the value *R*, the *x*-coordinate of a random point *R*, is calculated. With this, R is calculated by multiplying *k* with the generator P_0. Hence $R = k * P_0$ and $r = R * x$.
4) Ultimately, the signature proof *s* is calculated $s = k^{-1} * (h + r * key_{priv})(mod\ q)$. Note that $k^{-1} * k = 1\ (mod\ q)$.

3.1.7.3 Verification Algorithm V

V takes the message *m*, the signature tuple (*r*, *s*), and the public key key_{pub} (the corresponding public key to the private key key_{priv} with which the signature tuple (*r*, *s*) was created) as input. As an output, V returns true if the provided signature tuple is an actual signature for *m* and false if not. V works as follows:

1) Calculate $h = H(m)$.
2) Calculate $s_1 = s^{-1}(mod\ q) = k.(h + r.key_{priv})^{-1}$.
3) Calculate value $r_1 = R_1.x$, based on the provided signature tuple (*r*, *s*). (Note that $key_{pub} = key_{priv}.P_0$).
4) Calculate $R_1 = (h.s).P_0 + (r.s_1).key_{pub}$

$$= \left(h + r.key_{priv}\right).s_1.P_0$$

$$= \left(h + r.key_{priv}\right).k.\left(h + r.key_{priv}\right)^{-1} mod\ q.P_0$$

$$= k.P_0.$$

5) Returns true if $r_1 = r$ holds; otherwise, it returns false.

In summary, it can be concluded that digital signatures make it possible to generate a unique digital signature for a message. The signature can be verified for authenticity by any recipient of the message. As shown in this dissertation, the principle of digital signatures is used in blockchain technology to confirm and verify the authenticity of transactions. The mathematical explanation is intended to help understand blockchains' security and third-party independence. Blockchains use digital signatures to sign transactions. In other words, transactions are notarized by the blockchain using digital signatures. Once a transaction has been notarized, it can only theoretically be changed, as section 3.1.10 will show.

3.1.8 Diffie Hellman Key Exchange

Diffie and Hellman (1976) presented a protocol for agreeing on a shared secret key. This protocol allowed two communication participants to agree on a common key over an insecure line. Before this dissertation formally specifies the Diffie Hellman Key Exchange, the idea of the key exchange should first be clarified. For this purpose, an analogy to mixing colors is used. The idea of Diffie Hellman Key Exchange can be described as mixing colors:

- Alice and Bob agree on a common (public) color.
- Each also chooses a secret (private) additional color.
- Alice and Bob mix an additional color by mixing their secret and public color.
- They each send the newly mixed color to their communication partner.
- In the end, each mixes their secret color into the previously exchanged mixed color.
- Alice and Bob thus get the same mixed color without knowing which private color the other has chosen.

From the mixed colors, it is now difficult to determine which private colors are in the mixture. The security of this method is based on the fact that it is difficult to filter out the exact original colors from a color mixture. The security of the Diffie Hellman Key exchange is based on the phenomenon that the discrete exponential function can be efficiently computed in cyclic groups. At the same time, however, it is assumed that there is no efficient algorithm for computing the discrete logarithm in cyclic groups. Based on the method presented by Diffie and Hellman, a prime number q and a generator $g \in [1;\ q-1]$ must be known to both communication partners and can be sent over an insecure channel. When two communication partners, A and B, want to generate a common secret key s, both communication partners simultaneously determine a private key (in the example above, the private color). Communication partner A determines $x_A \in [1;\ q-1]$ as the private key, while communication partner B determines $x_B \in [1;\ q-1]$. The parties do not share their private keys with each other. Instead, the parties generate a public key (in the example above, the public color) with the help of the computed private keys. For this, party A computes $A_{pub} = g^{x_A}$ mod q and party B computes B_{pub} = g^{x_B} mod q. Now, both parties exchange their public key A_{pub} and B_{pub} via an insecure communication channel. Both parties then have access to A_{pub} and B_{pub} and can compute $s = B_{pub}^{x\,A}$ mod q = $(g^{x\,B})^{\,x\,A}$ mod q = $(g^{x\,A})^{\,x\,B}$ mod q = $A_{pub}^{x\,B}$ mod q. This dissertation uses the Diffie Hellman protocol for three parties. Therefore, it is assumed that parties A, B, and C agree on a shared key. The Diffie Hellmann protocol can be easily extended to three parties as follows (Diffie and Hellman 1976):

1) Each of the three parties creates a private key $x_A, x_B, x_C \; \in [1, q-1]$.
2) Each party calculates its public key $A_{pub} = g^{x\,A}$ mod q, $B_{pub} = g^{x\,B}$ mod q, $C_{pub} = g^{x\,C}$ mod q.
3) Now A sends A_{pub} to B, B sends B_{pub} to C, and C sends C_{pub} to A.
4) After all parties have exchanged their keys, A calculates $CA = C^{x\,A}$ mod q, B calculates $AB = A^{xb}$ mod q, and C calculates $BC = B^{xC}$ mod q.
5) A sends CA to B, B sends AB to C, and C sends BC to A.
6) A computes $s = BC^{x\,A}$ mod q, B computes $s = CA^{x\,B}$ mod q, and C computes $s = AB^{x\,C}$ mod q.
7) Finally, all parties have access to the same secret key s.

Note that:

$s = BC^{x\,A}$ mod q

= $((g^{x\,B})^{x\,C})^{x\,A}$ mod q

= $((g^{x\,C})^{x\,A})^{x\,B}$ mod q

= $CA^{x\,B}$ mod q

= $((g^{x\,C})^{x\,A})^{x\,B}$ mod q

= $((g^{x\,A})^{x\,B})^{x\,C}$ mod q

= $AB^{x\,C}$ mod q

3.1.9 Trusted Third Parties

As pointed out in the introduction, HTTPS improves WWW security compared to HTTP by introducing encryption and integrity protection. Encryption and integrity protection was made possible by exchanging encryption keys using the Diffie and Hellman (1976) method (see 3.1.8). However, the issue with exchanging keys is that when the keys are exchanged, attackers could intercept the actual key and replace it with their key (Khader & Lai, 2015). Attackers can thus insert themselves into communication and make both parties believe they are dealing with the other. This attack is known as MITM. MITIM attacks enable attackers to undetected interrupt encrypted connections and read them in plain text (Khader & Lai, 2015). An attacker can use MITM to access secret information, usernames, passwords, or bank data. To prevent a MITM attack, the exchanged keys had to be authenticated (i.e., the sender's authenticity had to be verified). Digital certificates were introduced to prove the authenticity of a key (Khader & Lai, 2015). By trusting the certifier, trust was also placed in the key received.

Currently, the internet's two main trust management systems are Web PKI and PGP's Web of Trust (Alexopoulos et al., 2017). The idea of both systems is shown in Figure 8, below. The core difference between the two systems (Web PKI and PGP) is how trust is managed. While Web PKI is strictly hierarchical, the Web of Trust is decentralized. With Web PKI, there is a root certificate that users trust. A certification authority (CA) uses this root certificate to issue further certificates. Since the users trust the root certificate and the CA certificates are derived from the root certificate, the users also trust the certificates issued by the CA. The CA can now issue additional certificates for web servers. Since users trust the CA, they ultimately trust the server certificates too. A chain of trust is thus formed (see 1.1).

The Web of Trust goes in another direction. With the Web of Trust, there is no hierarchy. Anyone can sign any key. The recipients of a public key then decide for themselves whether they trust the people who signed the key. Thus, decentralized management of the trust is utilized. In simplified terms, Figure 8 (right) shows the idea of the Web of Trust. The Web of Trust can be described as a Transitive Trust Network.

- Alice signs Bob's key and thus trusts Bob,
- Bob signs A's key and C's key and thus trusts A and C,

- A signs B’s key and C’s key, and thus A trusts B and C,
- since Bob trusts A and A trusts B, Alice trusts B's key.

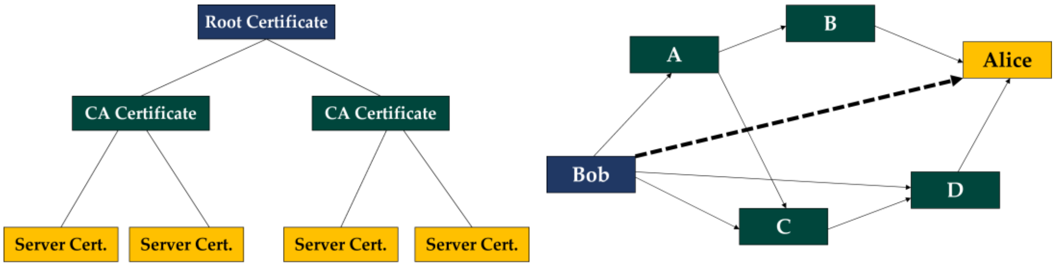
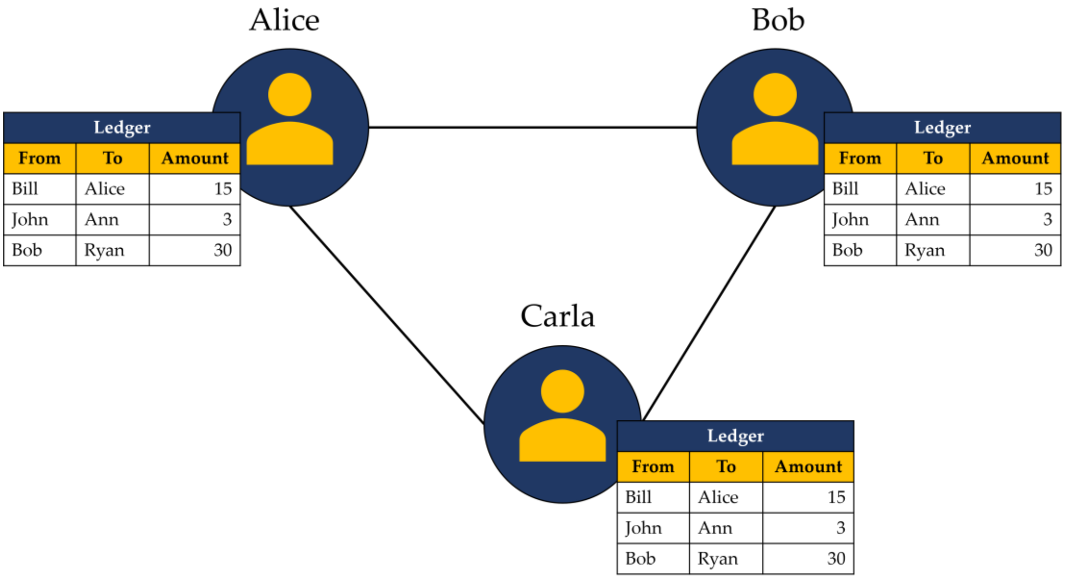


Figure 8: Schematic Representation of the Web PKI (left) and the Web of Trust (right)

3.1.10 Blockchain

Based on the idea of decentralized trust management, Satoshi Nakamoto proposed his idea of a decentralized peer–to–peer (P2P) cryptocurrency called Bitcoin in 2008 (Nakamoto, 2008). In doing so, he introduced *blockchain technology*. Formally, “[a] blockchain is a distributed data structure that manages transactions transparently, chronologically, and immutably in a computer network.” (Prinz et al., 2022, p. 167). In other words, a blockchain offers the possibility of creating transparent transactions that are traceable over time and cannot be changed. Concerning the risks mentioned above, it is clear that if a cloud application were configured utilizing blockchain technology, the configuration would already be transparent and non-repudiable due to the blockchain technology. However, it is not yet clear whether the shift of configurations to the blockchain is possible, what challenges are associated with this, for which environment this would be advantageous, and whether the risks mentioned can be significantly reduced with blockchain technology. This must be shown in the course of this dissertation.

As shown in Figure 9, the blockchain can be seen as a publicly distributed ledger (Mohanta et al., 2019). Hence, each entity has the same shared knowledge in the bitcoin network. The ledger is not centrally stored and does not belong to anyone.



From	To	Amount
Bill	Alice	15
John	Ann	3
Bob	Ryan	30

From	To	Amount
Bill	Alice	15
John	Ann	3
Bob	Ryan	30

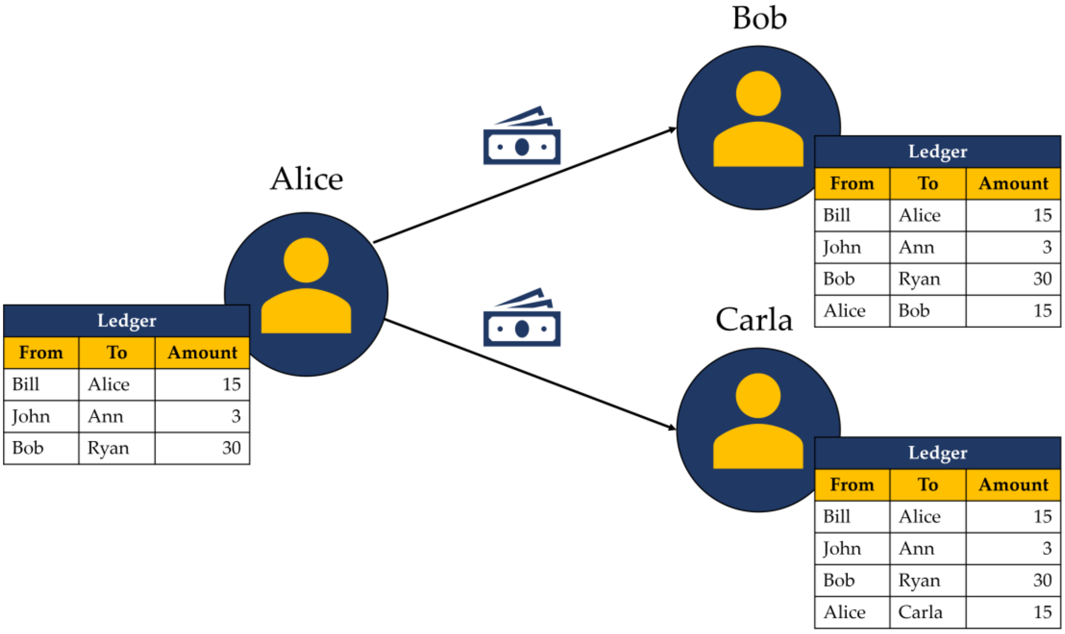
From	To	Amount
Bill	Alice	15
John	Ann	3
Bob	Ryan	30

Figure 9: Schematic Structure of a Distributed Ledger

The idea of a publicly distributed ledger was not new when Nakamoto introduced Bitcoin (2008). However, for many years the use of decentralized ledgers had one problem, the so-called double-spending problem (Chohan, 2017).

> the double spending problem is a potential flaw in a cryptocurrency or other digital cash scheme whereby the same single digital token can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or falsified (Chohan, 2017, p. 1).

Details of this definition are shown in Figure 10, below. In a distributed ledger, each participant has the same information. So, Bob and Carla know that Alice has 15 units of money. Alice can now send this money once to Bob and once to Carla. Both can check on the distributed ledger whether Alice has the money. However, neither can check whether Alice has already transferred this money to someone else in the meantime. Alice could send her money at the same time to both parties. Neither party would know that Alice had already used her money to pay the other party. Hence, Alice could pay both Bob and Carla and double her money—this problem is thus called double-spending. Double spending has long been an open issue and has remained a limitation of digital currencies for many years (Chohan, 2017).



Ledger

From	To	Amount
Bill	Alice	15
John	Ann	3
Bob	Ryan	30

Ledger

From	To	Amount
Bill	Alice	15
John	Ann	3
Bob	Ryan	30
Alice	Bob	15

Ledger

From	To	Amount
Bill	Alice	15
John	Ann	3
Bob	Ryan	30
Alice	Carla	15

Figure 10: Schematic Representation of the Double-Spending Problem

Nakamoto's blockchain approach resolved this limitation and paved the way for newer decentralized approaches (Buterin, 2014). The starting point for overcoming the double-spending problem is transactions; transactions are used in the blockchain to overcome the double-spending problem. Figure 11, below, illustrates the concept of transactions schematically. Transactions utilize the ECDSA. Therefore, each transaction has a version. The version is needed to understand the content of the transaction. Different versions of transactions might have different content (e.g., signing algorithm). To make sure that transactions a understand the same way, each transaction contains its version.

Moreover, each transaction has a defined amount of money that should be spent. Furthermore, each transaction has one or more previous transaction(s) as input and one or more addresses as output. A transaction's addresses can be simplified as public keys of senders or receivers of messages. The public keys are used similarly to addresses in the real world. The input addresses define from whom the money was received. The output addresses define where the digital money should be transferred. In this scenario, input and output addresses are public encryption keys generated by a generator algorithm (see 3.1.7.1). By providing the origin address of the money to be sent and the address to which it is sent, each participant can verify the money flow based on transactions. The flow of money can therefore be traced from address to address. However, the concept of transaction makes it necessary to prevent fraud. Fraudsters could create a transaction and set the output address as money receivers, as transactions are digital information that can be easily copied and updated (see double-spending). To prevent fraudulent activities, each transaction must be authorized through a digital signature (see 3.1.7). Hence, a transaction may not be signed with an arbitrary key. Following the flow of money, this flow has a beginning (the moment the money was created) and an end (the last transaction that transfers the original money to an output address). In the blockchain principle, the person who owns the last public key (output address) of a money flow is now the owner of the money. The possession of the public key and thus the possession of the money is proven by a private key. If an owner wants to transfer the money received, they must create another transaction in which they specify the output address to which they want to transfer the money. As the input address of this new transaction, they use their own address (public key). By digitally signing the newly created transaction with their private key, the transferor's address (public key) can be used to determine whether that person is actually the owner of the money (public key). All that is needed is to match the input address of the new transaction (public key/output address of the previous transaction) with the digital signature of the new transaction (see 3.1.7.3). In a nutshell, the money is always bound to a public key. Only the person owning the corresponding private key can further process the money.

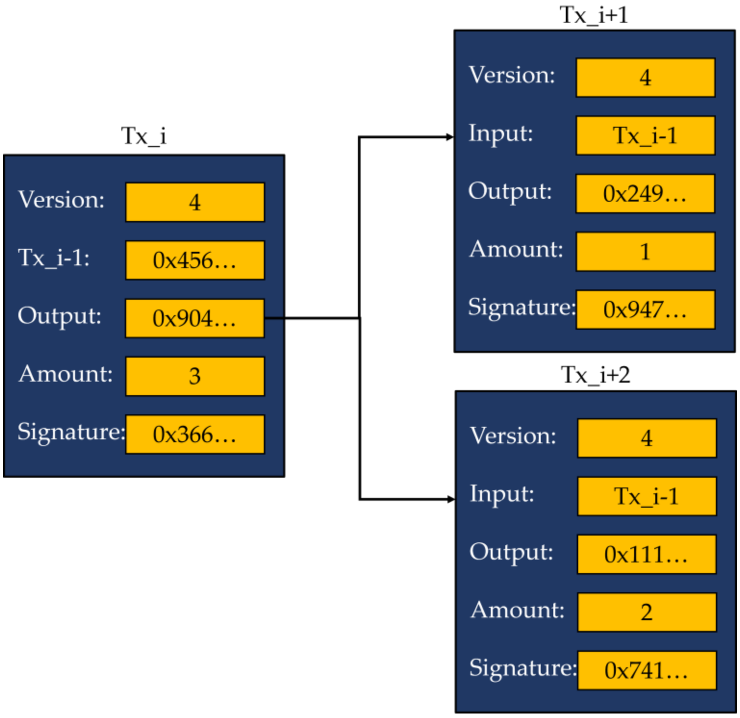


Figure 11: Schematic Representation of a Transaction

In a centralized system, such as a bank, a central authority would verify each transaction. Then, if the verification was positive, the bank would transfer a specified amount of money from the input address of the transaction to the output address. Hence, all customers must trust that the bank will not engage in malicious activities that could harm the clients. In a decentralized system, however, this is not possible as no central entity exists. In the blockchain network, transactions are transmitted using digital signatures. Participants receive the money transferred to their public address (represented by the receiver's public key). The transfer is made using the digital signature of the money sender. The recipient of the money can verify whether the sender has the money sent by tracing the chain of transactions to see how the sender of the money obtained it. The receiver of the money must verify that the sender of the money has received it legitimately through previous transactions. However, two things are mandatory for this.

First, previous transactions must be available. To facilitate this, multiple transactions are bundled into a so-called block. The previous block's hash and all transactions are included in a block. Hence, a chain of blocks is formed. This chain of blocks is called the blockchain. Figuring out whether the sender of the money has received it is now easy. The recipient checks the blockchain and sees when and from whom the sender of the money received it. If the receiver is unable to do this, the transaction is rejected.

Second, manipulating a block in the blockchain must be difficult. The money receiver can verify whether the sender has the claimed money with the first requirement. However, a fraudulent money sender could manipulate one transaction in a block and recreate the blockchain. The manipulation of a transaction could lead to a situation where the recipient of the money accepts the payment based on a manipulated money origin. Therefore, as a second requirement, manipulating the blockchain must be impossible. More precisely, it must be ensured that a blockchain participant who wants to add a block to the blockchain is more "qualified" than the others (Nguyen & Kim, 2018). By consensus, it must then be decided who is most qualified to add a new block. Once a consensus has been formed, the new block is accepted as such by all blockchain participants. A common consensus algorithm is needed to establish consensus and decide which block will be accepted by all parties next in the blockchain.

A consensus algorithm is a method whereby all users in a blockchain network come to a consensus on the actual position of the public ledger (Nguyen & Kim, 2018).

Consensus algorithms can generally be divided into two categories (Nguyen & Kim, 2018). Public blockchains like Bitcoin mostly use "proof-based" consensus algorithms. In proof-based consensus algorithms, participants must demonstrate that they are more prepared to do the adding task than the others. With Bitcoin, Nakamoto introduced the Proof of Work (PoW) consensus algorithm as one such proof-based algorithm (Nakamoto, 2008; Nguyen & Kim, 2018). The main goal of the PoW is to solve a complex mathematical problem and provide its solution first to the blockchain network. If the network can verify the solution, it agrees to add the proposed block. However, PoW has the well-known problem of using considerable amounts of energy compared to other consensus procedures. Hence, PoW is associated with environmental concerns and the perception that blockchain is generally an energy-intensive technology (Bentov et al., 2014).

As a result of this problem, newer proof-based consensus algorithms like Proof of Stake (PoS) are gaining popularity. The idea behind PoS is that a weighted random selection of the network participant is allowed to add the next block. The more stake a participant has in the blockchain network, the more likely they will be allowed to add the next block. The idea is that the more stake someone has in the network, the less interest they have in corrupting it (Nguyen & Kim, 2018). The public blockchain Ethereum has already announced a switch of consensus algorithm from PoW to PoS (Hertig, 2017).

Besides proof-based systems, there are also "voting-based" consensus algorithms. Voting-based consensus algorithms are mainly used in private and consortium blockchains (Nguyen & Kim, 2018). This is because voting-based algorithms require that voters know most blockchain participants in order to agree with them on the next block through joint voting.

Overall, the blockchain is not environmentally harmful per se. Rather, its environmental impact depends on selecting the proper consensus algorithm. The common belief that the blockchain is environmentally harmful is based on the assumption that blockchain always uses a PoW consensus algorithm, which is energy intensive. By contrast, PoS and voting-based consensus algorithms are less energy intensive and could represent a more environmentally sustainable future for blockchain. Looking at the limitations of Web PKI and Web of Trust and the future viability of blockchain technology, this dissertation focuses on using blockchain as a new way of trust management.

3.1.11 Smart Contracts

Nick Szabo initially introduced the concept of smart contracts in 1994 (Szabo, 1997). A smart contract is a digital contract that is self-verifying, self-executing, and tamperproof. A smart contract is a program that can be executed without a third party. The smart contract consists of an address, value, functions, and status (Bahga & Madisetti, 2016). As input, the smart contract receives instructions from a transaction; the smart contract executes these instructions without the intervention of a third party. Based on the instructions of the transaction, the smart contract functions are executed, and the status is changed. Due to its security against counterfeit transactions, the blockchain is a suitable medium for providing smart contracts (Mohanta et al., 2018). Smart contracts are written in a Turing-complete programming language and can be executed by a user or predefined event. A programing language is called Turing complete if it can run any program (irrespective of the language) that a Turing machine can run given enough time and memory (Grigore, 2017). In the Ethereum blockchain yellow paper, Buterin (2014) indicated that Bitcoin made remarkable progress in developing cryptocurrencies by introducing blockchain technology. However, Bitcoin has significant limitations regarding smart contracts (Buterin, 2014). To overcome these limitations, Buterin (2014) developed the Ethereum blockchain, through which users can execute smart contracts. To ensure the execution of smart contracts, Ethereum relies on the Ethereum Virtual Machine (EVM). The EVM is a virtual component necessary for all network participants and can execute bytecode for smart contracts.

Consequently, any participant in the Ethereum network can execute smart contracts using EVM. Since the execution of smart contracts requires the network's computational power, the execution is not free. A fee must be paid for every transaction executed on the Ethereum network. Ethereum Gas estimates the computing power of running transactions in the Ethereum network. Ethereum Gas is comparable to kilowatt-hours (kWH) for measuring a household's electricity consumption. Typically, electricity is billed by kWH and later paid in euros (or the relevant regional currency). In Ethereum, the payment is made to the finder of the new block and is intended to provide additional motivation. Programs to run on the EVM—smart contracts—are made available in Ethereum's programming language, EVM bytecode.

Smart contracts are typically not written directly in EVM bytecode but in a higher-level programming language, Solidity. The program code is then compiled into EVM bytecode so that the Ethereum Virtual Machine can process the information. The EVM achieves Turing completeness by enabling a market that settles transaction costs per software instruction executed rather than per monetary transaction performed, as with Bitcoin (Buterin, 2014). Instead of a transaction price, there is a fee for executing software.

Supply chain management, Internet of Things (IoT), healthcare systems, Identity and Access Management (IAM), data sharing, digital rights management, insurance, financial systems, real estate, and gambling are only a limited list of use cases for smart contracts (Buterin, 2014; Mohanta et al., 2018).

Smart contracts can be explained with the following IoT example. Before doing so, there is no clear definition of IoT (Shancang Li et al., 2015). Depending on the area of application and the technology used, the definitions of IoT can differ. IoT generally describes everyday objects or machines in an industrial environment interconnection via the Internet (Shancang Li et al., 2015). Devices are given a unique network address and are developed into intelligent things using operating systems and application software. As a result, devices can communicate via the Internet and automatically perform tasks on command. Intelligent devices are often referred to as smart devices. In addition to the possibility of communication between devices (machine-to-machine communication), devices can also be operated and controlled by users from any location via the Internet.

Due to their frequent use in industrial environments and the possibility of measuring environment data via sensors (i.e., temperature, volume, position, etc.) IoT devices are suitable for collecting data (Yunru Zhang et al., 2018). One use case of smart contracts in combination with IoT is to share the collected data from smart devices with interested parties via the Internet (e.g., for statistical analysis). Since IoT devices usually have limited computing and storage capacity, the data is usually not stored directly on the devices but in the cloud (Yunru Zhang et al., 2018). Consequently, data exchange is controlled via the cloud, and IoT devices send their data to the cloud. Smart contracts can now act as a contract to access the data stored in the cloud. To do this, a smart contract is first created on the blockchain. In this contract, it is agreed that this smart contract regulates access to the data in the cloud, and every user in this contract is allowed to access the cloud data. If a user now wants to access cloud data via a cloud application, the cloud application first checks whether the user is also in the smart contract. The cloud application releases the data collected using IoT devices if this is the case. In the example described here, the smart contract controls access to the cloud data.

3.1.12 Discussion

This section presented the basic definitions necessary for this dissertation. As mentioned in detail, this dissertation aims to configure cloud applications using blockchain technology. The trust shall be shifted from the cloud provider to the blockchain. In doing so, the risk of cloud adoption should be mitigated based on the three identified compliance-related adoption risks.

First, the goal of the dissertation thus includes the topic of cloud computing. The necessary terms and ideas were presented in the first part of this chapter. Furthermore, this dissertation aims to shift trust to the blockchain and thus mitigate the adoption risk of the three described cloud risks. The necessary definition of trust and risk, as well as their interaction, were also presented in this section. The final goal of this dissertation is to shift trust to the blockchain. Therefore, the mathematical models and proofs for the structure and security, as well as the function of the blockchain and the technology of the smart contracts closely connected with the blockchain, were likewise presented. The rest of this dissertation will be built on the concepts introduced in this section.

3.2 ENVIRONMENT AND SCOPE OF THE DISSERTATION

“The environment defines the problem space in which reside the phenomena of interest” (Hevner et al., 2004, p. 79). According to the DSR methodology, distinguishing its problem space is the first step in designing an artifact for an identified problem. Therefore, according to the DSR approach, it must first be clarified in which environment the related problem occurs, viz., the dissertation's scope. This leads directly to the first research question, RQ1 (see 1.4.2). Hypothesis H1 is that “the problem described in this dissertation mainly occurs in business environments and affects the adoption of cloud applications on public clouds”. The prediction is that experts in cloud computing, information security, and enterprise management will confirm that the described problem exists and arises primarily in the business environment when adopting cloud applications from public cloud services. In addition, the compliance-driven configuration of cloud applications plays a minor role in the private adoption of cloud applications. Hence, experts will confirm that risks due to cloud adoption mainly arise in the business sector.

An observation that builds on RQ1 is that blockchain technology has gained significant importance in cloud computing, trust management, risk management, and compliance in recent years (Anjum et al., 2017; Ladia, 2021). This observation leads to RQ2 (see 1.4.2). Hypothesis H2 is that “experts consider blockchain a promising technology for tamperproof tracking compliance requirements and recommend using the blockchain to overcome the compliance risks described in this dissertation”. When asked about the problem of this dissertation, it is predicted that experts will suggest the blockchain as a possible technology to solve the problem described in this thesis—namely, the problem of adoption risks arising from compliance-driven cloud application configurations. Therefore, the assumption is that blockchain technology is predestined for the use case at hand and that experts will recognize this. The predictions from RQ1 and RQ2 must now be verified and confirmed using scientific methods. To do this, a focus group discussion was conducted (as described in 2.1.1).

3.2.1 Conducting the Focus Group Discussion

Seven experts participated in the focus group discussion, and the author of this dissertation moderated the focus group. Moderators of a focus group discussion take a passive role. They ensure that the participants do not digress too much and that the rules of conduct are observed (Krueger, 2014). In combination with the publication of the transcript from the focus group discussion, the author's participation in the focus group discussion is not a limitation of the work.

The focus group discussion was conducted in 2021. Due to the ongoing Covid-19 pandemic, strict contact rules were in place. Hence, the focus group discussion was conducted online using Microsoft Teams software and an engagement tool provided by “Mentimeter,” an interactive presentation software (Vallely & Gibson, 2018). Conducting the focus group online allowed all participants to participate in the discussions at home in a familiar environment. According to Krueger (2014), the well-being of the participants is a central aspect of a successful group discussion. Hence, the online conduction of the focus group discussion is not a limitation of this dissertation.

3.2.1.1 Planning

Based on Krueger (2014), the first phase of conducting a focus group discussion is planning the discussion. As part of the planning process, the author first investigated whether a focus group discussion is the right method to answer RQ1 and RQ2. As already described (see 2.1.1), a focus group was indeed found to be the most suitable method for conducting this research. Focus group discussions are ideal for digging into a specific topic and discussing it from multiple points of view, and a view from multiple angles is needed to answer RQ1 and RQ2. The question to be answered through the focus group discussion was tested in the next step. To be more precise, it was determined whether the planned focus group questions could answer RQ1 and RQ2.

The target audience chosen for the focus group results directly from the content of the research questions. Experts in cloud computing, economics, IT security, software development, or IT managers are needed to answer the questions. Whether a person is an expert was determined based on the following criteria:

- Educational background
- Career Path and years of working in at least one of the named research areas: Blockchain, Business Administration, Cloud Computing, Compliance, Risk Management, Software Architecture, Software Engineering, Trust Management
- Publications in at least one of the named research areas
- Certifications in the relevant research field
- Consistency of opinions and knowledge with research findings

In addition to these criteria, it was determined that the chosen experts should not know each other—in order to reduce possible bias—and that the number of participants should be between five and ten. Finally, the planning also included brainstorming on where to recruit the focus group participants and how to analyze and evaluate the focus group session. The applicable participants were selected from the network of the dissertation’s author. Specifically, the business network LinkedIn was searched for experts who have at least one qualification in the mentioned research areas. These were then added to a list and numbered. Using an equally distributed random number generator, seven participants were selected from the numbered experts and invited to a focus group discussion. If the persons contacted did not respond within a week, or if the participants canceled, another participant was randomly selected from the list using a random number generator. In the end, seven experts were invited to the focus group discussion in the abovementioned areas.

Additionally, participants were asked to provide anonymous feedback about the session. As a result, a slide providing the opportunity to evaluate the session was added to the focus group discussion. The focus group analysis followed the qualitative content analysis described by Mayring (2000) (see 2.1.5.3). At the time of the focus group discussion, the scope of this dissertation was unclear. However, some relevant literature regarding cloud computing, blockchain, trust, compliance, and risk management exists. To fill the gap of knowledge between existing literature and the content of this dissertation, extra material was needed.

3.2.1.2 Description of the Categorization

A first categorization for the later evaluation of the focus groups following the qualitative content analysis was done deductively, based on the theoretical background knowledge and the research question. The main categories are:

- Compliance and Configuration Environment
- Trust Environment
- Cloud Computing

After the interview phase, an inductive revision of the categorization was planned to optimize the category system (see 2.1.5.3 for a detailed description and examples of the words deductively and inductively).

3.2.1.3 Questions

The focus group discussion was planned for 90 minutes. Due to this time constraint, care was taken in selecting questions. In particular, the author took care to avoid choosing too many questions or questions that were too difficult to answer within the allotted time. Were participants presented with too many questions, they may not have answered all the questions thoughtfully; were they presented with questions that were too difficult, room for misunderstanding and interpretation would have arisen. When creating the questions, care was also taken to ensure that the requirements for the questions set in the planning were achievable. As a result, six focus group questions (FGQs) were developed. The developed questions were then tested on a group of three students to determine whether the questions were understood correctly and logically built on each other. After small adjustments, the following FGQs were deployed:

FGQ1: What do you think of when you hear cloud computing / What do you associate this idea with?

FGQ2: What do you see as the biggest challenges in cloud computing?

FGQ3: What are the trust issues when configuring cloud services?

FGQ4: Is there a specific user group particularly concerned with the issue of trust in cloud applications?

FGQ5: What technology can increase trust in cloud applications?

FGQ6: What criteria could be used to evaluate whether an application can increase trust in cloud applications?

FGQ1 serves as a warm-up question. The idea of FGQ1 is to introduce the focus group discussion topic slowly. Whether participants are experts in their fields can be verified in multiple ways — for example, by their career, education, publications, or archived certificates in the research field. Within this dissertation, a further evaluation element is used. In addition to education, career, publications, and certificates, it is examined to what extent the opinion of the experts corresponds to scientifically supported facts in the research field. The assumption is that the experts' opinions will align with scientific findings. FGQ2 was developed for this type of evaluation. The answers to this question were later used to evaluate the group's competence in the level of cloud computing. The question aims to determine whether the participants see similar challenges in cloud computing as the research has already shown. To what extent do the participants' opinions in the focus group agree with science? To be more precise, do the participants see similar challenges in cloud computing, or is there a bias?

FGQ3 aims to determine to what extent the compliance-driven configuration of cloud applications poses a risk to enterprises. In other words, it asks whether experts see any trust issue in the compliance-driven configuration of cloud applications and whether they see an associated risk to this. The answers to FGQ3 and FGQ4 show whether the prediction to RQ1 is correct and whether H1 holds or needs to be rejected. Similarly, FGQ5 aims to check whether the prediction of H2 is correct and thus provides an answer for RQ2. The experts' answers are then confirmed or rejected in H1 and H2.

Hevner et al. (2004) have already discussed various ways to evaluate a developed artifact. The last of the presented focus group discussion questions —

FGQ6 — aims to obtain an independent assessment of the expert group regarding the evaluation of the artifact. The input of the experts is then used to get a starting point and indication of a suitable evaluation tool for the artifact to be developed.

3.2.1.4 Recruiting

Participants were selected from the author's network according to the criteria defined in the planning of the focus group discussion (see 3.2.1.1). Initial contact, continuing correspondence, and coordination of the date for the focus group discussion took place via email.

The focus group consisted of the following participants:

- Participant #1: a Chief Executive Officer (CEO) from a software company (developing a SaaS cloud application) with more than 15 years of professional experience. Participant #1 also holds a Ph.D. in industrial engineering.
- Participant #2: a Chief Executive Officer (CEO) from a software company (developing a SaaS cloud application) with more than 15 years of professional experience. Participant #2 holds a master's degree in computer science and has more than 15 years of professional experience in computer science and development.
- Participant #3: a Team Lead for collaboration services. Participant #3 has an educational background and completed an apprenticeship in computer science. Participant #3 also has more than 15 years of professional experience in computer science and more than two years of experience in team leading.
- Participant #4: a professional cloud application administrator. Participant #4 has an educational background and completed an apprenticeship in computer science. Participant #4 also has more than 15 years of professional experience in computer science and service administration.
- Participant #5: a senior software tester. Participant #5 has an educational background and completed an apprenticeship in computer science. Participant #5 has more than 15 years of professional experience in

computer science and holds several certificates in software testing and cyber security.

- Participant #6: an IT security specialist working as a researcher in a research institute. Participant #6 holds a master's degree in computer science. Participant #6 has more than one year of professional experience in computer science and cloud services.
- Participant #7: a development and operations (DevOps) engineer. Participant #7 holds a master's degree in mechanical engineering, focusing on software administration. Participant #7 has more than five years of professional experience in computer science and cloud operations.

3.2.1.5 Moderating

The author of this dissertation moderated the focus group. The main moderation tasks were to ensure that all participants were heard, ensure that the discussion stayed professional and on topic, and follow up in case of inaccuracies. I.e., the main task of the moderator was to facilitate a useful group discussion.

3.2.2 Qualitative Content Analysis

The result of the focus group discussion was analyzed using qualitative content analysis based on Mayring (2000; see 2.1.5.3). Qualitative content analysis represents a method of evaluating fixed communication systematically utilizing a set of categories. It is guided by rules and theory and measures itself against quality criteria. The qualitative element consists of the category development and the content-analytical systematization of the assignment of categories to text components (Pohontsch, 2019). As seen in 2.1.5.3, Mayring (2000) described two types of content analysis applicable to this dissertation: deductive and inductive. Both content analyses were used during the analysis of the focus group discussion.

Moreover, for this focus group, a transcript-based analysis was chosen. The transcript of the focus group discussion can be found in Appendix A. The advantage of the transcript-based analysis is that it has a high level of rigor and a low risk of error (Krueger, 2014). Decisions and statements based on the focus group discussions can thus be transparently reviewed and understood. Transcripts provide researchers with an unbiased view of conversations and allow them to review findings critically. Due to their transparency, transcripts are good scientific practice for comprehensible research (Krueger, 2014). The text material was coded using the deductively created categories discussed in 2.1.5.3—Compliance and Configuration Environment, Trust Environment, and Cloud Computing—and MAXQDA Analytics Pro 2021 software (Kuckartz & Rädiker, 2019).

3.2.3 Categorization and Coding of the Focus Group Discussion

An initial category system was deductively created based on the literature review and research question (see 2.1.5.3). No new categories emerged after completing the research phase and reviewing the data material. However, additional subcategories were formed. Including the subcategories inductively, finally, the following categories could be built:

- Cloud Computing
    - Cloud Advantages
    - Cloud Challenges
- Trust Environment
- Compliance and Configuration Environment
- Risk and Trust Management Technologies
    - Enhancing Technologies
    - Blockchain

3.2.4 Meta-Analysis of the Results

Figure 12 and Figure 13, below, provide an initial graphical overview of the course of the focus group discussions. Figure 12 shows the individual topic clusters that emerged during the focus group discussion, based on how often they were mentioned together. In total, three topic clusters emerged. The first topic cluster contains topics related to the categories of *Cloud Computing*, *Cloud Advantages*, and *Compliance and Configuration Environment*. The second cluster contains topics related to *Cloud Challenges*, *Risk and Trust Management Technologies*, *Blockchain,* and

Trust Environment. The third category consists of *Enhancing Technologies*. The clusters were formed based on the frequency and connection of statements from the individual categories. Details on the used clustering algorithm can be found in the MAXQDA manual (Kuckartz & Rädiker, 2019).

The first cluster shows that the benefits of cloud computing were frequently mentioned. However, governance and compliance requirements were frequently discussed when speaking of benefits. It is not surprising that the topic of compliance is strongly connected with cloud computing.

Cluster two shows that *Trust Environment* and *Risk and Trust Management* were frequently mentioned together. *Blockchain* was frequently mentioned in connection with *Risk and Trust management*. The evaluation of the statements showed that security and trust are strongly linked to the challenges in the cloud and technologies for increased security and trust. Therefore, the second cluster is also strongly linked to the third cluster, *Enhancing Technologies*.

Overall, the topic cluster can be explained meaningfully and provide a picture that initially supports the underlying hypotheses to be investigated. An analysis of each cluster can be found in the following section, 3.2.5.

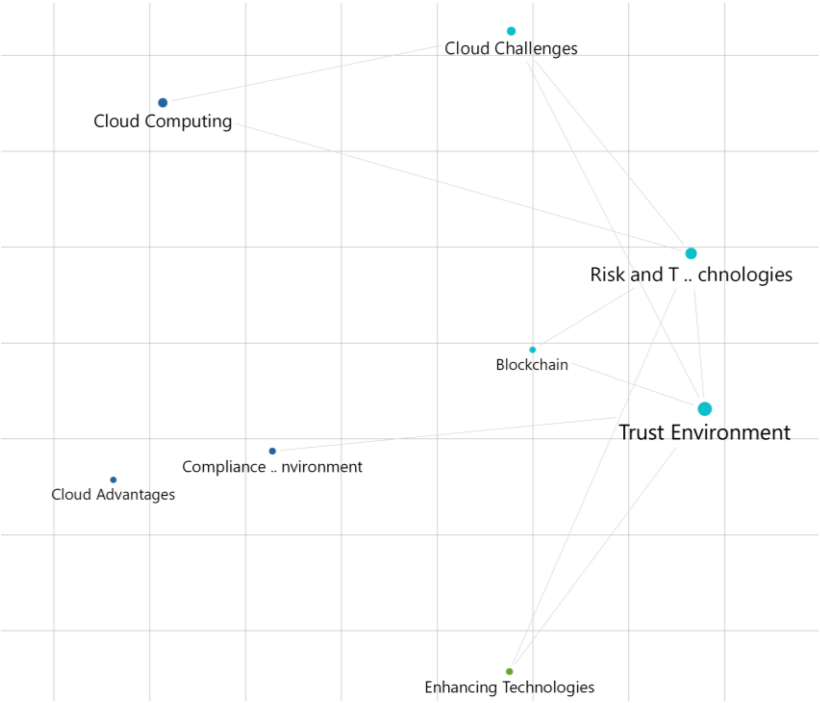


Figure 12: Focus Group Topic Cluster

Figure 13 shows the word cloud of the focus group discussion, i.e., which words, after removing stop words such as “and,” “but,” “like,” etc., were mentioned most frequently. The word cloud provides an overview of the most frequently mentioned words in the group discussion. The size of words in the word cloud represents the frequency with which they were used. So, the largest words were the most commonly spoken. Looking at Figure 14, it can be noted that “trust” was mentioned topmost 106 times, followed by “cloud” mentioned 86 times and “application” 42 times mentioned. Again, it can be concluded that the discussion topics were adequate to investigate the hypotheses raised.

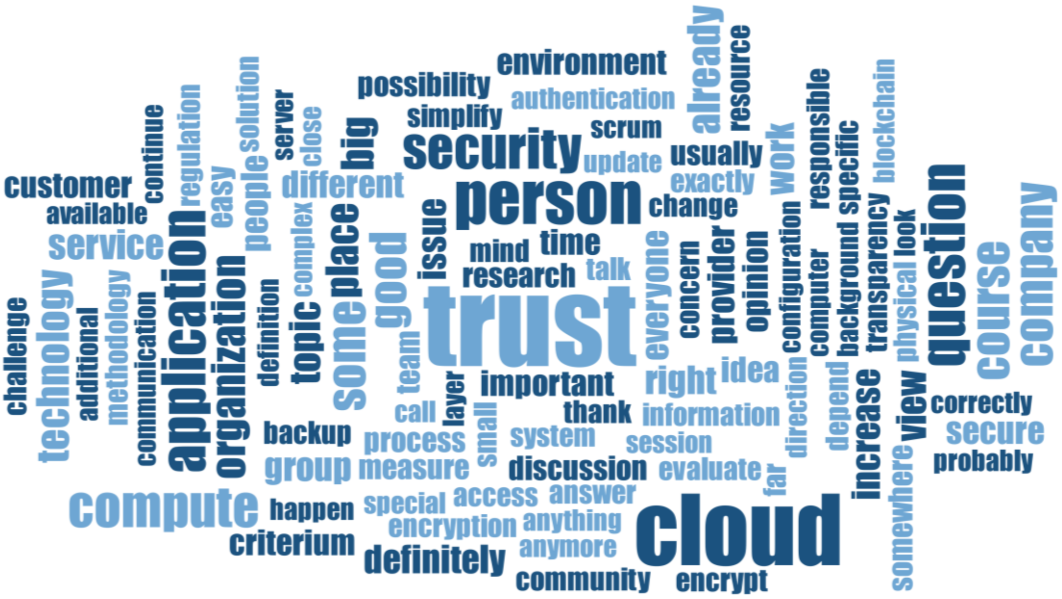


Figure 13: Focus Group Discussion Word Cloud

3.2.5 Analysis of the Results

The main results of the focus group discussion are presented in the following section. For this, the statements from the focus group discussion are referred to, presented, and, if necessary, substantiated by literature. The results are ordered by the categories identified in advance (see 3.2.3). All quotes in this section are from focus group participants.

3.2.5.1 Cloud Computing

The focus group showed that cloud computing is an important future technology. Participant #2 stated,

> *Because also in a professional way your upcoming things are going faster and faster. And when we are thinking how fast the environments are growing, it's even better to organize you and your data maybe from time to time in the cloud, just more scalable to, to scale up your own environment and all your IT things in that same situation. Like, growing companies with much more data, with computing things are just more scalable, reliable.*

This statement also supports the report already made more than a decade ago by Armbrust et al. (2009). In 2009 the authors stated that "Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased" (Armbrust et al., 2009, p. 1). This statement shows that cloud computing and this dissertation topic are still important in the business environment. Moreover, the statements show that this dissertations environment includes the business sector.

Participant #7 added, "a lot of stuff is right now going into the cloud, everyone is going to cloud, it's a lot of stuff [that] is outsourced to clouds. So, from [the] operation side, we are getting more and more dependent on cloud providers." Participant #7 indicated that cloud computing is like outsourcing a service, which might create additional trust and risk issues for companies. Similar findings have been presented by (Bomhard & Daum, 2021). Overall, it can be shown that the focus group strongly agrees with existing literature when it comes to statements about cloud computing and the fact that this dissertation is at least relevant for the business sector.

3.2.5.2 Cloud Computing Advantages

Overall, the participants saw cloud computing as a forward-looking technology with many advantages. Participant #2 stated:

> *Because sometimes, especially for [a] small company the physical access is, so physical security to secure your server rooms, things like that is, is a much more effort if you have to do it for yourself. Or if you let a big cloud provider, like [Organization] or some companies like this do it, because they can, yeah, of course provide this in a great manner.*

Participant #1 added here the possibility of accessing data at any place and any device as an advantage of cloud computing:

> *if I need a quick access to my data from my mobile phone I can do it. Or if I want to modify or update some data more professional, I can do it with my computer. So, cloud computing is a system to store data, which makes it available whenever and wherever I can.*

As these quotes show, focus group participants felt that cloud computing has several advantages over traditional data storage methods. These findings align with current literature (Bello et al., 2021; Pearson & Benameur, 2010). Furthermore, these statements indicate that this dissertation's environment might also be in the private sector, as cloud applications are accepted for private use. However, this statement does not point out whether compliance-driven configurations are as important in the private sector as already shown for the business sector (see 1.3).

3.2.5.3 *Cloud Computing Challenges*

However, it also became clear in the discussion that cloud computing has some weaknesses. Literature can also substantiate these (J. Huang & Nicol, 2013; Lyons, 2021; Moreno-Vozmediano et al., 2013; Takabi et al., 2010). Trust in the cloud and security concerns were seen as the biggest obstacles to cloud adoption. Participant #1 stated here that "security plays a major role, because you have to make sure to secure your data paths and data pipeline to the cloud and back, so that no one else can access your data in the virtual layer, but also, of course, physical security is extremely important." Participant #7 noted, "it's very important that the responsible people who are using the cloud and administrating the cloud have a very, very deep understanding of all functions and functionalities that are used inside the cloud." These findings are also in line with previous research (C. Huang et al., 2021; Michael, 2009; van der Werff et al., 2019; Q. Zhang et al., 2010). The discussion revealed that trust in cloud providers often leads to adoption risks. In particular, it was also found that this applies to the business context. This finding confirms the initial assumption that the environment in which the problem described in this dissertation occurs is particularly the corporate environment. This was also shown by the fact that the examples used by the focus group were always in the corporate context. Overall, this section shows that the challenges of cloud computing and the adoption of cloud services are particularly in the corporate context.

3.2.5.4 *Trust Environment*

The focus group discussions also illuminated mechanisms to increase trust in cloud providers. Participants positively regarded certificates, service level agreements, and existing technical solutions. Based on the focus group discussions, it appears that these measures increased trust in the cloud providers.

However, the focus group discussion also clarified that there is still room for improvement. Participant #4 noted a general risk when adopting cloud services, remarking that "You can only trust the provider that they are doing everything they can, everything they deemed necessary, everything they deem worth the cost to protect your own data. But other than trust them and maybe money is off or any data leaks, you have no control over your own data once it's in the cloud." Furthermore, Participant #4 stated that:

> *Take, for instance, this [Microsoft] Team's meeting we can't encrypt anything there, it's just a recording now somewhere wherever it is recorded. And well, we can switch to Chinese or any other language, but it's not an encryption we have at our hands. So, if you use this for a discussion about company secrets, like most companies using Teams do, they have no control whatsoever about this type of information. [Organization] says we encrypt everything end to end or whatever, it's not open source. We can't prove it that they do, we can only trust them.*

The statements from Participant #4 align with the findings of a variety of studies (Bomhard and Daum 2021; Cayirci and de Oliveira 2018; Michael 2009). Bomhard and Daum (2021, p. 169), for example, found that "in the context of outsourcing and cloud projects, an increasing tension can be observed between the established contractual standards of the IT service providers and the customer-specific IT security requirements. In practice, this tension can only be resolved through customized contract annexes that adequately address all customer requirements." In other words, specific compliance-driven security requirements of customers can only be met by using individually drafted contracts. The idea of this dissertation goes one step further. The idea of this dissertation is that these individual contracts can be signed via blockchain in a transparent, automated and non-repudiable way.

Participant #1 made another observation on trust in the cloud. The participant pointed out that when using cloud applications, it is clear that not only directly provided data is entrusted to the cloud provider. Rather, metadata is also created and made available to the cloud provider. Collecting and analyzing metadata gives rise to further business risk. Participant #4 stated:

> *if you're using a cloud application, you do not just store some data, you store some information, not just information you provide, also other information like metadata. Metadata could also concern other people who are not using the cloud system at all. And if you have… for sure, you can have more sensitive data, if you are a company who is something like, that's looking about innovative solutions, then you should think about if you're really able to use the cloud application.*

3.2.5.5 Compliance and Configuration Environment

Experts noted that adopting a cloud application comes with risks for companies. Cloud users have little to no mechanisms to see all configurations the cloud application provider makes. Participant #2 stated: "[...], also for simple things like data or data loss prevention, you can do this [configure the cloud application], but you have to do in the right way. And you have to know all the more than 1,000 configurations […] to prevent, data loss prevention.” Participant #4 underlined the compliance issue in the business environment with the statement: “I think there is a more fundamental trust problem with cloud computing, because there usually is no way for any customer of a cloud service to independently encrypt or secure otherwise their own data.” In other words, experts see a fundamental trust problem in the cloud because they don't see a way to individually secure their data, as would be necessary for compliance requirements, for example. Overall, it was clearly demonstrated in the Compliance and Configuration Environment category that there is a trust problem with cloud providers. More transparency and non-repudiable traceability of configurations and changes are current requirements of experts for existing cloud applications. Furthermore, during the focus group discussion, it could be shown that cloud customers must trust the cloud provider when configuring the cloud application and that cloud adoption risks primarily occur in the business environment. Participant #3 stated:

> *from my point of view as big as a company is, then more trust should come from the security side or from the security department to the cloud computing. Because the technology side knows about technology and can provide a good solution in the cloud. But the security department should know what's good, what's bad, and that comes to personality. So, some people are known that… in [Place] we have some laws that are set up to where data has to live, and where not. So, I think that should also be a discussion side that trust is not only the technology, that's also a view from the person who cannot, don't know about the technology behind that.*

3.2.5.6 Risk and Trust Management Technologies

Having agreed on the occurrence of — and parties involved in — the configuration of cloud applications, the focus group was asked about technologies that can help overcome existing limitations. The interview yielded three findings in this regard. As already seen in 3.1.4, threats might occur from people, processes, and technologies. Unsurprisingly, the focus group implicitly named those three factors as risk influencing factors.

Participant #2 addressed the simplification of processes, stating: “from my point of view, simplifying things is also a thing to increase trust in applications, know what you are doing”. Technical threats were noted by Participant #1. Participant #1 stated that secure authentication—for example, via multiparty authentication—is an absolute must for today's cloud applications: “What also came to my mind was of course things like multifactor authentication. It's also technology that in the end makes you trust more in the application." Technologies for securing data transmission and data storage were also mentioned. In particular, the encryption of information was discussed.

Finally, the human factor was also addressed as a risk. It was noted, in particular, that the administration of the cloud is a decisive risk factor. Customers must be able to rely on companies entrusting administration to qualified administrators with extensive knowledge. Specifically, Participant #7 noted that: "in my opinion, it's very important that the responsible people who are using the cloud and administrating the cloud have a very, very deep understanding of all functions and functionalities that are used inside the cloud."

3.2.5.7 Enhancing Technologies

After the risks were recorded, the question of how to overcome them followed. In summary, the focus group agreed that current trust mechanisms are insufficient and trust issues are a key barrier to cloud applications' adoption. This also relates to current research (Lynn et al., 2021). Technical solutions such as configurable password policy, single sign-on, or multifactor authentication increase security and trust in the cloud application. Also, provider-independent audits might higher trust in cloud applications. However, when it comes to implementing service level agreements by cloud providers (such as backup policy, geolocation of data storage, the configuration of the firewall, and intrusion detection systems), it becomes essential to trust the service provider. Due to their market position, bilateral agreements with service providers are often possible, either to a limited extent or not. All participants considered a blockchain-based approach for a transparent, notarized, and fully automated configuration to improve the existing practice. Whether blockchain can be used as a technology to solve the problem described in this thesis must be clarified with the help of the knowledge base.

3.2.5.8 Blockchain

In enhancing technologies, the blockchain was also considered a trust-enhancing technology. The focus group noted that blockchain technology could certainly be used to make cloud applications more secure and trustworthy. In particular, developing new trust-enhancing and risk-reducing technologies was addressed as a mandatory need. Participant #6 noted:

> *I would… maybe not necessarily a technology or methodology to increase the trust issue, but also that… I mean, it is definitely important to implement or develop new technologies or methodologies so that the trust issue is increased for the people who are using it.*

One technology specifically mentioned for this was blockchain technology. Participant #1 stated:

> *One technology to create trust, of course, it's in general the blockchain. So, you can include data and you cannot change it afterwards anymore and replace it without having the history. So, technology could be using that in applications, to make sure that, to say that data hasn't been changed or has been changed and by whom.*

With this statement, Participant #1 already implicitly showed that transparency could help overcome trust issues in configuring applications. This statement was additionally confirmed by Participant #2, who remarked: "Maybe on top of this also transparency regarding what you're using and how are you doing it. It's quite close to it, I would say. I mean, there are also from kind of technologies of course, I mean blockchain definitely is a possibility."

3.2.6 Discussion

The goal of this focus group was to identify the environment for the problem identified in this dissertation. To be more precise, the focus group discussion was conducted to obtain an answer to RQ1 and RQ2 (see 1.4.2). For this purpose, a focus group discussion was conducted.

Summarizing and answering RQ1, it can be stated that trust issues, in general, can affect all cloud application users. As soon as data is transferred from one's responsibility to a third-party provider, it must be trusted that the third-party provider will store, process, and protect the transferred data as agreed. Monitoring and auditing the contractually negotiated configurations is difficult. Cloud users must rely on the cloud provider’s configuration specifications with reduced scope for intervention. However, the focus group discussion also showed that compliance requirements, in particular, require that a provider of cloud services must be trusted. In compliance-driven configurations, it can be concluded that compliance-driven risks are primarily attributable to the business sector. The environment considered in this dissertation is, therefore, the business environment.

Besides the environment, the focus group discussion also identified the business need of this dissertation. The participants stated that they are not yet aware of any architecture that can be used to configure cloud applications independently of providers. Although cloud application providers have done a lot to increase trust in their services—for example, enacting reputation-based trust, cloud transparency mechanisms, external certifications, or offering Service Level Agreements [SLAs]—there is still much to be done in configuring cloud applications (J. Huang & Nicol, 2013). In particular, the participants stated that the ability to independently adapt cloud applications to their compliance requirements (e.g., encryption algorithms used) is usually lacking. The desire for the individual configuration of cloud applications in combination with transparency that configurations have been implemented, as discussed, are factors that experts classify as trust-reducing.

Thus RQ1—which asked about the research environment—was answered through the focus group discussion, and the business need of this dissertation was identified. H1 could be confirmed. In addition, an answer to RQ2—which asked how experts rate the trust shift from the cloud application provider to a trusted third party for overcoming compliance-driven adoption risks—could be derived from the focus group discussion. Hence, also H2 could be confirmed. In short, focus group participants rated the trust shift as a promising step to help enterprises assess risks related to cloud application adoption.

The focus group has shown some possible technical approaches to overcome the described issue of this dissertation. The focus group also clearly identified blockchain as the most promising approach. The following subchapter compares the results from the focus group discussion with existing knowledge and research. Comparing the output of this focus group discussion with existing literature supports identifying the exact research gap of this dissertation.

3.3 SYSTEMATIC LITERATURE REVIEW

In the previous subsection (3.2), answers to RQ1 and RQ2 were presented. Thus, the environment of this dissertation has been identified. Consequently, it must be investigated which research approaches fitting to the identified environment already exist and how this dissertation connects to them. To discover this, RQ3 asks:

What relevant blockchain-based software approaches exist to increase trust in cloud applications or reduce adoption risks?

A temporal hypothesis and a content-related hypothesis are made in response to RQ3. The temporal hypothesis, H3a, is that "Research on cloud compliance and the associated topics of trust and risk involving blockchain technology has increased steadily over the last five years." The content hypothesis, H3b, says, "Yet, no approach for the blockchain-based compliance-driven configuration of cloud applications exists." Through the utilization of a systematic literature review, RQ3 should be answered.

As early as the 1970s, Garfield (1977) recognized that the literature review is of scientific importance since it represents an "essential first step and foundation when undertaking a research project" (M. J. Baker, 2000, p. 1). The literature review aims to screen existing sources for research relevant to the research problem. It, therefore, forms the basis for this dissertation's scientific rigor and relevance (Baker 2016). At the same time, reviewing existing literature ensures that this thesis does not investigate or develop anything already available and known. Thus, the literature review helps to avoid unnecessary effort. Subsequently, related works and those necessary for the structure of this dissertation are presented. The literature was collected, reviewed, and evaluated using a systematic literature review (Kitchenham, 2004).

This section discusses each of the conducted literature review steps, following those steps described in section 2.1.2. First, the STIRL described by Buchkremer et al. (2019) was applied. Based on the STIRL outcome, a systematic literature review, according to vom Brocke et al. (2009), was performed (see 2.13). The following paragraphs will describe these steps in detail.

3.3.1 STIRL-based Literature Grouping

For the literature review, this work implemented the STIRL approach (Buchkremer et al., 2019). This approach, introduced in 2.1.2 of this dissertation, allows for an AI-supported systematic literature review. The author qualitatively determined online research databases that were highly maintained; these were selected as data sources (Falagas et al., 2008; Martín-Martín et al., 2018). As shown in Table 4, below, the literature was selected using online literature databases and search strings. Specifically, online databases Web of Science (WoS), Institute of Electrical and Electronics Engineers (IEEE), Sage, Science Direct (ScDi), Multidisciplinary Digital Publishing Institute (MDPI), and Wiley were searched for the literature review of this dissertation.

Table 4: Knowledge Database

	WoS	IEEE	Sage
Search Term	Cloud* AND (Trust* OR Risk* OR Compliance*) AND Blockchain*	Cloud* AND (Trust* OR Risk* OR Compliance*) AND Blockchain*	Cloud* AND (Trust* OR Risk* OR Compliance*) AND Blockchain*
Search Field	Publication Title, Abstract	Publication Title, Abstract	Publication Title, Abstract
Additional Requirements	Articles, Proceedings Papers, Review Articles	Journals, Conferences	Research Article, Review Article
Hits	979	366	276

	ScDi	MDPI	Wiley
Search Term	Cloud AND (Trust OR Risk OR Compliance) AND Blockchain	Cloud* AND (Trust* OR Risk* OR Compliance*) AND Blockchain	Cloud* AND (Trust* OR Risk* OR Compliance*) AND Blockchain
Search Field	Publication Title, Abstract	Publication Title, Abstract	Publication Title, Abstract
Additional Requirements	Review Articles, Research Articles	Article, Review	Journals
Hits	79	39	24

Table 4 above shows how each database returns and the literature found from each. “Search Term” indicates the term used to trawl the database. “AND” and “OR” are search functions; “AND” indicates that the search must return results with both terms, e.g., both cloud and trust. “OR” indicates an inclusive or, such that results that contain only one of the search terms or both will be returned. “Search field” indicates on which parts of a document the search string was applied. Finally, “Additional Requirements” specifies the type of document which should be found on the named online database. Vom Brocke et al. (2009, p. 8) suggest that a systematic literature review requires “a broad conception of what is known about the topic and potential areas where knowledge may be needed." Ambiguous abbreviations, imprecise terminology, and inconsistent definitions can significantly limit the ability to find relevant work.

Buchkremer et al. (2019) have described the problem of ambiguous abbreviations using the example of the abbreviation "crm." This abbreviation is used for ′′customer relationship management" but may also be used as "certified reference material". Therefore, it is important to avoid abbreviations in the definition of the search string.

Imprecise terminology can also arise from the restriction of search strings. In the context of this dissertation, searching for the term "computing" would certainly not be sufficient. Related topics such as grid computing, cloud computing, and cluster computing would be included and thus distort the search result (Sadashiv & Kumar, 2011).

Finally, inconsistent definitions occur whenever there is no uniform definition for a term in the scientific community. An example of this is the term "smart city." It is not clear from the literature what exactly "smart" means. The term can be understood to indicate, e.g., an "Intelligent," "Digital," "Sustainable," or "Learning" city (Cocchia, 2014). The same inconsistency problem holds for the phrase "cloud computing." Xia et al. (2017) use "cloud service." Giurgiu et al. (2009) use the term "cloud" or "cloud application." Considering the listed challenges, the search string for this dissertation was created as follows.

Since compliance is related to trust, "Trust" and "Compliance" were used as search keywords. Furthermore, as seen in 3.1.5, trust and risk are related. For this reason—and considering the scope of this dissertation (see 3.2)—the keyword "Risk" was also selected. The keywords "Trust," "Compliance," and "Risk" were thereby connected by an OR. The OR connection ensures that relevant literature containing at least one of the named keywords is returned. The other keywords selected were "Cloud" and "Blockchain." The keywords "Cloud" and "Blockchain" were connected by AND, as the author determined that both keywords should be part of the searched literature.

In addition, some online databases allow the use of wild cards. Wild cards are characters that allow searching for zero, one, or more characters. The placement of the wild card character is crucial, whether before, in the middle, or after the word that is searched for possible further characters. For example, while the keyword "Blockchain" would search for articles containing "Blockchain," adding the wildcard * at the end of the keyword "Blockchain*" would also find articles containing the word "Blockchain-based." If the wildcard search option was available, it was used. Hence, the final search string was:

Cloud AND (Trust OR Risk OR Compliance) AND Blockchain

This search string has been extended to include the wild card search whenever possible. Only the papers' titles and abstracts were searched to ensure that only papers focused on the selected keywords were identified. The focus of the search was on identifying high-quality scientific literature. Therefore, only peer-reviewed articles were searched, as is generally recommended in research (Rowley & Slack, 2004). In total, 1,763 peer-reviewed articles were found. After removing duplicates, 1,102 papers remained as a *literature corpus*. To implement the STIRL approach, the Natural Language Toolkit (nltk) developed in Python was used (Loper & Bird, 2002).

First, the snowball algorithm was applied for stemming (Porter 2001). As explained in 2.1.3, stemming involves tracing remaining words in the literature corpus to their respective common root forms. Next, using the nltk, the stop words were removed from the literature corpus, in addition to the standard stop words (like "a", "an", "the", "of", "in") which were provided by nltk, the following list of stop words was removed. (Note that the stop words were given in the stem form since stemming is applied before removing the stop words. This reduces the number of stop words that need to be provided since now only the root form of the word to be removed needs to be provided.):

> [achiev, analysis, application, approach, author, base, bases, basic, basis, block, build, chain, challenge, collaborate, communicate, compute, consensus, custom, decentralize, design, develop, digital, distributed, edge, effect, emerge, en, enable, encrypt, enhance, environment, execute, exist, framework, futur, however, implement, integer, integr, key, latency, many, method, model, multi, network, node, offer, optimize, outsource, owner, paper, perform, platform, present, privat, problem, process, proof, propos, propose, protect, protocol, provid, provide, recent, record, reliabl, research, resource, result, review, scheme, server, servic, service,

serving, sevice, show, simulate, solution, study, survey, system, task, technology, time, transaction, use, user, work]

The processed literature corpus was then analyzed using LDA. LDA groups data based on the probability that each data point matches the characteristic of a specific value representing different data groups (see 2.1.3). More specifically, LDA is used to form random word combinations from a literature corpus. The LDA procedure then tests how high the probability is that individual works from a literature corpus match the random word groups. The number of word groups and the corresponding word combinations are then used to assign the works stored in a literature corpus to a group based on the probability of its membership.

Nine trending topics (shown in Figure 14, below) related to the search strings were identified. LDA is not a strict clustering algorithm; thus, the same words might be used in multiple topics (Blei et al., 2002). The statistical word distribution of each identified topic is shown in Figure 15. The normal distribution shown in Figure 16 for each word group indicates that the length of documents via which the topics were created is nearly normally distributed. Because the number of words in the papers that led to identifying the topics are approximately normally distributed, the author accepted the LDA-created topics. If this were not the case, the topic could be distorted. Suppose there is a literature corpus with three articles: two articles of length ten words, one article of length 10,000 words. It is statistically extremely likely that the topic of this group of papers will be generated based on the 10,000 words of the third article. The two papers of length ten would be statistically underrepresented in the generated topic. The nine identified trending topic groups were named as follows:

- Topic 0: Smart Contract
- Topic 1: Cloud Computing
- Topic 2: Internet of Things (IoT)
- Topic 3: Information and Risk Management
- Topic 4: Healthcare
- Topic 5: Blockchain Architecture
- Topic 6: Industry 4.0
- Topic 7: Legal and Trust
- Topic 8: Authentication and Security

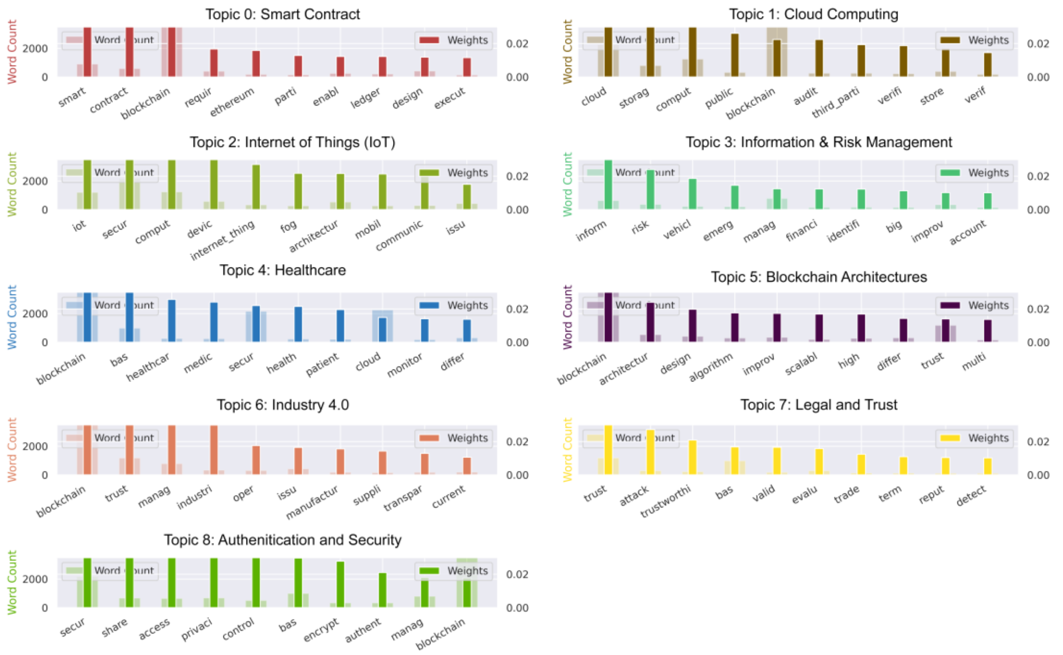


Figure 14: Identified Word Groupings Utilizing LDA

The statistical word distribution of each identified topic is shown in Figure 15, below. The number of identified words in each trending topic is nearly normally distributed. Hence, the created groups were accepted for this dissertation. Once the trends and their interrelationships were identified, this work was placed in the context of the trends. Based on the content and aim of this thesis, this thesis can be mapped to Topic 0, Topic 1, Topic 7, and Topic 8.

Topic 0 includes work that deals with the topic of smart contracts. Since smart contracts conclude blockchain agreements, topics from this category are related to this work. Topic 1 contains work from the area of cloud computing. Since this work aims to configure cloud applications using blockchain, both Topic 1 and Topic 7 were selected as related to this work. Finally, this work also has a security aspect. The secure configuration of cloud applications and the storage of compliance requirements must be ensured. Therefore, Topic 8 was also selected as related to this work. 492 of the 1,102 identified papers were assigned to the named topics. Those identified papers were later used as the starting point for a systematic literature review described by vom Brocke et al. (2009; see 2.1.3). According to vom Brocke et al. (2009), the literature review's scope must first be defined for conducting the literature search. This scope resulted from the findings of RQ1 and is discussed in the following section.

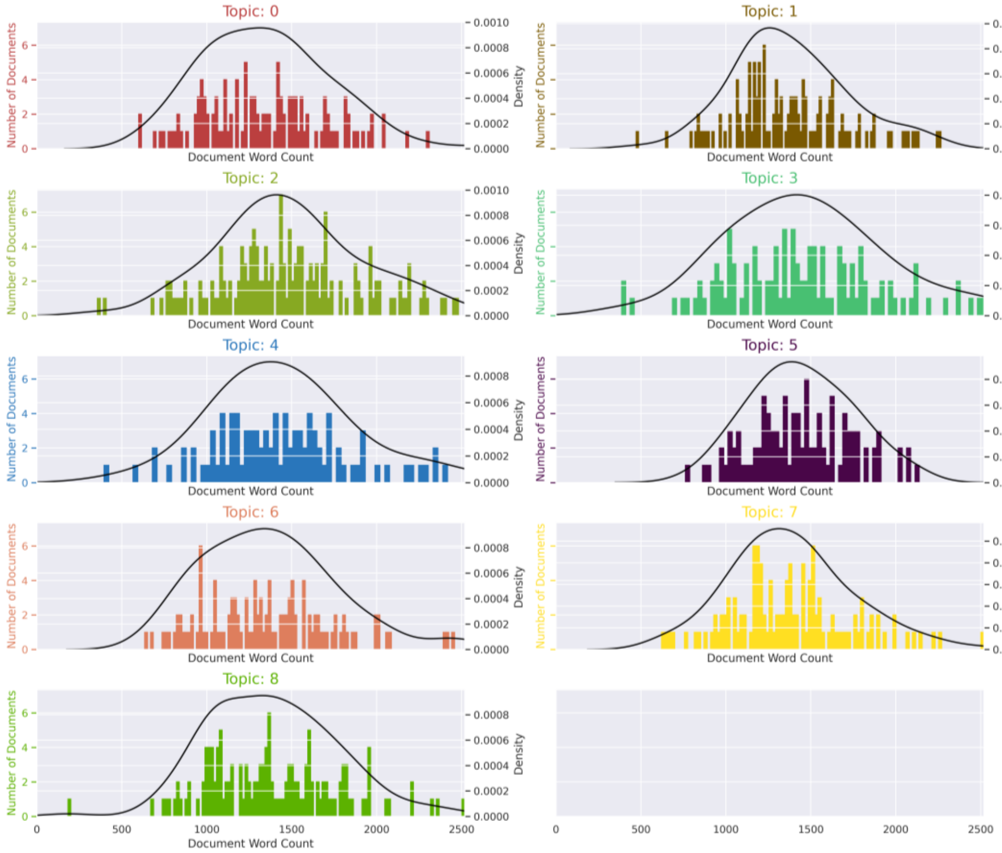


Figure 15: Word Counts of the Identified Topics

3.3.2 Definition of Review Scope

As described in 2.1.3, this dissertation follows the systematic literature search proposed by vom Brocke et al. (2009). This research includes the utilization of Cooper's taxonomy (1988). Table 5, below, illustrates the taxonomy used and the categories selected for the performed literature review. The six categories of Cooper's taxonomy (1988) introduced in 2.1.3 are *focus*, *goal*, *organization*, *perspective*, *audience*, and *coverage*.

The *focus* of the literature review could be on research outcomes, methods, theories, or applications. This literature review focuses on all journal articles, including theories or applications. The *goal* of this research is divided into integration and central issues. Hence, the literature review should discover the gap between existing approaches, integrate them into a new approach, and identify central issues. For example, it must ask which approaches have been studied in the past and what has previously hindered these topics. A concept matrix was used for grouping the review; thus, the *organization* is conceptual. Thereby, the review will be presented from a neutral *perspective*. This systematic literature review's *audience* is specialized scholars and computer science specialists. Finally, the review has representative *coverage*.

Table 5: Taxonomy of the Literature Review. (Adapted from vom Brocke et al., 2009)

Characteristic	Categories			
focus	research outcomes	research methods	theories	applications
goal	integration	criticism	central issues	
organization	historical	conceptual	methodological	
perspective	neutral representation		espousal of position	
audience	specialized scholars	general scholars	Practitioners/ politicians	general public
coverage	exhaustive	exhaustive and selective	representative	Central/pivotal

3.3.3 Conceptualization of Topic

Phase II of vom Brocke's (2009) methodology describes choosing the correct search phrase commonly used in the specific research area. Since this dissertation uses the AI-supported STIRL method for identifying the topic conception, this step was skipped. Instead of using vom Brocke's (2009) methodology, the search string was defined using the STIRL approach (see 3.3.1).

3.3.4 Literature Search

Vom Brocke et al. (2009, p. 10) suggest that the third phase "involves database, keyword, backward, and forward search, as well as an ongoing evaluation of sources." Figure 16, below, indicates the general literature search process of this dissertation: (a) first, the literature databases were selected; (b) next, keywords and search criteria were defined; (c) based on the search results, a backward and forward search was applied; (d) finally, the found literature was evaluated.

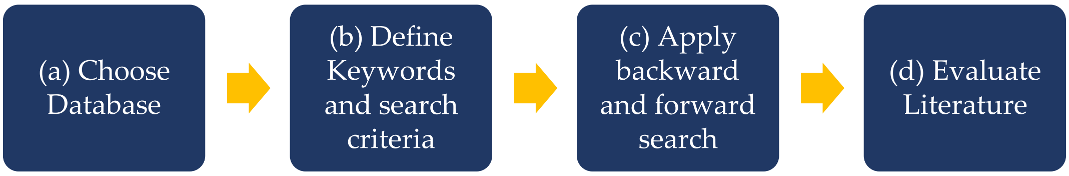

(a) Choose Database
(b) Define Keywords and search criteria
(c) Apply backward and forward search
(d) Evaluate Literature

Figure 16: Overview of the Literature Search Process

Due to the initial literature search from section 3.3.1, steps (a) and (b) are already performed. In total, 492 papers could be identified that fit into one of this dissertation's four selected topics (Topic 0, Topic 1, Topic 7, and Topic 8). The 492 papers were assigned to these groups based on their likelihood of textual content (see 2.1.2). In this process, LDA was used to determine the likelihood of a paper belonging to a topic group.

Manual performance of a forward and backward search of the 492 potential papers of interest was not possible in terms of time. Therefore, a heuristic was used for the literature search. For this purpose, the ten papers with the highest probability of belonging to one of the four selected topic groups were used for a forward and backward search. In other words, the ten papers most likely to represent one of the four topic groups were selected for the forward and backward search. Because there were four topic groups, a forward and backward search was performed with 40 papers altogether. The assumption is that if there are other relevant papers in the 492 potentially interesting papers, these will also be found with the forward-backward search from the top ten papers of the respective topic groups.

After excluding patents, citations, and early access articles, 136 papers were found. The resulting 136 peer-reviewed articles were added to the ad-hoc literature review database. This database has been called the "Literature Review Collection Database" (*LRC-DB*). The database was managed by the software "Mendeley" (Reiswig, 2010). Within this database, each paper refers to an entry and is characterized by the following attributes:

- publication type
- title of the publication
- authors' name(s)
- name of the publication document
- publication year
- abstract
- tags
- keywords
- publisher

This pool of papers was considered sufficient to gain a comprehensive overview of the research topic and thus to answer RQ1. Figure 17 illustrates the search strategy as a business process.

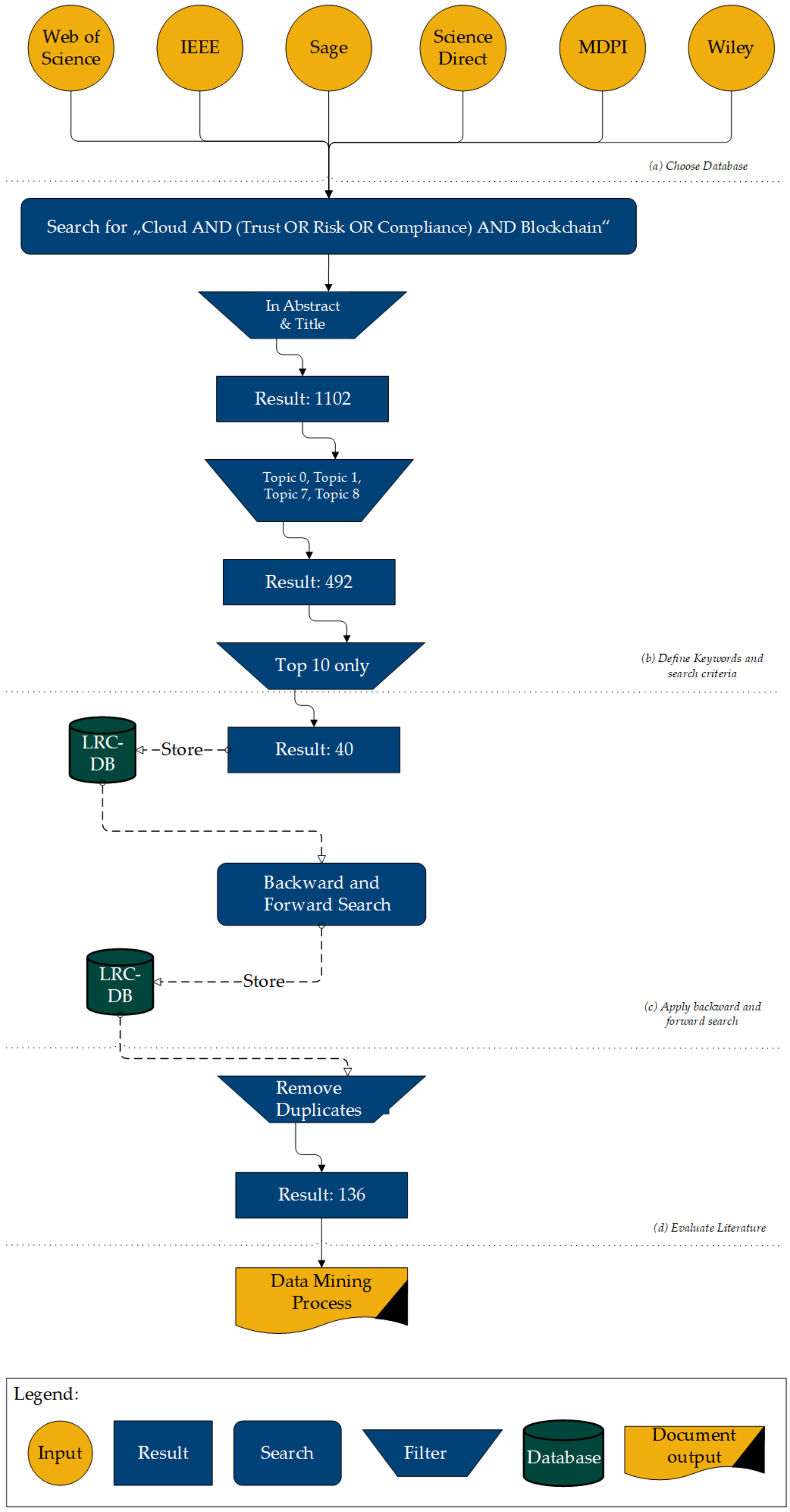


Figure 17: Search Strategy for the Systematic Literature Review

3.3.5 Literature Analysis and Synthesis

"After collecting sufficient literature on a topic it has to be analysed and synthesised" (Vom Brocke et al., 2009, p. 9). This is Phase IV of the systematic literature review process. Within this phase, the articles stored in the LRC-DB are analyzed based on two aspects: *time analysis* and *concept analysis*. *Time analysis* is performed to investigate the development of the research topic from a historical perspective. For this, the 136 papers collected were organized based on the year of publication. Afterward, the number of papers published in one year was counted. This sum was later used to test H3a.

Concept analysis identifies different approaches and cloud application areas in which blockchains are used as a trust-enhancing mechanism. Within this step, a concept matrix categorizes the research-relevant literature into concepts. Using this classification, it is possible to identify the different blockchain applications that can be used to overcome the trust barrier. Thus, the result of the concept matrix is used to test H3b. The test results of H3a and H3b are then used to answer RQ3.

3.3.6 Research Agenda

As mentioned in the introduction to this section (3.3), the literature search supports identifying the current state of the science. This identification is important to avoid work duplication and link the current research to existing approaches. Additionally, the review will identify research gaps, which will lead to a new research agenda. This new research agenda will help deepen the research topic and achieve new results in cloud computing and evaluate them with the articles stored in the LRC-DB.

3.3.7 Systematic Literature Research Result

This section describes the literature review results stored in the LRC-DB. The review results are used to build a current state of the research. Later, the current research state is used to test H3a and H3b and answer RQ3.

3.3.7.1 *Time Analysis*

The time analysis is intended to provide information about the historical course and emergence of cloud applications through which blockchain technology has been used to overcome trust, compliance, or risk challenges. For this purpose, the papers in the LRC-DB were analyzed according to their year of publication. The assumption is that the number of new publications in a year can provide information about the research interest in this topic.

The results from this count are shown in Figure 18, below. The first relevant literature was published in 2016, and in 2017 there were two relevant works. In subsequent years, publications increased significantly: in 2018, there were 13 relevant papers, and through 2020, the number of papers has almost doubled yearly. In 2019 there were 28 relevant papers, and in 2020, 43. In the first half of 2021, there are already 49 relevant papers. Two conclusions can be drawn from this time analysis.

First, increasing trust in cloud computing using blockchain is a relatively new research area. The oldest relevant works that could be identified were from 2016. This can be explained by the fact that blockchain is itself a relatively new technology, as are its technical prerequisites. The idea of a decentralized ledger was introduced by Satoshi Nakamoto in 2008 (2008). In 2013, Vitalik Buterin presented the first yellow paper discussing how smart contracts and decentralized applications could be realized (Buterin, 2014). The "Ethereum" blockchain was subsequently implemented in 2015 (Corbet et al., 2018). Hence, the development of decentralized applications and smart contracts was open to a wide audience from 2015 onwards, and this dissertation's technical prerequisites were created. The publication of a first paper about the topic suitable in this dissertation (i.e., a peer-reviewed academic publication) appearing in 2016 is thus consistent with the literature mapped in the LRC-DB.

Second, the time analysis reveals that the topic of using blockchain to increase trust in cloud computing is gaining in popularity. This is demonstrated by the significant increase in the number of relevant papers over recent years. The yearly increase of relevant research articles confirms H3a. The main reason for this increase might be that cloud computing has become increasingly important in economic and technical matters in recent years (Gourisaria et al., 2020). The desire to remove adoption barriers is a logical consequence of this increased importance.

Despite the increased scholarly interest in this topic and the importance of this area of research, the challenges are many and require many new approaches to reduce adoption risks (Lynn et al., 2021).

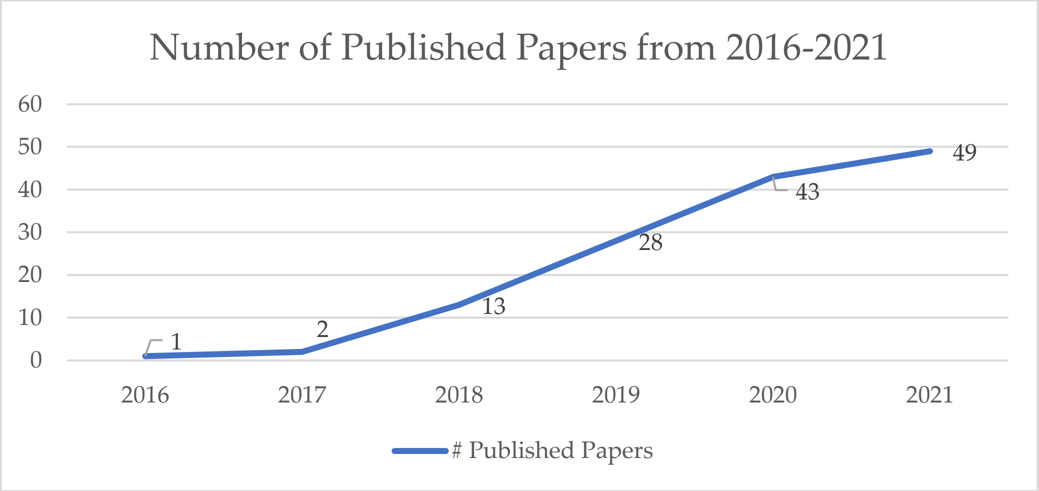


Figure 18: Time Analysis: Number of Relevant Research Papers by Year

3.3.7.2 *Concept Analysis*

The search for relevant literature resulted in 136 relevant peer-reviewed articles. The aim of the concept analysis is now twofold. On the one hand, the analysis aims to identify existing approaches and thus avoid duplicate work within this dissertation. On the other hand, it aims to identify and describe the research gap that will be closed within this dissertation. For the purpose of the concept analysis, the concept matrix originally proposed by Webster and Watson (Webster & Watson, 2002) is used (see 2.1.3). The 136 relevant papers were analyzed based on their abstracts and classified into a concept matrix. The resulting concept matrix is shown in Table 6, which can be found at the end of this subsection. The relevant papers are listed on the left-hand side of the table. Each relevant article is represented as one line of the concept matrix based on the appearance date.

The classification of the relevant work is based on (a) the *type* of work, (b) the *focus* of the work's content, and (c) the *use case* in the article-utilized blockchain. The type of work can be either a *review* work or an *implementation*. An implementation covers an application's actual development, framework presentation, or conceptual architecture proposal. The focus of a paper describes its emphasis. Based on the topics identified using the STIRL analysis (see 3.3.1), a total of ten different focus groups and five blockchain use cases were identified. In order to make the topics obtained from the STIRL approach more tangible and refined, some topics were further divided during the analysis. Specifically, Topic 3, "Information and Risk Management," was refined into "Big Data" and "Vehicular." Topic 6, "Industry 4.0," was refined into "Smart City" and "Mobile Operation."

Note that a paper was only classified into a focus group if the paper had a clear focus in one of these groups. For example, the work was not necessarily classified in the Security focus, even if blockchains use cryptographic procedures. However, if a new security protocol, algorithm, or procedure was developed within the work, the work would be classified in the Security focus.

The *Cloud* focus group represents STIRL Topic 1 and contains work focusing on cloud computing. A focus on cloud computing may contain papers about connecting to a cloud service, providing a cloud authentication mechanism, or proposing an approach for offloading work from or to a cloud service.

IoT reflects STIRL Topic 2 and indicates work with a focus on the Internet of Things. The term IoT is broadly used for the literature review and may include articles on specialized IoT topics like the Industrial Internet of Things (IIoT) or Internet of Mobile Things (IoMT). Expressed differently, section 3.1.11 already briefly introduced the topic of IoT. It was mentioned here that devices are turned into smart devices by installing software and operating systems. Today, the scientific community has established specialization in various smart devices. For example, specialization in smart industrial devices such as manufacturing machines is IIoT. Specialization in mobile devices such as vehicles or drones is called IoMT.

The *Big Data and Vehicular* focus groups are part of STIRL Topic 3 (Information and Risk Management) and contain approaches that have been developed with a focus on big data and processing a large amount of data. The *Vehicular* focus group indicates approaches with a specialization in the automotive industry or autonomous driving. Papers in this group may contain the exchange of location data while driving, the share of traffic information, and approaches specialized for the automotive supply chain.

Healthcare represents STIRL Topic 4 and focuses on medical or pharmaceutical application areas. Such a focus may contain the exchange of medical data or a focus on patient data.

As mentioned earlier, the smart city is not clearly defined (Nam & Pardo, 2011). Rather, a variety of definitions exist (Cocchia, 2014). This dissertation uses the definition of a smart city established by Caragliu et al. (2013). Caragliu et al. (2013) define

> A city to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance. (Caragliu et al. 2011, p. 50)

Thus, *Smart Cities* (a subgroup of STIRL Topic 6, "Industry 4.0") includes papers focusing on intangible cities and their connectivity. The focus group *Mobile Operation* (the second subgroup of Topic 6) contains papers focusing on applications for mobile usage. For example, these include articles with a focus on smartphone applications.

The focus group *Legal and Trust*, representing STIRL Topic 7, indicates work focusing on legal or compliance-specific topics such as audits, SLAs, or contractual agreements.

Finally, STIRL Topic 8 is represented by the focus group *Security*. Works that focus on developing new security protocols, encryption, or authentication mechanisms are included within this group.

Two topics identified by the STIRL approach—Topic 0, "Smart Contract," and Topic 5, "Blockchain Architectures"—were divided into five blockchain use cases to obtain a detailed overview of why they utilized blockchain technology. These use cases were *Sharing*, *Configuration*, *Access Control*, *Cloud Management*, and *Decision Making*.

Sharing describes works using blockchain technology to share information, data, or resources. This group also includes approaches that utilize the blockchain to provide evidence of shared information, data, or resources. The blockchain use case *Configuration* describes applications used to configure applications, for example, to control or configure sensors. *Access Control* describes applications that use blockchain technology, e.g., for access, control, monitoring, or securing access to applications or systems. Articles describing approaches to configure cloud applications or the cloud management system are grouped in *Cloud Management*. Finally, *Decision Making* groups articles that use blockchain technology for making decisions or voting. Electronic votes are just one example within this group.

This dissertation is an implementation focused on the cloud, security, and legal groups (Topic 0, Topic 1, Topic 7, and Topic 8). Furthermore, this dissertation aims to use the blockchain for sharing configurations and managing cloud applications.

Table 6: Concept Matrix of Identified Relevant Papers

	Type		Focus										Blockchain use case				
Author	**Review**	**Implementation**	**Cloud**	**Big Data**	**Auth. & Security**	**Healthcare**	**Vehicular**	**IoT**	**Smart City**	**Mobile Operation**	**Trading**	**Legal and Trust**	**Sharing**	**Configuration**	**Access Control**	**Cloud Management**	**Decision Making**
This dissertation		X	X		X							X	X	X			
(Yue et al., 2016)		X	X			X							X		X		
(Xia, Sifah, Asamoah, et al., 2017)		X	X	X		X							X		X		
(Xia, Sifah, Smahi, et al., 2017)		X	X														
(Kim & Jeong, 2018)		X								X					X		
(Yunru Zhang et al., 2018)		X	X					X					X		X		
(Yinghui Zhang, Deng, Liu, et al., 2018)		X	X								X				X		
(B.-K. Zheng et al., 2018)		X	X										X				
(de la Vega et al., 2018)		X	X					X			X		X				
(Yinghui Zhang, Deng, Shu, et al., 2018)		X	X										X				
(Prasad et al., 2018)	X		X														
(Reed et al., 2018)	X		X									X					
(Yu et al., 2018)		X	X					X					X				
(Pustisek et al., 2018)		X	X					X					X		X		
(C. Yang et al., 2018)		X	X												X		
(Reyna et al., 2018)	X							X									

	Type		Focus										Blockchain use case				
Author	**Review**	**Implementation**	**Cloud**	**Big Data**	**Auth. & Security**	**Healthcare**	**Vehicular**	**IoT**	**Smart City**	**Mobile Operation**	**Trading**	**Legal and Trust**	**Sharing**	**Configuration**	**Access Control**	**Cloud Management**	**Decision Making**
(Z. Li et al., 2018)		X	X					X									
(Liu et al., 2019)		X				X											
(Nadeem et al., 2019)		X	X		X		X						X				
(S. Wang, Wang, et al., 2019b)		X	X								X						
(Naz et al., 2019)		X			X								X				
(Pustišek et al., 2019)		X						X									
(J. Xie et al., 2019)	X								X								
(Weber & Prinz, 2019)		X	X					X			X		X				
(Kochovski et al., 2019)		X	X	X				X					X				
(S. Guo et al., 2019)		X					X						X		X		
(Jayasinghe et al., 2019)		X	X					X							X		
(Haiyan Wang & Zhang, 2019)		X			X			X							X		
(D. Zheng et al., 2019)		X			X		X						X				
(Si et al., 2019)		X			X			X					X				
(B. Shen et al., 2019)		X	X			X							X				
(S. Wang, Zhang, et al., 2019)		X			X	X							X				
(R. Li et al., 2019)		X	X		X			X						X			
(Dilawar et al., 2019)		X	X					X					X				
(Viriyasitavat et al., 2019)		X						X							X		
(Memon et al., 2019)		X	X					X							X		
(Q. Zhu et al., 2020)	X							X									
(Deng et al., 2019)		X	X		X										X		
(Hao et al., 2019)		X											X				
(M. Ma et al., 2019)		X	X					X							X		
(S. Wang, Wang, et al., 2019a)		X	X		X								X				
(L. Xie et al., 2019)		X			X		X	X					X				

	Type		Focus										Blockchain use case				
Author	**Review**	**Implementation**	**Cloud**	**Big Data**	**Auth. & Security**	**Healthcare**	**Vehicular**	**IoT**	**Smart City**	**Mobile Operation**	**Trading**	**Legal and Trust**	**Sharing**	**Configuration**	**Access Control**	**Cloud Management**	**Decision Making**
(Feng et al., 2019)	X				X												
(Bernal Bernabe et al., 2019)	X				X							X					
(R. Li et al., 2019)		X						X			X		X				
(Mhaisen et al., 2020)		X						X					X		X		
(Cao et al., 2020)		X				X							X				
(Malamas et al., 2020)		X				X									X		
(R. Xu et al., 2020)		X							X				X				
(Kumari et al., 2020)	X		X						X				X				
(Z. Huang et al., 2020)		X	X					X					X				
(X. Zhu et al., 2020)		X													X		
(Bakogiannis et al., 2020)		X	X										X	X	X		
(Peral et al., 2020)		X				X							X				
(Talamo et al., 2020)		X			X							X		X	X		
(Eltayieb et al., 2020)		X	X										X				
(Cui et al., 2020)		X			X						X		X				
(Shahriar Rahman et al., 2020)		X			X								X				
(Khurshid, 2020)		X				X							X				
(Taghavi et al., 2019)		X	X								X	X	X				
(Song Li et al., 2020)		X										X	X				
(P. Huang et al., 2020)		X	X									X	X				
(S. Guo et al., 2020)		X						X					X				
(Z. Khan et al., 2020)		X							X								X
(Cheng et al., 2020)		X				X							X		X		
(R. Chen et al., 2020)		X							X				X				
(Bera et al., 2020)		X						X							X		
(A. Kumar et al., 2020)		X				X							X				
(Yun Zhang et al., 2020)		X			X							X	X		X		

	Type		Focus										Blockchain use case				
Author	**Review**	**Implementation**	**Cloud**	**Big Data**	**Auth. & Security**	**Healthcare**	**Vehicular**	**IoT**	**Smart City**	**Mobile Operation**	**Trading**	**Legal and Trust**	**Sharing**	**Configuration**	**Access Control**	**Cloud Management**	**Decision Making**
(Dorsala et al., 2020)		X	X								X		X				
(Fan et al., 2020)		X						X				X	X				
(Janjua et al., 2020)		X	X		X			X				X			X		
(Xevgenis et al., 2020)		X									X		X				
(J. Li et al., 2020)		X	X	X								X	X				
(Abou-Nassar et al., 2020)		X				X		X					X				
(Tahir et al., 2020)		X						X									
(Baniata & Kertesz, 2020)	X							X							X		
(P. Zhang & Zhou, 2020)	X				X												
(Zhao et al., 2020)		X			X			X							X		
(Velmovitsky et al., 2020)		X															X
(Pinheiro et al., 2020)		X	X										X				
(Siddiqui et al., 2020)		X	X					X							X		
(X. Yang, Li, et al., 2020)		X	X		X	X							X				
(X. Yang, Chen, et al., 2020)		X	X		X								X		X		
(Wei et al., 2020)		X	X		X								X				
(Lockl et al., 2020)		X						X					X		X		
(Chenthara et al., 2020)		X				X							X				
(Sifah et al., 2020)		X							X			X					X
(Tao et al., 2021)		X			X								X				
(Naresh et al., 2021)		X			X	X							X		X		
(Dwivedi, Roy, et al., 2021)	X		X		X			X									
(Abbas et al., 2021)		X						X	X				X				
(B. Wang et al., 2021)		X	X									X					X
(J. Zhang et al., 2021)		X	X					X							X		
(Y. Guo et al., 2021)		X		X	X								X				

	Type		Focus										Blockchain use case				
Author	**Review**	**Implementation**	**Cloud**	**Big Data**	**Auth. & Security**	**Healthcare**	**Vehicular**	**IoT**	**Smart City**	**Mobile Operation**	**Trading**	**Legal and Trust**	**Sharing**	**Configuration**	**Access Control**	**Cloud Management**	**Decision Making**
(Vivekanandan et al., 2021)		X	X		X										X		
(Rahman et al., 2021)		X			X										X		
(Honar Pajooh et al., 2021)		X		X				X					X				
(Subramanian & Thampy, 2021)		X					X						X				
(Hei et al., 2021)		X	X		X								X				
(Panja & Roy, 2021)		X	X												X		X
(H. Zhou et al., 2021)		X	X	X									X				
(T. Li et al., 2021)		X						X				X	X		X		
(Bhattacharya et al., 2021)		X				X							X				
(Randhir Kumar & Tripathi, 2021a)		X			X			X					X				
(Loch et al., 2021)		X										X					X
(Gimenez-Aguilar et al., 2021)	X				X												
(Jeong & Sim, 2021)		X	X					X				X	X				
(Hardin & Kotz, 2021)		X				X							X				
(Lin et al., 2021)		X	X								X		X				
(Yuankai Zhang et al., 2021)		X	X										X				X
(Y. Chen et al., 2021)		X				X							X				
(J.-S. Zhang et al., 2021)		X	X		X								X				
(Ardagna et al., 2021)		X						X					X				
(Elsayeh et al., 2021)		X				X									X		
(C. Huang et al., 2021)		X	X		X							X		X			
(Jan et al., 2021)	X							X									
(W. Shen et al., 2021)		X		X	X								X				

	Type		Focus										Blockchain use case				
Author	Review	Implementation	Cloud	Big Data	Auth. & Security	Healthcare	Vehicular	IoT	Smart City	Mobile Operation	Trading	Legal and Trust	Sharing	Configuration	Access Control	Cloud Management	Decision Making
(Randhir Kumar & Tripathi, 2021b)		X									X		X				
(H. Xu et al., 2021)		X									X		X				
(Uriarte et al., 2021)		X										X		X	X		
(Zuo et al., 2021)		X	X		X								X				
(Siva Kumar et al., 2021)		X	X								X		X				
(Mamta et al., 2021)		X			X	X							X				
(Jiang et al., 2021)		X					X						X				
(X. Ma et al., 2021)		X	X		X								X		X		
(H. Chen et al., 2021)		X									X	X					X
(Manzoor et al., 2021)		X			X			X					X				
(Han Wang et al., 2021)		X											X		X		
(K. Wang et al., 2021)		X						X									X
(C. Yang et al., 2021)		X	X		X										X		
(Alnafrani & Acharya, 2021)		X				X							X				
(Lejun et al., 2020)		X			X	X							X				
(P. Singh et al., 2021)		X	X					X					X				
(C. Li et al., 2021)		X	X										X		X		X
(Dwivedi, Amin, et al., 2021)		X					X						X				
(S. K. Singh et al., 2021)	X		X		X												

Table 6 (above) shows that the relevant literature contains 122 implementations and 14 review papers. The left side of Figure 19, below, indicates the number of relevant articles in each of the ten identified focus groups (including subgroups). When looking at the focus of the work, three major focal points can be seen in the publications. Since the search string explicitly included papers from the cloud area, it is certainly not surprising that this focus group covers a plurality of papers. It may seem much more surprising that this is only 59 of 136 papers, or about 43%. After cloud, the two major focal points are security (41 of 136 papers, or about 30%) and IoT (44 of 136 papers, or about 32%).

This ratio can be explained by the fact that some papers use the term cloud in the abstract, but the papers themselves do not focus on cloud computing. An example of this is Gimenez-Aguilar et al. (2021). In this work, the term "cloud" is used in the abstract, but the review paper focuses on security. Although not discussing cloud in the sense of cloud computing, the Gimenez-Aguilar et al. (2021) work and other relevant works regarding security are, of course, also relevant for this dissertation. In the context of this dissertation, among other things, compliance-driven configurations are to be exchanged securely. For this, novel blockchain-based protocols are necessary. These protocols do not necessarily have to be initially conceived or presented for use in cloud computing. Integrating blockchain into existing technologies may require new protocols and approaches to ensure confidentiality, integrity, and availability. Therefore, it seems understandable that many papers focus on security.

The strong focus in the research field of IoT might be surprising. However, upon closer examination, it soon becomes clear that the combination of blockchain and IoT has great potential. IoT devices, for example, are often used along the entire supply chain of a product. An example of this is the production of coffee. IoT devices can be used on a coffee plantation to monitor temperature and humidity. Then, IoT devices can be used to monitor roasting and transportation. Finally, IoT devices can also be used to monitor coffee production, such as the brewing temperature and pressure of the coffee machine. The notarization of data, configuration, or access to systems are just some of the challenges that can be overcome in the field of IoT using blockchain technology.

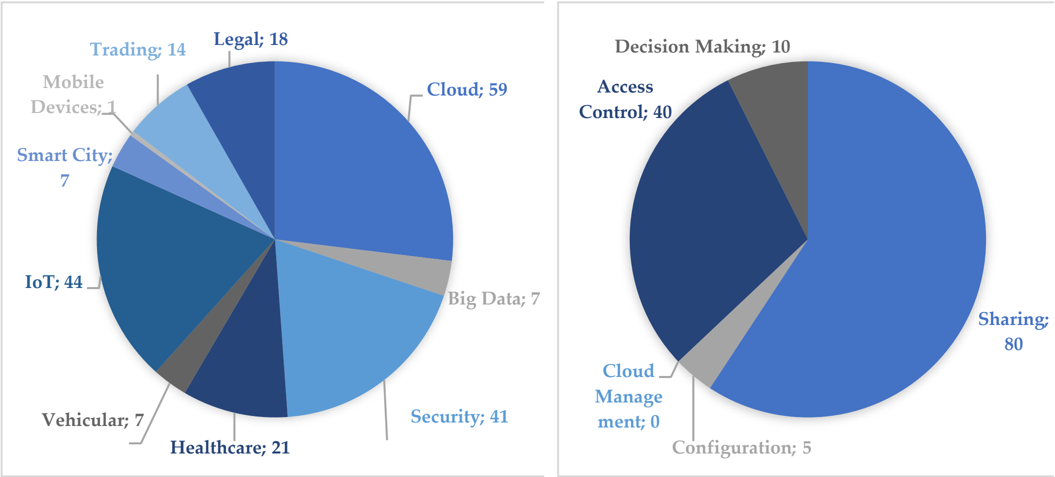


Figure 19: Representation of Focus Groups (left), Use Cases for Which the Blockchain was Used by Number of Relevant Papers in Each Category (right)

When looking at the use cases for which the blockchain was used in the relevant work (right part of Figure 19, above), it becomes clear that sharing data or other information makes up the main part of the work for which blockchain has been used. With 80 of the 136 papers (or about 59%), sharing is by far the most frequent use case. With 40 papers (about 30%), access control and authentication are the second most common use case. This ranking is followed by decision-making with ten tasks (about 7%) and the configuration of applications with five tasks (about 4%). Not a single work could be identified using the blockchain to configure the cloud or a cloud application. Thus, a clear research gap is revealed here.

3.3.8 Discussion

This section aimed to identify what relevant blockchain-based software approaches exist to increase trust in cloud applications or reduce adoption risks. A systematic literature review was used to identify 136 relevant approaches and transfer them into a concept matrix—the concept matrix allowed for a precise classification of the relevant approaches. At the same time, the systematic literature review enabled the classification of this dissertation within the existing research framework.

The systematic literature review has shown some research in blockchain-based risk management in recent years. Nevertheless, it has also shown that there has been very little research regarding applying blockchain-based software approaches to the compliance-driven configuration of cloud applications. Thus, by utilizing the concept matrix, H3b could be confirmed. Furthermore, the concept matrix revealed a significant research gap. Using the literature review method that Buchkremer et al. (2019) proposed, H3a and H3b could be confirmed. Furthermore, the analyzed literature allowed answering RQ3. The next steps are to show how the existing knowledge can be used to answer the main research question of this dissertation.

3.4 RELATED WORK

RQ3 has laid the foundation for RQ4. With the relevant work identified in 3.3, it is now possible to determine how this work ties into existing approaches. Thus, this section provides an answer to the question (RQ4):

> *To what extent can this dissertation connect to existing blockchain-based software approaches for reducing adoption risks in the compliance-driven configuration of cloud applications?*

On the one hand, keeping this question in mind ensures that this dissertation is built on the latest research and knowledge. And, on the other hand, it prevents the author from doing double work by inadvertently replicating existing research. The core of the related work section focuses on five topics:

- The literature overview,
- the importance of blockchain technology in the area of compliance,
- how cloud configurations could be shared via the blockchain,
- how confidentiality through the share of cloud configurations via blockchain could be archived,
- and how a possible solution architecture of this dissertation might look.

Over a decade ago, Bret Michael observed that trust plays an important role in cloud computing (Michael, 2009). Since then, various approaches have been proposed for improving trust or reducing risk in adopting cloud applications. These approaches include contracts (or SLAs), reputation-based mechanisms, standardization, certifications, and transparency mechanisms (J. Huang & Nicol, 2013; Lynn et al., 2021). Satoshi Nakamoto laid the foundation for new technology in 2008 with the publication of "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008). Nakamoto described a new way of preventing double-spending in a P2P network in his paper (see 3.1.9). With this new approach, Nakamoto set the foundation for a new technological solution to overcome trust issues through blockchain technology (Lemieux, 2016). Although Nakamoto initially addressed the financial aspects, it soon became apparent that blockchain technology has widespread applicability due to its primary goal: providing trust and compliance (Anjum et al., 2017; Werbach, 2018).

The blockchain can provide integrity protection, transparency, availability, trustworthiness, and privacy in cloud computing (Miraz & Ali, 2018). Consequently, many studies published in recent years consider blockchain a central element for overcoming trust barriers or reducing risks (Alexopoulos et al., 2017; S. Guo et al., 2019; C. Huang et al., 2021; Haiyan Wang & Zhang, 2019; H. Xu et al., 2021). In the following sections, articles containing approaches later used in this dissertation are briefly presented and thematically classified. The section aims to provide an in-depth overview of the existing approaches and to answer RQ4.

3.4.1 Literature Overview

The healthcare sector was one of the first application areas that began using the blockchain for overcoming trust and compliance issues. One main use case is data sharing. In recent years, several authors have presented a wide variety of applications that handle patient data (Abou-Nassar et al., 2020; Alnafrani & Acharya, 2021; Bhattacharya et al., 2021; Cao et al., 2020; Y. Chen et al., 2021; Chenthara et al., 2020; Hardin & Kotz, 2021; Khurshid, 2020; A. Kumar et al., 2020; Lejun et al., 2020; Mamta et al., 2021; Naresh et al., 2021; Peral et al., 2020; B. Shen et al., 2019; S. Wang, Zhang, et al., 2019; Xia, Sifah, Asamoah, et al., 2017; X. Yang, Li, et al., 2020; Yue et al., 2016). The presented applications provide solutions to multiple areas in the healthcare sector. These services include, e.g., the blockchain-based monitoring of creating, sharing, or deleting patient data and connecting and authenticating blockchain-based applications to cloud-based healthcare systems. Of the many recent works on this topic, the work of Xia et al. (2017) is particularly worth mentioning. This is because Xia et al.'s (2017) work has been used as a basis for many other blockchain-based works and thus is frequently cited in the literature. In their article, Xia et al. (2017) introduced MeDShare, a system that addresses the issue of medical data sharing among medical big data custodians in trustless environments.

Related to MeDShare, Sato et al. (2019) proposed a method to manage system operations using a smart contract for blockchain-based systems (Sato et al., 2019). The smart contract 'OpsSC' manages an operational item's operational rules and configuration parameters in their proposed method. In addition, operational agents execute operations based on the smart contract and record the results and evidence of the execution on-chain. Within their study, the authors described system backups as a one-use case. However, the presented reference architecture of this dissertation focuses on the generic configuration of cloud applications and their associated business processes. Therefore, this can be seen as a further development of the approach presented by Sato et al. (2019). In addition to individual applications exchanging data and increasing trust in applications, there are also dedicated platforms for this. Hyperledger Fabric (HF) is an open-source system used for deploying and operating permitted blockchains and one of the Hyperledger projects hosted by the Linux Foundation (Androulaki et al., 2018). So-called 'System chaincodes' are specialized smart contracts used for managing the configuration values of the blockchain network onto the blockchain and smart contracts. Wang et al. (2019) developed a blockchain-based data integrity scheme for large-scale IoT data. They provided an experimental result on the HF that demonstrates that the proposed verification scheme significantly improves the efficiency of integrity verification for large-scale IoT data, with no need for a trusted third party. Even though HF is a recognized permission blockchain framework, this dissertation focuses on describing an independent architecture; it is conceivable that the architecture developed in this dissertation can also be mapped using HF. It should be noted, however, that the architecture developed in this dissertation is intended to be generic – blockchain-independent.

Furthermore, many recent review articles (also called survey articles) have been published on blockchain-based compliance and trust in cloud computing. Among those publications, one of the first was published by Prasad et al. (2018). The authors identified and analyzed various critical success factors (CSFs) that might facilitate the success of blockchain-based cloud services. Similarly, Reed et al. (2018) focused on the legal aspects of using blockchain as an asset.

In addition to legal aspects, some more specialized reviews in connectivity, blockchain technology, and cloud computing have also been published in recent years. The authors of the review articles (Reyna et al., 2018; Q. Zhu et al., 2020) focused on the challenges in blockchain-based IoT applications and surveyed the most relevant work in this area. These authors analyzed how blockchain could potentially improve the IoT and its connection to cloud applications. Other researchers have also investigated the topic of blockchain and IoT. Focusing on Industrial IoT, Dwivedi et al. (2021) investigated IoT integration with blockchain technology and provided an in-depth study of the blockchain-enabled IoT and IIoT systems. Focusing on integrating IoT devices into Multi-Media Cloud (IoMT) services, Jan et al. (2021) proposed a comprehensive review of the existing literature for IoMT in the context of security and blockchain.

In addition to IoT-based reviews, AI-based approaches were also investigated. Kumari et al. (2020) reviewed existing AI-based approaches and the advantages and challenges of integrating them to cloud systems. Xie et al. (2019) provided a comprehensive literature survey involving blockchain technology and applications applied to smart cities. Literature reviews on compliance and security-related threats, challenges, and opportunities of using blockchains in conjunction with cloud applications were conducted by (Bernal Bernabe et al., 2019; Feng et al., 2019; Gimenez-Aguilar et al., 2021; S. K. Singh et al., 2021; P. Zhang & Zhou, 2020). Finally, an access control-oriented literature review addressing the state-of-the-art Fog Computing-Blockchain integration was conducted by Baniata and Kertesz (2020).

In summary, the papers and surveys presented in this section show that many past applications have already been developed with which trust could be shifted to the blockchain. The papers also show that blockchain is a technical solution that does not require central management, unlike Web PKI. Nevertheless, the survey papers also show that no work has yet been published that allows blockchain to configure compliance-driven cloud applications. Furthermore, the survey papers show no definition of cloud application configurations yet. Thus, existing knowledge and definitions cannot be relied upon to answer RQ5. As described in more detail later (see 4.1), RQ5 has to be elaborated using existing mathematical models during the dissertation.

3.4.2 Importance of Blockchain in Compliance Management

An emerging area since 2020 has been using blockchain to solve cloud-based payment transactions or audit compliance in cloud services. Xevgenis et al. (2020) proposed a blockchain-based solution that allows network providers to trade their processing and networking resources. Also, addressing the sale of free resources, H. Chen et al. (2021) proposed the SmartStore. The SmartStore is an auction mechanism based on blockchain technology that can be used to allocate edge resources. The authors Kumar and Tripathi (2021a) proposed a secure trading framework based on blockchain techniques—including decentralization, immutability, and integrity—to solve the trust issue in centralized provenance-based systems. Focusing on auctions, Xu et al. (2021) presented the blockchain-based trust and fair system and developed a smart contract for auctions and transactions.

S. Li et al. (2020) presented a blockchain-based system for resisting malicious auditors targeting cloud storage. Loch et al. (2021) provided a blockchain protocol for selecting microservice providers and auditing contracts to enable contract establishments in unreliable environments. To address trust issues in current SLA solutions, Uriarte et al. (2021) proposed a novel SLA management framework. Uriarte et al.'s (2021) framework facilitate the specification and enforcement of dynamic SLAs that enable one to describe how and under which conditions the offered service level might change. Providing another approach for overcoming semi-trusted Third Party Auditors, H. Wang et al. (2021) proposed a blockchain-distributed data integrity audit scheme. They were utilizing smart contracts as a trusted authority for evaluating contributions and allocation rewards, C. Li et al. (2021) proposed a blockchain-based crowdsourcing framework named TFCrowd.

In summary, it can be clearly shown that, on the one hand, the number of works dealing with monitoring compliance requirements using blockchain has increased significantly in recent years. This may indicate an increased interest in this area. On the other hand, it can also be shown that there are already the first functioning approaches for monitoring compliance requirements and audit evidence in the blockchain. However, the work presented also shows that there is as yet no application for the compliance-driven configuration of cloud applications using blockchain. The further course of the literature review must show which existing approaches can be taken up to solve the use case described in this dissertation.

3.4.3 Sharing Cloud Configurations

As Figure 19 (left side, in 3.3.7) indicates, cloud applications appeared most frequently in the systematic literature search. Given the search terms selected, this is certainly not surprising. However, it must be noted that in many articles, the cloud was only part of the solution presented. In most cases, the cloud itself was not the focus. Articles in which the cloud was part of the research but in which application fields such as IoT or security are in the foreground are not included in this section. Rather, this section contains only those articles in which supporting and enhancing trust in cloud applications was the primary focus. In particular, access control and the monetization of services and resources were central topics of the published works in this section.

Addressing access control, Xia et al. (2017) presented a data-sharing framework that addresses access control challenges associated with sensitive data stored in the cloud. An approach for paying cloud services and managing access via blockchain was presented by Wang et al. (2019b). Zhang, Deng, Shu, et al. (2018) address the challenge of outsourcing data into the cloud using blockchain-based keyword searches. Weber and Prinz (2019) have presented an architecture for sharing user data, including payment. The presented work exchanged user data between a client application and the blockchain. Even though the presented architecture shares large amounts of user data via external data storage, the architecture still shows how communication between the blockchain and users can be realized. The authors have used Remote Procedure Calls (RPCs) to communicate between users and the blockchain.

RPC is a programming interface for starting procedures on remote computers. RPC is based on common network protocols and is a frequently used technique for implementing client/server architectures (Birrell & Nelson, 1983). The RPC protocol works in a client/server model: first, the client application sends an

RPC message to the server. The RPC receiver application installed on the server receives this RPC request, reads the data it contains via the application, and then forwards it to the respective server application. Subsequently, the server application processes the request and sends a response back to the client. This principle is also used in the architecture of Weber and Prinz (Weber & Prinz, 2019). The blockchain can be seen as a server and the user application as a client, retrieving or storing data, in the case of this dissertation, compliance-driven configurations.

The presented approaches are related to this work, as they manage access to cloud data and the blockchain. As the work presented above shows, confidentiality, i.e., the fact that information can only be read by the parties for whom it is intended, is a central challenge. Transparency is a central element of blockchain technology, as seen in 3.1.10. In other words, data stored in the blockchain can, in principle, be viewed by any person. Remember, this dissertation aims to configure cloud applications via blockchain. For this work, however, the fully transparent storage of compliance-driven cloud configurations in the blockchain might be a problem. More precisely, compliance-driven configurations may contain confidential data such as open firewall ports or backup frequencies. If this information were available to every blockchain user, potential attackers could specifically search for vulnerabilities on open ports or could find a potential weakness in the backup strategy. Therefore, this dissertation must state that although the cloud configuration can be transparently stored on the blockchain, only those parties for whom the cloud configuration is of interest can read it. In particular, these are the provider of the cloud application, the consumer of the cloud application, and the cloud application itself.

At the same time, it was also shown that exchanging data between the user and the blockchain via RPCs is possible. RPCs have proven to be a feasible method to enable communication between blockchain and users in the past and can be adopted for this dissertation's configuration exchange.

3.4.4 Ensuring Confidentiality in Cloud Configurations

Ensuring the confidentiality of data has already been investigated by a number of authors in the context of blockchain technology. Using the Paillier cryptosystem to ensure the confidentiality of shared data, B.-K. Zheng et al. (2018) provided a blockchain-based data-sharing system. Taking the data-sharing approach further, Cui et al. (2020) have presented the “pay as you decrypt” approach, which focuses on the decryption of outsourced data using functional encryption and blockchain. A blockchain-assisted framework that can support trustworthy data sharing services and allow data owners to outsource their sensitive data to distributed systems in encrypted form was proposed by Guo et al. (2021). Introducing five algorithms to handle data access requests, data sharing, blockchain transactions, and detecting and punishing misbehaving entities, Shahriar Rahman et al. (2020) addressed the trust issue of data sharing that relies on a relaxed trust assumption. Naz et al. (2019) implemented a secure data-sharing platform using blockchain and an interplanetary file system. Zuo et al. (2021) proposed a blockchain-based ciphertext-policy attribute-based encryption scheme for the secure sharing of cloud data without relying on trusted third parties. Addressing searchable encryption with multiple keywords, Ma et al. (2021) presented a secure and trusted data-sharing framework based on attribute-based encryption. Siva Kumar et al. (2021) developed sensitivity-oriented blockchain encryption to improve cloud data security. To share data in the multi-cloud, Tao et al. (2021) built a data-parsing protocol using smart contracts with the aim of querying shared cloud data more efficiently.

It remains to be noted that various approaches to confidently store data on the blockchain already exist. The Paillier cryptosystem is additive-homomorphic, whereby unknown plaintexts can be added by operations on encrypted texts (B.-K. Zheng et al., 2018). This has a particular advantage in applying e-voting systems but is too over-designed for the use case at hand. The use case described in the dissertation needs the possibility to store and retrieve cloud configurations in the blockchain in a lightweight way. As presented by Cui et al. (2020) and Naz et al. (2019), the approach of an independent data sharing platform is also conceivable for this dissertation but is too overweight in its implementation. Data can be stored within the blockchain as part of smart contracts. Due to the high gas prices of storing large data, an external data store is used if larger amounts of data need to be stored (usually, more than one megabyte). Based on the discussed proposals, the cloud configuration would not have to be stored directly in the blockchain but on an additional external data store. However, since compliance-driven configurations are textual commands (usually a few hundred bytes), they can be stored in a smart contract, and the implementation or provision of an external data store can be avoided.

This dissertation follows the idea presented by Guo et al. (2021) of providing simple methods for encrypting and decrypting cloud data on the side of the receiver and the sender of configurations, respectively. For this purpose, well-known encryption methods are used. The client-side encrypted text is then stored in the blockchain, as Tao et al. (2021) described. For encryption and decryption, a theoretical distinction can be made between symmetric methods (encryption and decryption keys are the same) and asymmetric methods (encryption and decryption keys are different) (Yassein et al., 2017). In general, asymmetric methods are significantly slower when encrypting and decrypting data (Yassein et al., 2017). Therefore, this dissertation focuses on symmetric encryption and decryption of compliance-driven configurations, while asymmetric methods are used for digitally signing transactions (see 3.1.7). The only question that remains unclear is how a shared symmetric key can be generated between the communication parties. For the lightweight blockchain-based creation of encryption keys, Ruggeri et al. (2020) suggest the use of the Diffie Hellman protocol (see 3.1.8). To be more precise, "The Extended Triple Diffie-Hellman (X3DH) protocol has been used for years as the basis of secure communication establishment among parties (i.e., humans and devices) over the Internet" (Ruggeri et al., 2020, p. 1). In their article, Ruggeri et al. (2020) describe how the blockchain can be used to establish a shared symmetric key between multiple communications parties to encrypt a common message. Creating a common shared key between all communication partners allows this dissertation to encrypt compliance-driven configurations in advance client-side and store them confidentially on the blockchain via smart contract for further processing. This idea will be used throughout the dissertation to achieve the goal of confidential storage and configuration of cloud applications using blockchain.

3.4.5 Architecture Design

The blockchain seems to have many use cases for increasing trust in IoT-supported cloud computing. In particular, data sharing and access control were in the foreground of the identified research. More precisely, Zhang, He, and Choo (

2018) proposed a privacy-preserving and user-controlled data sharing architecture with access control based on the blockchain. Related to this, Pustišek et al. (2019) investigated possible design approaches to decentralized applications based on the Ethereum blockchain for the IoT. The authors proposed and evaluated three application architectures differing in communication, computation, storage, and security requirements focusing on data traffic needed to run the blockchain clients and their applications.

From the architectures presented by Pustišek et al. (2019) and the structure of encrypted configurations discussed in 3.4.4, an architectural idea for this dissertation can be derived. The architecture must be divided into three parts. The central pivot of the architecture is the blockchain, on which a smart contract must exist, via which the cloud application configuration can be retrieved and stored by the cloud application in a non-repudiable manner. Communication with the blockchain can be ensured via RPCs (see 3.4.3). To ensure that the cloud configuration can be read confidentially (only by the cloud application provider, the customer, and the cloud application itself), it must be encrypted on the client side.

Consequently, the architecture must consist of a client-side application that enables the cloud application provider and customer to set cloud configurations and, on the other hand, enables the cloud application to read out these set cloud applications via blockchain (see 3.4.4). In the course of this dissertation, this idea of a trust-shared architecture will be further elaborated and described. It will also be clarified how the protocol described by Ruggeri et al. (2020) can be used to generate a common encryption key via blockchain.

3.4.6 Discussion

Looking at the related work, four main points can be made. First, no architecture has been presented so far that solves the problem described in this dissertation. This dissertation, therefore, deals with a problem that has not yet been solved.

Next, it is also noticed that there is still no unified definition of cloud configurations. Thus, existing knowledge cannot be used to answer RQ5. At the same time, it must also be clear that RQ5 must first be answered before the implementation of software architecture can start. To be more precise, it must be clear what a cloud configuration looks like and how it can be defined before it can be stored and implemented in software.

The Related Work part also shows that this dissertation builds on a current trend. A large number of works could be identified that try to track compliance requirements using blockchain. The focus of these works was especially on the tracking of audit reports.

Last, the previous research could also show a possible architecture for configuring cloud applications. Section 3.4.5 showed that a possible architecture consists of three parts, which must be further described and implemented in this dissertation.

Overall, the related work showed that this thesis could tie in with existing research. The detailed analysis of the identified literature showed how this work could be linked to existing research. RQ4 could thus be answered, taking into account RQ3. The next chapter is about implementing the identified approaches using scientific methods.

4 IMPLEMENTATION

After establishing the environment and knowledge base through a focus group discussion and systematic literature review, the dissertation now moves to discuss the implementation. This chapter is divided into two parts. First, chapter 4.1 uses the knowledge gained from the related work part to describe compliance-driven configurations mathematically. This mathematical description is essential for implementing the configuration of cloud applications in software. The development of an approach for blockchain-based configuration of cloud applications using the configurations defined in chapter 4.1. takes place in section 4.2. Section 4.2 is about implementing the artifact—designing the generic approach for shifting trust for compliance-related configurations from the cloud application providers to the blockchain. For this purpose, RAD, as described in 2.1.4, is combined with the DSR presented by Hevner et al. (2004) and discussed in 2.1 are applied.

4.1 CLOUD APPLICATION CONFIGURATIONS

The answer to RQ3 has shown that cloud applications' compliance-driven configuration currently represents a research gap. As noted in 3.3.7.2 of the 136 papers considered in the systematic literature review, no works using the blockchain to configure cloud applications were identified. Therefore, it is not surprising that in answering RQ4—*To what extent can this dissertation connect to existing blockchain-based software approaches for reducing adoption risks in the compliance-driven configuration of cloud applications?*—it was impossible to draw on existing literature for a formal definition of cloud configurations. However, this mathematical definition is necessary since software development always follows fixed mathematical structures. Up to now, there has only been a textual description of compliance-driven configurations. However, this cannot be transferred to software. The formal representation of configurations using mathematical functions is necessary to transfer to software. This chapter thus aims to develop a formal definition of cloud configurations. The research question that arises from this, RQ5, is:

How can compliance-based cloud application configurations mathematically be described?

The hypothesis, H5, is that "Cloud configurations can be described by defining a mathematical function allowing it to be implemented in software." In simple terms, compliance-driven configuring concerns adapting the software behavior to compliance requirements. During the systematic literature research, the work of Marmsoler could be identified (Marmsoler & Gidey, 2019). While the work does not directly aim to move the trust to the blockchain, it describes a way of defining cloud configurations mathematically. To be more precise, the authors used the interactive systems theory to describe a model for dynamic architectures. In the model Marmsoler and Gidey (2019) described, components (in the case of this dissertation, cloud applications) communicate via ports. In other words, the behavior of applications is determined via a port. Based on the input port, a specific application output is created. This behavior is already very close to the idea of cloud configurations. Suppose a compliance requirement is that a cloud application backup must be made every 12h. An administrator would then – via an interface – configure the cloud application to backup every 12 hours.

Simply put, the cloud administrator will use an interface as input to create a desired cloud application output – a 12-hour backup cycle. The administrator's input will cause the cloud application to "reprogram" itself to backup every 12 hours. Based on the administrator's input, "create a backup every 12h", the cloud application has reprogrammed (or reconfigured) itself to perform a backup every 12h. Or in other words, the administrator's input has led to a new state of the cloud application, which ensures that a backup is created every 12 hours. In summary, the configuration is nothing more than creating a modified output based on an input – a configuration sets a specific output behavior to a cloud application.

Hence, abstracting from the model that ports influence behavior, this dissertation needs to define a function based on which textual inputs can change the output behavior of cloud applications. The theory of defining a specific output behavior based on a textual input is based on the mathematical and logical definitions of interactive systems developed by Broy and Stølen (2001). According to Broy and Stølen (2001),

> A system is a technical or a sociological structure consisting of a group of entities combined to form a whole and to work, function, or move interdependently and

> harmoniously. The parts of which a system consists of are called its components or subsystems, and they can be understood as systems on their own. Thus, systems are hierarchically structured into subsystems. (Broy & Stølen, 2001, p. 2)

Thereby, systems are described based on their *input/output behavior*. This specification language is called FOCUS (Broy & Stølen, 2001). FOCUS allows for the formal definition and development of interactive systems – which cloud applications are. The main idea of FOCUS is that the relevant interfaces of interactive systems can be described by characterizing their message interaction history. FOCUS can describe the internal interaction between various system components and any interaction with the system environment. System components can be seen as cloud application functions like the graphical user interface that an administrator sees or specific software functions like setting the backup frequency, the backup location, or the encryption algorithm. Between system components, information is exchanged through communication lines called *channels*. In other words, if an administrator enters a backup frequency of 12h in the user interface, this information is transferred via channels to the software component which manages the backup frequency. Through such channels, information *messages* are exchanged. In the example, messages are the information "set the backup frequency to 12h".

A channel that only transmits messages in one direction is termed a *directed channel*. The communication history of a directed channel is represented through *streams*. A distinction can be asserted between *untimed and timed streams*. Untimed streams represent a sequence of messages in their order of transmission.

Regarding the definition of configurations, timed streams were used in this study. Time streams are sequences of messages, including the associated time ticks. Discrete time periods during which no message is transmitted are represented by √. Timed streams allow the discrete representation of the time a message arrives in the sequence. While with untimed streams only the sequence of the messages can be represented, timed streams can also have their temporal appearance modeled. Thus, with timed streams it can be shown at which time a message appeared and the time interval duration between two messages. Timed streams represent the complete communication history and are always infinite since time never stops.

To apply this to the example above, a stream would be the collection of all backup configurations set on the cloud application by the administrator in chronological order. This process is similar to writing a log file. In untimed streams, the changes made by the administrator are written away in chronological order. In the case of timed streams, a check would be made at fixed intervals to see if a configuration change needs to be written to the log file, i.e., if a configuration change has been made. If this is not the case, then a "blank" would be written on the log file. In this way, the log file can be used to trace exactly which state of the cloud application was set at which point in time. Streams can be used to describe the behavior of compliance-driven configurations formally. To clarify what a configuration is and how a configuration affects cloud applications, the formal basics of a configuration will be defined.

4.1.1 Formal Definition of Streams

This dissertation represents the set of messages with *M* and a timed stream with *s*. If all messages in *s* are contained in *M*, this dissertation calls *s* a timed stream over *M*. This dissertation defines √ as a discrete-time period in which no messages arrive. Note that √ is not a message and thus $\surd \notin M$. Further, this work defines the set of all finite time streams over *M* as $M^{\underline{*}}$, and the set of all infinite streams over *M* as $M^{\underline{\infty}}$. Furthermore,

$$M^{\underline{\omega}} := M^{\underline{*}} \cup M^{\underline{\infty}}$$

is the set of all timed streams. Thus, timed streams can represent mathematical functions mapping natural numbers to messages.

$$M^{\underline{*}} := \bigcup_{n\in\mathbb{N}} \left([1 \ldots n] \to M \cup \{\surd\}\right)$$

$$M^{\underline{\infty}} := \left\{s \in \mathbb{N}_{+} \to M \cup \{\surd\} \,\middle|\, \forall j \in \mathbb{N} : \exists k \in \mathbb{N} : k \geq j \wedge s(k) = \surd\right\}$$

Assume we have given a time stream starting with a message *m*1, followed by *m*2. Consequently, we do not receive any messages √ within the next two time slots, √ ending with two messages *m*1, *m*3. We can characterize this stream by the function:

$$s \in \{1,2,3,4,5,6\} \rightarrow \{\surd, m_1, m_2, m_3\}$$

Where

$$s(1) = m_1, s(2) = m_2, s(3) = \surd, s(4) = \surd, s(5) = m_1, s(6) = m_3$$

Thus, streams map the indices in their domains to their messages.

4.1.2 Formal Definition of Configurations

We define Σ^* as the set of all finite texts that can be generated using the 8-Bit Universal Coded Character Set Transformation Format (UTF-8) alphabet. Furthermore, based on the definitions presented by Ringert and Rumpe (2011), we define $f\colon I^{\underline{\omega}} \rightarrow O^{\underline{\omega}}$ as a stream processing function that maps an input stream to a corresponding output stream. If we now consider all the preceding definitions, we define a software configuration as

$$c\colon \Sigma^* \rightharpoonup (I^{\underline{\omega}} \rightarrow O^{\underline{\omega}})$$

Thus, a configuration c is a partial function that maps a UTF-8 text $e \in \Sigma^*$ to a function that maps an input-timed stream to a corresponding output-timed stream. Note that c is a partial function and maps configurations to an input/output stream if and only if the configuration is valid for the corresponding system. This definition allows changing a cloud application's input/output behavior based on textual commands. A software configuration is thus the user-based definition of an input/output behavior of a software package at a definite point in time.

To render this more concrete, let's assume we want to set the behavior of a firewall. Let's further assume that the behavior of the firewall can be set textually via

$$e = \langle key_1 \colon value_1, \ldots, key_n \colon value_n \rangle, n \in \mathbb{N}.$$

Note that the assumption of a textual configuration is w.l.o.g. (without loss of generality). The function $f: I^{\underline{\omega}} \rightarrow O^{\underline{\omega}}$ consequently describes firewall behavior. For a given input stream, the firewall generates a given output stream. Based on the definition of this dissertation, the function f thus depends on the set text e. Suppose $e = \langle\rangle$, i.e., the empty configuration. The result would be that each input stream from the firewall would reflect the output stream. In other words, the input behavior would be equal to the output behavior, which means that the firewall would accept all incoming and outgoing packets. Accepting all packets, however, reflects a firewall without any configuration.

The configuration $e' = \langle port: 80, status : closed \rangle$ would, in turn, lead to an input stream routed to the output stream only if it does not involve port 80. Streams affecting port 80 would thus be blocked. A configuration $e'' = \langle noconfig \rangle$ would not map to any input/output behavior, since e'' is not a valid setting. The example of e'' in addition explains why c is a partial function. Not every setting can lead to a certain input/output behavior.

4.1.3 Discussion

The research gap identification has shown that the configuration of cloud applications using blockchain is still a fairly new topic. At the same time, using the systematic literature analysis, it could also be shown that there is still no research in the area of this dissertation. Consequently, no clear definition of a cloud application configuration could be presented prior to this research. To gain a uniform basis regarding the meaning of a configuration for the course of this dissertation, the definition of a configuration had to be developed within the scope of this dissertation. The development of this configuration was part of RQ5.

Using the description language FOCUS, cloud configuration could be mathematically defined. It was shown that streams were frequently used in science to describe interactive systems (Ritchie, 1984). Their use in the context of this dissertation is thus only the continuation of an already investigated description basis. In the context of this dissertation, configurations are finally understood as partial functions that influence the input and output behavior of interactive systems (cloud applications).

Understanding configurations as textual descriptions is not a limitation of the thesis. Unix-based operating systems (e.g., Linux, macOS) follow the paradigm "everything is a file" (Both, 2020). Consequently, the configuration can also be seen as a file, one which affects the behavior of systems based on the UTF-8 code. Nevertheless, it can be assumed that, in reality, applications are configured with more than one text file. Therefore, the assumption that an application is configured via only one configuration file can be seen as an abstraction from reality. However, this is no restriction in the philosophy of Unix-based operating systems.

With the definition function *c*, it could be shown that cloud configurations can be represented mathematically. Using a literature review as the research method, H5 could thus be confirmed—and RQ5 answered.

4.2 ARTIFACT DEVELOPMENT

By answering RQ1–RQ5, this dissertation has set the theoretical foundation for developing the artifact. The scope and the required knowledge have been clarified. The next step is to apply the theoretical concepts to develop the software artifact: more precisely, the software architecture for shifting trust from the cloud application providers to the blockchain. Following the DSR methodology developed by Hevner et al. (2004), the artifact is implemented using the design cycle (see 2.1). The design cycle is followed by utilizing the RAD method (see 2.1.4).

4.2.1 Requirements Planning Phase

The goal of RQ6 is to provide a software architecture that allows various cloud applications to be configured via smart contracts. Hence, the architecture development aims to provide a generic (technology-independent) software architecture that utilizes blockchain technology for compliance-driven configuring cloud applications. This goal is also reflected in the artifacts' requirements. Anton (2003, p. 44) instructs us to "[u]nderstand the problem before expressing the requirements." According to Bass et al. (2003, p. 21):

> The software architecture of a program or computing system is the structure or structures of the system, which comprise software components, the externally visible properties of those components, and the relationships among them.

As seen from the discussion of RQ1, one major factor limiting cloud adoption relates to business risks. The developed artifact must overcome this limitation. Therefore, this dissertation aims to develop a software artifact that allows cloud applications to be configured transparently, automated, and non-repudiable using blockchain technology.

Figure 20, below, indicates that the developed artifact should bridge concrete cloud application requirements and specific software implementations. In other words, a software architecture always meets certain application requirements. Based on the input from the focus group discussion and the literature findings, the artifact's requirements have been identified. In concrete terms, it was shown via focus group discussion that the scope of this work lies in the business environment and, in principle, concerns all cloud applications. Therefore, a generic (technology-independent) architecture is necessary to solve the problem identified in this dissertation.

Moreover, the focus group discussion and knowledge base reviled that a software architecture to overcome existing compliance configuration requirements consists of *three communication parties*. More precisely, the focus group discussion participants mentioned that the architecture must involve two *application users* interacting within the to-be-developed architecture and the *cloud application* itself as the third communication party. The cloud application users can further be divided into the cloud application consumer and the cloud application provider.

The cloud *application consumer* (customer) is a user of the cloud application that the cloud application provider provides. In the scope of this dissertation, this might be a customer of a cloud application who wants to configure a cloud application based on compliance requirements (e.g., backup frequency or firewall ports).

The cloud *application provider* (provider) is a customer at a public cloud vendor (see 3.1.1). The cloud vendor might be (but is not limited to) one of the big public cloud vendors like Microsoft Azure, Google Cloud, or Amazon Web Services (Muhammed & Ucuz, 2020). The cloud provider delivers its cloud application via the cloud services of one of the cloud vendors. Hence, the provider provides the third component involved in the architecture. The provided provides the (compliance-driven) configurable *cloud application* hosted on one of the cloud instances of the cloud vendor.

Furthermore, this cloud application will be configured through the blockchain (reflecting the findings from RQ2 and RQ4; see 3.4.5). Note that the cloud application consumer may also act as an application consumer. This is the case if the cloud application provider wants to configure the cloud application.

Besides the three communication parties identified in the focus group discussion, the literature review (see 3.4.5) has shown that the target architecture must consist of *three components* (see 3.4.5).

1. A *smart contract* as a central element for exchanging compliance-driven cloud configurations between cloud application users
2. A *client-side* application that can be utilized to configure cloud applications.
3. A *cloud-side* application that can read configurations from the smart contract and implement them on the cloud application to be configured.

After the three communications parties and three components of the software architecture have been understood, utilizing focus group discussions and related work, it is now part of this chapter to convert them into software architecture and a prototype. Following the RAD method (see 2.1.4), software architecture development starts with identifying the architecture's requirements. The requirements must further be brought to technical documentation before they can be broad to a software architecture design (Martin, 1991). Hence, the documentation of requirements is the first step in moving from the theoretical framework to software architecture (Martin, 1991).

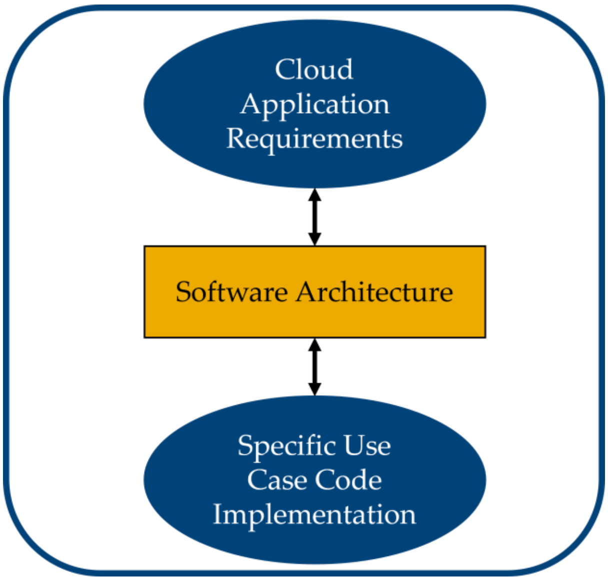

Cloud Application Requirements
Software Architecture
Specific Use Case Code Implementation

Figure 20: Schematic Representation of Software Architecture as a Bridge

In the course of this dissertation, requirements are documented via use case diagrams. Documenting requirements via use case diagrams has two advantages (Aleryani, 2016). First, use cases allow determining what the planned application should finally achieve. Second, use cases represent the basis for the required architecture components. Consequently, the next subchapter (4.2.2) utilizes the documented requirements of this subchapter (4.2.1) for designing the software architecture to overcome the identified issues of this dissertation.

The use case diagram derived from the focus group discussion findings and the related work section is shown in Figure 21 (below). The use case diagram is divided into three communication parties: the application provider, the application consumer, and the cloud application.

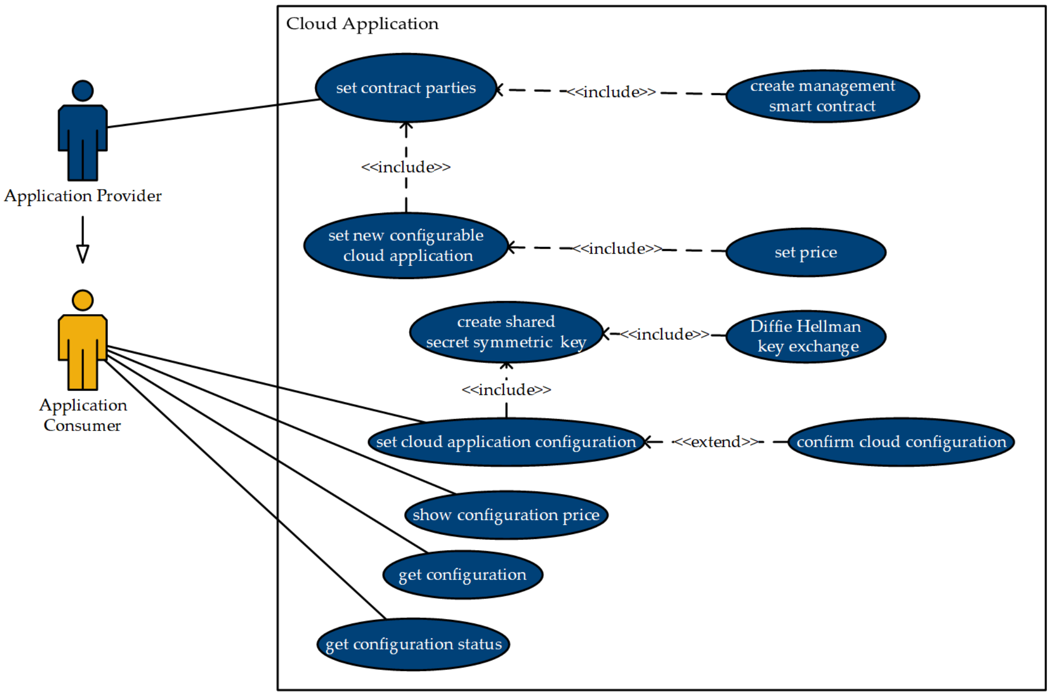


Figure 21: Use Case Diagram of the Cloud Configuration Application

The first use case of the developed architecture is that the provider must be in a position to determine who is allowed to configure what parts of the provided cloud application and to assign prices based on this (see 3.4.3). The provider must therefore be able to define the communication parties contractually (*set contract parties*). This contract (a smart contract; see 3.1.11) must provide three functions:

(1) The contract must contain information about who the participating parties are. To be more precise, the contract must provide the capability of defining who can change the cloud configuration.

(2) The contract must specify which cloud application(s) and settings might be configured (*set new configurable cloud application*). To stay with the example used in this dissertation and the CapitalOne Bank case, it can be assumed that the cloud

application configured is a firewall. An application user might be allowed to configure this firewall's backup location, frequency, and network ports. In addition to setting configurations, contracting parties must also be able to monitor the current status and content of the cloud configuration. Further use cases that can be derived from this are the display of the currently set configuration and its status. Finally, contracting parties must also be transparently and promptly informed about which configuration content has been set by which contracting party and with which status (i.e., successful or failure).

(3) Based on the information about which application(s) may be configured, the price (*set price*) of a configuration change must also be contractually regulated ex-ante. The communication parties must always be able to track the costs of configuring the cloud application transparently. This price tracking is to prevent hidden costs (see 1.3.2). The architecture to be developed must also allow for defining the costs of the automated configuration change in advance via smart contract.

Once the application provider can offer the previously described smart contract (*create management smart contract*), all involved communication parties must be able to access the smart contract securely (see 3.4.4). In this context, "secure" means considering the information security objectives of confidentiality, integrity, and availability, as commonly done by security experts (Tchernykh et al., 2019). Due to the usage of blockchain technology and the related digital signing of the transaction (see 3.1.10), the *availability* and *integrity* of the cloud configuration are provided. As related work has shown (see 3.4.4), if a cloud configuration were stored without encryption, every blockchain user could read it and would be in a position to gain confidential details about the configuration of a cloud application. Hence, the *confidentiality* of the proposed architecture must be ensured (Tchernykh et al., 2019).

The confidentiality goal can be achieved via encrypted storage of the cloud configuration in smart contracts (see 3.4.4). The encrypted storage of cloud configurations includes generating a shared key (*create shared secret symmetric key*) between all communication parties. Hence, the developed architecture must ensure the possibility of creating a shared secret key between the involved three communication parties. Related work has shown that the architecture of this thesis must ensure the key generation via the Diffie Hellman Key Exchange protocol

(*Diffie Helman key exchange*) (see 3.1.8 and 3.4.4). Using the negotiated encryption key, the communication parties must be able to store cloud application configurations on a smart contract (*set cloud application configuration*). The storage of cloud configurations also includes that the communication parties must receive a digitally signed confirmation of the storage and (if applicable) implementation of the cloud configuration (*confirm cloud configuration* and *get configuration status*). These confirmations are part of the audit trail and can be used in case of doubt to prove configuration changes in a tamper-proof and non-repudiable way in a court case.

Besides providing transparency and non-repudiation, the automation of configuration changes is a goal of the architecture to be developed (see 1.4). Process automation can provide reliability. To be more precise, process automation eliminates the need to wait for manual feedback (see 1.3.2 and 3.2.5). The costs and duration of processes are known in advance. The possibility of displaying the costs and, if necessary, the duration of a configuration change (*show configuration price*) are essential requirements for process automation. Transparency and non-repudiation can finally be achieved via the blockchain-based digitally signed storage, retrieval, and confirmation of cloud configurations (*get configuration*). Based on the use cases defined, the necessary architecture can now be derived in the user design phase.

4.2.2 User Design Phase

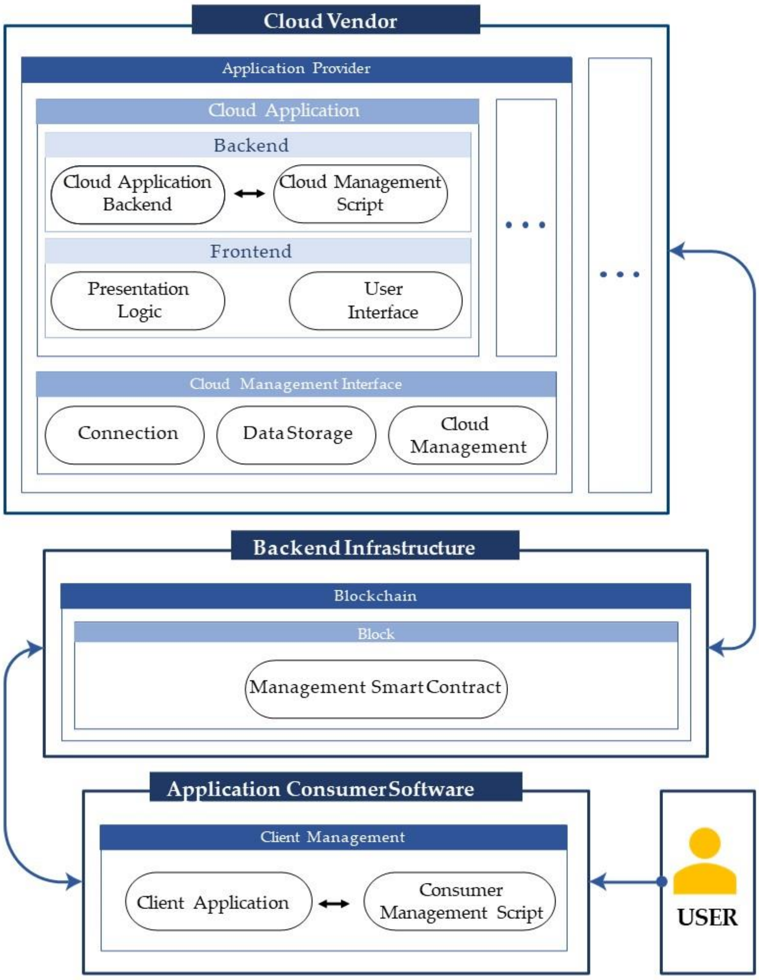


Figure 22: The General Structure of the Proposed Architecture

Derived from the findings of RQ4 and the use cases of the requirements phase (see 4.2.1), the general architectural design of the solution approach can be defined. This architecture can be divided into a frontend and a backend (Bass et al., 2003). On the one hand, the frontend has an interface via which automated, or manual interactions with the proposed solution are possible. On the other hand, it also has a backend. The solution's backend can be described as the "heart" of the architecture, as it is where the main components of the solution are located. Access to the backend is strictly protected from unauthorized input (Richards & Ford, 2020). In the dissertation's architecture, the blockchain is the backend infrastructure, and the smart contract provided on the blockchain is the backend (see 3.4.3). Access to the backend can be automated via the cloud application (cloud-side access) or manual via user input through a client-side application. The frontend of the architecture is thus divided into a cloud- and client-side application. The general architecture design components are shown in Figure 22. It is evident from the related work that the proposed software architecture can be divided into three components (compare with 4.2.1). The three components are:

1. The blockchain-based *backend infrastructure* (hosting the smart contract),
2. the *cloud application* hosted on the provided infrastructure of a *cloud vendor* (cloud-sided application),
3. and the *application consumer software* (client-sided application).

Each of these parts is described in more detail in the subsequent subsections. The communication between the backend and frontend is realized via RPCs, as already shown in the related work section (see 3.4.3). The blockchain is thereby the server and the cloud application resp. the application consumer software the clients.

4.2.2.1 Management Smart Contract (Smart Contract)

The backend infrastructure is based on blockchain technology, as described in Section 3.1.10. A fundamental aspect of the proposed architecture is that each participant interaction is managed via a smart contract (see 3.1.11). This communication is realized by introducing the *Management Smart Contract*. The Management Smart Contract is a smart contract that the cloud application provider creates in order to configure the cloud application via the blockchain. For each cloud application consumer of a specific cloud application, a new Management Smart Contract is deployed on the blockchain. Hence a new backend is created. The blockchain address (the address of the block on which the Management Smart Contract was deployed) of the Management Smart Contract is then individually provided from the cloud application provider to the cloud application consumer (see *set contract parties* and *create management smart contract* use case 4.2.1). Through the creation of a Management Smart Contract, cloud application configurations can be implemented. It is noteworthy that the Management Smart Contract is used for exactly two things. The first is the exchange of compliance-driven configurations, and the second is creating a common shared symmetric key for encrypting the exchange of compliance-driven configurations. (see *set new configurable cloud application* and *set price* use case 4.2.1).

Compliance-driven configurations are stored and exchanged as text files, as already described in 4.1. The text files are then used to store the configuration data. The details of the configuration exchange are explained in 4.2.2.3.

Since configurations may contain confidential information (e.g., the backup policy, firewall configuration, etc.) and smart contracts are transparent for all blockchain users, all configurations must be stored in encrypted form (see 3.4.3). For this to occur, all communicating parties must be able to exchange configurations in an encrypted form.

The presented architecture utilizes the three-party Diffie Hellman key exchange protocol (see 3.1.8 and 3.4.4) to ensure the creation of a shared encryption key for encrypted exchanging cloud-driven configurations (see *create shared secret symmetric key* and *Diffie Helman key exchange* use case 4.2.1). The sequence diagram of the symmetric key generation is shown in Figure 23, below. Figure 23 shows the sequence diagram of how a shared secret key (as discussed in 3.4.4) will be created on the proposed architecture of this dissertation. Based on Figure 23, the provider first creates the initial Management Smart Contract at the blockchain using a *Constructor* function. The provider then provides the public Diffie Hellman key exchange protocol values (*g* and *q),* and the communication parties that are allowed to interact with the Management Smart Contract (public key of (1) themselves / provider, (2) the consumer, and (3) the cloud application) (see 3.1.8 and 3.1.11). Ultimately, using the public Diffie Hellman values, the three communication parties, and RPCs enables the creation of a shared symmetric key *s*.

Specifically, the provider, consumer, and cloud application monitor the Management Smart Contract for changes to the stored public Diffie Hellman values *g* and *q*. As soon as they detect a change of *g* and *q*, they contact the Management Smart Contract via RPCs and request the changed Diffie Hellman values. The Diffie Hellman values are requested via the *getSymmetricParameters* function, which is part of both the cloud and client-side applications. This function returns *g* and *q* to the provider, the consumer, and the cloud application. The communication parties now calculate the public keys *A*, *B*, and *C* (see 3.1.8) and store them via the *setFirstSymmetricKey* function back to the Management Smart Contract. Specifically, the provider stores the public key *A*, the consumer stores the public key *B*, and the cloud application stores the public key *C*.

At the same time, the three communication parties monitor the Management Smart Contract for changes to stored public keys in addition to changes to the public Diffie Hellman values. In other words, the cloud and client-side application also check whether the public keys *A*, *B*, and *C* – stored on the Management Smart Contract – have changed. Specifically, the provider checks if the public key *C* on the Management Smart Contract changes, the consumer checks if *A* changes and the cloud application checks if *B* changes. If this is the case, they also download them via RPCs and the *getFirstSymmetricKey* function. As a result, the provider now has access to *A* and *C*, the consumer to *B* and *A*, and the cloud application to *C* and *B*. Using the public keys, *A* and *C*, the provider can now generate the public key *AC* and store it on the Management Smart Contract via RPCs and the *setSecondSymmetricKey* function. In parallel, the consumer stores *AB* and the cloud application *CA*.

The provider now uses the *getSecondSymmetricKey* function to monitor not only the Diffie Hellman public values *g* and *q* and the public key *C* but also whether the public key *BC* on the Management Smart Contract has changed. In parallel, the consumer does this with the public key *CA* and the cloud application with the public key *AB*. If they detect a change in this key, they retrieve it from the Management Smart Contract via the *getSecondSymmetricKey* function. In the end, the provider has access to *BC*, the consumer to *CA*, and the cloud application to *AB*. As shown in 3.1.8, the communication participants can now generate common symmetric key *s* with these public keys.

Two facts remain to be taken away from this subsection. First, the protocol described in Figure 23 aims to generate a symmetric key *s* via a three-party Diffie Hellman procedure on the part of the provider, consumer, and cloud application (see 3.1.8). After executing the Figure 23 described protocol, all communication parties have access to a common symmetric key *s*. Moreover, following Figure 23, the Management Smart Contract must be provided via the blockchain. Provider and consumer execute the protocol described in Figure 23 via a client-sided application (see 4.2.2.3). The cloud application executes the described protocol via a cloud-sided application (see 4.2.2.2). The two frontend applications described are explained in detail in the following subsections.

Second, since the in 3.1.8 described protocol is vulnerable to MITM attacks, the created Management Smart Contract must ensure the authenticated provisioning of the public Diffie Hellman keys (Khader & Lai, 2015). Since all public Diffie Hellman values are stored and retrieved from the Management Smart Contract using transactions, each communication step is digitally signed (see 3.1.7) and documented on the blockchain. MITM attacks are, therefore, not possible.

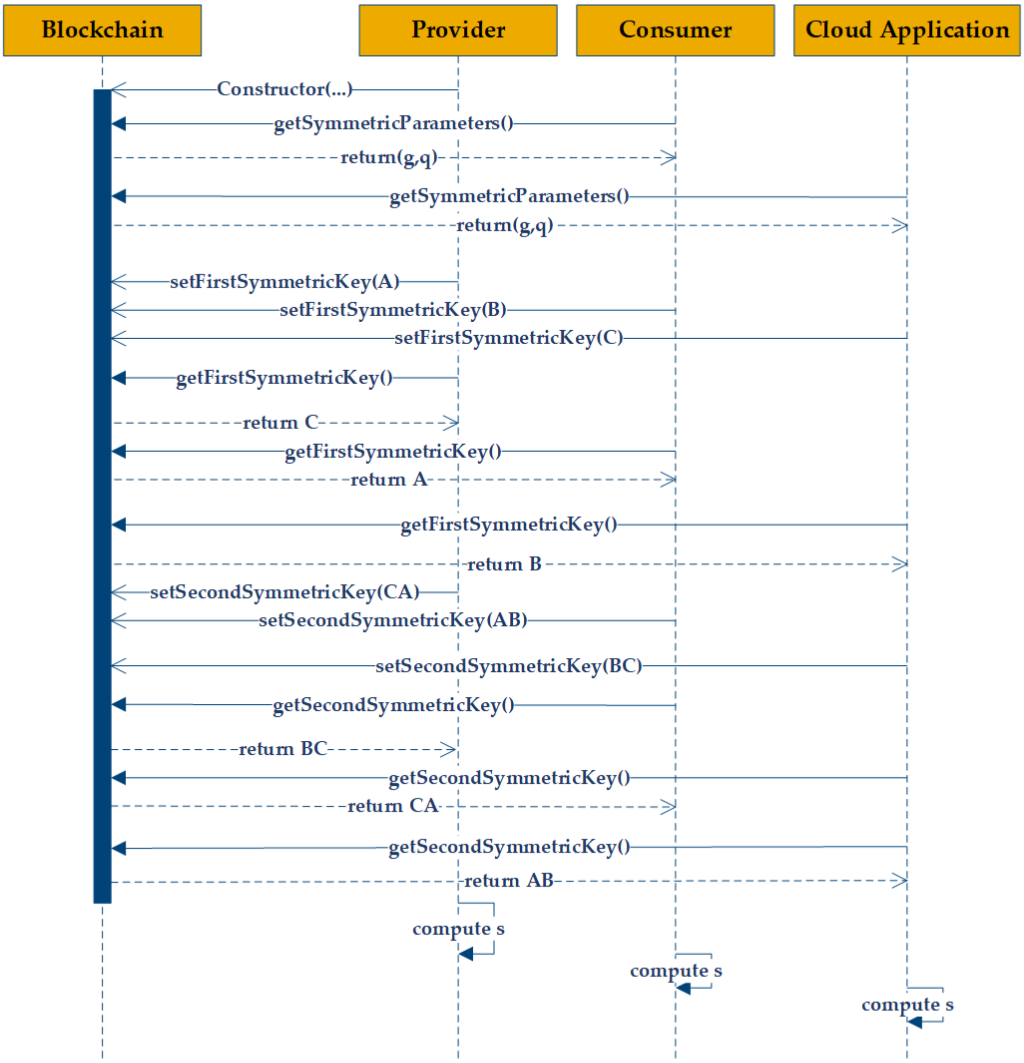


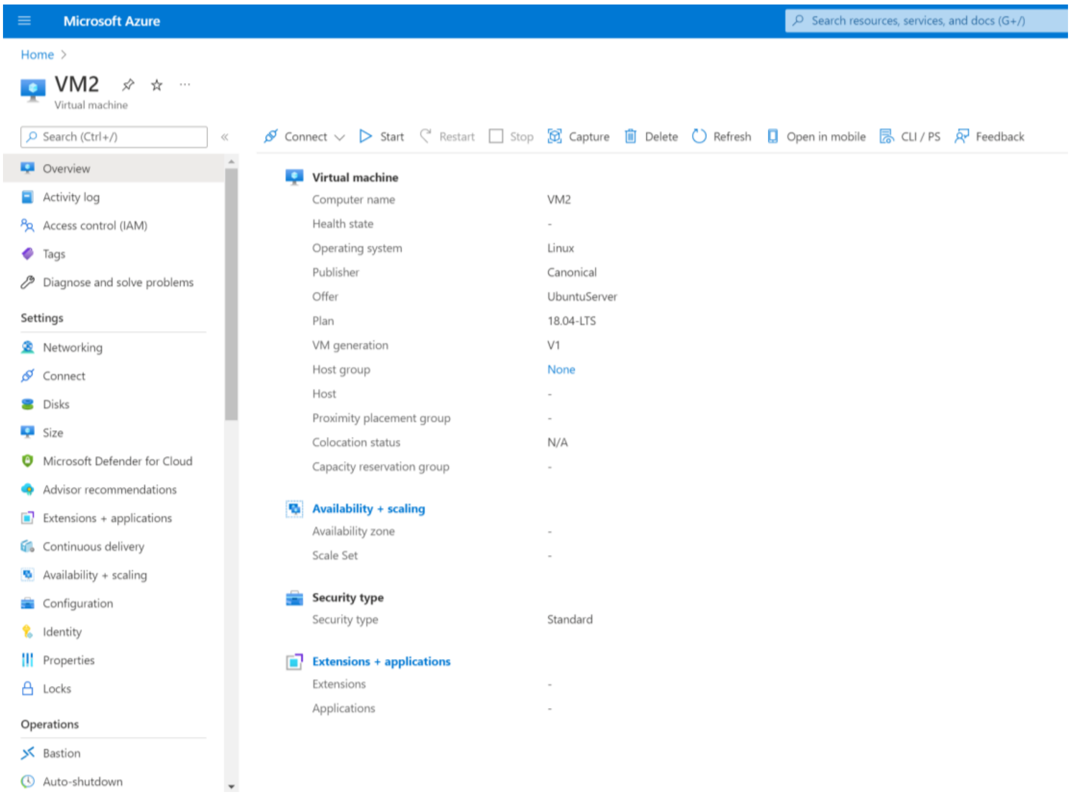
Figure 23: Initial Sequence Diagram of Negotiating a Shared Symmetric Encryption Key

4.2.2.2 *Cloud Management Script (Cloud-Side Application)*

In addition to the blockchain, the cloud is an essential component of the proposed artifact design. In the presented architecture design, the provider of cloud instances is referred to as a cloud vendor. For example, this provider could be Microsoft Azure, Google Cloud, or Amazon Web Services. The cloud vendor offers its cloud services to the application provider. The application provider pays the cloud vendor based on the model described in 3.1.1. The cloud application provider may run multiple cloud instances on the infrastructure provided by the cloud provider. The respective cloud instances are each independent software environments with independent operating systems.

Virtual machines (VMs) are usually used to describe these kinds of multiple independent software environments (Z. Huang et al., 2020). Cloud application providers can offer various software applications on the respective VMs. Like the interaction of the frontend and backend of the architecture presented, cloud and client applications can also be divided into a frontend and a backend. On the proposed architecture, the *Cloud Management Script* is assumed to run as part of a cloud application's backend, which should be compliance-driven configured.

The connection to a VM, the data storage, and the management of the VM resources (such as processor performance, memory, or graphics cards) are managed via a cloud management interface (CMI). The cloud vendor usually provides the CMI. Figure 24, below, shows an example CMI from Microsoft Azure. In addition to the graphical configuration of cloud instances, as shown in Figure 24, cloud applications can also be configured textually. Textual configuration via the command line enables the automation of actions. As the developed architecture aims for process automation, the command line version of the CMI is used in the context of this dissertation.



Virtual machine	
Computer name	VM2
Health state	-
Operating system	Linux
Publisher	Canonical
Offer	UbuntuServer
Plan	18.04-LTS
VM generation	V1
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Availability + scaling	
Availability zone	-
Scale Set	-
Security type	
Security type	Standard
Extensions + applications	
Extensions	-
Applications	-

Figure 24: Example Microsoft Azure Cloud Management Interface

As a reminder, the Management Smart Contract provides exactly two functionalities. The exchange of compliance-driven configurations and the generation of a common symmetric key *s*. The Cloud Management Script now implements these functionalities in the backend of the cloud applications using two communication flows and the command line CMI.

The intended backend communication of the Cloud Management Script is shown in Figure 25, below. The Cloud Management Script is part of the cloud application's backend. It must be able to communicate with the blockchain infrastructure and the provided cloud application (see *set cloud application configuration, confirm cloud configuration* and *get configuration status* use case 4.2.1). Based on the use cases identified, two communication flows could occur— the *key management flow* and the *configuration implementation flow*.

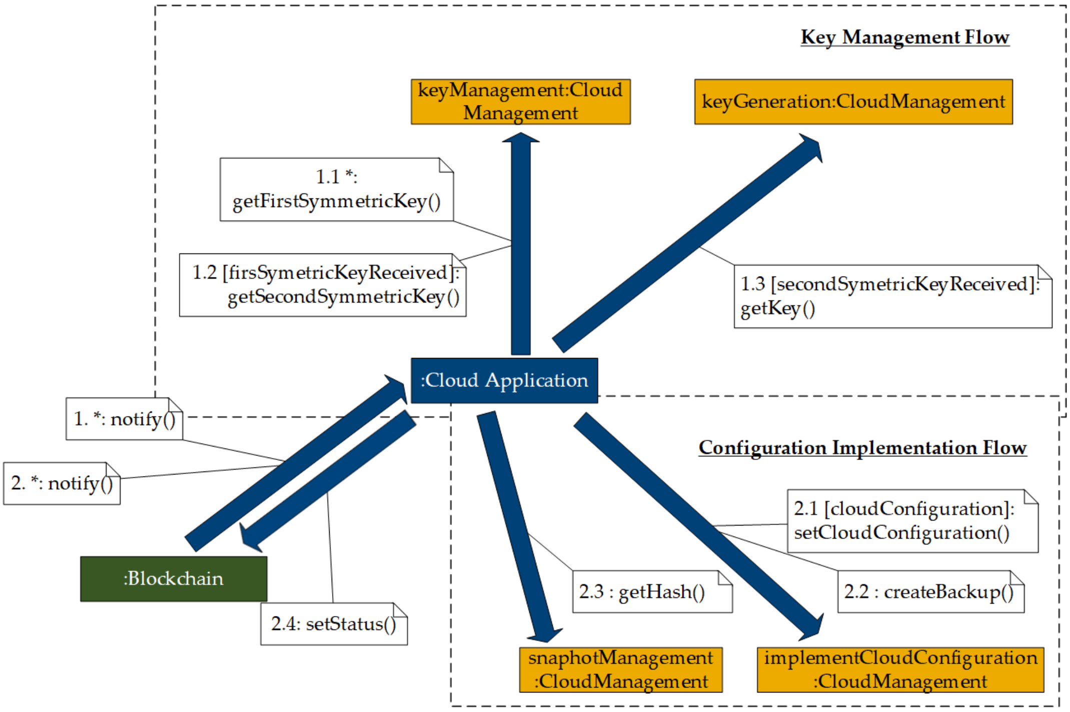

Key Management Flow
keyManagement:Cloud Management
keyGeneration:CloudManagement
1.1 *: getFirstSymmetricKey()
1.2 [firsSymetricKeyReceived]: getSecondSymmetricKey()
1.3 [secondSymetricKeyReceived]: getKey()
:Cloud Application
1. *: notify()
2. *: notify()
:Blockchain
2.4: setStatus()
Configuration Implementation Flow
2.1 [cloudConfiguration]: setCloudConfiguration()
2.3 : getHash()
2.2 : createBackup()
snaphotManagement :CloudManagement
implementCloudConfiguration :CloudManagement

Figure 25: Cloud Management Script Communication Diagram

The starting point for data communication is the Management Smart Contract (*:Blockchain*) in both communication flows. The Cloud Management Script (*:Cloud Application*) synchronizes with the Management Smart Contract via RPCs and the *notify* function (as depicted in steps 1.* and 2.* in Figure 25 above).

The *key management flow* realizes the creation of the symmetric key *s* on the side of the cloud application and is triggered if a Diffie Hellman key value has been changed or newly created on the Management Smart Contract. The functions indicated in the *key management flow* of Figure 25 are already described in 4.2.2.1.

The *configuration implementation flow* realizes the configuration exchange and is triggered by detecting a changed configuration on the Management Smart Contract (see 4.2.2.3 how configurations are changed on the client side). As a small reminder, configurations are textual descriptions (see 4.1). Hence, a configuration change applies exactly when two configurations are textually different from each other. This textual difference is determined by comparing the hash value of two configurations. Furthermore, due to the nature of blockchains, a configuration can only be changed when a new block is added to the blockchain. New configurations are passed on to the Management Smart Contract via a blockchain transaction (see 3.1.11). As already shown in detail, transactions are always added to the blockchain in the form of blocks. Consequently, a configuration may only change when a new block is added. By monitoring the blockchain for new blocks using RPCs and comparing the hash value of a configuration – stored on the Management Smart Contract – before and after a new block, it can be determined without a doubt whether a configuration has changed.

Suppose a participant wants to change a cloud application configuration. If the Cloud Management Script detects such a change, it executes a function to receive the encrypted configuration of the monitored Management Smart Contract. Since the Cloud Management Script has access to the secret symmetric key, it uses the system described in 3.1.7 to verify and decrypt the configuration to be implemented. The Cloud Management Script injects the newly received cloud configuration via the *setCloudConfiguration* function into the cloud application (step 2.1 in Figure 25). For example, such an injection can be ensured via an application programming interface (API) or the storage of a configuration file in a local configuration folder. As soon as the Cloud Management Script has injected the new configuration, it monitors the cloud application status for its implementation. The monitoring of the cloud configuration implementation status can be ensured by, for example, monitoring responses received by the REST interface or log files of the cloud application. The status returned by the cloud application is either *successful* or *failed (*see *confirm cloud configuration* and *get configuration status* use case 4.2.1).

If the cloud application reports a successful status (i.e., that the implementation of the configuration succeeded), the Cloud Management Script triggers the execution of a snapshot via the *createBackup* function from the current cloud instance through the CMI (step 2.2 in Figure 25); this snapshot is a full backup of the current cloud instance on which the cloud application is running. Thus, this snapshot includes the successfully configured cloud application and as well as all required data to restore the current cloud instance. This snapshot is later used to store proof of configuration implementation on the blockchain. Before that, however, the snapshot must be accessed to be able to generate proof of the conversion.

Modern cloud vendors are storing this snapshot on a separate external data storage location (Reagan, 2018). However, via the CMI, the Cloud Management

Script can retrieve the snapshot at any time. This retrieval possibility can load the backup into the VM on which the cloud application runs. In the proposed architecture design, the Cloud Management Script downloads the created snapshot from the external data storage onto the local instance. Next, the Cloud Management Script creates the snapshot's cryptographic hash value and then deletes the snapshot again from the local instance (see 3.1.7 for details on cryptographic hashing). The calculated snapshot's hash value is then written to the blockchain. This ensures that a hash value of the VM is generated and cached by the Cloud Management Script via the *getHash* function (step 2.3 in Figure 25). The storage of the snapshot's hash value, which contains the successful configuration, offers the possibility of non-repudiable evidence of the configuration implementation and is thus a significant improvement of existing approaches.

Assuming, as in the CapitalOne case, a legal dispute arises due to an incorrect firewall configuration. If the issue lies with the cloud application provider (in this case, the firewall), the customer must trust the cloud application provider to disclose the implemented configuration. With the existing model, the cloud application customer has no way to know which configuration has actually been implemented, nor does he have the possibility to obtain proof of the implementation. The customer must rely on the cloud application provider to disclose the configuration in case of doubt. By storing the hash value of the snapshot on the blockchain, this is now different. The stored hash value is a cryptographic hash. Hence, the hash value is second pre-image resistant (see 3.1.7).

Consequently, it is (computational) impossible to create a second snapshot different from the actual snapshot, which generates the same hash value as the one stored on the blockchain. If a dispute arises, the hash value of the configuration confirmed on the blockchain can be presented to the court. Theoretically, three cases can now arise from this.

First, the cloud application provider presents the snapshot matching the hash value to the court. Since the snapshot is an exact image after the implementation of the configuration stored on the smart contract, an independent expert can judge whether the implemented configuration (and thus the configuration stored in the snapshot) is indeed the one stored in the smart contract. Based on the blockchain and the associated audit trail of configuration changes, it is possible to determine the entity that configured the cloud application (firewall) wrongly. Due to the tamper-proof nature of the blockchain, this can be verified without a doubt.

The second case is that the provider presents the snapshot belonging to the hash value stored in the blockchain, but the snapshot does not contain the configuration stored in the smart contract. The cloud application then confirmed the configuration implementation without actually implementing it in the cloud application. Here, the court can clearly understand that the fault lies with the cloud application provider.

The third case is the opposite case to case one. The cloud application provider may not be able to present the snapshot to a hash value stored in the smart contract. For example, providers may want to hide a misconfiguration on their part. This case can be protected organizationally. On the one hand, it is possible to (contractually) agree that the cloud application consumer must also have access to the snapshots. Another option is to store the snapshot in a data location that all contracting parties can access. Finally, the court can also order the cloud vendor to hand over any snapshots related to the court case.

Overall, storing the hash value on the blockchain provides a legally secure way of proving configurations in case of doubt.

To write the snapshot's hash value to the blockchain, the Cloud Management Script utilizes the *setStatus* function (step 2.4 in Figure 25). The generated hash value is the hash value of a full backup of the cloud instance under which the cloud application is running. If an entity restores the snapshot associated with the stored hash value, it will have a cloud instance that reflects the immediate status after the cloud application has been successfully configured. The execution of the configuration subsequently ends in this case. The Cloud Management Script continues monitoring the Management Smart Contract.

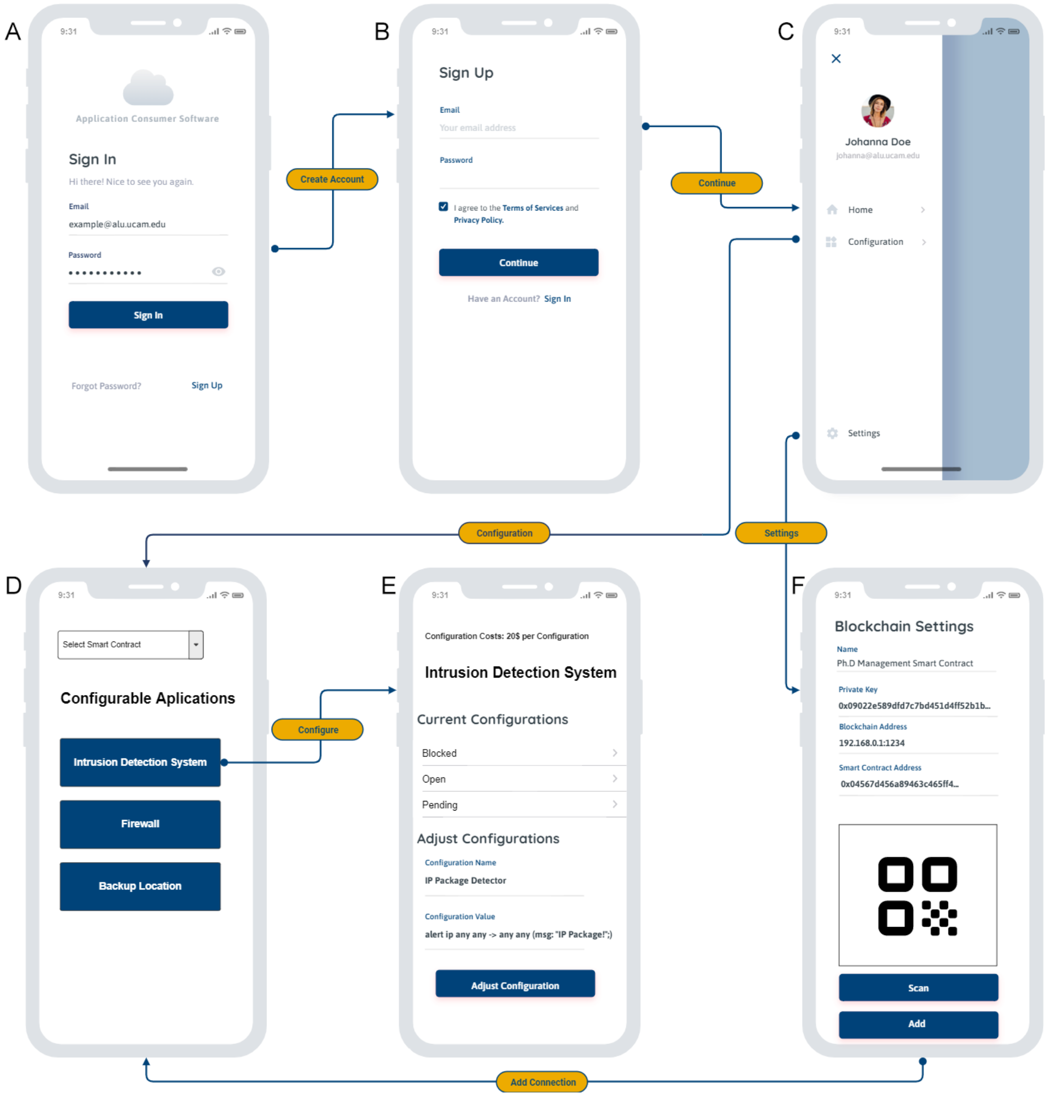
While the above describes a successful implementation, an implementation might also fail. In this case, the Cloud Management Script writes the implementation error to the blockchain via *setStatus*, terminates the cloud configuration, and continues monitoring the Management Smart Contract. In both cases, the implementation status is written to the Management Smart Contract and thus stored in a contractually binding and notarized way via digital signatures.

4.2.2.3 *Consumer Management Script (Client-Side Application)*

For setting client-sided configurations on a blockchain, the concept of decentralized applications (dApps) is used (Mayukh Mukhopadhyay, 2018). dApps are applications hosted on the blockchain and accessed via an individual frontend (Cai et al., 2018). dApps have their code on smart contracts (in this case, the Management Smart Contract). They use the blockchain for data storage and smart contracts for their app logic. In the case of this dissertation, the dApp stores the configuration resp. public Diffie Hellman values on the blockchain and uses the Management Smart Contract as logic to store or retrieve them. The RPC access to the Management Smart Contract is provided via the *Consumer Management Script*. dApps enable participants to execute the protocol described in Figure 23 automatically.

Important note, to avoid mixing up the different architectures. A dApp consists of a frontend (the *application consumer software*) and a backend (the Management Smart Contract). The communication between both is ensured via the Consumer Management Script. The dApp frontend, the application consumer software, again consists of a frontend (*client application*) and a backend (Consumer Management Script). Hence, the client application communicates via the Consumer Management Script with the Management Smart Contract on the blockchain.

An example of a dApp design is shown in Figure 26, below. The application consumer software (see Figure 22), as the cloud application, is divided into the client application (frontend) and the Consumer Management Script (backend), which enable client management. The application consumer software is an individual frontend to access the dApp's backend–the Management Smart Contract. To interact user-friendly with the Management Smart Contract, the application consumer software provides a client application. The client application is connected to the Consumer Management Script, which communicates via RPCs with the Management Smart Contract (see *show configuration price* and *get configuration* use cases 4.2.1). The client application can be a Windows, macOS, or Linux application. However, it might also be a mobile application (e.g., Android, iOS). The mockup shown in Figure 26 illustrates the client application graphically. It is a demo application and is not mandatory for the proposed software artifact. It aims to support describing the artifact and the function of the Consumer Management Script.



Email
example@alu.ucam.edu
Password
•••••••••••

Configuration Costs: 20$ per Configuration

Configuration Name
IP Package Detector
Configuration Value
alert ip any any -> any any (msg: "IP Package!";)

Name
Ph.D Management Smart Contract
Private Key
0x09022e589dfd7c7bd451d4ff52b1b...
Blockchain Address
192.168.0.1:1234
Smart Contract Address
0x04567d456a89463c465ff4...

Figure 26: Schematic Illustration of the Application Consumer Software Design

Figure 26 is divided into six sub-images (labeled A–F). The sub-images are used to depict the individual client management functions as exemplary. The client application stores the consumer's private blockchain key in the above example. The client application must provide a user authentication mechanism to ensure that only the user owning the private blockchain key can access the stored key. The authentication steps are shown in sub-images A–C. Only an authenticated user can access the client application and its related private blockchain key. Hence, only an authenticated user can adjust and digitally sign blockchain transactions and, thus, finally, cloud configurations.

Besides the authentication, the client application must store: (1) the private key to be used at the Management Smart Contract for signing transactions; (2) the network address of the blockchain to be used as backend infrastructure; (3) the address of the Management Smart Contract provided by the application provider (see 4.2.2.1). Items 1–3 are stored in the settings of the client application (sub-image F). After the necessary information is stored using the client application, the Consumer Management Script can then be used to access those and configure cloud applications (sub-image D). The Consumer Management Script is part of the application consumer software's backend and sets cloud application configurations on the client side.

RQ5 and Section 4.1 noted that cloud configurations must be mathematically defined. The definition of cloud configurations allows them to be mapped by software. The definition of cloud configurations set in this dissertation ensures that cloud configurations are stored textually in the UTF-8 encoding. Consequently, a configuration is understood as a text document. This textual document can be generated by the client application, encrypted, and written to the Management Smart Contract via the Consumer Management Script (see sub-image E).

The communication of the Consumer Management Script, and the data flow of compliance-driven configuring a cloud application via Management Smart Contract, is shown in Figure 27, below. The initial starting point is that all communication participants have already executed the key management flow described in Figure 23. Thus, all parties have access to the shared secret key s.

Note: the cloud application receives the symmetric key s via the Cloud Management Script. The provider and consumer receive the key through the Consumer Management Script. As soon as every participant in the architecture has access to the symmetric key s, s can be used to encrypt and decrypt configurations. Based on the mathematical definition of a configuration (see 4.1), the Consumer Management Script provides an input function via which customers can textually enter their configuration (see sub-image E). As customers enter their new configuration, the Consumer Management Script executes the protocol described in Figure 27. The encrypted configuration (cyphertext c) and the corresponding authentication tag t can be generated on the client side since each communication participant has access to the symmetric key *s*, which can be used to generate both *c* and *t*, as will be shown in detail later. The described protocol includes the encrypted configuration (cyphertext *c*) and the authentication value of the configuration (tag *t*). The Consumer Management Script automatically stores both values on the Management Smart Contract via the *SetConfiguration(c,t)* function.

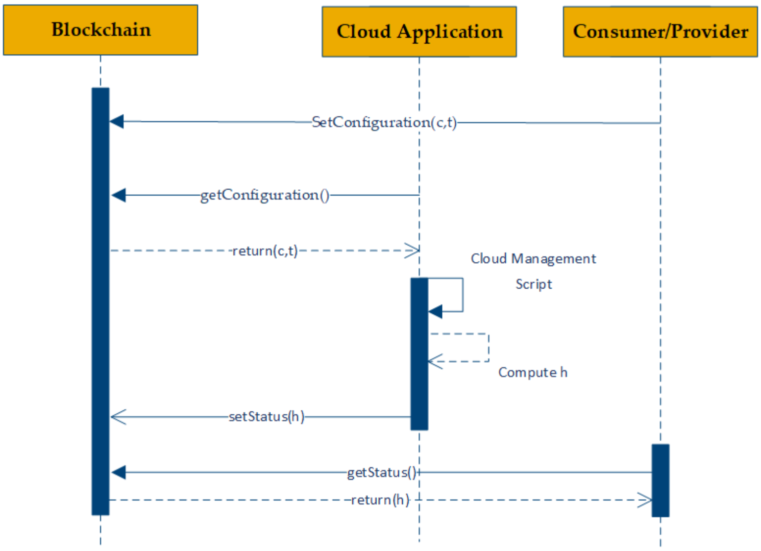


Figure 27: Sequence Diagram of Configuring a Cloud Application

As soon as a new configuration is stored at the Management Smart Contract, the configuration implementation flow of the Cloud Management Script is triggered (see 4.2.2.2 for more details). After the configuration implementation flow of the Cloud Management Script is executed, the blockchain stores the configuration implementation status of the cloud configuration. The Consumer Management Script uses this status to inform the customer about the configuration implementation's success or failure(see 4.2.2.2 for more details).

Finally, there is only one problem with this approach, which must be overcome. The current issue can be explained in more detail using the example of languages. Assume that a message (cloud configuration) is to be transported textually (definition of configuration) from person A (cloud application consumer) to person B (cloud application). Even if person A gives the message to person B, it must be ensured that both person A and person B speak the same language. If person A writes German and person B only understands Spanish, both parties cannot exchange messages, even though they have agreed on a standard for communication (textual). It is essential that both communication parties also speak the same language via the defined communication channel. This is similar to cloud configurations. Even if both applications know they are exchanging via text (definition of configurations, see 4.1.2), they must speak the text in the same computer language. As later will be shown in detail, the Extensible Markup Language (XML) or JavaScript Object Notation (JSON) format are two possible computer formats for exchanging textual messages in a standardized way (Nurseitov et al., 2009).

4.2.2.4 The Business Process in a Nutshell

In addition to the software architecture design for cloud applications' transparent, automated, and non-repudiable configuration, this dissertation proposes an associated business process. As the software architecture, the business process is kept generalized. It can thus be used to configure a wide range of cloud applications. The intention for the provision of the business process is to provide decision-makers with a tool (see Table 2, point 7). The process provided can estimate the possible cost and effort of migration to the introduced software architecture.

Meanwhile, the process description presents a guide showing how existing architectures can be converted to reference architecture. The necessary steps for introducing the reference architecture are illustrated in Figure 28, below. Each step is described in detail in the following paragraphs.

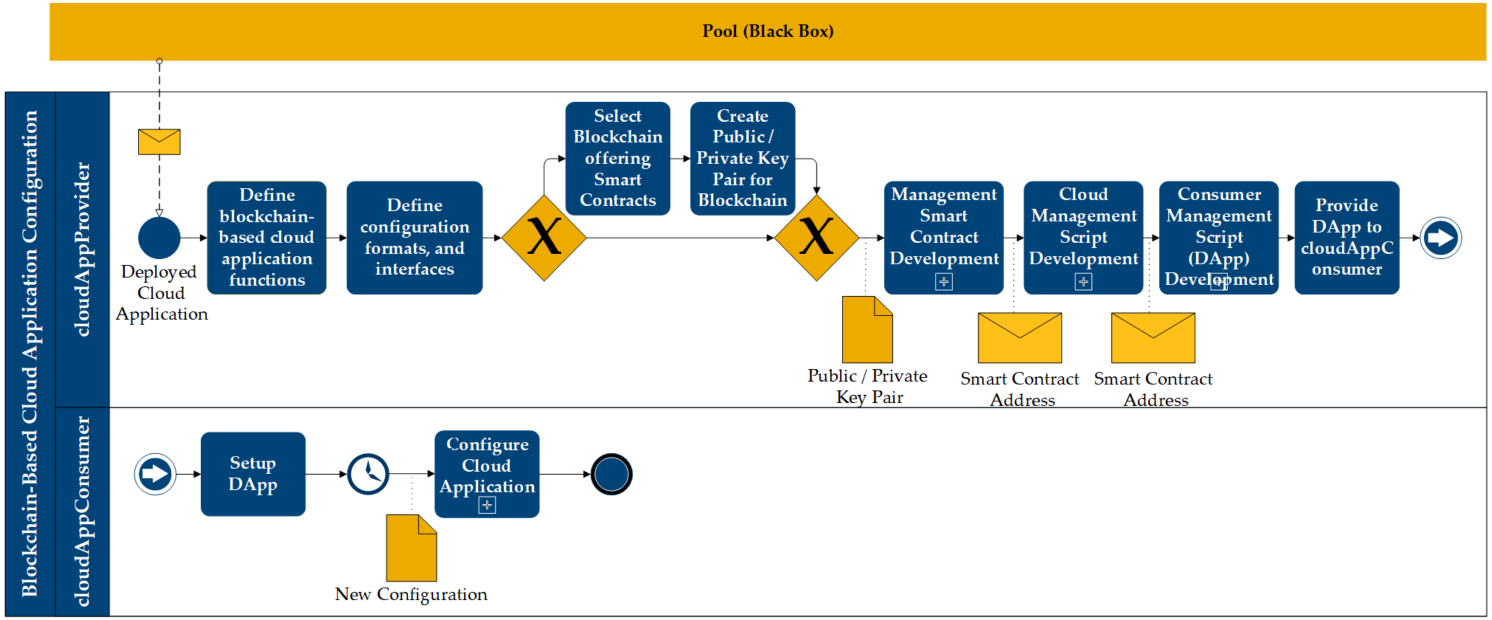

Pool (Black Box)
Blockchain-Based Cloud Application Configuration
cloudAppProvider
cloudAppConsumer
Deployed Cloud Application
Define blockchain-based cloud application functions
Define configuration formats, and interfaces
Select Blockchain offering Smart Contracts
Create Public / Private Key Pair for Blockchain
Public / Private Key Pair
Management Smart Contract Development
Cloud Management Script Development
Consumer Management Script (DApp) Development
Smart Contract Address
Smart Contract Address
Provide DApp to cloudAppC onsumer
Setup DApp
Configure Cloud Application
New Configuration

Figure 28: Business Process for Implementing Cloud Configurations Blockchain-based

As Figure 30 shows, the starting point of this proposed business process is a pre-deployed cloud application. This is not a mandatory requirement; the business process can also be modified to consider the proposed software architecture design within cloud software development. However, this work assumes that an existing architecture is converted into the presented software architecture, as this case might be more likely. Therefore, the starting point of the presented business process is the fully deployed cloud application.

Furthermore, it is assumed that a cloud application provider wants to migrate this application to the proposed architecture. During the first step (see Figure 30), the provider must define which cloud application functions should be configured automatically via the blockchain. Based on the mathematical definition of the configuration (see 4.1.2), the provider must define the partial function

$$c\colon \Sigma^* \rightharpoonup (I^{\underline{\omega}} \to O^{\underline{\omega}}).$$

This can be defined using a requirements analysis for a change project. In other words, a project responsible for switching from the existing cloud architecture to the new architecture proposed in this dissertation. Within a change project, the provider must define the interfaces over which the configuration changes are to be implemented. From a mathematical perspective, the cloud application provider must specify which software interfaces they want to reflect the behavior of the partial function c (see 4.2.1). After completing the theoretical part of the change project, the provider must implement the requirements into the proposed software architecture. The architecture design uses blockchain technology to automate configuration exchange, track changes, and notarize successful configuration changes. Hence, a blockchain wallet (public and private key pair) is essential. If the provider does not yet have this, they must initially create it. To perform this step, the provider must select the blockchain that best reflects their requirements (e.g., concerning speed, visibility, transaction costs, or consensus mechanism). As the proposed architecture of this dissertation is generic, it allows for selecting the best-suited technology for a specific use case.

Once the blockchain wallets exist, the public/private key pairs are used to develop the Management Smart Contract described in 4.2.2.1 (see also Figure 30). The provider can deploy the developed Management Smart Contract on the previously selected blockchain using the private blockchain key. To perform this step, the provider must initially define the business costs of a configuration change.

In essence, the provider must ask how much it should ultimately cost the customer (or the provider itself) to change a cloud configuration. Subsequently, the provider must contact the customer and create a blockchain wallet together (if the customer does not yet have a wallet). Deriving from the created wallet, the provider subsequently requires the customer's public key. This public key is later used to verify transactions and to prove configuration changes. As described in 4.2.2.1, the cloud provider must now develop and provide the Management Smart Contract on the blockchain. Subsequently, the provider needs to communicate the address of the Management Smart Contract to the customer. The Management Smart Contract Development process is finished when these steps are completed.

Once the Management Smart Contract is deployed, the cloud application provider is able to commence developing the Cloud Management Script. The details of this have been discussed in 4.2.2.2. Essentially, the creation of the Cloud Management Script can be divided into three process steps: (1) the definition of the smart contract communication mechanism; (2) the implementation of the cloud application communication mechanism; and (3) the implementation of the cloud management connection for receiving, decrypting, reading, and validating changes from the blockchain. Once these three process steps have been implemented, the design of the Cloud Management Script Development is completed, and the development of the Consumer Management Script can be initiated.

During a final sub-process, the Consumer Management Script must be developed. As 4.2.2.3 indicates, the Consumer Management Script is a dApp. This provides a user-friendly interface for automated blockchain-based configuration of the cloud application. The main process steps in developing the dApp are the definition of the frontend layout. The frontend definition describes which inputs a cloud application consumer should be able to perform via the dApp, as well as which Management Smart Contract functions the dApp is allowed to access. An example of a frontend layout is shown in Figure 26. After the customers have authenticated themselves to the dApp with their local user name and password (as described in Figure 26-B), they can store the address of a new cloud application or access already stored cloud applications. If customers want to register a new cloud application (Figure 26-F), they must first enter a name for it in the dApp. The user can later find the stored cloud application based on this name. In addition to the name, users can also enter the private key with which they want to confirm the blockchain transactions – and thus the execution of the Management Smart Contract. Finally, users can also store the address of the Management Smart Contract and the Internet Protocol (IP) address of the blockchain on which the Management Smart Contract was deployed in the application. It should be noted that a user receives this information (Management Smart Contract address and blockchain address) from the cloud application provider as soon as the provider has deployed the Management Smart Contract for the customer on the blockchain (see 4.2.2.1).

In parallel, accessing cloud applications that have already been stored is also possible. Users can access a list of cloud applications that have already been deployed and released for configuration. As shown in Figure 26-D, a variety of cloud applications, such as an intrusion detection system (IDS), a cloud application-based firewall, or the backup location of the cloud application, can be configured via smart contract. If, for example, a user now wants to configure the stored system for the intrusion detection system, they can open it by clicking on it (see Figure 26-E). Users then see all output behaviors, which they can modify with their input via the input menu. For example, in Figure 26-E, a user could specify the network connections for which they would like to receive a warning message on their mobile device. Further details on this are described in detail in section 4.2.4.

Once the cloud provider has developed the graphical consumer interface for automated configuration of the cloud application, they can provide the dApp. The provisioning of the dApp can be done, for example, via a download link or directly at the time of delivery of the cloud application. The migration process for the cloud application provider is completed with the provision of the dApp. Once they receive the dApp, cloud application consumers can use it to configure the cloud application they have paid for in a transparent, automated, and non-repudiable manner without resorting to classic consulting processes. Thus, the software architecture design and associated business process presented in this dissertation represent a significant improvement on existing cloud application technology. This is because cloud application customers no longer have to trust that the cloud application provider has actually implemented discussed configurations. Instead, cloud application consumers can now see the implementation on their dApp transparently. Because the cloud application writes a confirmation back to the Management Smart Contract, cloud application consumers have a complete and tamper-proof audit trail on the blockchain. Based on the entries in the blockchain (and the use of a private key to sign the transaction), it is possible to trace in a tamper-proof and non-repudiable manner which user applied which configuration at which time and at which time which configuration was confirmed as successfully implemented by the cloud application.

Consequently, the points of reaching transparency and non-repudiation (as mentioned in section 1.3) of cloud configurations are fulfilled with this implementation and business process. In addition, there is no longer any need for an employee to take care of implementing the cloud configuration manually. The implementation of cloud configurations is automated using the Cloud Management Scripts. Hence, the required point of process automation (see 1.3.2) is also tackled by the presented architecture and the connected business process. Once a cloud application consumer has access to the dApp for configuring the cloud application, they only need to link the dApp to the created blockchain wallet. Subsequently, a consumer can perform cloud application configurations at any time and without the intervention of the cloud application provider. To perform this step, a consumer must only provide a valid configuration using the dApp (see 4.2.2.2).

However, as we will see in the following section, the practical applicability of this architecture remains to be seen.

4.2.3 Construction Phase

Inspired by this dissertation’s scope and the related work, section 4.2.2 has shown what a software architecture for overcoming this dissertation's identified issue might look like. As indicated in Figure 20 (see 4.2.1), the expected artifact of this dissertation is a generic software architecture. Currently, the presented software architecture exists only as a textual description (see 4.2.2). It is unclear whether the architecture design can be implemented in software. Hence, the software architecture has not demonstrated its practical applicability yet. The proof of feasibility is the basis for RQ6 (see 1.4.4). To answer RQ6, it must be determined what the practical implementation of the designed architecture may look like.

This section aims to show that the developed architecture can be implemented in software. Hence, this chapter presents a proof of concept (PoC).

This section describes the development process from concept to finished implemented software. The proposed software architecture (described in 4.2.2) and the related business process (4.2.2.4) will be applied to construct the software application and to answer RQ6. This chapter illustrates the software development cycle of the software prototype and explains step by step which steps were made to transform the concept into a running application. Note that this chapter does not deal with the code of the software. The code of the software can be found on GitHub (Weber & Buchkremer, 2022a).

The general implementation concept is shown in Figure 22 (in 4.2.2). As discussed in 2.1.4, this dissertation aims to verify the architecture based on a prototype implementation of the proposed architecture. In the past, Python has already proven itself as a programming language for prototyping several times (Van Rossum, 2007; Weber & Prinz, 2019). Python version 3.8 was chosen as the programming language for developing the cloud and Consumer Management Script (Van Rossum, 2007). The Ethereum blockchain, described in 3.1.9 and 3.1.10, was used to implement the Management Smart Contract on a specific blockchain. The Ganache Command Line Interface (CLI) v7.0.4 was used (Truffle Suit, 2021) to provide a blockchain development environment since this combination has shown its feasibility for smart contract development (Weber & Prinz, 2019).

For the connection between the Cloud and Consumer Management Script and the Ethereum blockchain, the web3py development library was used. Several papers have already discussed the web3py development library for inter-blockchain communication (Chamola et al., 2022; Di Francesco Maesa et al., 2018; Salem et al., 2022). The web3py library enables RPC calls between a client (Cloud and Consumer Management Script) and a server (blockchain). The documentation of web3py (Ethereum, 2021) describes itself as a lightweight Python library designed for working with smart contracts and integrating with nodes on the Ethereum blockchain; thus, it is well suited for developing this software artifact. The overall web3py concept is shown in Figure 29, below. The web3py RPC concept in Figure 29 is divided into three parts. The Python part represents the Python developer environment (Cloud and Consumer Management Script).

A Python developer can transfer digital money (ether), create a new smart contract, or call an existing smart contract through the web3py API. Internally, the core of the web3py library takes care of the API call. Therefore, the web3py library allows Ethereum transactions to be created using Python code. The transaction creation includes the definition of the recipient and the calculation of the gas necessary for executing the transaction (see 3.1.11). The web3py library also has access to the executing entity's private key. This access is used to sign the transaction created as a part of Python development. The signature of the transaction is thus generated client-side (see 3.4.5). The complete transaction, including the digital signature, is then passed to the Ethereum network. The transaction is processed there as described in 3.1.10. The transaction manager of the web3py core takes care of the transaction's status. The transaction manager keeps track of whether the transaction has already been included in the blockchain and, if so, where the transaction is located in the blockchain. In addition, the transaction manager returns this information to the developer via the web3py API.

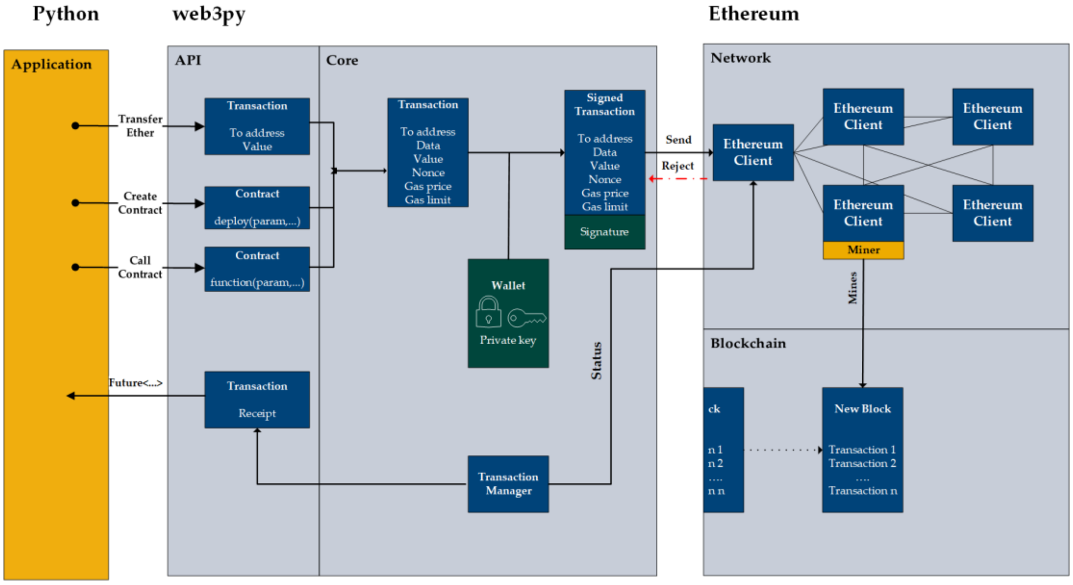


Figure 29: Overview of the web3py Library Concept

4.2.3.1 *Management Smart Contract Implementation*

As discussed in section 4.2.2.1, the Management Smart Contract is a deployed smart contract through which it can exchange compliance-driven cloud configurations and negotiate a shared symmetric key. The cloud application provider initially creates the Management Smart Contract on the blockchain (see 4.2.2.1). Following this step, the Management Smart Contract is then used by the provider, consumer, and cloud application to configure the cloud application. The Management Smart Contract class diagram is shown in Figure 30, below. The basic functions of the Management Smart Contract are:

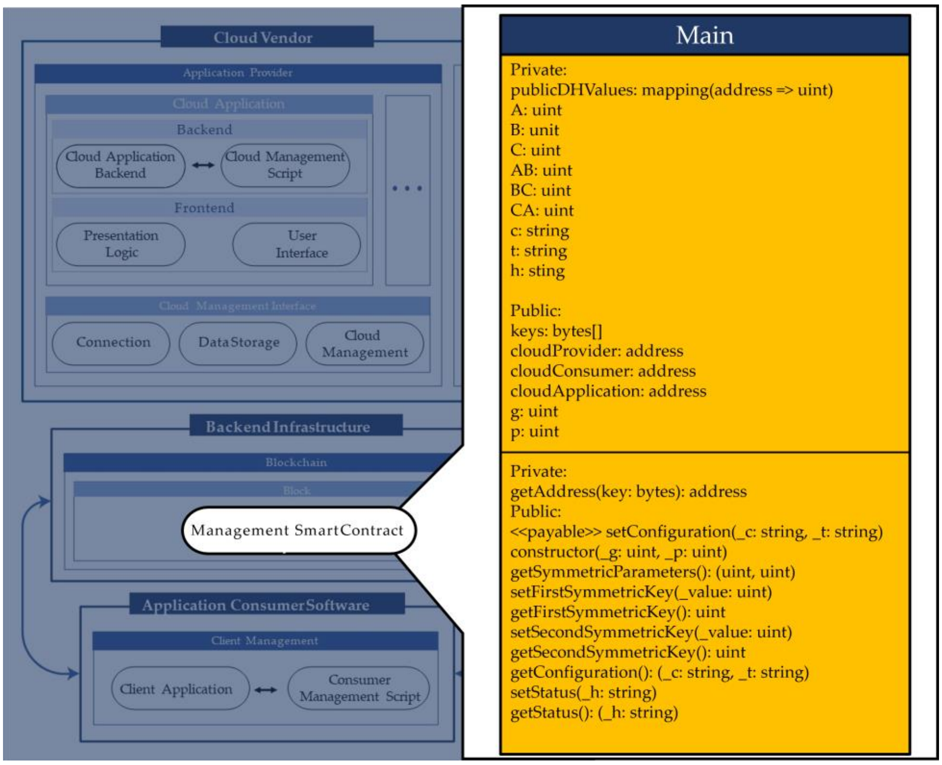

Cloud Vendor
Application Provider
Cloud Application
Backend
Cloud Application Backend
Cloud Management Script
Frontend
Presentation Logic
User Interface
Cloud Management Interface
Connection
Data Storage
Cloud Management
Backend Infrastructure
Blockchain
Block
Management Smart Contract
Application Consumer Software
Client Management
Client Application
Consumer Management Script
Main
Private:
publicDHValues: mapping(address => uint)
A: uint
B: unit
C: uint
AB: uint
BC: uint
CA: uint
c: string
t: string
h: sting
Public:
keys: bytes[]
cloudProvider: address
cloudConsumer: address
cloudApplication: address
g: uint
p: uint
Private:
getAddress(key: bytes): address
Public:
<<payable>> setConfiguration(_c: string, _t: string)
constructor(_g: uint, _p: uint)
getSymmetricParameters(): (uint, uint)
setFirstSymmetricKey(_value: uint)
getFirstSymmetricKey(): uint
setSecondSymmetricKey(_value: uint)
getSecondSymmetricKey(): uint
getConfiguration(): (_c: string, _t: string)
setStatus(_h: string)
getStatus(): (_h: string)

Figure 30: Class Diagram of the Management Smart Contract

Constructor(uint g, uint q, address cloudAppProvider, address cloudAppConsumer, address cloudApp): the Constructor of the Management Smart Contract. The unsigned Diffie Hellman $g, q \in [1, q-1]$ must instantiate a new Management Smart Contract. Moreover, the Constructor expects the public key (blockchain wallet addresses) for all three communicating parties. The values g and q are later used for creating a shared secret key between the communicating parties. The blockchain address of the cloud application provider (cloudAppProvider), the cloud application consumer (cloudAppConsumer), and the cloud application (cloudApp) are all employed for authenticating smart contract requests. All Management Smart Contract requests are authenticated based on the digital signature of placed transactions.

getSymmetricParameters(): returns the public Diffie Hellman key exchange values *g* and *q*. The values are initially set at the construction of the Management Smart Contract.

setFirstSymmetricKey(uint value): past research (Khader and Lai 2015) has shown that the Diffie Hellman key exchange protocol is vulnerable to MITM attacks. Therefore, public keys should only be exchanged in an authenticated manner. The *setFirstSymmetricKey* function ensures an authenticated storage of the public Diffie Hellman keys.

getFirstSymmetricKey(): Using the *setFirstSymmetricKey* function, the public Diffie Hellman keys are stored on the Management Smart Contract. The *getFirstSymmetricKey* ensures that the set public keys can be retrieved from the Management Smart Contract.

setSecondSymmetricKey(uint value): running immediately after the *getFirstSymmetricKey* function, the *setSecondSymmetricKey* function ensures an authenticated second exchange of the public Diffie Hellman keys (see Figure 23).

getSecondSymmetricKey(): running simultaneously as the *getFirstSymmetricKey* function, the *getSecondSymmetricKey* function ensures that the public keys can be retrieved from the Management Smart Contract.

setConfiguration(string c, string t): Using the Diffie Hellman key exchange protocol, a shared symmetric key *s* is created among the three communicating parties (see 4.2.2.1). Using the secret key *s*, the cloud application provider and consumer can create an encrypted configuration *c* and its authentication tag *t* (McGrew & Viega, 2004). The input values *c* and *t* are used within this function to store the cloud configuration and the related authentication tag on the Management Smart Contract (see 4.2.2.3).

getConfiguration(): Returns *(c,t)* from the Management Smart Contract; the latest set configuration.

setStatus(string h): This function should only be called by the cloud application (see 4.2.2.2). It stores a hash value within the Management Smart Contract.

getStatus(): Returns *h* from the Management Smart Contract; the last hash value of a cloud instance successfully implemented using the *setStatus(string h)* function.

4.2.3.2 *Cloud Management Script Implementation*

Figure 31, below shows the Unified Modeling Language (UML) diagram of the Cloud Management Script implementation. Since the Cloud Management Script implementation is a prototype, it was also implemented in Python. The main function is used to start the script. The main function ensures that the shared symmetric key is created and kept up to date by the cloud application. Once the script has been started, it monitors the defined Management Smart Contract for changes via the web3py library. The credentials are stored and protected from access by other applications using the environment variable. Environment variables are configurable variables in software development that contain paths to specific values or data that multiple places in software can use. Environment variables serve the maintainability of the source code. Instead of changing a path in all areas of the source code, paths to values or data can be managed centrally using environment variables.

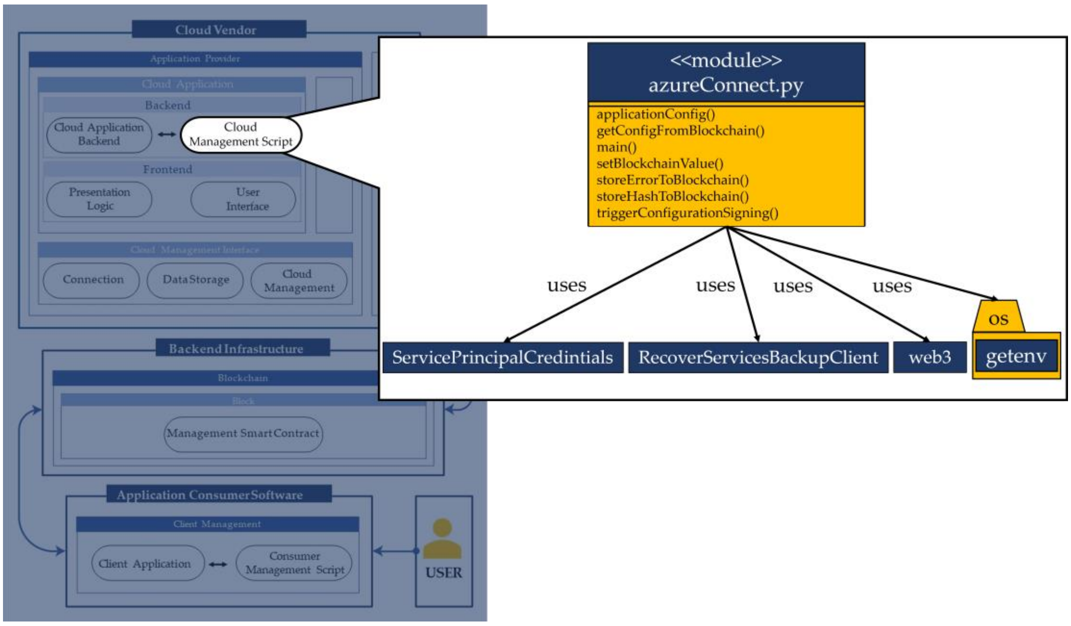


Figure 31: Class Diagram of the Cloud Management Script

If a new block has been added to the blockchain, it uses the *getConfigFromBlockchain* function to check whether the configuration in the Management Smart Contract has changed. If the configuration changes, the *getConfigFromBlockchain* function loads this from the Management Smart Contract into the Cloud Management Script. Using the symmetric key, it is decrypted there and implemented in the respective cloud application via the *applicationConfig* function. The *applicationConfig* function must specify how the received configuration will be implemented in the actual cloud application. Once the configuration has been successfully implemented, a cloud-side backup is started via the *triggerConfigurationSigning* function. The execution of the backup is monitored via the *triggerConfigurationSigning* function until the backup has been completely executed. Afterward, the function loads the backup from the cloud storage into the cloud instance, creates the hash value of the backup, deletes the backup again, and writes the hash value back into the Management Smart Contract using the *storeHashToBlockchain* function and the web3py library. If the application configuration fails, no backup is created, and the error is written to the Management Smart Contract using the *storeErrorToBlockchain* function.

In implementing the backup-hashing function, a cryptographic hash function was used. Cryptographic hash functions ensure that the hash value generated from the backup can be used in litigation to prove that a configuration has been changed (see 3.1.7). It is not computationally feasible to preserve the original input value of a cryptographic hash function (Gueron et al., 2011). Using a cryptographic hash function thus ensures that a generated hash value cannot be implemented with a manipulated VM and thus prevents forged configuration.

The proposed architecture prototype uses the SHA-512 hash function. Although SHA-256 is often used in blockchains, the SHA-512 hash function was used in the proposed approach because the operating system performs the hashing. Today's operating systems mostly run with 64-bit memory management. Due to parallelization, research has shown that the SHA-512 hashing algorithm runs faster than SHA-256 on 64-bit systems (Gueron et al., 2011).

In summary, the Cloud Management Script and the related process ensure non-repudiation of configuration changes. Once a configuration has been implemented on the cloud application side, the cryptographic hash value is generated over the virtual instance in which the cloud application is running. As shown in Section 3.1.7, generating an original value to a cryptographic hash value is difficult. Consequently, it is difficult to forge a virtual instance to generate the same cryptographic hash value stored on the blockchain. In the event of a legal dispute, the hash value stored on the blockchain and the corresponding virtual instance on which the configured application ran can be shown to the court. If the virtual instance presented to the court generates the hash value confirmed on the blockchain, it is, without a doubt, the configuration valid at the time of the investigation. Based on this configuration, a court case can be conducted without a doubt. Neither the provider of the cloud application nor the consumer can deny the configuration presented to the court. Denying is impossible since the blockchain's digital signatures can be used to show that both parties have agreed on the investigated configuration at a specific point in time.

The possibility of proving configurations beyond doubt at a certain time significantly improves the existing cloud configuration process. Currently, a cloud application consumer has to rely on the cloud application provider forwarding the proof of changes to a court (in case of doubt, even to his disadvantage).

4.2.3.3 Consumer Management Script Implementation

Following the process described in 4.2.2.4, the Consumer Management Script was implemented last. Again, Python 3.8 and the web3py library were used to implement the use cases and communication processes described in 4.2.1 and 4.2.2. To distinguish between tasks that communicate with the Management Smart Contract and those that are responsible for the client-side calculation, the Consumer Management Script was divided into four classes. The overall classes of the Consumer Management Script are shown in Figure 32, below.

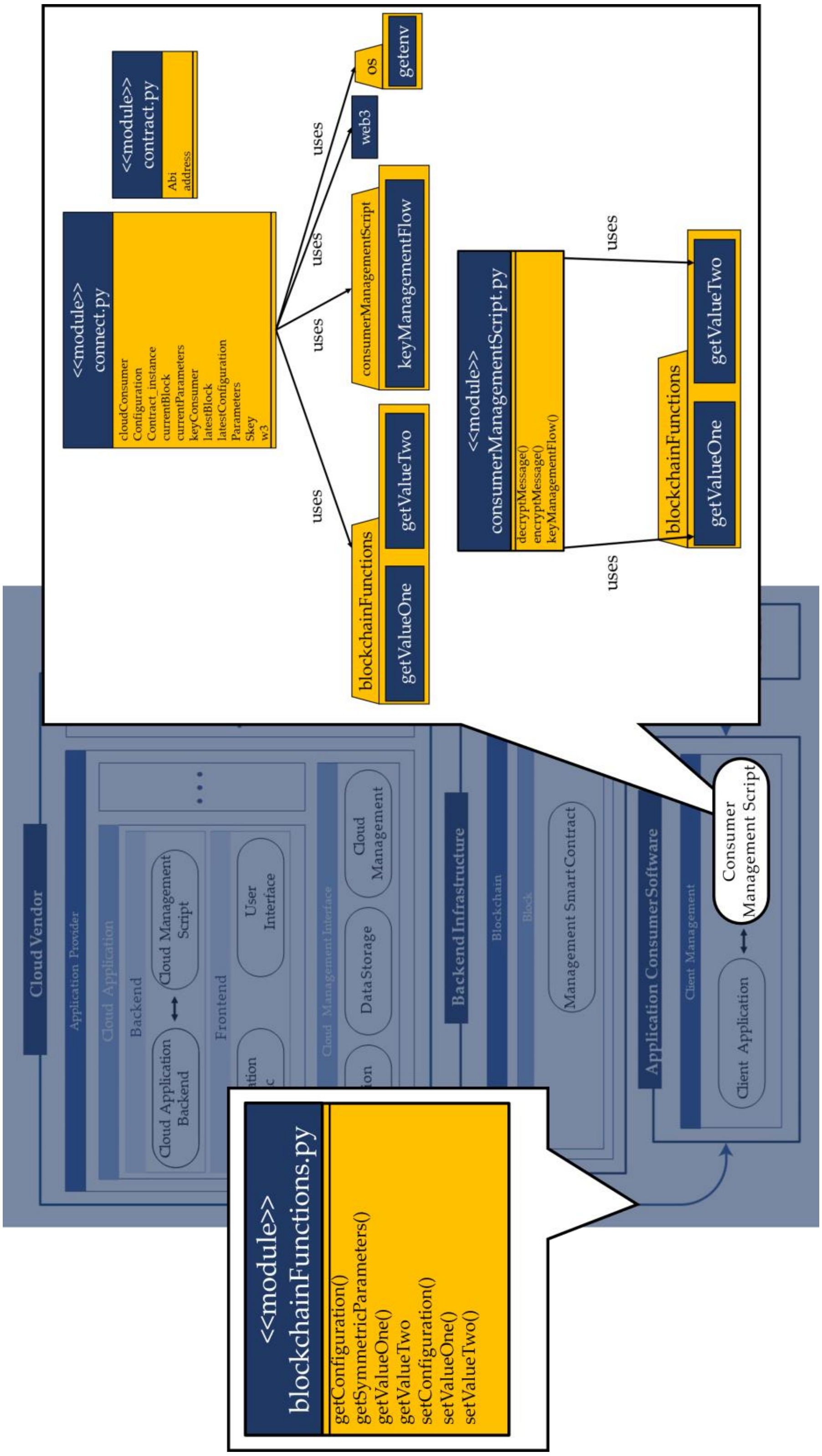


Figure 32: Class Diagram of the Consumer Management Script

The *contract.py* class provides the Application Binary Interface (ABI) and the blockchain addresses of the communication parties used in the Constructor function (see 4.2.2.1). To access the Management Smart Contract functions via Consumer Management Script, Python needs an ABI to communicate on the Ethereum EVM deployed Management Smart Contract. As explained in 3.1.11, smart contracts are pieces of code stored on the blockchain and executed by the EVM. The EVM also provides a comprehensive instruction set called opcodes which execute certain instructions. Opcodes are low-level codes similar to the processor's instruction set. The common Ethereum opcodes can be accessed from the Ethereum yellow paper (Buterin, 2014). The smart contract is compiled and stored in the form of bytes or binary representation in the Ethereum blockchain. For Ethereum and the EVM, a smart contract is just a single program running on this sequence of bytes. Solidity defines how a smart contract request gets from the program's entry point to the entry point of a particular smart contract function. When an external application or another smart contract wants to interact with the blockchain, it needs to know a smart contract's interface, such as a way to identify a method and its parameters. The Ethereum ABI provides this navigation (Buterin, 2014). Furthermore, the *contract.py* class also contains the address of the deployed smart contract. Both values might be set through a frontend client application described in 4.2.2.3.

The *connect.py* manages the dApp communication. This class creates the web3py object, which is then used in the *blockchainFunctions.py* class to ensure RPC communication with the blockchain (Management Smart Contract). In addition, this class also accesses the user's private key and synchronizes with the blockchain every 60 seconds. Like the Cloud Management Script, the *connect.py* class reacts to changes in the Management Smart Contract (see 4.2.2.1). As soon as the monitoring function in the *conncect.py* class detects a change in a configuration or a public Diffie Hellman value, it forwards the changes to the *consumerManagementScript.py (*see *notify* function Figure 25*)*. According to the detected changes, either a new symmetric key is generated or a new encrypted configuration is exchanged with the Management Smart Contract (see 4.2.2.1).

The *blockchainFunctions.py* class is used by the *connect.py* class and contains the functions necessary to communicate with the blockchain and interact with the Management Smart Contract. Specifically, the functions can be divided into "getter" and "setter" functions. The getter functions take the Management Smart Contract representation provided by the ABI (*contract_instance*) and the consumer's private key (*key*) as input. The setter functions take the web3py library (*w3*) as a transaction template, and some additionally take the Management Smart Contract address provided by the ABI (*address*) as input. In detail, the functions operate as follows:

getConfiguration(contract_instance, key): gets the current configuration set in the Management Smart Contract.

getSymmetricParameters(contract_instance, key): gets the Diffie Hellman values *g* and *p* from the Management Smart Contract. The values *g* and *p* had to be specified initially when the Management Smart Contract was created (see 4.2.3.1).

getValueOne(contract_instance, key): gets the first public Diffie Hellman value intended for the consumer.

getValueTwo(contract_instance, key): gets the second Diffie Hellman value intended for the consumer.

setConfiguration(w3, contract_instance, address, c, t, key): sets a new encrypted configuration *c* and its authentication tag *t* on the Management Smart Contract, which is signed using the private key of the consumer.

setValueOne(w3, contract_instance, address, value, key): sets the first Diffie Hellman value of the consumer on the Management Smart Contract. See 3.1.8 and 4.2.2.1 for more details on this function.

setValueTwo(w3, contract_instance, address, value, key): sets the second Diffie Hellman value of the consumer on the Management Smart Contract. See 3.1.8 and 4.2.2.1 for more details on this function.

The last class, shown in Figure 32, is the *consumerManagementScript.py* class. This class implements the two communication flows shown in Figure 25. This class implements three functions:

keyManagementFlow(w3, contract_instance, blockchainAddress, pubKey, g, p): this function takes an instance of the web3py library (*w3*), the Management Smart

Contract instance (*contract_instance*), the address of the Management Smart Contract (*blockchainAddress*), the sender's public key (*pubKey*), and Diffie Hellman public values g and p as input. This function implements the protocol described in 3.1.8 and returns the shared symmetric key s. Each time a participant changes the Diffie Hellman values g and p, this function is executed, and the new symmetric key is calculated (see 4.2.2.1).

encryptMessage(s, m): this function receives the current symmetric key s and the plaintext m as input. It returns the encrypted configuration c and the related authentication tag t (see 4.2.2.3). As indicated in the related work (see 3.4.5), this dissertation follows the idea presented by Guo et al. (2021) of providing simple methods for encrypting and decrypting cloud data on the side of the receiver and the sender of configurations. Specifically, for encryption and decryption, the symmetric algorithm advanced encryption standard (AES) operating in Galois/Counter Mode (GCM) is used (McGrew & Viega, 2004). GCM is an operating mode in which AES can be operated for symmetric encryption (McGrew & Viega, 2004). As a key feature, GCM provides an authenticated encryption mode to enable authentication and encryption of messages. For the receiver of the configuration (the cloud application), the receipt of authenticated configurations has the additional advantage that it can be verified for authenticity. When the configuration is encrypted and decrypted on the part of the cloud application, errors can occur (e.g., due to an attacker's manipulation of the encrypted configuration). To ensure that only the configurations that the client intended are implemented, the use of an authentication tag is mandatory. The authentication tag is generated directly when the configuration is encrypted using GCM mode and has to be passed on to the cloud application for verification together with the encryption. This is done, as already described in detail, using the Management Smart Contract. In concrete, the following steps are performed by the Consumer Management Script:

1. Use existing symmetric key s,
2. Compute $(c,t) = AES/GCM_{skey}(m)$, where c is the cipher text of m and t is the authentication tag of the message. Based on the definition of AES/GCM, both values (c,t) are calculated during the execution of AES/GCM,
3. Send (c,t) to the blockchain, using the *setConfiguration* function from the *blockchainFunctions.py* class.

decryptMessage(s, c, t): this function receives the current symmetric key *s*, the encrypted configuration *c*, and the associated authentication tag *t* as input. It returns the decrypted configuration *m* if and only if the decryption was successful. Else the function returns an error.

For decryption, a participant takes (*c*,*t*) and computes:

1. Use existing secret key *s*,
2. $(m, v) = AES/GCM^{-1}_{skey}(c, t)$, where *m* is the plain text and *v* is the verification result of the message.

4.2.4 Cutover Phase

After implementing the basic architecture in the previous subsection, this subsection now discusses the process of going live with the concrete implementation of the architecture. Utilizing the architecture implementation of subsection 4.2.3, this subsection answers RQ6—*what can a prototype implementation look like that utilizes blockchain-based trust for configuring cloud applications?* In this subsection, the complete implementation of a prototype in a live environment is presented. To use the example of building a house from 2.1.4, section 4.2.1 provided the project requirements for building a house. Section 4.2.2 provided the blueprint for building the house. Section 4.2.3 built the individual components of the house. In this section, the task is to assemble the components built in the previous section into a functioning house.

It should be noted that a house and its components can be assembled in various environments. It can be on a meadow, a building site in the city, in a desert, or on a mountain. Similarly, it behaves also with the software which will be developed. It can be deployed in many environments. For example, for a cloud application to configure backup frequency or a firewall (see CapitalOne use case). Thus, it should be noted that the implementation presented in this section is one of many possible environments in which the architecture described in 4.2.2 can be implemented. Rather, the implementation of this phase is intended to provide evidence that the developed architecture can be translated into reality.

The RAD method (see 2.1.4) used in this research requires the live circuit of a concrete approach in the last step. Thus, since the IDS approach is a well-described security mechanism found in many business environments, it is presented here as an example of a potential concrete use case. Hence, this section implements the described architecture in the environment of IDSs. Referencing Figure 20 (see 4.2.1), the cloud application requirements of the cutover phase are the implementation of an IDS. The software architecture used is the proposed architecture from 4.2.3.

4.2.4.1 Background on Intrusion Detection Systems

Monitoring safety-critical areas such as buildings, rooms, or streets with Closed Circuit Television (CCTV) cameras have been a standard practice for many years. CCTV cameras are not only used to deter criminals; a proprietor can use them to record attacks and events, too. Law enforcement services can use such visual data to solve crimes. This system has been successfully used for decades (Bace and Mell 2001; Debar et al. 1999; W. Lee and Stolfo 2000).

Denning (1987) described the initial idea of IDSes. Subsequently, this idea was further researched by Axelsson (1998), Khraisat et al. (2019), and Liao et al. (2013). It was also specialized in a wide variety of applications such as wireless sensor networks (Can & Sahingoz, 2015), the Internet of Things (Zarpelão et al., 2017), smart grids (Jow et al., 2017), and cloud computing (García-Teodoro et al., 2009). Essentially, IDSes can be classified into two categories, which differ in their manner of attack detection (Zarpelão et al., 2017).

A signature-based Intrusion Detection System (SIDS) detects attacks by monitoring events such as log files or network traffic and comparing them to a database of known and unwanted patterns. The SIDS triggers an alarm instantly when there is a match. Attack detection is, thus, based on pattern matching and must be determined in advance.

The second category is an Anomaly-based Intrusion Detection System (AIDS). AIDS is a statistic-based, knowledge-based, and machine-learning-based system (Khraisat et al., 2019). The basic assumption of AIDS is that legitimate users and malicious behavior can be distinguished from each other. Thus, AIDS utilizes machine learning, heuristics, or statistical models to distinguish between users and malicious events—and triggers an alarm when a malicious event occurs. Unlike SIDS, a database of known attack patterns is unnecessary.

Moreover, depending on the deployment location, AIDS and SIDS can be classified according to their monitoring location (García-Teodoro et al., 2009). IDSes that primarily monitor local systems, events, and log files are classified as host-based intrusion detection systems (HIDS). On the other hand, IDSes monitoring network traffic are classified as network-based intrusion detection systems (NIDS).

4.2.4.2 Deployment

It should be noted once again that the configuration of IDS is only one of many use cases for the presented generic architecture. Possibly any cloud application could be configured using the presented approach. The concept of the implementation is illustrated in Figure 33, below. The developed prototype should transparently, automatically, and non-reputable configure an IDS and notarize its compliance-driven configuration implementation. In the evaluation (chapter 5), this dissertation presents other use cases and experts' evaluations of their plausibility.

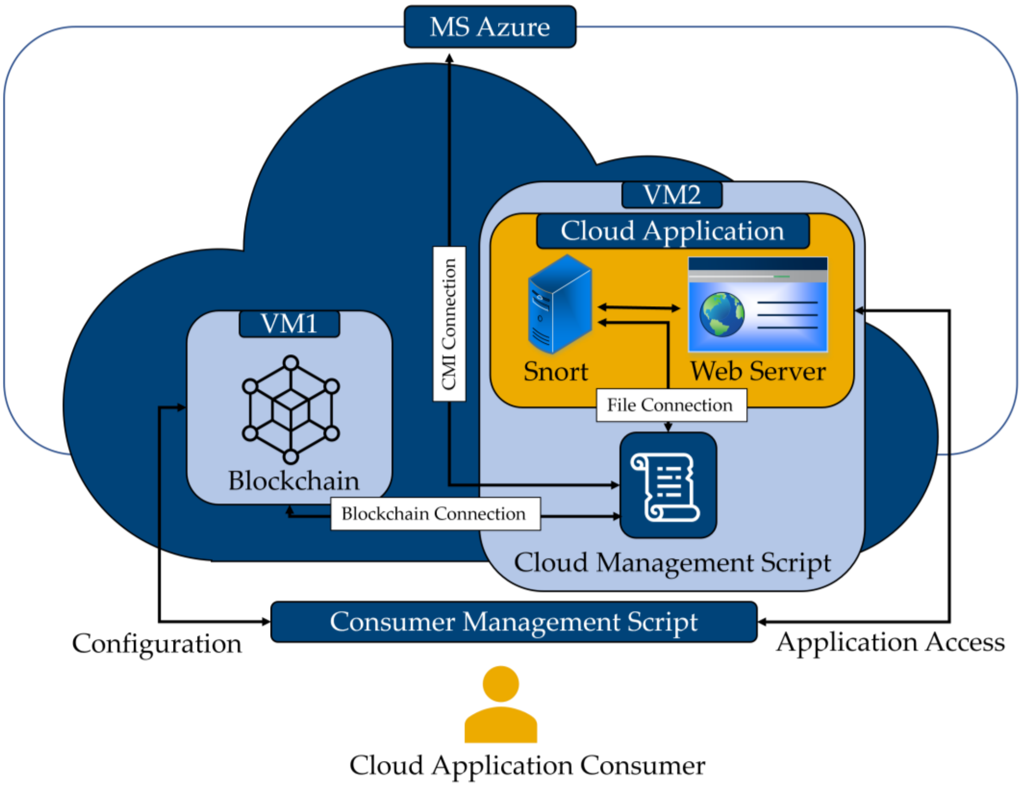


Figure 33: Deployed Prototype Architecture

There are four major public cloud providers on which the proposed architecture could be deployed for cutover. These are Microsoft Azure, Amazon Web Services, Google Cloud, and Alibaba Cloud, sorted in descending order of their distribution in the environment relevant to this dissertation (RightScale, 2019). In order to be able to support as many public cloud users as possible with the developed cutover code in the implementation of the architecture presented in this dissertation, the presented architecture is deployed based on a *Microsoft Azure (MS Azure)* Cloud instance. Hence, the live demonstration used the Microsoft Azure Cloud as a cloud instance and deployed two *VM* of the "Standard B4ms" type, five vCPUs, 16 GiB RAM, and 30 GiB disk storage on the MS Azure cloud. For identification, the deployed VMs were named *VM1* and *VM2*. Ubuntu Server 18.04 Long Term Support (LTS) was installed on both VMs as the operating system.

Regarding the notarized configuration of the IDS, the *Ethereum blockchain* (Buterin, 2014) was subsequently employed to implement sign transactions. On VM1, Ganache Command Line Interface (CLI) v7.0.4 was installed (Truffle Suit, 2021). The blockchain provided by the Ganache CLI could be accessed through a standardized interface. This standardized interface enabled the script-based use of the blockchain provided in VM1. Solidity (Dannen, 2017) was the programming language allowing the Management Smart Contract, web3py, to interact with the Ethereum blockchain via a script-based client (Ethereum, 2021), the digital signing scheme that the Ethereum blockchain provides.

Within VM2, this prototype ran two *applications* and the proposed Cloud Management Script (see 4.2.3.2). Microsoft Azure Software Development Kit (Microsoft, 2021) was employed for the *CMI connection*. The initial application was an Nginx version 1.21.0 *web server*, which was used for providing a template website containing static demo web content. The second application was the *IDS* compliance-driven configured using this proposed approach (see 4.2.3).

The IDS *Snort* version 2.9.8, a signature-based intrusion detection system upstream of the web server, was used (Beale, 2004). For the implementation of the live prototype, a cryptographic hash function was used to generate the snapshot hash value described in 4.2.3.3. Cryptographic hash functions ensure that a VM's hash value can be used in litigation to prove that a configuration has been changed. It is not computationally feasible to preserve the original input value of a cryptographic hash function (Gueron et al., 2011). This computational infeasibility thus ensures that a generated hash value cannot be implemented with a manipulated VM—it, therefore, prevents forged configuration.

4.2.4.3 Cloud Application Configuration

Based on RQ5, configurations are defined as $c\colon \Sigma^* \rightharpoonup (I^{\omega} \to O^{\omega})$ (see 4.1). In the deployed IDS, Σ^* are the characters that can be generated using the UTF-8 encoding. Mapping of input characters to an Input/Output behavior $(I^{\omega} \to O^{\omega})$ takes place if and only if Σ^* matches a valid rule description of the Snort IDS. Figure 34, below, shows the exemplary structure of a *Snort IDS rule*. With Snort, administrators can check network traffic for suspicious packet activity or dangerous connections. In addition to the predefined rules, administrators can create their own rules to detect port scans or other server attacks, for example. These advanced rules can be implemented by customizing Snort monitoring policies. Based on the example rule (see Figure 33), the Snort IDS would always raise an alert containing the alert message "IP Package detected!" if an IP packet from any source IP and Port were sent to any destination IP and Port. Snort gets its rules from a local file. The rules that Snort should implement are written line by line in this local advanced rules file. Adding or removing a rule changes Snort's detection.

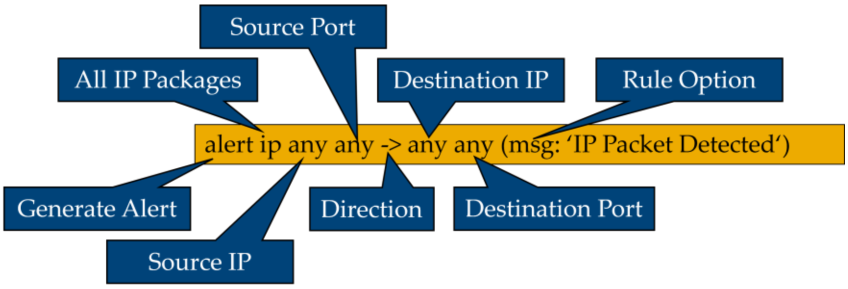


Figure 34: Snort Example Rule

As explained in 4.1, it is not enough to define configurations alone. It is also necessary to specify the exchange language in which communication takes place. In the proposed architecture of 4.2.3, the web3py library was used for RPCs. The web3py library uses JSON-RPC for exchanging messages (Ethereum, 2021). Hence, following the architecture of the web3py library, JSONs were used to define a common language between configuration and cloud application. A Snort IDS *configuration* was defined in the deployed implementation using JSON format. Hence, the deployed Cloud Management Script expected a JSON of the form shown in Figure 35 (below). In order to directly implement the rule change, the Cloud Management Script was configured to decrypt and copy received configurations to Snort's local rule file and to restart the Snort application from the command line. To gain feedback regarding the implementation status of the newly set rules, the Cloud Management Script monitored the log files of Snort. Based on the log files, the Cloud Management Script analyzed whether the rules added to Snort could be implemented successfully and whether Snort restarted successfully.

```
{
    “rules“ : [
        {
            “type“: “alert“,
            “package“: “ip“,
            “source_IP“: “any“,
            “source_Port“: “any“,
            “direction“: “->“,
            “destination_IP“: “any“,
            “destination_Port“: “any“,
            “message“: “IP Package Detected“
        }
    ],
    “time“: “timestamp“
}
```

Figure 35: JSON Structure of the Configuration File

The Cloud Management Script triggered a VM snapshot if the configuration was successfully written and applied. Once the snapshot was successfully created, the Cloud Management Script loaded it from the external cloud storage to the local VM storage; it then calculated the hash value of the snapshot and deleted it from the local VM storage again. The generated hash value is automatically written back to the blockchain (see 4.2.3.2 for details).

In the past, cloud users relied on their compliance-based cloud application configurations being implemented by a cloud application provider. The cloud application provider, therefore, centralized the configuration of the cloud application. The cloud application provider had to be trusted to implement the configurations as agreed, implement them as promptly as possible, and make them available to a court in case of a legal dispute (if necessary, to its own disadvantage).

This section has now shown how an IDS can be configured decentrally (not by the cloud application provider) using the architecture developed in 4.2.3. Specifically, it was shown how the blockchain could be used to build an audit trail from the definition of an IDS configuration to the implementation and monitoring of it. The IDS example shows how cloud applications can be configured using the architecture developed in this thesis. At the same time, this example also shows that it is no longer necessary to trust the cloud application provider to implement a cloud configuration. As soon as a cloud application consumer saves a new cloud configuration within the Management Smart Contract, the consumer can track whether the cloud application provider implements it. Traceability is given because the cloud application writes the cryptographic hash value of the virtual instance under which the application runs to the blockchain when it is successfully implemented. Suppose consumers discover that although they have saved the cloud application configuration on the Management Smart Contract, they do not receive any confirmation from the cloud application via the hash value of the virtual instance written to the Management Smart Contract. In that case, the user can be sure that the cloud application did not implement the configuration.

Similarly, a hash value successfully written to the blockchain by the cloud application indicates that a configuration has been successfully implemented in the cloud application. If a dispute arises, the hash value written to the Management Smart Contract and the associated virtual instance can be used to identify the exact cause of the error and the person responsible in the event of a misconfiguration. As a result, the cloud application provider no longer has to be trusted to implement the cloud application, but the blockchain since error identification is now based purely on blockchain entries. Consequently, this represents a trust shift from the cloud application provider to the blockchain. Finally, this shift of trust fulfills the goal of this dissertation. The following chapter examines the degree to which the trust shift to the blockchain ensures that adoption risks are reduced. In other words, it must be investigated whether shifting trust to the blockchain also reduces the adoption risk of cloud applications, which is the assumption of this dissertation.

4.3 DISCUSSION

RQ6 asked what an application to shift trust from the cloud provider to the blockchain could look like. Through the focus group discussion (see 3.2) and the systematic literature review (see 3.3), this research showed that new software architecture is needed to overcome the existing limitations of cloud applications. For the development of the new software architecture, the RAD method was used (see 2.1.4). A software prototype was developed using an iterative approach.

In the first phase, the general requirements for the architecture were collected (see 4.2.1). Requirements engineering was used to translate the requirements identified in RQ1 into use cases. The goal was to design an architecture that enables cloud applications' transparent, automated, and notarized configuration. The use cases were then transferred into a general software architecture with associated communication relationships.

Based on the collected requirements, the software architecture's theoretical design could be derived (see 4.2.2). This architecture was explicitly designed to be used for a variety of cloud applications. Based on the components of Management Smart Contract, Cloud Management Script, and Consumer Management Script, it was possible to design a theorized concept that enables the shift of trust to the blockchain.

The theoretical software architecture was then implemented as a PoC (see 4.2.3). By implementing the PoC, it was possible to show that the theoretical architecture works in practice. During the implementation process, theoretical requirements from the architecture had to be translated into concrete steps. For this purpose, general concepts such as the shared symmetric key generation of all parties, the encryption and decryption of configurations, and the hashing of backups had to be implemented using explicit functions.

It should be noted that the algorithms used here are not unique. Rather, algorithms such as threshold schemes or multiparty computation could also be used to generate a shared key. The choice of encryption and decryption algorithms could also be different in future implementations. The deciding factor here is that the requirements set in the architecture are fulfilled.

Finally, the backup can be hashed using other hashing functions. The specific implementation of the architecture made it possible to make it available for cloud applications in a live environment. Initial testing of the application has shown that hashing might be the current bottleneck of the architecture. Processing times of up to 10 minutes were possible here. In other words, this ensures that configurations can only be changed about every 10 minutes. This may be sufficient for configuring backup frequencies since the backup strategy in a company is rarely adjusted. However, this may not be sufficient for services that require rapid configuration changes, such as services for load-balancing network traffic. Load balancers must decide in real time which server has the lowest possible load and redirect network traffic to these services. A reconfiguration of 10 minutes would severely limit the concept of load balancing. The duration of the hash generation depends mainly on two factors. The hash function and the size of the input are to be hashed.

Further research must show to what extent other hash functions can be used to hash the virtual instance. Or whether it is also sufficient to hash only parts of the virtual instance and not the entire VM. This could reduce the size of the hash input significantly.

In the final phase, the implemented software architecture was used to deploy a concrete cloud application use case (see 4.2.4). Specifically, it was used to deploy an IDS configured via the newly implemented architecture. It remains important to note that the architecture and implementation are not limited to SaaS or IDS applications. The case is merely an example deployment to test the developed PoC in a live environment. The IDS scenario was chosen because IDSes are used in many business environments, are easy to implement, and are familiar to many users.

Overall, utilizing the newly designed software architecture, configurations can now be confidentially stored and retrieved in the blockchain using a smart contract. A digital signature authenticates the storage of a configuration. Hence, it is possible to trace which communication participant stored which configuration at any time. Regular synchronization with the blockchain transfers configuration changes directly to the backend of cloud applications, where they are implemented without delay.

Moreover, implementations of configurations are secured against failure by creating a backup, and the non-reputability of configurations is ensured by creating cryptographical hashes of backups. By digitally signing the cryptographical hash of a backup in a smart contract, it can be uniquely identified and forensically examined in case of doubt. The denial that implementation was not assigned or that a specific participant did not carry out the implementation is hardly possible with the proposed approach; rather, operators must only trust that the blockchain is secure against tampering. Section 4.2 can thus be seen as an answer to RQ6. The next step is to show whether the approach can reduce the adoption risk of cloud applications—and, if so, to what extent.

5 EVALUATION

The previous section presented a software architecture designed for shifting trust and configuring cloud applications toward the blockchain. The design was done in multiple phases following the RAD method (see 2.1.4). Yet, it is still unclear to what extent the developed architecture might reduce the adoption risk of cloud applications. The answer to this is addressed in this chapter.

Thus, this chapter addresses the evaluation of the developed architecture and answers RQ7 (see 1.4.5). As Abowd et al. (1997, pp. 1–2) stated, "A software architecture evaluation assesses the ability of the architecture to support the desired qualities." In recent years, several methods for evaluating software architectures have been presented (Raza et al., 2019). Today, software architecture evaluation approaches can be divided into scenario-based, mathematical modeling, simulation-based, and experience-based methods (Roy & Graham, 2008).

Scenario-based approaches are the most frequently chosen and represent a mature evaluation method for software architecture evaluation (Patidar & Suman, 2015). For these reasons, a scenario-based approach is taken in this dissertation. A scenario briefly describes a single stakeholder interaction with a system (Bass et al., 2003). The scenario-based evaluation methods assess the capability of software architecture for a set of scenarios of interest (Shanmugapriya & M. Suresh, 2012).

Software architectures can be examined based on defined scenarios using the scenario-based evaluation method. The goal of scenario-based software architecture evaluation is to evaluate whether a defined scenario can be executed and how the architecture of software behaves in a defined scenario (Bengtsson et al., 2004). Through the involvement of multiple stakeholders, a detailed software architecture evaluation from different points of view can be achieved. Specifically, a scenario-based evaluation is used in this dissertation to clarify to what extent the developed software architecture (see 4.2) manages to reduce the adoption risk for cloud applications in the identified scope—and, thus, to answer RQ7.

Many concrete scenario-based evaluation methodologies are known from the literature (Shanmugapriya & M. Suresh, 2012). Figure 36 (below) illustrates the general procedure for performing a scenario-based evaluation. The starting point is a problem identified via requirements and design constraints. For this dissertation, these requirements and constraints come from the qualitative analysis of RQ1 (see 3.2).

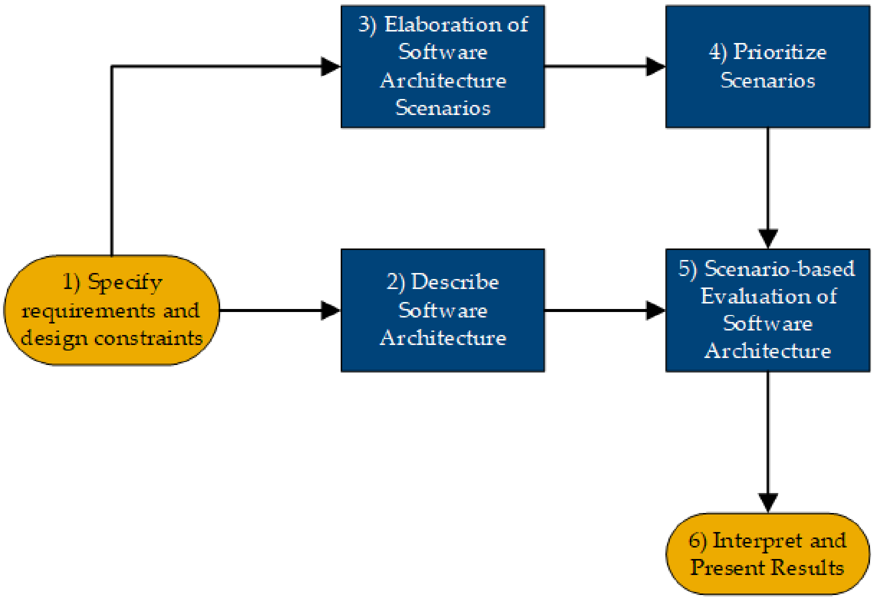

3) Elaboration of Software Architecture Scenarios
4) Prioritize Scenarios
1) Specify requirements and design constraints
2) Describe Software Architecture
5) Scenario-based Evaluation of Software Architecture
6) Interpret and Present Results

Figure 36: General Scenario-based Evaluation Process. (Adapted from Shanmugapriya & M. Suresh, 2012)

The second step is to describe the software architecture. The description of the software architecture used can be found in section 4.2. In the third step, scenarios in which the software architecture is applied must be described. If needed, these scenarios can additionally be prioritized. Finally, the software architecture is then evaluated based on the defined scenarios—the results obtained from the evaluation answer RQ7.

ALMA, developed by Bengtsson et al. (2004), is used to evaluate the architecture described in this dissertation (see 2.1.5 for details on ALMA). The selection of ALMA as a scenario-based software architecture method is especially suitable for this research because ALMA allows the comparison of multiple software architectures (Bengtsson et al., 2004). Based on the ALMA method, selecting the most appropriate architecture for a given scenario is possible. In the context of the dissertation, this means the architecture with the lower adoption risk for a certain scenario in which a cloud application should be configured compliance-driven. The authors of ALMA have demonstrated the ability to compare architectures in the past (Bengtsson et al., 2004). ALMA is carried out in five steps. These five steps are briefly explained in the following sections, and their application to this dissertation is described.

5.1 STEP ONE: SET THE GOAL OF THE EVALUATION

According to the authors of ALMA, this method can be used for three purposes: maintenance cost prediction, risk assessment, and *software architecture selection* (Bengtsson et al., 2004). This dissertation pursues the goal of selecting a software architecture. That is, it aims to compare the existing and the newly developed architecture and to deliver the optimal candidate for the use case. The selection of the architecture is based on the identified compliance-based adoption risk.

Consequently, the architecture that offers a lower overall adoption risk for the identified cloud application (see 3.1.6) will be selected. Hence, the evaluation aims to determine whether this dissertation developed a software architectural approach that reduces cloud applications' compliance-based adoption risk. It will be investigated whether the risks identified in 3.1.6 can be reduced. As a reminder, these risks are:

- The risk is that the cloud application provider does not implement a contractually mutually agreed configuration. (Transparency)
- The risk of delaying configuration changes due to slow or untransparent configuration update processes. (Automation)
- The risk of denying the configuration implementation in case of a dispute. (Non-repudiation)

The evaluation must answer whether the developed software approach can reduce cloud adoption risk, to what extent it can achieve this, and whether it opens up new adoption risks.

5.2 STEP TWO: DESCRIBE SOFTWARE ARCHITECTURE

In the second step, the respective software architectures are described in detail. It is not sufficient to present only a diagram of the architecture. The interaction and architecture components must be named in this phase. For this dissertation, the cloud architecture described in 3.1.1 and the newly developed architecture in this dissertation's context (see 4.2.3) are compared.

5.3 STEP THREE: ELICIT SCENARIOS

Bengtsson et al. (2004, p. 134) describe this step as follows:

> Change scenario elicitation is the process of finding and selecting the change scenarios to be used in the evaluation step. Eliciting change scenarios involves such activities as identifying stakeholders to interview, documenting the scenarios that result from those interviews, etc.

In other words, step three consists of preparing an empirical method and scenario on which the newly developed software architecture should be evaluated. The developed generic software architecture will be examined in various scenarios to determine to what extent the developed architecture can reduce the adoption risk. Therefore, scenarios must be designed in which the two architectures to be compared are used. It is important to ensure that the design includes a wide range of scenarios. This ensures that the developed architecture and the associated trust shift are evaluated across multiple points of view. Examining several scenarios should also provide an answer to the questions of whether there are scenarios for which the developed architecture is more suitable than others and which adoption risks might be more affected by shifting trust to the blockchain.

The scenarios were created using the case study method described by Robert Yin (2017) (see 2.1.5.1). This dissertation performs a multiple-embedded case study to provide broad coverage of the problem's scope. Within these case studies, there is always a cloud adoption scenario. However, the scenarios differ in the following variables:

- *Company Size*: the number of employees in a company
- *Company revenue*: the amount of revenue a company makes
- *Industry*: the sector in which the company operates

- *Compliance Case*: which compliance requirement (e.g., backup location, intrusion detection configuration, website layout, etc.) a company wants to implement using the presented architecture.

Since there are a variety of international compliance and legal requirements, this dissertation's case studies are limited to companies headquartered in Europe (Mishra, 2015).

5.3.1 Scenario A: Medium-sized Company Wants to adopt a Cloud Application from an ISO 27001-certified Company

CompanyA is a medium-sized company (80,000,000€ revenue per year) headquartered in Europe. It employs about 400 people and develops artificial intelligence (AI) software, enabling machine builders to detect failure early. The key to this company’s success is predictive maintenance (Predictive maintenance uses measurement and production data from machines and plants to derive maintenance information. The aim is to maintain the machines and plants and minimize downtimes proactively). The company has been on the market for around ten years and has an ISO27001-certified information security management system (ISMS). The company culture is very open, the management structure is flat (as opposed to hierarchical), and the company is managed by one female CEO. The company's customers are mainly machine and plant manufacturers of larger enterprises, and the corporate culture of the customers is relatively conservative. As a result, innovations take time to implement, and great importance is attached to issues such as personal contact and trust.

CompanyA is now running up against its limits with its accounting and would like to introduce a SaaS-supported accounting software. It is extremely important to the company that the data is stored securely. A data leak due to a hacker attack could lead to the economic end for the company. In this context, CompanyA has chosen the company ProviderA to host the accounting software. This company has an annual turnover of 180,000,000€, is a limited liability company, and is certified according to ISO 27001. Furthermore, ProviderA sells exclusively online and has its headquarters in Europe.

5.3.2 Scenario B: Large-sized Company Wants to Adopt a Cloud Application from a Low-cost Supplier

CompanyB is a global player with its head office in Europe. It employs 80,000 people and specializes in producing chemical products (16,000,000,000€ revenue per year). The company has been in the market for about 100 years and is certified with all current international pharmaceutical, chemical, quality, and safety certifications. Support services such as human resources, IT, and logistics are outsourced to subcontractors and managed by small teams at the head office. The company culture is open but hierarchical. A board of nine members manages the company. The company's customers are mainly pharmaceutical, food, and chemical companies. The company culture among the customers is very mixed, and there is no clear tendency to modern or conservative company culture. Personal contact exists only with large customers. Many transactions are carried out online without direct contact.

Environmental activists often criticize CompanyB since it uses non-renewable resources for its production. Therefore, it has often happened that activists have tried to hack into CompanyB's network. CompanyB has drawn up a precise list of intrusion detection rules to detect attackers at an early stage. CompanyB would now like the subcontractor responsible for the network to implement these rules. Based on CompanyB's policy of choosing the lowest price of three offers, ProviderB was selected. This company has an annual turnover of 20,000,000€, no certifications but a Google Rating of 4.3 out of 5 (from 400 ratings) and is a limited liability company. Furthermore, ProviderB sells exclusively by means of a sales and consultant service. ProviderB has its headquarters in India.

5.3.3 Scenario C: Regional Group Wants to Run a Website from the Existing Software Provider

CompanyC is an association of several farmers from one region in Europe with a current revenue of 500,000€ per year. The association consists of seven farmers who aim to sell their goods locally on the market and across the region via the Internet. The company was founded a few weeks ago. The owners are not very tech-savvy and want to rely on a SaaS-based Enterprise Resource Planning (ERP) system to expend as little IT effort as possible. The customers of CompanyC are mainly young people and families with higher incomes. Personal contact is only available in the market; online customers have no personal contact with CompanyC. CompanyC needs to be able to make quick adjustments on the website. CompanyC also wishes to minimize the number of goods thrown away, so goods about to expire must be advertised more prominently online. Here CompanyC has chosen the company ProviderC, as they already have other licenses at CompanyC and offer a free SaaS service. This company has an annual turnover of 100,000,000,000€ and is a publicly-traded company. ProviderC is a global corporation with its headquarters in the USA.

Furthermore, ProviderC sells its software exclusively online. Sales and consultant services can be booked against additional payment. ProviderC is certified according to all current worldwide certifications.

5.4 STEP FOUR: EVALUATE SCENARIOS

This step is a question of examining the effects of the two software architectures on the respective scenarios (Bengtsson et al., 2004). Bengtsson et al. (2004) do not prescribe a specific method for this. Rather, the authors recommend a quantitative or qualitative method suitable for achieving the evaluation goal. As described in 2.1.5.2, interviewing experts is ideal for viewing and evaluating the targeted software architectures from different perspectives. Hence, this dissertation uses the method of expert interviews for risk rating the provided software architectures in the described scenarios.

The challenge with expert interviews is determining what an expert is in the relevant field (Flick, 2018). Besides the criteria of 3.2.1.1, this dissertation relies on the participants' self-evaluation. Each interviewee was given several interview questions during the interview and asked to answer them. There are no specifications for the interviewee regarding the answer to the question. Rather, interviewees can set their priorities and digress from the actual question with their answers.

The interview guide was created based on the current literature by W.C. Adams (2015). In his paper, W.C. Adams developed a four-phase framework for conducting semi-structured expert interviews. Based on the phases—(1) selecting and recruiting the respondents, (2) drafting the questions and interview guide, (3) techniques for this type of interview, and (4) analyzing the information gathered—the software architectures were evaluated.

5.4.1 Selecting and Recruiting the Respondents

As shown in the focus group discussion (see 3.2), the environment in which the dissertation's problem occurs is primarily the business environment. More specifically, in the environment of managers, IT employees, and cloud users. According to W.C. Adams (2015), the interviewed persons (interviewees) must come from this environment. However, W.C. Adams (2015) keeps open how many people should be interviewed, as this may depend heavily on the topic. The author randomly selected persons from the target environment out of his network. The selection of evaluation participants was done randomly using a random number generator, as described below. The environment in which this dissertation move is the business environment. To avoid conducting the interviews too long and thus overloading the participants with new information, persons will be selected from the described environment who probably understand the architecture presented in this dissertation as quickly as possible. Specifically, the author of this dissertation has identified the following expert areas: cloud computing, computer science, cybersecurity, or cryptography (and blockchain). The selection of random participants should ensure that participants are not selected based on personal bias or personal preferences of the author. Expert interviews are conducted until saturation of the answers, i.e., no more new insights can be gained via interviews.

The exact number of necessary participants is determined according to the procedure described by Guest et al. (2006). Guest et al. (2006) have shown that twelve participants are usually sufficient to achieve saturation on average. This dissertation follows Guest et al. (2006) in choosing this number of participants. For the purpose of selecting the twelve experts to be interviewed, 31 potential interview partners were identified from the author's network. These persons were numbered from Participant #1 to Participant #31. Subsequently, twelve numbers were drawn using an equally distributed random number generator. The drawn participants were then invited to the interview.

It should be noted that twelve participants are the initial upper limit of the interviews. If a settlement of the statements is already apparent beforehand, not all twelve candidates will be interviewed. The same applies if, after twelve statements, there are still no signs of settlement. If the evaluation shows that the statements are not yet saturated, additional interview partners must be randomly selected from the pool.

Due to the ongoing Covid-19 pandemic in 2021 and 2022, participants were invited for interviews via video conference. The interviews were conducted using Microsoft Teams and recorded, with the interviewees' consent, for later transcription. Since all participants had been working in the home office for at least one year at the time of the interviews, the author of this study did not anticipate that conducting virtual interviews would negatively impact data quality.

5.4.2 Drafting the Questions and Interview Guide

The semi-structured expert interview guide was developed based on the current literature and existing theoretical knowledge. It includes research-relevant questions and narrative prompts for the interview and serves as a "baseline" for the conversation. In the first step, all thematically possible questions were collected without elaborating them in detail. In the second step, the collection was reviewed and reduced to those questions most relevant to the research interest and the expected answer. The questions were structured according to a logical and content-related sequence. In other words, the interview starts with a brief explanation of the objective of the interview. This is followed by a questioning of the experts about their background. Next, the interview moves on to the main part. In the main part, the actual architecture evaluation takes place. Finally, the interview is closed with a thank you and further information about the course of the dissertation.

The interview guide contains both qualitative and quantitative elements. Thus, the response to RQ7 was not purely qualitative but a mixed-method approach (Tashakkori et al., 1998). To be more precise, it was an embedded mixed-method approach. In this approach, a dominant method is combined with a subordinate method (Doyle et al., 2009). In answering RQ7, the qualitative part dominated, and a quantitative part was used to support the qualitative statements. The interview guide is structured so that the interview begins with an information phase in which the interviewer asks the interviewee to explain their motive for the interview and necessary background knowledge.

After polishing the interview techniques (see 5.4.3), the SSI consists of five phases with 26 questions. Each aims to obtain as much information as possible to answer the research question. The elaborated interview guide is provided in Appendix B. All interview questions were reviewed according to W.C. Adams's (2015) SSI guide, paraphrased, and explained in the context of this research below:

1. Allow enough time for pretesting and conducting interviews. Five months were allotted for planning, creating, testing, and conducting the interviews. The preparation of the interviews started in December 2021, allowing a buffer until June 2022.
2. The agenda was structured as described above and contained essentially (besides the introduction and the conclusion) only relevant aspects for evaluating the dissertation.
3. Where possible, open questions were used. These leave room for the interviewee to answer and reduce bias (W. C. Adams, 2015).
4. All interviewees are non-native English speakers. To ensure transparency and avoid translation errors, all interviews were prepared and conducted in English. Before the interviews were conducted, all interviewees were informed that they could use a dictionary or translator at any time to compensate for missing vocabulary or to check words' meanings in case of uncertainty. The dissertation's author is aware that there may be minor translation errors or misuse of words. However, this is acceptable since the focus is on overall statements rather than on the exact meaning of individual words. If the meaning of a single word is of precise importance, the interviewer asked the interviewee if the chosen word was meant that way.
5. Among other things, the pretest checked whether any questions asked could be considered awkward or personal. At the same time, it was also checked whether one of the questions could cause a social bias (i.e., lead the interviewee to produce a socially-expected answer). The pretest with two persons did not reveal any of the abovementioned aspects.
6. Attention was paid to the establishment of the most natural interview flow. For this purpose, questions were divided into thematic groups. The division of topics into these groups ensured that all open points from a

thematic block were clarified first before jumping to the next thematic point. However, the author also acknowledges that skipping or returning to topics outside of thematic order can never be ruled out in an SSI. If there were jumps in the questions, the skipped questions were taken up again afterward.

As already noted, the SSI contains both quantitative and qualitative elements. The qualitative elements were evaluated utilizing the qualitative analysis described by Mayring (see 2.1.5.3). For this purpose, deductive categories were formed based on the literature of Bengtsson et al. (2004). The resulting categorization is:

- Architecture requirements
- Notes on the architecture
- Risk Management
- Wishes or Requests

A revision of the categorization to optimize the category system was planned after the interview phase. The steps of the interview process are now described in detail.

A warm-up and introductory phase follow the information phase to create a pleasant narrative flow and request relevant information. This phase contains qualitative and quantitative elements to assess the interviewee's background. The mixture of methods makes it possible to establish connections between statements and expertise later in the evaluation (Tashakkori et al., 1998). The main phase then starts with a quantitative part. For the main phase, the scenarios defined in 5.3 were presented to the interviewed participants. Once the case studies were presented to the participants and the interviewer ensured that the participants understood the case studies, the evaluation began.

The first step in each interview was ensuring that the participants understood the risk management described in 3.1.4 and that they could apply the risk matrix shown in Table 7, below. The risk matrix is a 5x4 risk matrix based on the risk management standard ISO 31000 (Purdy, 2010). The y-axis shows the probability of a risk occurring, while the x-axis shows the expected impact on the company (in euros). The amount of risk is then calculated from the probability and the impact.

It should be noted that the impact is viewed relative to the company's annual turnover. Consequently, the absolute impact values differ for two companies with different annual turnovers and the same impact class. The risk values can be displayed either as numbers or as text. For easier processing, words were used to describe risks later transferred to quantitative values. The risk values 1 (Low), 2 (Medium), 3 (High), and 4 (Very High) are used for this work. Risk assessments are therefore measured quantitatively by the participants. In the later evaluation, this allows a clear comparison of the risks from both architectures. Since the distances between the values cannot be interpreted, risks are measured on an ordinal scale (Gomez & Mouselli, 2018).

Table 7: Risk Matrix

Probability	**Impact**			
	Negligible [<10%] Turnover / Year	Marginal [>=10%, < 30%] Turnover / Year	Critical [>=30%, < 80%] Turnover / Year	Catastrophic [>80%] Turnover / Year
Certain [>= 90%]	High	High	Very high	Very high
Likely [>= 60%, <90%]	Medium	High	High	Very high
Possible [>= 30%, <60%]	Low	Medium	High	Very high
Unlikely [>= 10%, <30%]	Low	Medium	Medium	High
Rare [<10%]	Low	Low	Medium	Medium

Once the participants have understood the scenarios, the risk management process, and the risk matrix, the quantitative risk assessment starts. During this assessment, the participants are first asked to rate the three adoption risks based on the architecture currently known to them for compliance-driven configuring cloud applications. Consequently, each participant has given nine risk scores at the end of the first risk assessment. It should be noted that the participants are not yet familiar with the architectural approach developed in this dissertation. The risk assessment is initially based solely on the currently-known cloud adoption process.

The architecture developed in this dissertation is presented to the participants in the next step of the main phase. Subsequently, the participants are asked to perform a risk evaluation based on the newly presented architecture. To be more precise, the participants are asked to assume that the provider from the scenarios offers its cloud application with the architecture developed in this dissertation. Participants are then asked to perform the adoption risk assessment, assuming the architecture developed in this dissertation. In general, the only change in assumptions on the part of the participants is that for the new architecture, they must assume the blockchain is a secure implementation. Implementation errors on the provider's end or internal attackers remain a possibility.

After the participants have also assessed the risks under the newly presented architecture, the qualitative part of the main phase starts. In the qualitative part, participants are asked for their opinions on the new architecture. Specifically, they are asked whether the use of blockchain in the example presented appears useful. The participants are additionally asked how they would evaluate the topics of transparency, automation, and non-repudiation (notarization) in the approach presented. As the conclusion of the main part, the participants have the opportunity to add points, give tips, or talk about newly emerging risks. As soon as there is nothing more to add, the interview's main phase ends. It then continues to the closing phase.

In the closing phase, each participant is asked to use school grades (1 - very good, 2 - good, 3 - satisfactory, 4 - sufficient, 5 - poor, 6 - insufficient) to rate their own experience in the presented topic area. Based on the self-assigned grades, it is possible to decide whether the interviewer is an expert or not when analyzing the interviews. Interviewees rated lower than 4 (sufficient) are not considered experts and were not admitted for the evaluation. Participants are thanked for participating in the closing information phase, and the interview is concluded.

5.4.3 Polishing Interview Techniques

As recommended by W.C. Adams (2015), care was taken during the interviews to ensure that participants were comfortable. For example, it was communicated that participants might change their answers at any time or jump back to a question. It is also important that participants are not forced to answer. Questions can be skipped or left open at any time. Overall, a passive interviewer role is assumed. The participants were only asked to follow up with questions in case of ambiguities or problems understanding. Therefore, the author's participation in the interviews is not a limitation of this work.

5.4.4 Conducting the Data Collection

After the interview was created according to the SSI guide described by W.C. Adams (2015), the SSIs were conducted. The conduction included the organization of a pretest. The purpose of the pretest is to optimize the guideline questionnaire before the actual data collection begins. The pretest is conducted with test subjects not part of the sample. The test phase makes it possible to check the questionnaire's structure and the questions' comprehensibility. The first pretest showed that the initial questionnaire contained too many questions and general formulations. The pretest also showed that the predefined case studies were not precise enough. These possibilities for improvement were then integrated into the questionnaire. The guidelines were optimized so that the questions contained qualitative and quantitative elements.

The pretest showed that a qualitative assessment of risks is very subjective. Therefore, the answers to RQ7 would also be highly subjective. Hence, in addition to qualitative criteria, the quantitative assessment of risk using a risk matrix was added. Furthermore, the question blocks or individual questions were supplemented with additional information so that the context of the question is more clearly emphasized and the interpretation of the questions is easier. A second pretest showed fewer understanding issues and a more objective risk assessment of the presented architectures. Overall, the pretests led to the guide being optimized. The final revised interview guide can be found in Appendix B.

As mentioned in 5.4.1, the interview participants were contacted in advance and asked to participate voluntarily. Before data collection, a data use and privacy consent form was sent to the interview participants for clarification and signature. The consent form template is attached in Appendix C.

Before the interview, organizational information was discussed with the person to be interviewed. The recording was then started, and the interview was conducted. After the interview, an outlook on the next steps and thanks for participation were provided.

Immediately after the interview, the interview recording was transcribed. Transcription of the interviews was carried out as described in 2.1.5.2. The transcripts can be found in Appendix D.

5.5 STEP FIVE: INTERPRET THE RESULTS

The following chapter describes the analysis method for the interview results, followed by a presentation of the results. While conducting the expert interviews, a rapid saturation of the statements became apparent. Consequently, a total of 11 experts were interviewed.

5.5.1 Qualitative Content Analysis

The survey results were evaluated based on the qualitative content analysis according to Mayring (2000). The evaluation was carried out according to the method described in 2.1.5.3. The qualitative content analysis focuses on forming categories (Mayring, 2000). The totality of all categories represents the category system. Categories can be formed either in advance and independently of the data material (deductively) or based on the data material during the content analysis (inductively).

5.5.2 Categorization and Coding of the Interview Results

An initial category system was formed deductively based on the literature review and research question in 5.4.2, allowing for more objective interpretation and comparability of the responses. After completing the research phase and reviewing the data material, an inductive reworking of the category system resulted since additional topic areas were revealed. In particular, the deductive categories were further detailed to delineate better the data obtained. The following categories resulted inductively:

- Background and Knowledge
- Case Study
- Risk Management
- Trust Management
- Architecture Notes
- Blockchain
- Wishes or Requests

The text material was coded using these inductive categories and MAXQDA Analytics Pro 2022 software.

5.5.3 Describing and Evaluating the Results

In the following, the results from the interviews—and thus the evaluation results—are presented and interpreted. The results are presented based on the predefined categories. Within each category, the answers of all interview participants are presented. Since the survey is a mixed-methods approach, qualitative and quantitative statements are presented in the categories.

5.5.3.1 Background and Knowledge

Interviewee #1 works as a software engineering research assistant at a university. Interviewee #1 has a master's degree in computer science and about one year of professional experience. Quantitative Statements:

- I am a computer science expert: *agree*
- I am an information security expert: *neutral*
- I am a cloud computing expert: *disagree*
- I am a cryptography expert: *agree*

Interviewee #2 works as an Information Security Specialist with more than one year of professional experience in a medium-sized company. Interviewee #2 is responsible for penetration testing, maintaining ISO 27001 certification, and securing software development. Interviewee #2 has a master's degree in computer science. Quantitative Statements:

- I am a computer science expert: *strongly agree*
- I am an information security expert: *strongly agree*
- I am a cloud computing expert: *agree*
- I am a cryptography expert: *agree*

Interviewee #3 works as a Development Operations (DevOps) Specialist with more than three years of professional experience in a medium-sized company that develops, sells, and operates cloud applications. Interviewee #3 is mainly responsible for deploying and configuring cloud applications and has regular customer contact. Interviewee #3 has a master's degree in mechanical engineering, focusing on service and software. Quantitative statements:

- I am a computer science expert: *agree*
- I am an information security expert: *neutral*
- I am a cloud computing expert: *agree*
- I am a cryptography expert: *disagree*

Interviewee #4 works as Chief Technology Officer (CTO) in a mid-sized software company. Interviewee #4 advises customers on adopting cloud applications and has internal technical responsibility for developing several cloud solutions. Interviewee #4 has a diploma in computer science (comparable to a master's degree). Quantitative statements:

- I am a computer science expert: strongly *agree*
- I am an information security expert: *agree*
- I am a cloud computing expert: *agree*
- I am a cryptography expert: *agree*

Interviewee #5 works as a Development Operations (DevOps) Specialist with more than one year of professional experience in a research institute and mainly supports the smooth operation of cloud-based software applications within a research institute. The research focus of the institute is energy and climate research. Interviewee #5 has a master's degree in computer science. Quantitative statements:

- I am a computer science expert: *agree*

- I am an information security expert: *agree*
- I am a cloud computing expert: *agree*
- I am a cryptography expert: *neutral*

Interviewee #6 has more than 15 years of professional software architecture and testing experience. Interviewee #6 works for a medium-sized company in software analysis and testing. Interviewee #6 has completed an apprenticeship as an IT specialist and started studying in the field of computer science. Quantitative Statements:

- I am a computer science expert: *agree*
- I am an information security expert: *agree*
- I am a cloud computing expert: *neutral*
- I am a cryptography expert: *disagree*

Interviewee #7 has worked as a system administrator and technical consultant. Interviewee #7 is currently responsible for administering a cloud-based email service and is the main contact person for questions regarding application configuration. Interviewee #7 has more than 15 years of professional experience in information technology and has completed an apprenticeship and started studying computer science. Quantitative Statements:

- I am a computer science expert: *strongly agree*
- I am an information security expert: *agree*
- I am a cloud computing expert: *agree*
- I am a cryptography expert: *neutral*

Interviewee #8 is a specialist in high-performance computing. Interviewee #8 is a master's student at a university with more than two years of experience teaching computer science mentees. Interviewee #8 focuses on benchmarking high-performance computers. Interviewee #8 has a bachelor's degree in computer science. Quantitative Statements:

- I am a computer science expert: *strongly agree*
- I am an information security expert: *strongly agree*
- I am a cloud computing expert: *agree*
- I am a cryptography expert: *agree*

Interviewee #9 works as an Information Security Consultant and data leakage specialist with more than twelve years of professional experience in finance companies. Interviewee #9 is responsible for leakage prevention and incident management and has a master's degree in computer science. Quantitative Statements:

- I am a computer science expert: *agree*
- I am an information security expert: *strongly agree*
- I am a cloud computing expert: *disagree*
- I am a cryptography *neutral*

Interviewee #10 works as a Team Lead for cloud application provisioning and has more than 14 years of professional experience in governmental positions and large-size companies. Interviewee #10 is responsible for team management and the strategic cloud application positioning of a large company in the food section. Interviewee #10 has an apprenticeship in a computer science-related subject. Quantitative Statements:

- I am a computer science expert: *agree*
- I am an information security expert: *agree*
- I am a cloud computing expert: *strongly agree*
- I am a cryptography expert: *neutral*

Interviewee #11 is a Security and DevOps team leader in a mid-size company with more than ten years of professional work experience. Interviewee #1 is responsible for team leading, maintaining ISO 27001 certification, DevOps tasks, maintaining the IT infrastructure, and securing software development. Interviewee #11 has a Ph.D. in computer science. Quantitative Statements:

- I am a computer science expert: *strongly agree*
- I am an information security expert: *strongly agree*
- I am a cloud computing expert: *strongly agree*
- I am a cryptography expert: *strongly agree*

5.5.3.2 Case Study

All interviewed participants stated that they understood the presented case study. Furthermore, all participants stated that the presented cases seemed realistic and representative of real-world scenarios. No concerns were expressed about the scope or bias within the cases described.

5.5.3.3 Risk Management

The evaluation was based on the ALMA approach. The approach aims to find the appropriate architecture for a specific use case. In the context of this dissertation, the appropriate architecture was understood to be the architecture with the lower overall adoption risk for the respective cloud application from the scenario case studies. Based on the three adoption risks presented in this dissertation, the experts were asked to evaluate the adoption risk for the respective scenarios (see 5.3). On the one hand, the experts were asked to assess the adoption risk based on a comparison of the cloud applications' currently used configuration mechanisms and the architecture presented in this dissertation. The participants were also asked whether risk management was the right approach for evaluating the software architecture. In other words, they were asked whether they would consider it useful to perform a risk assessment for the adoption decision in the case studies presented. All participants indicated that they understand the cases presented and would consider risk management extremely useful for decision support.

5.5.3.4 Trust Management

All of the people interviewed agreed that it makes sense to shift trust away from the cloud application provider to a third, independent party. The main goal to be achieved here is a more tamper-proof audit trail. In other words, any configuration change must be stored in a tamper-proof way to achieve a trusted configuration of cloud applications. Interviewee #9 noted,

> *Having some kind of audit trail makes things more transparent. That's the reason why all auditors I know who performs here his audits, for example, like [Organization] once in an audit trail and through, it's one of the key requirements for example, German insurances, for German banks to have some kind of audit trail where you can see who did at which time which changes. So, I think in case of transparency, it [audit trail] really matters there.*

Most participants also see the blockchain as the appropriate technology for this purpose. For example, Interviewee #10 stated: "we implement things like the blockchain where we're documenting a lot of things in a way that can't be changed without a log. That's the best way for investigation, and sounds good."

5.5.3.5 Architecture Notes

Interviewee #1 noted that the risk could be further reduced if an implementation error on the part of the cloud provider could be ruled out or checked. Interviewee #1 sees the highest improvement potential for the presented approach here. Interviewee #1 suggested a black box testing approach, with which the correct implementation of the approach on the part of the cloud application provider could be checked via the blockchain.

> *That would be […] having some sort of verification or tests system for the cloud application that the consumer can, so that the consumer has as a way to verify, or at least test if the cloud application is working as intended. So, at the very least some sort of black box testing would be nice, which could also start the results on the blockchain if you want to*

In this context, black-box testing refers to a software testing method (Pressman, 2005). In black box testing, tests are developed based on the specification or requirement. In other words, tests are developed without any knowledge of the inner workings or, in the case mentioned by Interviewee #1, the implementation of the system under test. The program to be tested is thus treated as a black box. Only externally visible behavior is included in the test. The black box test is therefore used to determine whether the architecture presented in this dissertation has been implemented correctly by the cloud application provider. To do this, a customer must first define the output expected from the black box, given a certain input. Specifically, customers could specify that they expect a hash value as a response when a correct cloud configuration is entered. Finally, using the black box test, it is possible to check whether the cloud application provider has correctly implemented the architecture without requiring direct access to its source code. Similar comments were made by Interviewee #11. The interviewee noted that

> *It [the architecture] makes sense for configuration changes in general. Yeah. I think there is complexity into the different types of configuration changes. And also if you have very frequent changes, then also towards maintaining sizing of the blockchain and computation power and so on. Yeah, depending on the use case, if you have a lot of changes all the time,*

> *then it could be technical issues also triggering all the time backups here and so on. Yeah. But in general it makes sense. Definitely.*

Hence, Interviewee #11 also mentioned that the proposed architecture might not be suitable for all kinds of use cases. Especially for use cases requiring frequent configuration changes, the proposed architecture might have limitations.

5.5.3.6 Blockchain

As already noted, most participants find the blockchain-based approach extremely useful, as it does not require trust (in contrast, e.g., to Web PKI providers). All interviewees agree with the statement that the approach presented in this dissertation shifts trust to the blockchain. However, Interviewee #9 noted that the blockchain might not be the only technology to achieve this goal. As mentioned in 3.1.9, various trust management technologies like Web PKI or Web of Trust exist. Interviewee #9 noted that those technologies might be useful as well for shifting trust.

However, as seen in section 3.1.9, the presented solutions have different limitations. Smart contracts allow for the storage of configurations. Other approaches like Web PKI or Web of Trust do not come with trusted data storage. Additional data storage for saving the cloud configurations would be needed if these technologies were used rather than the blockchain. Hence, it might be possible to use other trusted third parties for shifting trust; however, those come with further limitations.

5.5.3.7 Wishes or Requests

Interviewee #1 noted that an ISO certificate, for example, is a useful way to build trust initially. Therefore, the approach presented should not be seen as an alternative to a certificate but rather as an extended mechanism to establish trust and reduce the adoption risk. Overall, few technical wishes were expressed for improving the architecture. The wishes were more process-oriented or directed at the change management required to introduce the newly presented architecture. Overall, it can be stated that the participants would like to have a mechanism for independent verification of the implementation. Similar to cryptographic methods, the implementation of the architecture presented in this dissertation must be trusted to be implemented correctly by the provider. This is where the participants see the biggest trust problem and risk of the presented approach. Furthermore, it must also be considered to what extent the architecture presented can be used for rapid configuration changes and how it can be ensured that the cloud application consumer has access to the backups created. Here, the participants would still like to see clear processes.

5.6 ANSWERING RQ 7

After analyzing the expert interviews, the next step is to answer RQ7. A total of 12 experts were selected for potential questioning. While conducting the expert interviews, a rapid saturation of the statements became apparent. Consequently, a total of 11 experts were interviewed. As shown in section 5.5.3, all experts had a computer science background. Experts with and without a leadership role were interviewed. All experts interpreted the presented case studies as realistic and having a broad scope.

The broad scope of the case study was also reflected later in the risk assessment. The same risks were evaluated differently in the individual case studies. It can be assumed that experts assessed the scenarios differently and had different risk perceptions. When asked about their experience with risk management, it became clear that all experts were familiar with the concept of a risk matrix.

Consequently, the interviewed experts quickly learned the risk matrix presented for evaluation. Overall, the risk matrix presented was rated as a realistic instrument for risk assessment. The risks presented were likewise considered to be realistic. All interviewed experts confirmed the existence of the three presented adoption risks. Conducting a risk assessment to determine the adoption risk was considered common practice—and rated as useful for the adoption cases presented—by all experts interviewed. The three risks—transparency, automation, and repudiation —were first considered separately to answer if and how far the architecture presented can reduce the adoption risk.

To compare whether a significant reduction in adoption risks could be achieved, nonparametric statistical tests were performed. Based on the initial analysis of the data and the pre-test, it could be assumed that the data (risks) are not nearly normally distributed. Therefore, not all requirements for the application of the *t*-test are met (Dexter, 2013). As an alternative to the *t*-test, the Wilcoxon-Mann-Whitney test (*U*-test) is used in this dissertation (Dexter, 2013). The Mann-Whitney *U*-test is a non-parametric alternative to the unpaired *t*-test (Larsen & Marx, 2005). Remember, parametric tests require the underlying distribution of the data to be known a priori (Larsen & Marx, 2005). The *t*-test is a parametric test that expects normally distributed data (Larsen & Marx, 2005). Non-parametric tests, such as the Mann-Whitney *U*-test, are used when the underlying data are not under a prior known distribution (Larsen & Marx, 2005). In particular, the *U*-test tests whether two independent samples are from the same population. *U*-tests are used primarily when the data are ordinally scaled or (as in the present case) the analyzed data is not normally distributed (Larsen & Marx, 2005). Non-parametric tests ignore the underlying distribution of the data. Therefore, non-parametric distributions are generally weaker than parameterized tests (Larsen & Marx, 2005). Therefore, the prediction of results is less accurate than using a *t*-test. However, as will be shown later, this is not a limitation since the results from the *U*-test are all very clear and well above the critical *U*-test values (see (Larsen & Marx, 2005)).

The Mann-Whitney *U*-test is used in psychology, for example, to compare attitudes or behaviors between two different groups. In medicine, it is used to compare the effects of two drugs. In marketing, it can be used to compare preferences for a product between men and women. (Larsen & Marx, 2005)

Eleven participants were asked to determine the adoption risk of two cloud architectures: the Existing Architecture (EA) and the Proposed Architecture (PA). There were three scenarios for each architecture—Scenario A, Scenario B, and Scenario C (see 5.3). Each scenario was assessed for three risks (see 1.3): transparency, automation, and non-repudiation.

Consequently, 18 risk values per participant were determined (2 architectures * 3 scenarios * 3 risks). A summary of the 18 risk values is shown in Table 8, below. Each of the 18 risk values is composed of 11 values for EA and 11 for PA. These 11 values reflect the ratings of the 11 interviewed participants. The data representation showed that the distributions of EA and PA of the 18 risk values are not nearly normal. The *U*-value is therefore formed based on each scenario and risk between the two architectures available for selection. Thus, a total of 9 *U*-values are determined. Since it has shown its value in the statistical analysis, the statistical tool R was used to calculate the *U*-value and the corresponding *p*-value (Larsen & Marx, 2005). It was examined whether the central tendencies of two independent samples, EA and PA, are different.

H_0: *The probability of an observation from the two distributions (EA and PA) is the same for each of the two distributions (in other words, the distributions are the same).*

H_A: The probability of an observation from the two distributions (EA and PA) is not the same for each of the two distributions (in other words: the distributions are not the same).

Since the *U*-test initially only provides exclusion of the population, the dissertation also calculates the standard deviation (SD) and distribution of the nine studies. If the SDs are nearly similar and the distribution is the same, but the *U*-value is different, it can be concluded that the mean values of the two architectures differ and that the risk in the mean value has been reduced. The H_0 is discarded for $p < 0.05$.

Table 8: Data Description Risk Assessment

Architecture	Scenario	Risk	Short	N	Mean	SD	Median	Min	Max
EA	A	1	EA_A1	11	2.73	0.47	3	2	3
PA	A	1	PA_A1	11	2.00	0.63	2	1	3
EA	B	1	EA_B1	11	3.18	0.98	3	1	4
PA	B	1	PA_B1	11	2.27	0.79	2	1	3
EA	C	1	EA_C1	11	1.82	1.08	1	1	4
PA	C	1	PA_C1	11	1.45	0.93	1	1	4
EA	A	2	EA_A2	11	2.18	0.60	2	1	3
PA	A	2	PA_A2	11	1.73	0.79	2	1	3
EA	B	2	EA_B2	11	2.18	0.75	2	1	3
PA	B	2	PA_B2	11	1.82	0.98	1	1	3
EA	C	2	EA_C2	11	2.00	1.00	2	1	4
PA	C	2	PA_C2	11	1.73	1.01	1	1	4
EA	A	3	EA_A3	11	2.64	1.03	3	1	4
PA	A	3	PA_A3	11	1.27	0.47	1	1	2
EA	B	3	EA_B3	11	3.00	0.77	3	2	4
PA	B	3	PA_B3	11	1.45	0.93	1	1	4
EA	C	3	EA_C3	11	2.09	1.14	2	1	4
PA	C	3	PA_C3	11	1.36	0.67	1	1	3

5.6.1 Transparency Risk

Figure 37, below, shows the evaluation of the transparency risk for Scenario A, Scenario B, and Scenario C. It remains to mention that the average was created for orientation purposes only. The risks' reasoning and evaluation are based on the median due to the underlying ordinal scale. On average, the experts rated the transparency adoption risk in the EA for Scenario A as 2.73, Scenario B as 3.18, and Scenario C as 1.82. Overall, it was also shown that in the mean value, the greatest transparency risk lies with ProviderB. The high transparency risk was mainly justified by the location of ProviderB, the low turnover, and the lack of external certifications in ProviderB (see 5.3.2).

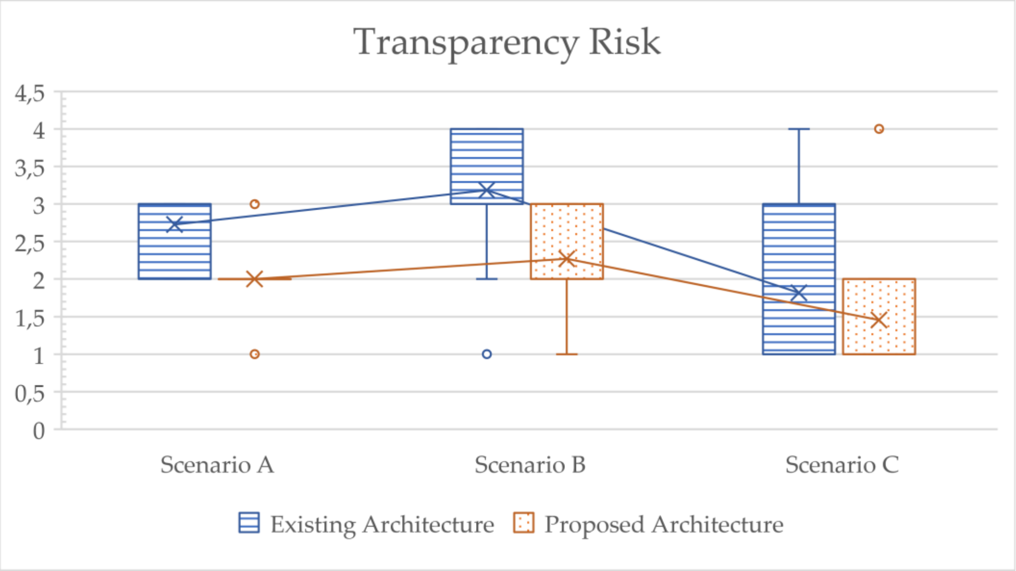


Figure 37: Results Transparency Risk Assessment Existing vs. Proposed Architecture

Compared with the architecture developed in this dissertation, Scenario A reached a value of 2.00, Scenario B had an average value of 2.27, and Scenario C had an average value of 1.45.

When looking at the *U*-test in Table 9, below, it is noticeable that H_0 must be rejected for Scenario A and Scenario B. Furthermore, in Table 9 it is also noticeable that the SDs are close to each other, and the distributions are the same. Overall, it can be concluded that the transparency risk for Scenario A and Scenario B could be significantly reduced. In Scenario A a *p*-value of 0.009 was calculated, and in

Scenario B, a p-value of 0.021 was calculated. There is no significant improvement for Scenario C (p-value of 0.359), and H_0 is accepted.

Table 9: Transparency Risk Results and p-Values

Participant #	Architecture	Risk	Rate A	Rate B	Rate C
1	EA	Transparency	3	2	3
2	EA	Transparency	3	1	3
3	EA	Transparency	2	2	2
4	EA	Transparency	2	2	1
5	EA	Transparency	3	3	3
6	EA	Transparency	3	3	2
7	EA	Transparency	3	2	1
8	EA	Transparency	3	3	3
9	EA	Transparency	3	1	1
10	EA	Transparency	2	3	1
11	EA	Transparency	3	4	2
1	PA	Transparency	2	3	1
2	PA	Transparency	3	1	1
3	PA	Transparency	2	1	1
4	PA	Transparency	2	2	1
5	PA	Transparency	2	3	2
6	PA	Transparency	2	1	1
7	PA	Transparency	1	1	1
8	PA	Transparency	2	3	1
9	PA	Transparency	3	1	1
10	PA	Transparency	1	3	1
11	PA	Transparency	2	2	1
***p*-value**			0.009	0.021	0.359

5.6.2 Process Automation Risk

Figure 38, below, shows the analysis of (process) automation risk. The mean risk value in Scenario A and Scenario B on the existing architecture was 2.18. In Scenario C, it was 2.00. The interviewed experts noted that neither the size of the company nor its location or certifications directly influence this factor. The decisive factor was the experts' experience configuring cloud applications and knowledge of how today's cloud providers are usually positioned in configuring cloud applications. During the interview, experts noted that today's processes are already automated in many parts.

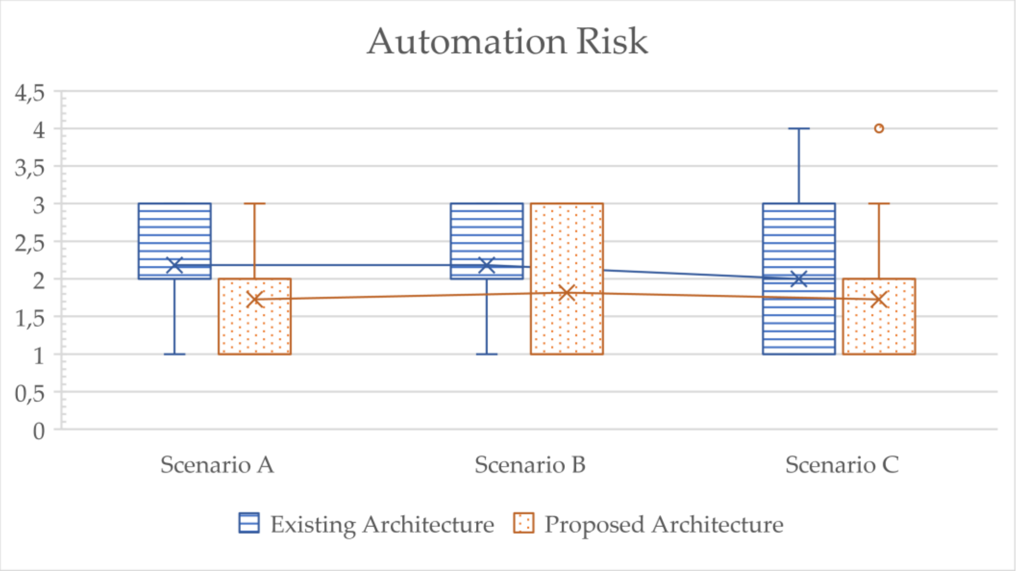


Figure 38: Results Process Automation Risk Assessment Existing vs. Proposed Architecture

Furthermore, during the interview, experts rated the risk of configuration errors due to manual processes as "medium" on the median. When considering the newly proposed approach, Scenario A had an average value of 1.73, Scenario B had a value of 1.82, and Scenario C had a value of 1.73. Furthermore, the median in Scenario B and Scenario C was reduced from 2 to 1.

When analyzing the U-values, as shown in Table 10, it was noticeable that in none of the studies could a p-value of less than 0.05 be achieved. Consequently, H_0 cannot be rejected in any of the three scenarios. Finally, this implies that the presented architecture could not significantly reduce the adoption risk in the automation field. The interviews showed two primary reasons for this. Participant #11 highlighted one of the reasons very clearly:

> *I think it's [automation risk] related to change management and the change management is, the technical part is really the minor thing towards it. So, yeah, I think it's then more, there are too many other stakeholders, and the change management is then driven by company size and processes and having better digital processes. Yeah, so the technical one is definitely helpful, but it's just the small piece I would say.*

Table 10: Process Automation Risk Results and p-Values

Participant #	Architecture	Risk	Rate A	Rate B	Rate C
1	EA	Automation	2	2	3
2	EA	Automation	1	2	2
3	EA	Automation	2	2	1
4	EA	Automation	2	2	1
5	EA	Automation	3	3	4
6	EA	Automation	3	1	2
7	EA	Automation	2	3	1
8	EA	Automation	3	3	3
9	EA	Automation	2	1	2
10	EA	Automation	2	2	1
11	EA	Automation	2	3	2
1	PA	Automation	1	1	1
2	PA	Automation	1	2	2
3	PA	Automation	1	1	1
4	PA	Automation	2	1	1
5	PA	Automation	3	3	4
6	PA	Automation	1	1	1
7	PA	Automation	1	1	1
8	PA	Automation	3	3	3
9	PA	Automation	2	1	2
10	PA	Automation	2	3	1
11	PA	Automation	2	3	2
***p*-value**			0.134	0.329	0.439

Consequently, the technical solution is not the primary concern when automating processes. Rather, when automating processes, the associated change management approach must be taken into account, as well as the processes associated with the automation, rather than the technical implementation. Secondly, automation risk has already been classified as the median "medium" for the existing architecture. Taking into account that automation does not only depend on the technical solution, but it also becomes clear that the newly presented architecture is not enough to achieve a significant reduction in process automation.

5.6.3 Repudiation Risk

The evaluation of the expert interviews showed that the approach presented in this dissertation could reduce the adoption risk most significantly. The evaluation of this is shown in Figure 39, below. On average, in the existing architecture, the repudiation risk of Scenario A was rated at 2.64. The adoption risk in Scenario B was evaluated with an average rating of 3.00. The adoption risk of denial in case of dispute is rated lowest in Scenario C, with an average rating of 2.09.

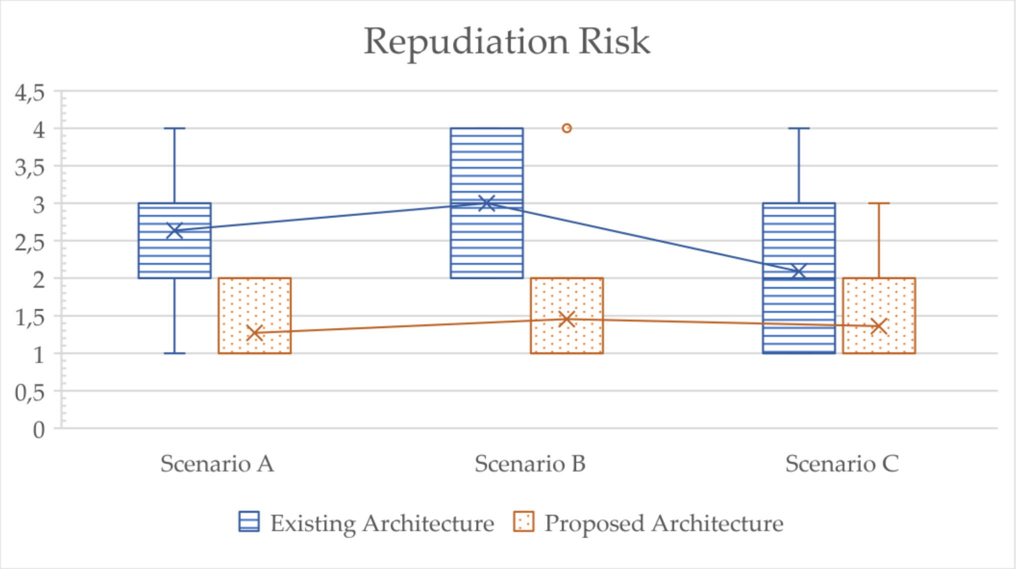


Figure 39: Results Repudiation Risk Assessment Existing vs. Proposed Architecture

Similar arguments as in the Transparency risk for Provider B were also given for the risk of denial of a configuration in case of a dispute. The doubtful legal situation and the lack of independently recognized certifications ensure that experts rate this provider's adoption risk as the highest. However, a comparison with the architecture presented in this dissertation showed the most significant risk reduction. Thus, in Scenario A, the adoption risk has reduced from 2.64 by 1.37 to 1.27. In Scenario B, the adoption risk was reduced from 3.00 by 1.55 to 1.45. And, in Scenario C, the adoption risk was reduced by 0.73, from 2.09 to 1.36. Thus, the adoption risk in Scenario B was significantly reduced by 1.55 risk points from an average median value of 3 to 1, or from "High" to "Low."

Regarding the *U*-values in Table 11, there are two noticeable points. First, the newly presented architecture significantly reduced the repudiation risk in Scenarios A and B. In Scenario A, the *p*-value is 0.002, and in Scenario B, 0.001. Considering the SD and the distribution of the functions, it can be concluded that introducing the architecture presented in this dissertation can significantly reduce the adoption risk in Scenarios A and B.

Table 11: Repudiation Risk Results and p-Values

Participant #	Architecture	Risk	Rate A	Rate B	Rate C
1	EA	Repudiation	3	3	1
2	EA	Repudiation	3	3	3
3	EA	Repudiation	2	3	1
4	EA	Repudiation	1	2	1
5	EA	Repudiation	3	2	4
6	EA	Repudiation	2	3	1
7	EA	Repudiation	1	3	2
8	EA	Repudiation	3	4	3
9	EA	Repudiation	4	2	1
10	EA	Repudiation	3	4	3
11	EA	Repudiation	4	4	3
1	PA	Repudiation	1	1	1
2	PA	Repudiation	1	1	1
3	PA	Repudiation	1	1	1
4	PA	Repudiation	1	1	1
5	PA	Repudiation	2	1	3
6	PA	Repudiation	1	1	1
7	PA	Repudiation	1	2	1
8	PA	Repudiation	1	1	1
9	PA	Repudiation	1	1	1
10	PA	Repudiation	2	4	2
11	PA	Repudiation	2	2	2
***p*-value**			0.002	0.001	0.110

Second, as in the Transparency risk, no significant reduction of the adoption risk in Scenario C could be achieved. The non-significant reduction in Scenario C is mainly because the reputation risk in Scenario C was already classified as "medium" in the median. A significant reduction using the technical approach presented could not be achieved.

5.7 DISCUSSION

The evaluation aimed to show to what extent the architecture developed in this dissertation, and thus the shift of trust to the blockchain, can contribute to reducing cloud adoption risks. For this purpose, the scenario-based architecture evaluation approach ALMA developed by Bengtsson et al. (2004) was used. The use of ALMA has the advantage of already being tested (Bengtsson et al., 2004). Furthermore, ALMA provided the needed design to answer RQ7 and could be ideally adapted to the present evaluation case.

ALMA is structured in five steps. Step one is the concrete choice of the evaluation goal. The goal of the present evaluation was to select the ideal software architecture for a given case. For this purpose, three possible adoption cases were created with the help of the method described by Yin for developing case studies (Yin, 2017). These case studies served as a basis. In the described cases, a cloud application was to be adopted. The best architecture was to be selected using ALMA. In the context of this dissertation, "the best" means the alternative that causes a lower cloud adoption risk concerning compliance-driven configurations. Experts evaluated the adoption risk based on the developed case studies. It is worth noting that the case studies were chosen to cover as broad a range of adoption risks as possible within the scope of the dissertation. The evaluation results showed that the risks presented were indeed suitably broad. The experts assessed the adoption risks in the three scenarios mentioned in significantly different ways.

Mixed-method-based SSIs were used (Tashakkori et al., 1998). The qualitative part of the interviews was reinforced by quantitative questions and a quantitative risk matrix. Initially, it was assumed that twelve experts would be consulted for the evaluation. During the interviews, however, it turned out that the experts' opinions regarding the developed architecture were unanimous. The architecture selection showed a clear picture regarding the reduction of adoption risks.

First and foremost, it can be stated overall that the experts did not see a higher adoption risk with the PA than with the EA. Rather, it was shown that the PA can reduce the adoption risk for all scenarios. However, a more detailed *U*-test analysis revealed different significance levels in reducing adoption risks. In particular, the adoption risk related to transparency was significantly reduced in Scenario A and

Scenario B. On the other hand, neither a significant reduction of the adoption risk nor a reduction of the risk median could be observed in Scenario C. It should be noted, however, that the transparency risk in Scenario C was already classified as "Low" in the median. A significant reduction was, therefore, only possible to a limited extent.

A different picture emerged for the automation risk. In this case, the median risk in Scenario B and Scenario C was reduced from "Medium" to "Low." Similar to the transparency risk, the automation risk in Scenario C was already "Low," so no reduction in the median could be achieved here. When considering the significance, however, it was noticeable that the adoption risk could not be significantly reduced in any of the three scenarios. Clarification on why the automation risk could not be reduced was given during the qualitative part of the SSI. Experts saw the automation risk less on the technical side. Rather, the experts believed that automation risks are primarily due to nontransparent internal process structures of cloud application providers and slow or non-existent change management. The introduction of PA thus has little influence on this risk.

The most significant reduction of adoption risks has been shown for repudiation. In Scenario A and B, a median reduction in repudiation risk from "High" to "Low" was achieved. Scenario C achieved a median risk reduction from "Medium" to "Low." Overall, in all three scenarios, the median risk was reduced. Looking again at the significance, a *U*-test showed that the adoption risk was significantly reduced in Scenarios A and B. In Scenario C, however, no significant reduction in the risk could be shown. However, the adoption risk in Scenario C was already lower than in the other two scenarios.

In conclusion, the SSI has shown that the presented architecture has the most significant potential to reduce the adoption risk in cases where an increased risk already exists. The SSI has also shown that increased adoption risks may arise due to a lack of independent certifications and legal enforcement capabilities. This finding of increased adoption risk aligns with existing literature (J. Huang & Nicol, 2013). However, as Scenario A shows, a reduction of the adoption risk can also be achieved if certifications and legal enforceability are available. Overall, the approach developed in this thesis could significantly reduce the adoption risk concerning compliance-driven configurations.

An important point in the evaluation was that an attack on the blockchain should not be assumed. However, other assumptions—such as the incorrect implementation of the developed approach or an insider attack—should be assumed. In the opinion of the author, this reflects reality. Overall, ALMA and the expert interviews showed that the approach developed in this dissertation could help reduce cloud applications' adoption risk. However, the expert interviews showed that the extent to which the adoption risk can be reduced depends on several factors. As shown in the past, factors such as the country in which the cloud application is developed and hosted, whether a cloud provider has been independently certified, and the annual revenue of the cloud provider plays a crucial role in assessing the adoption risk (J. Huang & Nicol, 2013). The interviewed persons barely considered rating systems by nonaccredited participants (such as Google ratings of a company) as trust-building. It could be shown that the architecture developed here can significantly reduce the adoption risk concerning compliance-driven configurations. The interpretation of the evaluation results also allows the conclusion that the goal of this dissertation could be achieved using the developed architecture.

6 CONCLUSION AND OUTLOOK

This final chapter aims to discuss the findings obtained in this dissertation. Based on the discovered results, a conclusion is then drawn. The limitations and outlook on future work are also presented at the end of the chapter.

6.1 DISCUSSION

It is widely accepted that cloud application adoption is a comprehensive and extensively researched area due to its significance (Avram, 2014; Rai et al., 2015; Swanson, 2010). This work has focused on shifting trust from the cloud application provider to the blockchain. More precisely, the present research has focused primarily on reducing the adoption risks that arise from shifting the task of configuring cloud applications into the blockchain due to compliance-driven cloud application configurations.

Configuring cloud applications is a challenge in cloud applications because users lack a mechanism to control the data (Armbrust et al., 2009; Sun, 2019). This dissertation relies on shifting trust away from the cloud application provider to the blockchain to overcome this challenge. Data security thereby plays an essential role. Compliance with the CIA security objectives (confidentiality, integrity, and availability) was a mandatory requirement for developing a solution approach. Due to the utilization of blockchain technology as a notary for compliance-driven configurations, integrity and availability for cloud configurations could already be ensured. The developed approach is based on data encryption to ensure the confidentiality of blockchain-stored cloud configurations.

A two-step approach has achieved confidentiality. First, a blockchain-based key exchange protocol based on the three-party Diffie-Hellman protocol is used to ensure an automated and authenticated key exchange between the cloud application provider, the cloud application consumer, and the cloud application itself (see 4.2.2). This results in the creation of a shared symmetric key. Based on the shared symmetric key, in a second step, the symmetric key is used to store configurations encrypted via smart contract on the blockchain. The cloud application is notified of changes in the configuration using a monitoring mechanism. The configuration changes are then uploaded to the cloud application and implemented by a cloud-side script. After the configuration has been successfully implemented, the cloud-side script triggers a snapshot of the cloud instance loaded from external storage to the cloud instance. On the cloud instance side, the cryptographic hash value of the snapshot is computed, which is then written to the blockchain. These steps happen automatically and require the user to provide a configuration encrypted with the negotiated key.

This dissertation illustrates that trust is a significant issue in cloud computing. Using the DSR approach, this dissertation has provided a software architecture for configuring cloud applications via the blockchain. The result of the study reveals that transparency and the resulting uncertainty are significant factors for trust issues in cloud adoption. Moreover, the literature survey has shown that blockchain technology can provide transparency and facilitate dealing with trust issues. The developed architecture allows the cloud provider and the customer to make auditable cloud configuration changes confirmed by the blockchain. During the usage of the proposed software architecture, it is possible to configure cloud applications to be:

Transparent. At any time, every participant can see which the last configuration was successfully implemented; moreover, the stored past configuration can also be seen due to blockchain technology.

Automatic. No manual user input is required to implement the configuration. Furthermore, configurations are implemented automatically without delays or human error.

Non-repudiable. If a cloud application succeeds, a snapshot is generated. The hash value of this snapshot will be stored in a smart contract. If a dispute or uncertainty regarding the configuration occurs, the blockchain can be used as an audit trail for configuration changes. Simultaneously, the snapshot associated with the stored hash value can be retrieved from the data storage of the cloud provider. The selected snapshot's integrity can be verified using the retrieved hash value. However, due to the properties of cryptographic hash values, a snapshot matching a hash value cannot be changed afterward. Thus, the cloud configuration has been documented in a tamper-proof manner. The prototype presented in this dissertation shows that the software architecture can be implemented. Here, the configuration of an IDS is only one possibility of the presented architecture.

6.2 CONCLUSION

As the introduction to this dissertation has shown, cloud computing has many economic advantages for software-selling companies. These companies can use the cloud infrastructure to cost-effectively provide their software as a cloud application without purchasing or operating their own infrastructure. On the other hand, providing software applications via the cloud also means that customers must trust this new infrastructure. In particular, customers must trust that their data and requirements are at least as well protected as they were on their resources. It has been shown that companies have a strong interest in compliance, i.e., adherence to regulations (Ackermann et al., 2011; Armbrust et al., 2009; Cayirci & de Oliveira, 2018; Phaphoom et al., 2015). The legally compliant configuration of software applications is relevant to the existence of many companies (ISC2 Foundation & Cybersecurity Insiders, 2022). By adopting cloud services, customers lose the opportunity to implement their specifications independently. Instead, customers are now forced to trust the providers of cloud applications (Michael, 2009). When adopting cloud applications, customers must trust that cloud application providers will operate how the customer expects and communicates. In addition, customers depend on receiving comprehensive information and support from cloud application providers, e.g., during a cyber-attack.

The existing model ensures that companies benefit financially by adopting cloud applications but have to dispense with autonomy in configuring the applications. In the context of this thesis, it could be shown that outsourcing cloud applications are connected with further risks for enterprises. These risks are referred to as cloud adoption risks and include the risk of transparency, process automation, and repudiation (see 1.3). Consequently, in its MRQ, this dissertation has asked:

> *To what extent can adoption risks arising from compliance-driven cloud application configurations be reduced by moving the trust to configure the cloud application to the blockchain?*

It has been shown that this question is more complex than it initially appears and, in fact, has six stages. Using existing literature, it was possible to show how trust and risk interact in adopting cloud applications (see 3.1.4).

In the first stage, it is important to note that reducing the adoption risk increases the probability of cloud application adoption (see 3.1.5). It was shown that the adoption probability of cloud applications can be increased by decreasing the adoption risk. It could be shown that reducing adoption risks leads to a higher adoption probability of cloud services. In the last instance, the degree to which the probability of adoption is increased depends here, among other things, on the personal willingness to take risks (Jøsang & Presti, 2004; Mayer et al., 1995). However, to what extent the adoption probability can be increased in this way remains an unsolved problem in research (Jøsang & Presti, 2004).

In the next stage, it was necessary to identify where the problem of adoption risks arises and which method should be used to respond to this problem. Since the MRQ poses a highly practical question, the DSR methodology described by Hevner et al. (2004) was used. In this context, DSR provides a framework for the scientific development of practical solutions (see chapter 2). Using DSR, it became clear that the MRQ could not be answered directly. Rather, it was first necessary to clarify the exact scope (environment) in which the problem described in the MRQ occurs. For this purpose, the DSR authors (Hevner et al., 2004) recommend qualitative methods. It would be conceivable, for example, to conduct expert interviews or focus group discussions.

In the context of this dissertation, a focus group discussion was conducted to answer the environment question (see 3.2). The goal of the focus group was to determine the scope of the work and understand the environment of compliance-related adoption risks. In the past, it has been shown that blockchain can be used as a technology for shifting trust (Werbach, 2018; Yun Zhang et al., 2020). Expert discussions were intended to determine whether this use case also falls within the scope of this dissertation. Qualitative methods, especially the focus group, are particularly suitable for this purpose, as they allow experts from different disciplines to discuss with each other (see 2.1.1). Utilizing the explicative content analysis proposed by Mayring (2000), it was possible to extend the existing theory to cover the scope of this dissertation scientifically.

Overall, the focus group discussion made two major contributions to this dissertation (see 3.2.5 and 3.2.6). First, it clarified the research question in which environment compliance-driven risks might occur. Thus, the scope of the thesis could be set. Second, the focus group discussion clarified that shifting trust away from the cloud application provider to the blockchain might be a reasonable way to reduce adoption risks. The argumentation of shifting trust to blockchain could later be substantiated via literature. Focus group discussion thus helped overall to determine the scope of this dissertation.

The third stage was building a knowledge foundation. Following the DSR methodology and based on the scope of the thesis, a knowledge base had to be built. All knowledge needed to answer the MRQ must be identified and presented based on the scope of the thesis. In the context of this dissertation, this was done using an AI-supported systematic literature review (see 3.3). AI, in this process, ensured that many relevant scientific papers could be searched and grouped. A systematic literature search was then conducted based on the AI-supported grouping. Through a systematic literature search, it was possible to show that this dissertation addresses an open research gap.

Moreover, the identified literature could also be used to identify existing relevant approaches. Overall, this allowed for building a scientifically sound knowledge base to answer the MRQ. The knowledge base showed that blockchain is a technology that has already been increasingly used to implement authentication risks or zero-trust architectures (see 3.3). Overall, the assumptions and statements from the focus group discussion could be scientifically substantiated, considering the knowledge base.

After investigating the scope and knowledge base of the dissertation, the fourth problem stage was to define configurations mathematically – to implement them in software later. It turned out that there is no definition of cloud configurations in the existing research (see 4.1). However, developing an application to perform a configuration is a mandatory requirement. The mathematically sound definition of the configuration was thus part of this dissertation.

It turned out that configurations can be described mathematically as partial functions. Here, the definition set of the partial function is the UTF-8 alphabet. The target quantity is an input/output behavior that provides a certain output in response to a concrete input. The mathematical definition was later used to develop an artifact based on the DSR methodology (see 4.2). For this dissertation, developing an artifact meant developing a software architecture that shifts trust from cloud providers to the blockchain, where it enables the compliance-driven configuration of applications. More precisely, with the findings from the knowledge base and the definition of configurations, an artifact described according to DSR mythology was developed. The developed artifact aimed to solve the MRQ and thus reduce the adoption risk of cloud applications.

The fifth stage involved architecture development. The generic (blockchain and programming language independent) architecture development was done systematically according to the Rapid Application Development approach so that there was a software architecture and a prototype at the end of the design cycle of the DSR framework (see 4.2).

The evaluation of this artifact was necessary to determine whether the developed artifact can shift trust to the blockchain and reduce adoption risks. The evaluation also reflected the sixth and last stage of answering the MRQ. Here, the evaluation could show two things. First, which architecture (EA or PA) causes fewer adoption risks when compliance-driven configuring cloud applications (see chapter 5). Second, to what degree adoption risks can be reduced. The scenario-based software evaluation approach was selected as this dissertation presented a software architecture. The scenario-based evaluation was chosen among the different architecture evaluation options because it can measure the performance of software architecture in different scenarios. Specifically, the presented architecture was evaluated using ALMA (see chapter 5).

A mixed-methods approach was used to conduct the evaluation scientifically. The evaluation showed that all experts would use the software architecture presented in this dissertation to configure cloud applications (see 5.7). The experts justified this in terms of a significantly lower adoption risk in some cases when configuring cloud applications. In particular, the evaluation showed that the risk of repudiating a configuration could be significantly reduced using the presented architecture. However, it also turned out that the adoption risk reduction varies from application scenario and adoption risk to adoption risk. The exact risk reduction depends on many other factors (such as company location, company size, external certifications, risk perception, etc.). These findings are also in line with scientific findings (see 5.7).

The DSR framework provides a scientific artifact that solves a problem in a defined problem scope. For this, however, the framework must be followed strictly. Identifying the problem scope using focus group discussions, creating the knowledge base using an AI-supported systematic literature review, and developing an artifact following RAD mythology show that this dissertation has followed each step of the DSR Framework using scientific methods. The evaluation further confirmed this and quantified the amount of risk reduction. Overall, it can thus be stated that this dissertation used scientific methods to develop an artifact that enables a shift of trust from cloud application providers to the blockchain. Scientific evaluation has shown that the developed artifact can significantly reduce the adoption risk for compliance-driven configurations. In conclusion, it can be stated that the goal of this dissertation has been fully achieved. The MRQ was answered following a scientific framework.

6.3 LIMITATIONS AND OUTLOOK

The main objective of this dissertation was to present a software architecture that allows for a shift of trust to the blockchain and thereby reduces the adoption risk of cloud applications. Using the adopted approach, once the Cloud Management Script has detected the successful implementation, it triggers a backup of the cloud instance, and the computed hash value forms a unique fingerprint of the cloud instance. If a dispute arises between two parties, the stored and created snapshot can be consulted, and its hash value is compared with the hash value stored in the blockchain. A legal dispute can be conducted based on this snapshot. Neither of the parties can deny that the snapshot is the actual configuration of the cloud application. The adopted approach thus eliminates repudiation risk (see 1.3.2).

This dissertation has grouped various compliance-related risks into three overall risks. Grouping the risks had the advantage that a broad spectrum of risks could be examined during the dissertation. At the same time, however, the abstraction has the disadvantage of losing details. Thus, it cannot be said that the approach presented here serves under all conditions to reduce compliance-related risks related to cloud adoption. Rather, this dissertation has shown that shifting trust to the blockchain is possible and that this can reduce the three risks generally described. When faced with doubt, the approach presented in this dissertation must be re-examined for adoption risk in an individual environment.

Moreover, while blockchain is a promising technology, it faces numerous challenges. These include scalability, privacy leakage, governance, and compliance with regulations (Murthy et al., 2020; Park & Park, 2017). In the context of this work, the underlying blockchain was abstracted. It was assumed that the risk of an attack on the blockchain could be excluded. This assumption represents a limitation of the work. Even though the blockchain technology has successfully established itself to date and Bitcoin or Ethereum run securely, for the most part, further research must investigate how the adoption risk of the architecture developed in this dissertation changes when different blockchains are used. For example, do public blockchains influence the adoption risk differently than private blockchains? This question could be the subject of further research.

The prototype implementation showed that creating a snapshot can be a bottleneck of the application (see 4.3). The prototype presented in this dissertation took almost ten minutes to set the configuration through a smart contract to confirm the configuration by saving the snapshot hash value. The main reason for this was the hash value generation of a 30 GiB snapshot. Therefore, operating the cloud instance with the smallest possible hard disk space is recommended. On the one hand, this ensures that the created snapshots are as small as possible and thus require little additional storage space. And, on the other hand, a reduced snapshot size leads to a faster hash value computation. However, this may limit the scope of the developed architecture.

In general, the presented architecture still has limitations in VM scaling. Thus, the presented approach is only suitable for a single VM. However, today's large-scale applications usually run on many distributed VMs or container instances. Future research must investigate how the architectural approach presented here can also be used with distributed systems and container instances.

The case studies used to evaluate the architecture differ in the annual revenue of the companies, the industry sector, and the compliance case that the companies want to solve using cloud application adoption (see 5.3). The case studies always target the adoption of cloud applications from a third-party provider. The adoption of in-house applications was not investigated within the scope of this dissertation and is a task for further research. Furthermore, scenario-based evaluation of software architectures is generally limiting. Software architectures can be used in a variety of environments. Even though care was taken when creating the scenarios to make them as broad as possible, not all possible software application scenarios can be represented. Nevertheless, the qualitative analysis of the evaluation shows that the selection of scenarios was rated as realistic by all evaluation participants.

Also, it should be mentioned that only companies with their headquarters in Europe were examined in evaluating the architecture. It remains an open research question to what extent the architecture presented in this dissertation influences the adoption risk of companies outside of Europe and not under the General Data Protection Regulation.

In addition to technical benefits such as the tamper-proof properties of blockchain entries, the use of blockchain for configuring applications also offers economic advantages. Cloud configurations are set using smart contracts. In addition to pure configuration, payments can also be linked to smart contracts. It is, therefore, conceivable to use cloud configurations as a business model for subcontractors. This way, the increased resource costs for storing snapshots can be compensated in payable smart contracts. Further research can reveal which acceptance and business model this can enable.

The generic software architecture presented in this dissertation enables a completely new way of configuring cloud applications. The expert interviews have shown that the architecture’s limiting trust factor is its correct implementation on the part of the cloud application provider. Future research must show how blockchain technology can be used to ensure the correct cloud/provider-side implementation of the architecture presented in this dissertation. Future research must also show which implementation-independent processes can be implemented around the architecture presented. For example, best practices or access procedures to the backups created during configuration must be implemented. Overall, future research must show how the newly presented architecture can be used to break old processes and implement new ways of configuring cloud applications in practice.

BIBLIOGRAPHY

Abbas, K., Tawalbeh, L. A., Rafiq, A., Muthanna, A., Elgendy, I. A., & Abd El-Latif, A. A. (2021). Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. *Security and Communication Networks*, *2021*, 1–13. https://doi.org/10.1155/2021/5597679

Abbate, J. E. (1994). *From ARPANET to INTERNET: A history of ARPA-sponsored computer networks, 1966-1988* [University of Pennsylvania ProQuest Dissertations]. https://repository.upenn.edu/dissertations/AAI9503730

Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O.-Y., Bashir, A. K., & El-Latif, A. A. A. (2020). DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, *8*, 111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468

Abowd, G., Bass, L., Clements, P., Kazman, R., & Northrop, L. (1997). *Recommended Best Industrial Practice for Software Architecture Evaluation.* Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Abuhussein, A., Alsubaei, F., & Shiva, S. (2020). Toward an Effective Requirement Engineering Approach for Cloud Applications. In *Software Engineering in the Era of Cloud Computing* (pp. 29–50). Springer. https://doi.org/10.1007/978-3-030-33624-0_2

Ackermann, T., Miede, A., Buxmann, P., & Steinmetz, R. (2011, June). Taxonomy of technological IT outsourcing risks: Support for risk identification and quantification. *19th European Conference on Information Systems, ECIS 2011*. http://tubiblio.ulb.tu-darmstadt.de/102182/

Adams, A., & Cox, A. L. (2008). *Questionnaires, in-depth interviews and focus groups*. Cambridge University Press.

Adams, W. C. (2015). Conducting Semi-Structured Interviews. In *Handbook of Practical Program Evaluation* (Vol. 4, pp. 492–505). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119171386.ch19

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the World Wide Web: From WEB 1.0 to WEB 4.0. *International Journal of Web & Semantic Technology*, *3*(1), 1–10. https://doi.org/10.5121/ijwest.2012.3101

Al-Marsy, A., Chaudhary, P., & Rodger, J. A. (2021). A Model for Examining Challenges and Opportunities in Use of Cloud Computing for Health Information Systems. *Applied System Innovation*, *4*(1), 15. https://doi.org/10.3390/asi4010015

Alali, F. A., & Yeh, C.-L. (2012). Cloud Computing: Overview and Risk Analysis. *Journal of Information Systems*, *26*(2), 13–33. https://doi.org/10.2308/isys-50229

Aleryani, A. Y. (2016). Comparative Study between Data Flow Diagram and Use Case Diagram. *International Journal of Scientific and Research Publications*, *6*(3), 124. www.ijsrp.org

Alexopoulos, N., Daubert, J., Muhlhauser, M., & Habib, S. M. (2017). Beyond the Hype: On Using Blockchains in Trust Management for Authentication. *2017 IEEE Trustcom/BigDataSE/ICESS*, 546–553. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.283

Ali, O., & Osmanaj, V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. *Computer Law & Security Review*, *36*, 105396. https://doi.org/10.1016/j.clsr.2020.105396

Alnafrani, M., & Acharya, S. (2021). SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking. *Health Policy and Technology*, *10*(2), 100510. https://doi.org/10.1016/j.hlpt.2021.100510

Alsubhi, A., Alzain, M. A., Masud, M., Jhanjhi, N. Z., Al-Amri, J., & Baz, M. (2021). Awareness of Security Threats in Social Media. *Turkish Journal of Computer and Mathematics Education*, *12*(10), 3093–3100. https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2020-0190/full/html

Anderson, S. W., Christ, M. H., Dekker, H. C., & Sedatole, K. L. (2014). The Use of Management Controls to Mitigate Risk in Strategic Alliances: Field and Survey Evidence. *Journal of Management Accounting Research*, *26*(1), 1–32. https://doi.org/10.2308/jmar-50621

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 1–15. https://doi.org/10.1145/3190508.3190538

Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain Standards for Compliance and Trust. *IEEE Cloud Computing*, *4*(4), 84–90. https://doi.org/10.1109/MCC.2017.3791019

Anton, A. I. (2003). Successful software projects need requirements planning. *IEEE Software*, *20*(3), 44–47. https://doi.org/10.1109/MS.2003.1196319

Ardagna, C. A., Asal, R., Damiani, E., El Ioini, N., Elahi, M., & Pahl, C. (2021). From trustworthy data to trustworthy IoT: A data collection methodology based on blockchain. *ACM Transactions on Cyber-Physical Systems*, *5*(1). https://doi.org/10.1145/3418686

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., & Stoica, I. (2009). *Above the Clouds: A Berkeley View of Cloud Computing*. Technical Report UCB/EECS-2009-28, EECS Department, University of California …. http://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*, 529–534. https://doi.org/10.1016/j.protcy.2013.12.525

Axelsson, S. (1998). *Research in intrusion-detection systems: A survey*.

Bace, R. G., & Mell, P. (2001). *Intrusion Detection Systems*. US Department of Commerce, Technology Administration, National Institute of~…. https://books.google.de/books?id=VoKrMQEACAAJ

Bahga, A., & Madisetti, V. K. (2016). Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, *09*(10), 533–546. https://doi.org/10.4236/jsea.2016.910036

Baker, J. D. (2016). The Purpose, Process, and Methods of Writing a Literature Review. *AORN Journal*, *103*(3), 265–269. https://doi.org/10.1016/j.aorn.2016.01.016

Baker, M. J. (2000). Writing a Literature Review. *The Marketing Review*, *1*(2), 219–247. https://doi.org/10.1362/1469347002529189

Bakogiannis, T., Mytilinis, I., Doka, K., & Goumas, G. (2020). Leveraging Blockchain Technology to Break the Cloud Computing Market Monopoly. *Computers*, *9*(1), 9. https://doi.org/10.3390/computers9010009

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support. *Communications of the Association for Information Systems*, *37*(1), 154–204. https://doi.org/10.17705/1CAIS.03708

Baniata, H., & Kertesz, A. (2020). A Survey on Blockchain-Fog Integration Approaches. *IEEE Access*, *8*, 102657–102668. https://doi.org/10.1109/ACCESS.2020.2999213

Bass, L., Clements, P., & Kazman, R. (2003). Software Architecture in Practice , Second Edition. In *Software Architecture*. Addison-Wesley Professional.

Beale, J. (2004). Snort 2.1 Intrusion Detection. In *Snort 2.1 Intrusion Detection*. Elsevier. https://doi.org/10.1016/B978-1-931836-04-3.X5000-0

Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Davila Delgado, J. M., Akanbi, L. A., Ajayi, A. O., & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441. https://doi.org/10.1016/j.autcon.2020.103441

Bengtsson, P., Lassing, N., Bosch, J., & van Vliet, H. (2004). Architecture-level modifiability analysis (ALMA). *Journal of Systems and Software*, *69*(1–2), 129–147. https://doi.org/10.1016/S0164-1212(03)00080-3

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246. https://doi.org/10.1016/j.dss.2011.07.007

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34–37. https://doi.org/10.1145/2695533.2695545

Bera, B., Chattaraj, D., & Das, A. K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Computer Communications*, *153*, 229–249. https://doi.org/10.1016/j.comcom.2020.02.011

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, *7*, 164908–164940.

https://doi.org/10.1109/ACCESS.2019.2950872

Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H. F., & Secret, A. (1994). The World-Wide Web. *Communications of the ACM*, *37*(8), 76–82. https://doi.org/10.1145/179606.179671

Beserra, P. V., Camara, A., Ximenes, R., Albuquerque, A. B., & Mendonca, N. C. (2012). Cloudstep: A step-by-step decision process to support legacy application migration to the cloud. *2012 IEEE 6th International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA)*, 7–16. https://doi.org/10.1109/MESOCA.2012.6392602

Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., & Kumar, N. (2021). BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1242–1255. https://doi.org/10.1109/TNSE.2019.2961932

Birrell, A. D., & Nelson, B. J. (1983). Implementing Remote procedure calls. *ACM SIGOPS Operating Systems Review*, *17*(5), 3. https://doi.org/10.1145/773379.806609

Blei, D. M., Ng, A. Y., & Jordan, M. T. (2002). Latent dirichlet allocation. *Advances in Neural Information Processing Systems*, *3*(Jan), 993–1022.

Bohn, R. B., Messina, J., Liu, F., Tong, J., & Mao, J. (2011). NIST Cloud Computing Reference Architecture. *2011 IEEE World Congress on Services*, *500*(2011), 594–596. https://doi.org/10.1109/SERVICES.2011.105

Bomhard, D., & Daum, A. (2021). Cybersecurity in outsourcing and cloud computing: a growing challenge for contract drafting. *International Cybersecurity Law Review*, *2*(1), 161–171. https://doi.org/10.1365/s43439-021-00029-4

Both, D. (2020). Everything Is a File. In *Using and Administering Linux: Volume 2* (pp. 43–66). Apress. https://doi.org/10.1007/978-1-4842-5455-4_3

Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, risk, and compliance in cloud scenarios. *Applied Sciences*, *9*(2), 320. https://doi.org/https://doi.org/10.3390/app9020320

Braun, J., Volk, F., Classen, J., Buchmann, J., & Mühlhäuser, M. (2014). CA trust management for the Web PKI. *Journal of Computer Security*, *22*(6), 913–959. https://doi.org/10.3233/JCS-140509

Bright, P. (2011). *How the comodo certificate fraud calls ca trust into question*. Arstechnica. https://arstechnica.com/information-technology/2011/03/how-the-comodo-certificate-fraud-calls-ca-trust-into-question/

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning*, *9*(4), 317–328. http://www.ncbi.nlm.nih.gov/pubmed/27318286

Broy, M., & Stølen, K. (2001). *Specification and Development of Interactive Systems*. Springer New York. https://doi.org/10.1007/978-1-4613-0091-5

Brychta, M., & Hagara, L. (2017). Certificate manager watchman. *2017 International Conference on Military Technologies (ICMT)*, 383–386. https://doi.org/10.1109/MILTECHS.2017.7988789

Buchkremer, R., Demund, A., Ebener, S., Gampfer, F., Jagering, D., Jurgens, A., Klenke, S., Krimpmann, D., Schmank, J., Spiekermann, M., Wahlers, M., & Wiepke, M. (2019). The Application of Artificial Intelligence Technologies as a Substitute for Reading and to Support and Enhance the Authoring of Scientific Review Articles. *IEEE Access, 7,* 65263–65276. https://doi.org/10.1109/ACCESS.2019.2917719

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. In *Etherum* (Issue January). http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized Applications: The Blockchain-Empowered Software System. *IEEE Access*, *6*, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy Magazine, 7*(1), 78–81. https://doi.org/10.1109/MSP.2009.12

Cambridge Dictionary. (2022). *Transparency*. Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/transparency

Can, O., & Sahingoz, O. K. (2015). A survey of intrusion detection systems in wireless sensor networks. *2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO),* 1–6. https://doi.org/10.1109/ICMSAO.2015.7152200

Cao, Y., Sun, Y., & Min, J. (2020). Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system. *Measurement and Control, 53*(7–8), 1286–1299. https://doi.org/10.1177/0020294020926636

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, *18*(2), 65–82. https://doi.org/10.1080/10630732.2011.601117

Cayirci, E., & de Oliveira, A. S. (2018). Modelling trust and risk for cloud services. *Journal of Cloud Computing*, *7*(1), 14. https://doi.org/10.1186/s13677-018-0114-7

Celar, S., Seremet, Z., & Turic, M. (2011). Cloud computing: definition, characteristics, services and models. *Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium*, *22*(1), 1–2.

Chamola, V., Goyal, A., Sharma, P., Hassija, V., Binh, H. T. T., & Saxena, V. (2022). Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. *Neural Computing and Applications*, 1–11. https://doi.org/10.1007/s00521-022-07087-7

Chen, H., Yu, J., Zhou, H., Zhou, T., Liu, F., & Cai, Z. (2021). SmartStore: A blockchain and clustering based intelligent edge storage system with fairness and resilience. *International Journal of Intelligent Systems*, *36*(9), 5184–5209. https://doi.org/10.1002/int.22509

Chen, R., Li, Y., Yu, Y., Li, H., Chen, X., & Susilo, W. (2020). Blockchain-Based Dynamic Provable Data Possession for Smart Cities. *IEEE Internet of Things Journal*, *7*(5), 4143–4154. https://doi.org/10.1109/JIOT.2019.2963789

Chen, Y., Meng, L., Zhou, H., & Xue, G. (2021). A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. *Wireless Communications and Mobile Computing, 2021*, 1–12. https://doi.org/10.1155/2021/6685762

Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C. (2020). Design of a Secure Medical Data Sharing Scheme Based on Blockchain. *Journal of Medical Systems*, *44*(2), 52. https://doi.org/10.1007/s10916-019-1468-1

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLOS ONE*, *15*(12), e0243043. https://doi.org/10.1371/journal.pone.0243043

Cho, J.-H., Chan, K., & Adali, S. (2015). A Survey on Trust Modeling. *ACM Computing Surveys*, *48*(2), 1–40. https://doi.org/10.1145/2815595

Cho, J.-H., Swami, A., & Chen, I.-R. (2011). A Survey on Trust Management for Mobile Ad Hoc Networks. *IEEE Communications Surveys & Tutorials*, *13*(4), 562–583. https://doi.org/10.1109/SURV.2011.092110.00088

Chohan, U. W. (2017). The Double Spending Problem and Cryptocurrencies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3090174

Choi, Y. B. (2021). Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases. *International Journal of Cyber Research and Education*, *3*(1), 58–64. https://doi.org/10.4018/IJCRE.2021010106

Chris Baraniuk. (2016). *Millions of Mexican voter records "were accessible online."* Bbc. https://www.bbc.com/news/technology-36128745

Cocchia, A. (2014). Smart and Digital City: A Systematic Literature Review. In *Smart city* (pp. 13–43). Springer. https://doi.org/10.1007/978-3-319-06160-3_2

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104–126. https://doi.org/10.1007/BF03177550

Corbet, S., Lucey, B., & Yarovaya, L. (2018). Datestamping the Bitcoin and Ethereum bubbles. *Finance Research Letters*, *26*, 81–88. https://doi.org/10.1016/j.frl.2017.12.006

Cristina Costa, A., & Bijlsma-Frankema, K. (2007). Trust and Control Interrelations. *Group & Organization Management*, *32*(4), 392–406. https://doi.org/10.1177/1059601106293871

Cui, H., Wan, Z., Wei, X., Nepal, S., & Yi, X. (2020). Pay as You Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain. *IEEE Transactions on Information Forensics and Security*, *15*, 3227–3238. https://doi.org/10.1109/TIFS.2020.2973864

Damgård, I. B. (1988). Collision Free Hash Functions and Public Key Signature Schemes. In *W.L. (eds) Advances in Cryptology — EUROCRYPT' 87. EUROCRYPT 1987. Lecture Notes in Computer Science: Vol. 304 LNCS* (pp. 203–216). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39118-5_19

Damgård, I. B. (1990). A design principle for hash functions. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *435 LNCS*, 416–427. https://doi.org/10.1007/0-387-34805-0_39

Dannen, C. (2017). Introducing Ethereum and Solidity. In *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress. https://doi.org/10.1007/978-1-4842-2535-6

Das, T. K., & Teng, B.-S. (1996). RISK TYPES AND INTER-FIRM ALLIANCE STRUCTURES. *Journal of Management Studies*, *33*(6), 827–843. https://doi.org/10.1111/j.1467-6486.1996.tb00174.x

Daud, N. M. N., Bakar, N. A. A. A., & Rusli, H. M. (2010). Implementing rapid application development (RAD) methodology in developing practical training application system. *2010 International Symposium on Information Technology*, *3*, 1664–1667. https://doi.org/10.1109/ITSIM.2010.5561634

de Haes, A. U. (2010). *Microsoft bpos cloud service hit with data breach*. Computerworld, December. https://www.computerworld.com/article/2511862/microsoft-bpos-cloud-service-hit-with-data-breach.html

de la Vega, F., Soriano, J., Jimenez, M., & Lizcano, D. (2018). A Peer-to-Peer Architecture for Distributed Data Monetization in Fog Computing Scenarios. *Wireless Communications and Mobile Computing*, *2018*, 1–15. https://doi.org/10.1155/2018/5758741

Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. *Computer Networks*, *31*(8), 805–822. https://doi.org/10.1016/S1389-1286(98)00017-6

Deng, Z., Ren, Y., Liu, Y., Yin, X., Shen, Z., & Kim, H.-J. (2019). Blockchain-Based Trusted Electronic Records Preservation in Cloud Storage. *Computers, Materials & Continua*, *58*(1), 135–151. https://doi.org/10.32604/cmc.2019.02967

Department of Justice. (2019). *United States v. Paige Thompson*. United States Attorneys Office. https://www.justice.gov/usao-wdwa/united-states-v-paige-thompson

Dexter, F. (2013). Wilcoxon-Mann-Whitney Test Used for Data That Are Not Normally Distributed. *Anesthesia & Analgesia*, *117*(3), 537–538. https://doi.org/10.1213/ANE.0b013e31829ed28f

Di Francesco Maesa, D., Mori, P., & Ricci, L. (2018). Blockchain Based Access Control Services. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1379–1386. https://doi.org/10.1109/Cybermatics_2018.2018.00237

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: Securing Internet of Medical Things (IoMT). *International Journal of Advanced Computer Science and Applications*, *10*(1), 82–89. https://doi.org/10.14569/IJACSA.2019.0100110

Dorsala, M. R., Sastry, V. N., & Chapram, S. (2020). Fair payments for verifiable cloud services using smart contracts. *Computers & Security*, *90*, 101712. https://doi.org/10.1016/j.cose.2019.101712

Doyle, L., Brady, A.-M., & Byrne, G. (2009). An overview of mixed methods research. *Journal of Research in Nursing*, *14*(2), 175–185. https://doi.org/10.1177/1744987108093962

Dwivedi, S. K., Amin, R., & Vollala, S. (2021). Blockchain-Based Secured IPFS-

Enable Event Storage Technique With Authentication Protocol in VANET. *IEEE/CAA Journal of Automatica Sinica*, *8*(12), 1913–1922. https://doi.org/10.1109/JAS.2021.1004225

Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey. *Security and Communication Networks*, *2021*, 1–21. https://doi.org/10.1155/2021/7142048

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*, S90–S98. https://doi.org/10.1016/j.diin.2012.05.001

Elsayeh, M., Ezzat, K. A., El-Nashar, H., & Omran, L. N. (2021). CYBERSECURITY ARCHITECTURE FOR THE INTERNET OF MEDICAL THINGS AND CONNECTED DEVICES USING BLOCKCHAIN. *Biomedical Engineering: Applications, Basis and Communications*, *33*(02), 2150013. https://doi.org/10.4015/S1016237221500137

Eltayieb, N., Elhabob, R., Hassan, A., & Li, F. (2020). A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. *Journal of Systems Architecture*, *102*, 101653. https://doi.org/10.1016/j.sysarc.2019.101653

Ethereum. (2021). *ethereum/web3.py*. Truffle Suite. https://github.com/ethereum/web3.py (Original work published 2016)

Etro, F. (2015). The Economics of Cloud Computing. In *Cloud Technology* (Vol. 4, pp. 2135–2148). IGI Global. https://doi.org/10.4018/978-1-4666-6539-2.ch101

Falagas, M. E., Pitsouni, E. I., Malietzis, G. A., & Pappas, G. (2008). Comparison of PubMed, Scopus, Web of Science, and Google Scholar: strengths and weaknesses. *The FASEB Journal*, *22*(2), 338–342. https://doi.org/10.1096/fj.07-9492LSF

Fan, K., Bao, Z., Liu, M., Vasilakos, A. V., & Shi, W. (2020). Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Generation Computer Systems*, *110*, 665–674. https://doi.org/10.1016/j.future.2019.10.014

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45–58. https://doi.org/10.1016/j.jnca.2018.10.020

Fikri, M. Al, Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Fischl, M., Scherrer-Rathje, M., & Friedli, T. (2014). Digging deeper into supply risk: a systematic literature review on price risks. *Supply Chain Management: An International Journal*, *19*(5/6), 480–503. https://doi.org/10.1108/SCM-12-2013-0474

Flick, U. (2018). *An introduction to qualitative research*. sage.

Gambetta, D. (2000). Can We Trust Trust? *Trust: Making and Breaking Cooperative Relations*, *13*, 213–237. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.5695&rep=rep1

&type=pdf

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

Garfield, E. (1977). PROPOSAL FOR A NEW PROFESSION-SCIENTIFIC REVIEWER. *Current Contents*, *14*, 5–8.

Gibbs, J. P., & Coleman, J. S. (1990). Foundations of Social Theory. *Social Forces*, *69*(2), 625. https://doi.org/10.2307/2579680

Gimenez-Aguilar, M., de Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems*, *124*, 91–118. https://doi.org/10.1016/j.future.2021.05.007

Giurgiu, I., Riva, O., Juric, D., Krivulev, I., & Alonso, G. (2009). Calling the Cloud: Enabling Mobile Phones as Interfaces to Cloud Applications. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 5896 LNCS* (pp. 83–102). Springer. https://doi.org/10.1007/978-3-642-10445-9_5

Gomez, J. M., & Mouselli, S. (2018). Modernizing the Academic Teaching and Research Environment. In J. Marx Gómez & S. Mouselli (Eds.), *Springer International Publishing Switzerland*. Springer International Publishing. https://doi.org/10.1007/978-3-319-74173-4

Goodin, D. (2016). *Firefox ready to block certificate authority that threatened web security*. Ars Technica. https://arstechnica.netblogpro.com/information-technology/2016/09/firefox-ready-to-block-certificate-authority-that-threatened-web-security

Gourisaria, M. K., Samanta, A., Saha, A., Patra, S. S., & Khilar, P. M. (2020). An Extensive Review on Cloud Computing. In *Advances in Intelligent Systems and Computing* (Vol. 1079, pp. 53–78). Springer. https://doi.org/10.1007/978-981-15-1097-7_6

Goyal, S. (2014). Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *International Journal of Computer Network and Information Security*, *6*(3), 20–29. https://doi.org/10.5815/ijcnis.2014.03.03

Grigore, R. (2017). Java generics are turing complete. *ACM SIGPLAN Notices*, *52*(1), 73–85. https://doi.org/10.1145/3093333.3009871

Gueron, S., Johnson, S., & Walker, J. (2011). SHA-512/256. *2011 Eighth International Conference on Information Technology: New Generations*, 354–358. https://doi.org/10.1109/ITNG.2011.69

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough? *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Guo, S., Dai, Y., Xu, S., Qiu, X., & Qi, F. (2020). Trusted Cloud-Edge Network Resource Management: DRL-Driven Service Function Chain Orchestration for IoT. *IEEE Internet of Things Journal*, *7*(7), 6010–6022. https://doi.org/10.1109/JIOT.2019.2951593

Guo, S., Hu, X., Zhou, Z., Wang, X., Qi, F., & Gao, L. (2019). Trust access authentication in vehicular network based on blockchain. *China Communications*, *16*(6), 18–30. https://doi.org/10.23919/JCC.2019.06.002

Guo, Y., Wang, S., & Huang, J. (2021). A blockchain-assisted framework for secure and reliable data sharing in distributed systems. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), 169. https://doi.org/10.1186/s13638-021-02041-y

Hao, K., Xin, J., Wang, Z., Cao, K., & Wang, G. (2019). Blockchain-Based Outsourced Storage Schema in Untrusted Environment. *IEEE Access*, *7*, 122707–122721. https://doi.org/10.1109/ACCESS.2019.2938578

Hardin, T., & Kotz, D. (2021). Amanuensis: Information provenance for health-data systems. *Information Processing & Management*, *58*(2), 102460. https://doi.org/10.1016/j.ipm.2020.102460

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Hei, Y., Liu, Y., Li, D., Liu, J., & Wu, Q. (2021). Themis: An accountable blockchain-based P2P cloud storage scheme. *Peer-to-Peer Networking and Applications*, *14*(1), 225–239. https://doi.org/10.1007/s12083-020-00967-6

Hertig, A. (2017). *Ethereum's Big Switch: The New Roadmap to Proof-of-Stake*. Online. https://www.coindesk.com/markets/2017/05/05/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Honar Pajooh, H., Rashid, M. A., Alam, F., & Demidenko, S. (2021). IoT Big Data provenance scheme using blockchain on Hadoop ecosystem. *Journal of Big Data*, *8*(1), 114. https://doi.org/10.1186/s40537-021-00505-y

Huang, C., Chen, W., Yuan, L., Ding, Y., Jian, S., Tan, Y., Chen, H., & Chen, D. (2021). Toward security as a service: A trusted cloud service architecture with policy customization. *Journal of Parallel and Distributed Computing*, *149*, 76–88. https://doi.org/10.1016/j.jpdc.2020.11.002

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *2*(1), 9. https://doi.org/10.1186/2192-113X-2-9

Huang, P., Fan, K., Yang, H., Zhang, K., Li, H., & Yang, Y. (2020). A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System. *IEEE Access*, *8*, 94780–94794. https://doi.org/10.1109/ACCESS.2020.2993606

Huang, Z., Mi, Z., & Hua, Z. (2020). HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain. *China Communications*, *17*(9), 1–10. https://doi.org/10.23919/JCC.2020.09.001

Huber, G. P., & McDaniel, R. R. (1986). The Decision-Making Paradigm of Organizational Design. *Management Science*, *32*(5), 572–589. https://doi.org/10.1287/mnsc.32.5.572

ISC2 Foundation, & Cybersecurity Insiders. (2022). *2022 Cloud Security Report*. https://www.isc2.org/-/media/ISC2/Research/Resource-

Thumbnails/Resource-Center/Research/2021-Cloud-Security-Report-FINAL.ashx

ISO 27005. (2018). *Information Technology. Security Techniques. Information Security Risk Management: ISO/IEC 27005: 2018*. International Organization for Standardization.

James Jr., H. S. (2002). The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization*, *47*(3), 291–307. https://doi.org/10.1016/S0167-2681(01)00214-1

Jan, M. A., Cai, J., Gao, X.-C., Khan, F., Mastorakis, S., Usman, M., Alazab, M., & Watters, P. (2021). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *Journal of Network and Computer Applications*, *175*, 102918. https://doi.org/10.1016/j.jnca.2020.102918

Janjua, K., Shah, M. A., Almogren, A., Khattak, H. A., Maple, C., & Din, I. U. (2020). Proactive Forensics in IoT: Privacy-Aware Log-Preservation Architecture in Fog-Enabled-Cloud Using Holochain and Containerization Technologies. *Electronics*, *9*(7), 1172. https://doi.org/10.3390/electronics9071172

Jarrow, R. A. (2008). Operational risk. *Journal of Banking & Finance*, *32*(5), 870–879. https://doi.org/10.1016/j.jbankfin.2007.06.006

Jayasinghe, U., Lee, G. M., MacDermott, Á., & Rhee, W. S. (2019). TrustChain: A Privacy Preserving Blockchain with Edge Computing. *Wireless Communications and Mobile Computing*, *2019*, 1–17. https://doi.org/10.1155/2019/2014697

Jeong, Y.-S., & Sim, S.-H. (2021). Hierarchical Multipath Blockchain Based IoT Information Management Techniques for Efficient Distributed Processing of Intelligent IoT Information. *Sensors*, *21*(6), 2049. https://doi.org/10.3390/s21062049

Jiang, Y., Shen, X., & Zheng, S. (2021). An Effective Data Sharing Scheme Based on Blockchain in Vehicular Social Networks. *Electronics*, *10*(2), 114. https://doi.org/10.3390/electronics10020114

Johns, E. (2020). Cyber security breaches survey 2020. *London: Department for Digital, Culture, Media & Sport*.

Jøsang, A., & Presti, S. Lo. (2004). Analysing the Relationship between Risk and Trust. In *International conference on trust management* (pp. 135–145). Springer. https://doi.org/10.1007/978-3-540-24747-0_11

Jow, J., Xiao, Y., & Han, W. (2017). A survey of intrusion detection systems in smart grid. *International Journal of Sensor Networks*, *23*(3), 170. https://doi.org/10.1504/IJSNET.2017.083410

Khader, A. S., & Lai, D. (2015). Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. *2015 22nd International Conference on Telecommunications (ICT)*, 204–208. https://doi.org/10.1109/ICT.2015.7124683

Khajeh-Hosseini, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2012). The Cloud Adoption Toolkit: supporting cloud adoption decisions in the enterprise. *Software: Practice and Experience*, *42*(4), 447–465. https://doi.org/10.1002/spe.1072

Khan, K. M., & Malluhi, Q. (2010). Establishing Trust in Cloud Computing. *IT Professional*, *12*(5), 20–27. https://doi.org/10.1109/MITP.2010.128

Khan, M. A., & Salah, K. (2020). Cloud adoption for e-learning: Survey and future challenges. *Education and Information Technologies*, *25*(2), 1417–1438. https://doi.org/10.1007/s10639-019-10021-5

Khan, Z., Abbasi, A. G., & Pervez, Z. (2020). Blockchain and edge computing–based architecture for participatory smart city applications. *Concurrency and Computation: Practice and Experience*, *32*(12). https://doi.org/10.1002/cpe.5566

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 20. https://doi.org/10.1186/s42400-019-0038-7

Khurshid, A. (2020). Applying Blockchain Technology to Address the Crisis of Trust During the COVID-19 Pandemic. *JMIR Medical Informatics*, *8*(9), e20477. https://doi.org/10.2196/20477

Kim, H.-W., & Jeong, Y.-S. (2018). Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain. *Human-Centric Computing and Information Sciences*, *8*(1), 11. https://doi.org/10.1186/s13673-018-0136-7

Kitchenham, B. (2004). Procedures for performing systematic literature reviews. *Joint Technical Report, Keele University TR/SE-0401 and NICTA TR-0400011T.1*, *33*(2004), 33. http://www.elizabete.com.br/rs/Tutorial_IHC_2012_files/Conceitos_RevisaoSistematica_kitchenham_2004.pdf%0Ahttp://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Kochovski, P., Gec, S., Stankovski, V., Bajec, M., & Drobintsev, P. D. (2019). Trust management in a blockchain based fog computing platform with trustless smart oracles. *Future Generation Computer Systems*, *101*, 747–759. https://doi.org/10.1016/j.future.2019.07.030

Kothari, C. R. (2004). Research Methodology: Methods and Techniques. In *New Age International*. New Age International Limited. https://books.google.de/books?id=8c6gkbKi-F4C

Krueger, R. A. (2014). *Focus groups: A practical guide for applied research*. Sage publications.

Kuckartz, U., & Rädiker, S. (2019). Analyzing Qualitative Data with MAXQDA. In *Analyzing Qualitative Data with MAXQDA*. Springer International Publishing. https://doi.org/10.1007/978-3-030-15671-8

Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V., & Hossain, E. (2020). A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access*, *8*, 118433–118471. https://doi.org/10.1109/ACCESS.2020.3004790

Kumar, Rakesh, & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1–48. https://doi.org/10.1016/j.cosrev.2019.05.002

Kumar, Randhir, & Tripathi, R. (2021a). DBTP2SF: A deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems. *Transactions on Emerging Telecommunications Technologies*, *32*(4). https://doi.org/10.1002/ett.4222

Kumar, Randhir, & Tripathi, R. (2021b). Data Provenance and Access Control Rules for Ownership Transfer Using Blockchain. *International Journal of Information Security and Privacy*, *15*(2), 87–112. https://doi.org/10.4018/IJISP.2021040105

Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *Journal of Parallel and Distributed Computing*, *143*, 148–166. https://doi.org/10.1016/j.jpdc.2020.05.004

Kydd, A. H. (2018). Trust and Mistrust in International Relations. In *Trust and Mistrust in International Relations*. Princeton University Press. https://doi.org/10.2307/j.ctv39x4z5

Ladia, A. (2021). Blockchain: A Privacy Centered Standard for Corporate Compliance. *IT Professional*, *23*(1), 86–91. https://doi.org/10.1109/MITP.2020.2975486

Lagerspetz, O. (1998). Trust: The Tacit Demand. In *Library of Ethics and Applied Philosophy* (Vol. 1). Springer Netherlands. https://doi.org/10.1007/978-94-015-8986-4

Larsen, R. J., & Marx, M. L. (2005). *An introduction to mathematical statistics*. Prentice Hall.

Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *46*(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392

Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security*, *3*(4), 227–261. https://doi.org/10.1145/382912.382914

Lejun, Z., Minghui, P., Weizheng, W., Yansen, S., Shuna, C., & Seokhoon, K. (2020). Secure and Efficient Medical Data Storage and Sharing Scheme Based on Double Blockchain. *Computers, Materials & Continua*, *66*(1), 499–515. https://doi.org/10.32604/cmc.2020.012205

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal*, *26*(2), 110–139. https://doi.org/10.1108/RMJ-12-2015-0042

Levy, Y., & J. Ellis, T. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: The International Journal of an Emerging Transdiscipline*, *9*, 181–212. https://doi.org/10.28945/479

Leymann, F. (2009). Cloud Computing: The Next Revolution in IT. *Proc. 52th Photogrammetric Week*, 3–12. http://www2.informatik.uni-stuttgart.de/cgi-bin/NCSTRL/NCSTRL_view.pl?id=INPROC-2009-65&engl=0

Li, C., Qu, X., & Guo, Y. (2021). TFCrowd: a blockchain-based crowdsourcing framework with enhanced trustworthiness and fairness. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), 168. https://doi.org/10.1186/s13638-021-02040-z

Li, J., Wu, J., Jiang, G., & Srikanthan, T. (2020). Blockchain-based public auditing for big data in cloud storage. *Information Processing & Management*, *57*(6), 102382. https://doi.org/10.1016/j.ipm.2020.102382

Li, R., Song, T., Mei, B., Li, H., Cheng, X., & Sun, L. (2019). Blockchain for Large-Scale Internet of Things Data Storage and Protection. *IEEE Transactions on Services Computing*, *12*(5), 762–771. https://doi.org/10.1109/TSC.2018.2853167

Li, Shancang, Xu, L. Da, & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, Song, Liu, J., Yang, G., & Han, J. (2020). A Blockchain-Based Public Auditing Scheme for Cloud Storage Environment without Trusted Auditors. *Wireless Communications and Mobile Computing*, *2020*, 1–13. https://doi.org/10.1155/2020/8841711

Li, T., Zhang, J., Lin, Y., Zhang, S., & Ma, J. (2021). Blockchain-Based Fine-Grained Data Sharing for Multiple Groups in Internet of Things. *Security and Communication Networks*, *2021*, 1–13. https://doi.org/10.1155/2021/6689448

Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing*, *54*, 133–144. https://doi.org/10.1016/j.rcim.2018.05.011

Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

Lin, C., He, D., Huang, X., & Choo, K.-K. R. (2021). OBFP: Optimized Blockchain-Based Fair Payment for Outsourcing Computations in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, *16*, 3241–3253. https://doi.org/10.1109/TIFS.2021.3073818

Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2020). Conducting systematic literature reviews and bibliometric analyses. *Australian Journal of Management*, *45*(2), 175–194. https://doi.org/10.1177/0312896219877678

Liu, X., Ma, W., & Cao, H. (2019). MBPA: A Medibchain-Based Privacy-Preserving Mutual Authentication in TMIS for Mobile Medical Cloud Architecture. *IEEE Access*, *7*, 149282–149298. https://doi.org/10.1109/ACCESS.2019.2947313

Loch, W. J., Koslovski, G. P., Pillon, M. A., Miers, C. C., & Pasin, M. (2021). A novel blockchain protocol for selecting microservices providers and auditing contracts. *Journal of Systems and Software*, *180*, 111030. https://doi.org/10.1016/j.jss.2021.111030

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. *IEEE Transactions on Engineering Management*, *67*(4), 1256–1270. https://doi.org/10.1109/TEM.2020.2978014

Loper, E., & Bird, S. (2002). NLTK: The Natural Language Toolkit. *Proceedings of the 42nd Annual Meeting of the Association for Computational Linguistics*, 1–4. https://doi.org/10.48550/arXiv.cs/0205028

Luhmann, N. (2017). *Trust and power*. John Wiley & Sons.

Lynn, T., van der Werff, L., & Fox, G. (2021). Understanding Trust and Cloud Computing: An Integrated Framework for Assurance and Accountability in the Cloud. In *Palgrave Studies in Digital Business and Enabling Technologies* (pp. 1–20). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-54660-1_1

Lyons, V. (2021). Justice vs Control in Cloud Computing: A Conceptual Framework for Positioning a Cloud Service Provider's Privacy Orientation. In *Palgrave Studies in Digital Business and Enabling Technologies* (pp. 79–104). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-54660-1_5

Ma, D. (2007). The Business Model of "Software-As-A-Service." *IEEE International Conference on Services Computing (SCC 2007)*, 701–702. https://doi.org/10.1109/SCC.2007.118

Ma, M., Shi, G., & Li, F. (2019). Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. *IEEE Access*, *7*, 34045–34059. https://doi.org/10.1109/ACCESS.2019.2904042

Ma, X., Wang, C., & Chen, X. (2021). Trusted data sharing with flexible access control based on blockchain. *Computer Standards & Interfaces*, *78*, 103543. https://doi.org/10.1016/j.csi.2021.103543

Makhlouf, R. (2020). Cloudy transaction costs: a dive into cloud computing economics. *Journal of Cloud Computing*, *9*(1), 1. https://doi.org/10.1186/s13677-019-0149-4

Malamas, V., Kotzanikolaou, P., Dasaklis, T. K., & Burmester, M. (2020). A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data. *IEEE Access*, *8*, 134393–134412. https://doi.org/10.1109/ACCESS.2020.3011201

Mamta, Gupta, B. B., Li, K.-C., Leung, V. C. M., Psannis, K. E., & Yamaguchi, S. (2021). Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System. *IEEE/CAA Journal of Automatica Sinica*, *8*(12), 1877–1890. https://doi.org/10.1109/JAS.2021.1004003

Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., & Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, *176*, 102917. https://doi.org/10.1016/j.jnca.2020.102917

Marmsoler, D., & Gidey, H. K. (2019). Interactive verification of architectural design patterns in FACTum. *Formal Aspects of Computing*, *31*(5), 541–610. https://doi.org/10.1007/s00165-019-00488-x

Martens, B., Walterbusch, M., & Teuteberg, F. (2012). Costing of Cloud Computing Services: A Total Cost of Ownership Approach. *2012 45th Hawaii International Conference on System Sciences*, 1563–1572. https://doi.org/10.1109/HICSS.2012.186

Martín-Martín, A., Orduna-Malea, E., Thelwall, M., & Delgado López-Cózar, E. (2018). Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories. *Journal of Informetrics*, *12*(4), 1160–1177. https://doi.org/10.1016/j.joi.2018.09.002

Martin, J. (1991). *Rapid application development*. Macmillan Publishing Co., Inc.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model Of Organizational Trust. *Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Mayring, P. (2000). Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *1*(2). https://doi.org/https://doi.org/10.17169/fqs-1.2.1089

Mayukh Mukhopadhyay. (2018). *Ethereum Smart Contract Development*. Packt Publishing Ltd. https://books.google.co.id/books?hl=en&lr=&id=AOlODwAAQBAJ&oi=fnd&pg=PP1&dq=Mukhopadhyay+private+blockchain&ots=rTyHUazM_j&sig=sxnCDxicycqC6DtIuU55VD86uB8&redir_esc=y#v=onepage&q=Mukhopadhyay private blockchain&f=false

McCafferty, D. (2015). *How Unexpected Costs Create a "Cloud Hangover."* CIO Insight. https://www.cioinsight.com/it-strategy/cloud-virtualization/slideshows/how-unexpected-costs-create-a-cloud-hangover.html

McFarlane, N. (2004). *Rapid application development with Mozilla*. Prentice Hall Professional.

McGrew, D., & Viega, J. (2004). The Galois/counter mode of operation (GCM). *Submission to NIST Modes of Operation Process*, *20*, 70–278.

Mell, P., & Grance, T. (2017). The NIST Definition of Cloud Computing. In *Application Performance Management (APM) in the Digital Enterprise* (pp. 267–269). Elsevier. https://doi.org/10.1016/B978-0-12-804018-8.15003-X

Memon, R. A., Li, J. P., Nazeer, M. I., Khan, A. N., & Ahmed, J. (2019). DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things. *IEEE Access*, *7*, 169073–169093. https://doi.org/10.1109/ACCESS.2019.2952472

Merna, T., & Al-Thani, F. F. (2008). *Corporate risk management*. John Wiley & Sons.

Meuser, M., & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In *Interviewing Experts* (pp. 17–42). Palgrave Macmillan UK. https://doi.org/10.1057/9780230244276_2

Mhaisen, N., Fetais, N., Erbad, A., Mohamed, A., & Guizani, M. (2020). To chain or not to chain: A reinforcement learning approach for blockchain-enabled IoT monitoring applications. *Future Generation Computer Systems*, *111*, 39–51. https://doi.org/10.1016/j.future.2020.04.035

Michael, B. (2009). In Clouds Shall We Trust? *IEEE Security & Privacy Magazine*, *7*(5), 3–3. https://doi.org/10.1109/MSP.2009.124

Microsoft. (2021). *Azure SDK*. Microsoft. https://azure.microsoft.com/en-us/downloads/

Miraz, M. H., & Ali, M. (2018). Applications of Blockchain Technology beyond Cryptocurrency. *Annals of Emerging Technologies in Computing*, *2*(1), 1–6. https://doi.org/10.33166/AETiC.2018.01.001

Mishra, N. (2015). Data localization laws in a digital world: Data protection or data protectionism? *Economics of Networks EJournal*, *19/05*.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*, *8*, 100107. https://doi.org/10.1016/j.iot.2019.100107

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of Smart Contract and

Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4. https://doi.org/10.1109/ICCCNT.2018.8494045

Moreno-Vozmediano, R., Montero, R. S., & Llorente, I. M. (2013). Key Challenges in Cloud Computing: Enabling the Future Internet of Services. *IEEE Internet Computing*, *17*(4), 18–25. https://doi.org/10.1109/MIC.2012.69

Muhammed, A. S., & Ucuz, D. (2020). Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–4. https://doi.org/10.1109/ISDFS49300.2020.9116254

Muris, T. J. (1981). Opportunistic Behavior and The Law of Contracts. *Minnesota Law Review*, *65*, 521–590. https://scholarship.law.umn.edu/mlr/2443

Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access*, *8*, 205190–205205. https://doi.org/10.1109/ACCESS.2020.3036812

Nadeem, S., Rizwan, M., Ahmad, F., & Manzoor, J. (2019). Securing Cognitive Radio Vehicular Ad Hoc Network with Fog Node based Distributed Blockchain Cloud Architecture. *International Journal of Advanced Computer Science and Applications*, *10*(1), 288–295. https://doi.org/10.14569/IJACSA.2019.0100138

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nalendra, A. K. (2021). Rapid Application Development (RAD) model method for creating an agricultural irrigation system based on internet of things. *IOP Conference Series: Materials Science and Engineering*, *1098*(2), 022103. https://doi.org/10.1088/1757-899X/1098/2/022103

Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. *Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times - Dg.o '11*, 282. https://doi.org/10.1145/2037556.2037602

Naresh, V. S., Reddi, S., & Allavarpu, V. V. L. D. (2021). Blockchain-based patient centric health care communication system. *International Journal of Communication Systems*, *34*(7). https://doi.org/10.1002/dac.4749

Naylor, D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò, M., Papagiannaki, K., & Steenkiste, P. (2014). The Cost of the "S" in HTTPS. *Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies*, 133–140. https://doi.org/10.1145/2674005.2674991

Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. *Sustainability*, *11*(24), 7054. https://doi.org/10.3390/su11247054

Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in Blockchain. *Journal of Information Processing Systems*, *14*(1), 101–128. https://doi.org/https://doi.org/10.3745/JIPS.01.0024

NIST, C. (1992). The digital signature standard. *Communications of the ACM*, *35*(7), 36–40. https://doi.org/10.1145/129902.129904

NIST, N. (2012). Guide for conducting risk assessments. In *Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Noraziah, A., Fakherldin, M. A. I., Adam, K., & Majid, M. A. (2017). Big Data Processing in Cloud Computing Environments. *Advanced Science Letters*, *23*(11), 11092–11095. https://doi.org/10.1166/asl.2017.10227

Nurseitov, N., Paulson, M., Reynolds, R., & Izurieta, C. (2009). Comparison of JSON and XML data interchange formats: A case study. *22nd International Conference on Computer Applications in Industry and Engineering 2009, CAINE 2009*, *9*, 157–162.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1954824

Panja, S., & Roy, B. (2021). A secure end-to-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications*, *59*, 102815. https://doi.org/10.1016/j.jisa.2021.102815

Park, J., & Park, J. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry*, *9*(8), 164. https://doi.org/10.3390/sym9080164

Patidar, A., & Suman, U. (2015). A survey on software architecture evaluation methods. *2015 International Conference on Computing for Sustainable Global Development, INDIACom 2015*, 967–972.

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. https://doi.org/10.1109/CloudCom.2010.66

Peral, J., Gallego, E., Gil, D., Tanniru, M., & Khambekar, P. (2020). Using Visualization to Build Transparency in a Healthcare Blockchain Application. *Sustainability*, *12*(17), 6768. https://doi.org/10.3390/su12176768

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software*, *103*, 167–181. https://doi.org/10.1016/j.jss.2015.02.002

Pinheiro, A., Canedo, E. D., De Sousa, R. T., & De Oliveira Albuquerque, R. (2020). Monitoring File Integrity Using Blockchain and Smart Contracts. *IEEE Access*, *8*, 198548–198579. https://doi.org/10.1109/ACCESS.2020.3035271

Pohontsch, N. J. (2019). Die Qualitative Inhaltsanalyse. *Die Rehabilitation*, *58*(06), 413–418. https://doi.org/10.1055/a-0801-5465

Pornin, T. (2013). *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*. https://doi.org/10.17487/rfc6979

Porter, M. F. (2001). *Snowball: A language for stemming algorithms*. http://snowball.tartarus.org/texts/introduction.html

Povey, D. (1999). Developing Electronic Trust Policies Using a Risk Management Model BT - Secure Networking — CQRE [Secure] ' 99. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and*

Lecture Notes in Bioinformatics) (Vol. 1740, pp. 1–16). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-46701-7_1

Powell, R. A., & Single, H. M. (1996). Focus Groups. *International Journal for Quality in Health Care*, *8*(5), 499–504. https://doi.org/10.1093/intqhc/8.5.499

Prasad, S., Shankar, R., Gupta, R., & Roy, S. (2018). A TISM modeling of critical success factors of blockchain based cloud services. *Journal of Advances in Management Research*, *15*(4), 434–456. https://doi.org/10.1108/JAMR-03-2018-0027

Pressman, R. S. (2005). *Software engineering: a practitioner's approach*. Palgrave macmillan.

Prinz, W., Rose, T., & Urbach, N. (2022). Blockchain Technology and International Data Spaces. In *Designing Data Spaces* (pp. 165–180). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_10

PRNewswire. (2019). *Capital One Announces Data Security Incident*. Capital One. //www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/

Purdy, G. (2010). ISO 31000:2009-Setting a New Standard for Risk Management. *Risk Analysis*, *30*(6), 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

Pustisek, M., Stefanic Juznic, L., & Kos, A. (2018). Blockchain Support in IoT Platforms. *IPSI BgD Transactions on Internet Research*, *14*(1), 13–20.

Pustišek, M., Umek, A., & Kos, A. (2019). Approaching the Communication Constraints of Ethereum-Based Decentralized Applications. *Sensors*, *19*(11), 2647. https://doi.org/10.3390/s19112647

Rahman, Z., Khalil, I., Yi, X., & Atiquzzaman, M. (2021). Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. *IEEE Communications Magazine*, *59*(5), 128–134. https://doi.org/10.1109/MCOM.001.2000679

Rai, R., Sahoo, G., & Mehfuz, S. (2015). Exploring the factors influencing the cloud computing adoption: a systematic study on cloud migration. *SpringerPlus*, *4*(1), 197. https://doi.org/10.1186/s40064-015-0962-2

Raza, A., Zafar, S., Rehman, S. U., & Khattak, U. (2019). Software Architecture Evaluation Methods: A Comparative Study. *International Journal of Computing and Communication Networks*, *1*(2), 1–9.

Razaque, A., Frej, M. B. H., Alotaibi, B., & Alotaibi, M. (2021). Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey. *Electronics*, *10*(21), 2721. https://doi.org/10.3390/electronics10212721

Reagan, R. (2018). Azure Data Storage Overview. In *Web Applications on Azure* (pp. 61–76). Apress. https://doi.org/10.1007/978-1-4842-2976-7_3

Reed, C., Sathyanarayan, U. M., Ruan, S., & Collins, J. (2018). Beyond BitCoin-legal impurities and off-chain assets. *International Journal of Law and Information Technology*, *26*(2), 160–182. https://doi.org/10.1093/ijlit/eay006

Reiswig, J. (2010). Mendeley. *Journal of the Medical Library Association : JMLA*, *98*(2), 193–194. https://doi.org/10.3163/1536-5050.98.2.021

Rescorla, E. (2000). HTTP Over TLS. In *IETF Standard*. https://doi.org/10.17487/rfc2818

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Richards, M., & Ford, N. (2020). *Fundamentals of Software Architecture*. O'Reilly Media. https://www.amazon.com/-/es/Mark-Richards-dp-1492043451/dp/1492043451/ref=mt_other?_encoding=UTF8&me=&qid=

RightScale. (2019). *State of the Cloud Report*. https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019

Ringert, J. O., & Rumpe, B. (2011). A Little Synopsis on Streams, Stream Processing Functions, and State-Based Stream Processing. *Int. J. Software and Informatics*, *5*(1), 29–53. http://www.se-rwth.de/publications/A-Little-Synopsis-on-Streams-Stream-Processing-Functions-and-State-Based-Stream-Processing.pdf

Ritchie, D. M. (1984). The UNIX System : A Stream Input-Output System. *AT&T Bell Laboratories Technical Journal*, *63*(8), 1897–1910. https://doi.org/10.1002/j.1538-7305.1984.tb00071.x

Ritter, T., & Pedersen, C. L. (2020). Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. *Industrial Marketing Management*, *86*, 180–190. https://doi.org/10.1016/j.indmarman.2019.11.019

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, *35*(1), 1–7. https://doi.org/10.1037/0003-066X.35.1.1

Rowley, J., & Slack, F. (2004). Conducting a literature review. *Management Research News*, *27*(6), 31–39. https://doi.org/10.1108/01409170410784185

Roy, B., & Graham, T. C. N. (2008). Methods for evaluating software architecture: A survey. *School of Computing TR*, *545*, 82.

Ruggeri, A., Celesti, A., Fazio, M., Galletta, A., & Villari, M. (2020). BCB-X3DH: a Blockchain Based Improved Version of the Extended Triple Diffie-Hellman Protocol. *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 73–78. https://doi.org/10.1109/TPS-ISA50397.2020.00020

Sadashiv, N., & Kumar, S. M. D. (2011). Cluster, grid and cloud computing: A detailed comparison. *2011 6th International Conference on Computer Science & Education (ICCSE)*, 477–482. https://doi.org/10.1109/ICCSE.2011.6028683

Salem, H., Mazzara, M., Saleh, H., Husami, R., & Hattab, S. M. (2022). Development of a Blockchain-Based Ad Listing Application. In *International Conference on Advanced Information Networking and Applications* (pp. 37–45). Springer. https://doi.org/10.1007/978-3-030-99584-3_4

Sato, T., Himura, Y., & Nemoto, J. (2019). Design and Evaluation of Smart-Contract-based System Operations for Permissioned Blockchain-based Systems. *ArXiv Preprint ArXiv:1901.11249*. https://doi.org/https://doi.org/10.48550/arXiv.1901.11249

Schwab, K. (2017). *The Fourth Industrial Revolution*. Crown Publishing Group.

Seaman, C. B. (2008). Qualitative Methods. In *Guide to Advanced Empirical Software Engineering* (pp. 35–62). Springer London. https://doi.org/10.1007/978-1-84800-

044-5_2

Shahriar Rahman, M., Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Wang, G. (2020). Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption. *IEEE Transactions on Engineering Management*, *67*(4), 1476–1486. https://doi.org/10.1109/TEM.2019.2960829

Shaikh, A. A., & Iyer, K. (2019). Security and Privacy Issues in Cloud Computing. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 26, pp. 1299–1306). Springer. https://doi.org/10.1007/978-3-030-03146-6_152

Shanmugapriya, P., & M. Suresh, R. (2012). Software Architecture Evaluation Methods A Survey. *International Journal of Computer Applications*, *49*(16), 19–26. https://doi.org/10.5120/7711-1107

Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. *Applied Sciences*, *9*(6), 1207. https://doi.org/10.3390/app9061207

Shen, W., Hu, T., Zhang, C., & Ma, S. (2021). Secure sharing of big digital twin data for smart manufacturing based on blockchain. *Journal of Manufacturing Systems*, *61*, 338–350. https://doi.org/10.1016/j.jmsy.2021.09.014

Shuai Zhang, Xuebin Chen, Shufen Zhang, & Xiuzhen Huo. (2010). The comparison between cloud computing and grid computing. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, *11*, V11-72-V11-75. https://doi.org/10.1109/ICCASM.2010.5623257

Si, H., Sun, C., Li, Y., Qiao, H., & Shi, L. (2019). IoT information sharing security mechanism based on blockchain technology. *Future Generation Computer Systems*, *101*, 1028–1040. https://doi.org/10.1016/j.future.2019.07.036

Siddiqui, M. S., Ali, T., Nadeem, A., Nawaz, W., & S., S. (2020). BlockTrack-L: A Lightweight Blockchain-based Provenance Message Tracking in IoT. *International Journal of Advanced Computer Science and Applications*, *11*(4), 463–470. https://doi.org/10.14569/IJACSA.2020.0110462

Sifah, E. B., Xia, H., Cobblah, C. N. A., Xia, Q., Gao, J., & Du, X. (2020). BEMPAS: A Decentralized Employee Performance Assessment System Based on Blockchain for Smart City Governance. *IEEE Access*, *8*, 99528–99539. https://doi.org/10.1109/ACCESS.2020.2997650

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027

Singh, P., Masud, M., Hossain, M. S., & Kaur, A. (2021). Cross-domain secure data sharing using blockchain for industrial IoT. *Journal of Parallel and Distributed Computing*, *156*, 176–184. https://doi.org/10.1016/j.jpdc.2021.05.007

Singh, S. K., Manjhi, P. K., & Tiwari, R. K. (2021). Cloud Computing Security Using Blockchain Technology. In *Transforming Cybersecurity Solutions using Blockchain* (pp. 19–30). Springer. https://doi.org/10.1007/978-981-33-6858-3_2

Siva Kumar, A., Godfrey Winster, S., & Ramesh, R. (2021). Efficient sensitivity orient blockchain encryption for improved data security in cloud. *Concurrent Engineering*, *29*(3), 249–257. https://doi.org/10.1177/1063293X211008586

Solhaug, B., Elgesem, D., & Stolen, K. (2007). Why Trust is not Proportional to Risk. *The Second International Conference on Availability, Reliability and Security*

(ARES'07), 11–18. https://doi.org/10.1109/ARES.2007.161

Subramanian, G., & Thampy, A. S. (2021). Implementation of Hybrid Blockchain in a Pre-Owned Electric Vehicle Supply Chain. *IEEE Access*, *9*, 82435–82454. https://doi.org/10.1109/ACCESS.2021.3084942

Sun, P. J. (2019). Research on the Tradeoff Between Privacy and Trust in Cloud Computing. *IEEE Access*, *7*, 10428–10441. https://doi.org/10.1109/ACCESS.2019.2891589

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECS-IJENS*, *11*(5), 23–29.

Swanson, E. S. (2010). A Primer on Functional Methods and the Schwinger-Dyson Equations. *International Journal of Information Technology*, *48*(1), 159–175. https://doi.org/10.1063/1.3523221

Sylvester, A., Tate, M., & Johnstone, D. (2013). Beyond synthesis: re-presenting heterogeneous research literature. *Behaviour & Information Technology*, *32*(12), 1199–1215. https://doi.org/10.1080/0144929X.2011.624633

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Taghavi, M., Bentahar, J., Otrok, H., & Bakhtiyari, K. (2019). A Blockchain-based Model for Cloud Service Quality Monitoring. *IEEE Transactions on Services Computing*, *13*(2), 1–1. https://doi.org/10.1109/TSC.2019.2948010

Tahir, M., Sardaraz, M., Muhammad, S., & Saud Khan, M. (2020). A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics. *Sustainability*, *12*(17), 6960. https://doi.org/10.3390/su12176960

Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine*, *8*(6), 24–31. https://doi.org/10.1109/MSP.2010.186

Talamo, M., Arcieri, F., Dimitri, A., & Schunck, C. H. (2020). A Blockchain based PKI Validation System based on Rare Events Management. *Future Internet*, *12*(2), 40. https://doi.org/10.3390/fi12020040

Tao, D., Yang, Z., Qin, X., Li, Q., Huang, Y., & Luo, Y. (2021). UEPF：A blockchain based Uniform Encoding and Parsing Framework in multi-cloud environments. *KSII Transactions on Internet and Information Systems*, *15*(8), 2849–2864. https://doi.org/10.3837/tiis.2021.08.008

Tashakkori, A., Teddlie, C., & Teddlie, C. B. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). Sage Publications, Inc.

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. https://doi.org/10.1016/j.jocs.2016.11.011

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for

Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, *14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Truffle Suit. (2021). *trufflesuite/ganache-cli*. ethereum. https://github.com/trufflesuite/ganache-cli

Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to Government Cloud Adoption. *International Journal of Managing Information Technology*, *6*(3), 1–16. https://doi.org/10.5121/ijmit.2014.6301

Uriarte, R. B., Zhou, H., Kritikos, K., Shi, Z., Zhao, Z., & De Nicola, R. (2021). Distributed service-level agreement management with smart contracts and blockchain. *Concurrency and Computation: Practice and Experience*, *33*(14). https://doi.org/10.1002/cpe.5800

Vallely, K. S. A., & Gibson, P. (2018). Engaging students on their devices with Mentimeter. *Compass: Journal of Learning and Teaching*, *11*(2), 1–6. https://doi.org/10.21100/compass.v11i2.843

van der Werff, L., Fox, G., Masevic, I., Emeakaroha, V. C., Morrison, J. P., & Lynn, T. (2019). Building consumer trust in the cloud: an experimental analysis of the cloud trust label approach. *Journal of Cloud Computing*, *8*(1), 6. https://doi.org/10.1186/s13677-019-0129-8

Van Rossum, G. (2007). Python Programming language. *USENIX Annual Technical Conference*, *41*(1), 1–36.

Velde, V., Parvez, F. A., & Chaitanya, J. (2022). A Blockchain Enabled System for Security, Non-Repudiation and Integrity of Judiciary Proceedings. *2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, 1–5. https://doi.org/10.1109/ICEEICT53079.2022.9768427

Velmovitsky, P. E., Miranda, P. A. D. S. E. S., Vaillancourt, H., Donovska, T., Teague, J., & Morita, P. P. (2020). A Blockchain-Based Consent Platform for Active Assisted Living: Modeling Study and Conceptual Framework. *Journal of Medical Internet Research*, *22*(12), 20832. https://doi.org/10.2196/20832

Viriyasitavat, W., Xu, L. Da, Bi, Z., Hoonsopon, D., & Charoenruk, N. (2019). Managing QoS of Internet-of-Things Services Using Blockchain. *IEEE Transactions on Computational Social Systems*, *6*(6), 1357–1368. https://doi.org/10.1109/TCSS.2019.2919667

Vivekanandan, M., V. N., S., & U., S. R. (2021). Blockchain based Privacy Preserving User Authentication Protocol for Distributed Mobile Cloud Environment. *Peer-to-Peer Networking and Applications*, *14*(3), 1572–1595. https://doi.org/10.1007/s12083-020-01065-3

Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, *10*(3152676), 10–5555.

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *ECIS 2009 Proceedings*, *161*, 2206–2217. https://doi.org/https://aisel.aisnet.org/ecis2009/161

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A.

(2015). Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. *Communications of the Association for Information Systems, 37*(1), 205–224. https://doi.org/10.17705/1CAIS.03709

Wang, B., Wang, P., & Tu, Y. (2021). Customer satisfaction service match and service quality-based blockchain cloud manufacturing. *International Journal of Production Economics, 240*, 108220. https://doi.org/10.1016/j.ijpe.2021.108220

Wang, Haiyan, & Zhang, J. (2019). Blockchain Based Data Integrity Verification for Large-Scale IoT Data. *IEEE Access, 7*, 164996–165006. https://doi.org/10.1109/ACCESS.2019.2952635

Wang, Han, Wang, X. A., Xiao, S., & Liu, J. (2021). Decentralized data outsourcing auditing protocol based on blockchain. *Journal of Ambient Intelligence and Humanized Computing, 12*(2), 2703–2714. https://doi.org/10.1007/s12652-020-02432-x

Wang, K., Chen, C.-M., Liang, Z., Hassan, M. M., Sarné, G. M. L., Fotia, L., & Fortino, G. (2021). A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain. *Information Fusion, 72*, 100–109. https://doi.org/10.1016/j.inffus.2021.02.011

Wang, S., Wang, X., & Zhang, Y. (2019a). A Secure Cloud Storage Framework With Access Control Based on Blockchain. *IEEE Access, 7*, 112713–112725. https://doi.org/10.1109/ACCESS.2019.2929205

Wang, S., Wang, Y., & Zhang, Y. (2019b). Blockchain-Based Fair Payment Protocol for Deduplication Cloud Storage System. *IEEE Access, 7*, 127652–127668. https://doi.org/10.1109/ACCESS.2019.2939492

Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable. *IEEE Access, 7*, 102887–102901. https://doi.org/10.1109/ACCESS.2019.2931531

Weber, T., & Buchkremer, R. (2022a). *Blockchain-based Cloud Configuration Scrips*. Github. https://github.com/WebThor/Cloud_Configuration_Sourcecode

Weber, T., & Buchkremer, R. (2022b). Blockchain-Based Reference Architecture for Automated, Transparent, and Notarized Attestation of Compliance Adaptations. *Applied Sciences, 12*(9), 4531. https://doi.org/10.3390/app12094531

Weber, T., & Buchkremer, R. (2021a). APPLYING AUGMENTED REALITY ON SMART GLASSES TO MINIMIZE HUMAN ERROR IN HANDS-FREE TECHNICAL TRAINING. *INTED2021 Proceedings*, 848–853. https://doi.org/10.21125/inted.2021.0201

Weber, T., & Buchkremer, R. (2021b). Monitoring Remote Service Platforms Using Artificial IntelligenceBased Distributed Intrusion Detection. *34th Bled EConference Digital Support from Crisis to Progressive Change: Conference Proceedings*, 705–717. https://doi.org/10.18690/978-961-286-485-9.50

Weber, T., & Prinz, W. (2019). Trading User Data: A Blockchain Based Approach. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 547–554. https://doi.org/10.1109/IOTSMS48152.2019.8939246

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly, 26*(2), xiii–xxiii.

https://www.jstor.org/stable/4132319

Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, *102*, 902–911. https://doi.org/10.1016/j.future.2019.09.028

Werbach, K. (2018). The Blockchain and the New Architecture of Trust. In *The Blockchain and the New Architecture of Trust*. The MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Xevgenis, M., Kogias, D. G., Karkazis, P., Leligou, H. C., & Patrikakis, C. (2020). Application of Blockchain Technology in Dynamic Resource Management of Next Generation Networks. *Information*, *11*(12), 570. https://doi.org/10.3390/info11120570

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access*, *5*, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843

Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information*, *8*(2), 44. https://doi.org/10.3390/info8020044

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794–2830. https://doi.org/10.1109/COMST.2019.2899617

Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access*, *7*, 56656–56666. https://doi.org/10.1109/ACCESS.2019.2913682

Xu, H., Liu, W., & Liu, X. (2021). Blockchain-Based Trust Auction for Dynamic Virtual Machine Provisioning and Allocation in Clouds. *Wireless Communications and Mobile Computing*, *2021*, 1–10. https://doi.org/10.1155/2021/6639107

Xu, M., David, J. M., & Kim, S. H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. *International Journal of Financial Research*, *9*(2), 90. https://doi.org/10.5430/ijfr.v9n2p90

Xu, R., Nikouei, S. Y., Nagothu, D., Fitwi, A., & Chen, Y. (2020). BlendSPS: A BLockchain-ENabled Decentralized Smart Public Safety System. *Smart Cities*, *3*(3), 928–951. https://doi.org/10.3390/smartcities3030047

Yang, C., Chen, X., & Xiang, Y. (2018). Blockchain-based publicly verifiable data deletion scheme for cloud storage. *Journal of Network and Computer Applications*, *103*, 185–193. https://doi.org/10.1016/j.jnca.2017.11.011

Yang, C., Zhao, F., Tao, X., & Wang, Y. (2021). Publicly verifiable outsourced data migration scheme supporting efficient integrity checking. *Journal of Network and Computer Applications*, *192*, 103184. https://doi.org/10.1016/j.jnca.2021.103184

Yang, X., Chen, G., Wang, M., Li, T., & Wang, C. (2020). Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme Based on Blockchain. *IEEE Access, 8,* 158765–158777. https://doi.org/10.1109/ACCESS.2020.3020841

Yang, X., Li, T., Xi, W., Chen, A., & Wang, C. (2020). A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud. *IEEE Access, 8,* 170713–170731. https://doi.org/10.1109/ACCESS.2020.3025060

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. *2017 International Conference on Engineering and Technology (ICET),* 1–7. https://doi.org/10.1109/ICEngTechnol.2017.8308215

Yazan, B. (2015). Three Approaches to Case Study Methods in Education: Yin, Merriam, and Stake. *The Qualitative Report, 8*(22), 149–182. https://doi.org/10.46743/2160-3715/2015.2102

Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications, 7*(1), 1–12.

Yin, R. K. (2017). Applications of Case Study Research. In *Sage*. Sage.

Yu, B., Wright, J., Nepal, S., Zhu, L., Liu, J., & Ranjan, R. (2018). IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain. *IEEE Cloud Computing, 5*(4), 12–23. https://doi.org/10.1109/MCC.2018.043221010

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems, 40*(10), 218. https://doi.org/10.1007/s10916-016-0574-6

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications, 84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

Zhang, J.-S., Xu, G., Chen, X.-B., Ahmad, H., Liu, X., & Liu, W. (2021). Towards Privacy-Preserving Cloud Storage: A Blockchain Approach. *Computers, Materials & Continua, 69*(3), 2903–2916. https://doi.org/10.32604/cmc.2021.017227

Zhang, J., Lu, C., Cheng, G., Guo, T., Kang, J., Zhang, X., Yuan, X., & Yan, X. (2021). A Blockchain-Based Trusted Edge Platform in Edge Computing Environment. *Sensors, 21*(6), 2126. https://doi.org/10.3390/s21062126

Zhang, P., & Zhou, M. (2020). Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues. *IEEE Transactions on Computational Social Systems, 7*(3), 790–801. https://doi.org/10.1109/TCSS.2020.2990103

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

Zhang, Yinghui, Deng, R. H., Liu, X., & Zheng, D. (2018). Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Information Sciences, 462*, 262–277. https://doi.org/10.1016/j.ins.2018.06.018

Zhang, Yinghui, Deng, R. H., Shu, J., Yang, K., & Zheng, D. (2018). TKSE:

Trustworthy Keyword Search Over Encrypted Data With Two-Side Verifiability via Blockchain. *IEEE Access*, *6*, 31077–31087. https://doi.org/10.1109/ACCESS.2018.2844400

Zhang, Yuankai, Zhang, L., Liu, Y., & Luo, X. (2021). Proof of service power: A blockchain consensus for cloud manufacturing. *Journal of Manufacturing Systems*, *59*, 1–11. https://doi.org/10.1016/j.jmsy.2021.01.006

Zhang, Yun, Tang, Z., Huang, J., Ding, Y., He, H., Xia, X., & Li, C. (2020). A Decentralized Model for Spatial Data Digital Rights Management. *ISPRS International Journal of Geo-Information*, *9*(2), 84. https://doi.org/10.3390/ijgi9020084

Zhang, Yunru, He, D., & Choo, K.-K. R. (2018). BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT. *Wireless Communications and Mobile Computing*, *2018*, 1–9. https://doi.org/10.1155/2018/2783658

Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management*, *57*(6), 102355. https://doi.org/10.1016/j.ipm.2020.102355

Zheng, B.-K., Zhu, L.-H., Shen, M., Gao, F., Zhang, C., Li, Y.-D., & Yang, J. (2018). Scalable and Privacy-Preserving Data Sharing Based on Blockchain. *Journal of Computer Science and Technology*, *33*(3), 557–567. https://doi.org/10.1007/s11390-018-1840-5

Zheng, D., Jing, C., Guo, R., Gao, S., & Wang, L. (2019). A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs. *IEEE Access*, *7*, 117716–117726. https://doi.org/10.1109/ACCESS.2019.2936575

Zhou, H., Shi, Z., Ouyang, X., & Zhao, Z. (2021). Building a blockchain-based decentralized ecosystem for cloud and edge computing: an ALLSTAR approach and empirical study. *Peer-to-Peer Networking and Applications*, *14*(6), 3578–3594. https://doi.org/10.1007/s12083-021-01198-z

Zhou, J., & Gollmann, D. (1996). Observations on non-repudiation. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 133–144). Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0034842

Zhu, Q., Loke, S. W., Trujillo-Rasua, R., Jiang, F., & Xiang, Y. (2020). Applications of Distributed Ledger Technologies to the Internet of Things. *ACM Computing Surveys*, *52*(6), 1–34. https://doi.org/10.1145/3359982

Zhu, X., Shi, J., Huang, S., & Zhang, B. (2020). Consensus-oriented cloud manufacturing based on blockchain technology: An exploratory study. *Pervasive and Mobile Computing*, *62*, 101113. https://doi.org/10.1016/j.pmcj.2020.101113

Zimmerman, D. K. (2014). Five cloud essentials for the boardroom: What banking and financial markets executives need to know about cloud computing. *Journal of Payments Strategy & Systems*, *8*(1), 84–93. http://libezproxy.open.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=95331748&site=eds-live&scope=site

Zuo, Y., Kang, Z., Xu, J., & Chen, Z. (2021). BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing. *International Journal of Distributed Sensor Networks*, *17*(3), 155014772199961. https://doi.org/10.1177/1550147721999616

APPENDIX A

I: Hello and welcome to the focus group session. My name is [Person] and you should know me. So if there there's someone who does not know me, please leave the team's call. If so, if everybody knows me, I'll start with a really short introduction of all the participants, such that you at least have a small picture of who's participating in that call, and then I will continue with the guidelines of that meeting. So as you can see, the meeting will be in English held. And today participating is [Person], [Person] is the managing director and he is from [Organization], and he's also strongly connected to our service team and he has a really strong contact with the people and is really close to our customers in our company. We have here [Person], [Person] I know you already from the army, you're a testing engineer at [Organization], as far as I could investigate. And, I think you have nearly every certificate in IT and scrum and all those stuff. So, that's more or less your background test, in testing engineering. We have [Person], [Person] you're a research assistant at the [Organization] in [Place]. I know you already from the university, that we together studied IT security, and I already know yours are from the mentoring. And I know that you have a strong background at this, this kind of special ability on mentoring and training. [Person], you are also a managing director of [Organization], and you have really strong technical background. You are the lead of the technical area in [Organization], and yeah, you have a strong background and also studied computer science here at [Organization]. Yeah, [Person], [Person] I know you from the army, you are the replacement of [Person] as far as I know. So you more or less, yeah, had the same position in my former work in [Place]. [Person] is now a team lead at [Organization] for collaboration services. And the funny thing is now [Person] is a member of your team. So, he joined you in the same team. So [Person] is also, I know him from the army and he's working in [Organization] in collaboration services together with [Person]. And last but not least, we have [Person]. [Person] is our dev ops engineer at [Organization], and he's really close to the cloud. And he's responsible for deploying platforms and he's really close when it comes to cloud services. Yeah, and I think I do not need to introduce myself because you all know me, hopefully. Okay, so that's so far from the introduction. And then continue with the program. Thank you very much for taking this (uncl. #00:03:04-0#) focus group today and discussion together with me the topic about cloud computing. On my research, I am following a so-called design science methodology, which is also shown here on the picture, here. This methodology is very similar to scrum, to the scrum approach. However, in DSR, in design science research, you also must contribute your resource to the scientific community to gain research effort, which will be done later here, via publishing a research paper. But the idea is exactly the same as on scrum. So today's session can be compared to the sprint planning for scrum project. What we would like to, or what I would like to do is determine today in form a group discussion, where the web problems, especially in form of trust in cloud application occurs, how or who is affected by those problems and how can they be overcome. As I already mentioned, you're all in a technical area. So all of you are somehow related to planning, managing, designing, implementing, operating, or testing information systems, or enable the development those.

And therefore I'm really blessed to have you all here. And yeah, thank you very much for joining that group session here. Any questions so far on the setup of the whole thing, of the whole topic, or all your familiar with everything? If so, I would start directly with the first question and ask you for your opinion. So, no questions. I hope you can all hear me, and then I will start. As I said, the topic is on cloud computing, the research results will be used for my PhD thesis. And the first questions is, okay, the guide/ oh, sorry, of course the guidelines, forgot those. So as I already mentioned, there are no right or wrong answers, it's all about your opinion. We are tape recording this. I will later on transfer that to written language. We are on the first name base, I think that's clear. You don't need to agree with others, but at least listen, so please do not interrupt others. Also think about me, I need to transcript it and if you're interrupting it's hard to transcript, so please let the others finish. I will not interrupt anything, I will not give my opinion to any topic, I will just work as a moderator. Then let's talk to each other also, that's also allowed, so you don't need to talk to me, it's a discussion. So if the guidelines are clear, I think that is. And then I would start with the first question. What do you think of when you hear cloud computing? What do you associate with the idea of cloud computing? You're free to speak, just unmute and then bring up your ideas of cloud computing. What do you think of when you hear the term cloud? #00:06:21-0#

Participant #2: Yeah, I mean/ then I start [Person]. When I hear the word cloud and cloud computing, that means that I do something not directly on my computer, or directly local, but instead to have it somewhere in the cloud, so somewhere remotely where I do some computing tasks. That's what I would associate with this idea. #00:06:53-0#

Participant #6: From my point of view, if I would just be a normal person and I would hear cloud computing I would see the two words, cloud and computing. So computing obviously is something to compute, to work with, and cloud something above in the air, something that you can't touch, something that/ you are computing something but somehow doesn't really concern you or your workspace. And yeah, also that if something is up or something is unclear, and little bit cloudy, that there's a lot more behind cloud computing than just the nice word cloud. And, yeah, of course, as (uncl. #00:07:54-0#) informatic, you know that there's a lot more behind it. You know that there are server, there are networks, there are security guidelines to ensure that, that the connections are stable, secure, and that the stuff that is on the cloud is also secure and not leaking some information that is somehow depending on the topic of a secret, or something sensible or something like that. Yeah. #00:08:29-0#

I: Okay. Okay. So if I, if I've got it right, you, you understand the cloud as/ yeah, you can not do write here, that's true. So you can also write your ideas if you want, if someone is talking and you need to store your mind you can also write here. And so you can, you think as the cloud as, as a computer space somewhere, which you're not really responsible, and you have to investigate security for it. Is it, is it summarized correctly? #00:09:06-0#

Participant #6: You're asking me the question? #00:09:10-0#

I: Just for a short summary of your statement. #00:09:14-0#

Participant #6: Yes. Yeah. #00:09:21-0#

I: Yeah, absolutely. Something to add here, someone? #00:09:26-0#

Participant #3: Yeah, of course. I wrote the sentence up here. A good scalable environment with trust in the service provider. So for me is a cloud computing IT somewhere else. So, you need the service provider who's responsible for the most of the environment. And I have scale up in, with all this security and what, what I want from this environment. So cloud computing means to me an environment from someone else. #00:10:08-0#

I: Okay. #00:10:11-0#

Participant #1: Yeah, more or less the same, in my opinion. When I hear cloud computing, I think about storing data. Yeah, the most time maybe private data, which I can, which whenever or wherever I want. Means, if I need a quick access to my data from my mobile phone I can do it. Or if I want to modify or update some data more professional, I can do it with my computer. So cloud computing is a system to store data, which makes it available whenever and wherever I can. Yeah. Whenever I want. #00:11:02-0#

Participant #3: Yeah. Just a quick comment from my side to what [Person] just said. It's also for a company very interesting to think about this situation, not only for private. Because also in a professional way your upcoming things are going faster and faster. And when we are thinking how fast the environments are growing, it's even better to organize you and your data maybe from time to time in the cloud, just more scalable to, to scale up your own environment and all your IT things in that same situation. Like, growing companies with much more data, with computing things are just more scalable, reliable. #00:11:59-0#

I: Absolute. Yep, yep. #00:12:04-0#

Participant #1: Yeah, and I might add from my perspective. When I think about cloud computing, it's about distributed data, so at different places, not just at one. And when I hear the word computing, it adds to me the basic idea that we also have any kind of distributed, yeah, computing or calculations analysis, topics like big data. So yeah, analytic topics that I would add to it. Whereas just the storage I would see as just the cloud, then came computing as an additional topic for me. But I'm also not an expert on that, so probably there's a Wikipedia definition that covers it all. #00:12:53-0#

I: Yeah, but it's regarding your opinion about it. So, that's fine. #00:12:59-0#

Participant #1: All right. #00:12:59-0#

I: Okay. Cool. Yeah, maybe to sum that a bit up, to sum it up, I think everyone has it seen as a service, which you're not directly responsible of, and somehow a service which is somewhere, to bring it somehow into two words if I got it correctly. And I think that's a good point to start already. The next question, what do you see as the biggest challenge in cloud computing? So what do you, your experience pay most attention to when comes to cloud computing? What do you think we need to pay most attention to, or from the experience from customers, from your company or whatever, what else are the main topics where we have to focus on if we are going to cloud computing? #00:13:50-0#

Participant #1: I go on, it's a rhetorical question [Person], of course it security plays a major role, because you have to make sure to secure your data paths and data pipeline to the cloud and back, so that no one else can access to your data in the virtual layer, but also of course, physical security is extremely important. #00:14:24-0#

Participant #3: I would say or/ to say this, it's like, yeah it is a challenge, but also find a good thing. So you have the data not in your system, not directly physical in your environment, but you trust someone else, who's then responsible for your data. Of course, you have for yourself to do some things that, even if you are not responsible directly physical to your data, that you do something that nobody has access to it. And, but on the other hand you definitely also have to trust in some levels the provider of the cloud. But I say it's not only a challenge, this could also be good thing. Because sometimes, especially for small company the physical access is, so physical security to secure your server rooms, things like that is, is a much more effort if you have to do it for yourself. Or if you let a big cloud provider, like [Organization] or some companies like this do it, because they can, yeah, of course provide this in a great manner. But nevertheless is, one thing is that everything is available everywhere on all your devices. So for mobile device, for your laptop, whatever, usually you have the cloud therefore somehow connected to the internet. And that means also that everyone, not only the people you would like to provide this service, can some are provide it. And then you have, of course, the challenge that you have to ensure that not the wrong people can access your data. #00:16:05-0#

Participant #6: I absolutely agree too, with [Person], or was it [Person] who spoke first? Correct me if I'm wrong. I don't/ yeah. Another, another point. #00:16:22-0#

I: [Person] first responded. #00:16:23-0#

Participant #6: Another point is, as [Person] said that you just have to trust that everything is working correctly. One example, especially because I am working in a research company, Forschungszentrum now, is very important that we have, when we want to know who is able to see those data, because it is research, it is sensitive, there are sensitive data. There are topics on there which is not official yet, where we are still researching, and there we also want to know, for example, where we're out of service, and if they are in [Place] then it's good, if they're in [Place], then it's okay. But what if they are in the [Place]: The rules for service and for security are little different there than here in [Place] or [Place]. Here in [Place] and [Place] we have a way more stricter regulations regarding the service, regarding the data, regarding the access possibility to it. So this is also an important point where I would take a look at. And also what happens if/ of course nobody wants it, but what happens if those servers are having some problems where the data is lost? Do we know that those data is backed up in another server, which is also in [Place] or [Place] or whatever country it is, so that if there's some loss of the data we can be sure? And that's why I totally agree that we have to trust and we want to be available and secure everywhere, that if it is lost the question is, is there backup for it? Because I rely on the system, that if I want to put it in a cloud system computing, whatever it is called, and something happens to me and it is lost, then I also want to know and to be sure that the data there is also safe or backed up somewhere. If it is an (uncl. #00:18:50-0#)backup somewhere, then it's just/ yeah. #00:18:53-0#

Participant #3: Yeah. From my experience, I would like to add there one thing. Usually at the big cloud computing providers, they usually give you the chance of (uncl. #00:19:06-0#), so you can choose to have a second location, for example, then for [Organization] Azure, that you have one in Amsterdam, but as well you have then the same data stored, for example, in Frankfurt, but additional costs, of course. So you have to pay for it. And you also keep in mind that there was, well, I think several months ago the big thing that they're even in France, there were big cloud, or big data center which was burned down. And, if you then would not have updated it, backed up somewhere else would be not cool. On the other end, again, if you do it for yourself and your server room, you also have to find a way to have a backup and things like this. So it's not that you have a bigger challenge here, I would say. #00:20:00-0#

Participant #6: Yeah, no, it's absolutely/ the effort is the same if you do it for yourself or if someone else is doing it, you just want to make sure that if something happens to it that you have a backup. So if you do it for yourself and you know that you want to have a backup or should have a backup, then you know that you did it. And somehow if you rely on someone else and just trust them blindly, then/ and you never ask if there's a backup if something happens, then this is just one point that should be also paid attention to it. #00:20:40-0#

I: I think the next hand I've seen is from [Person]. #00:20:46-0#

Participant #7: Yes, thanks. So from my side I want to add here something due to all the facts that are already meant by the others. So, I think the opportunities and possibilities in the cloud are nearly/ yeah, so we can do everything there, but due to all the possibilities we have, the major challenge in my opinion is to take care of all the responsibilities. So, I mean, if we go into the cloud, as everyone said, we need a good IT security data protection regulations to take care of this. Also, we can scale up everything, but we need a very deep understanding from our services we should use, so take care of all stuff we can do in the cloud. So in my opinion, it's very important that the responsible people who are using the cloud and administrating the cloud to have a very, very deep understanding of all functions and functionalities that are used inside the cloud. #00:22:08-0#

I: Yep. Absolutely. [Person] you had something to add? #00:22:16-0#

Participant #3: If I find the mute (uncl. #00:22:18-0#). Yeah, in my point of view there is a different way to administrate. So if you are a local administrator, you know your environment. In cloud computing everything is changing quite often, and if you start to research also good administrators for this it's quite difficult, not even to find someone who know the environment, like (uncl. #00:22:49-0#) 65, just only know all the configurations, all the processes and all the governance processes the cloud for you prepare, and what your company right now needs, that's not even the same. And also the security what we hear in the (uncl. #00:23:12-0#) quite often. It's not even the security, it's also simple processes what the environment opens up for every company. They offer the cloud, but for your company it shouldn't the best solution. So you work different than a couple other companies, so the process is not the same for you, and you should prepare the cloud computing for your own process. And that is a lot of governance and process work and that is behind all the cloud thing. So it doesn't matter, it changes a lot because your (uncl. #00:23:53-0#) world runs way more different than your cloud. So that's also from my point of view, one of the biggest challenge, because you don't find the right person to know all the differences for the quick change that we are running in right now. #00:24:14-0#

I: Absolutely. Okay. Yeah, really good feedback here so far. As I said, my topic on the PhD is going to trust, and I will now focus a bit more on those questions. So the next question is exactly going in the direction of trust. I mean, we already had a lot of discussions regarding governance, regarding processes, and also we had the topics of IT security and trust. And I would like to continue in the area of trust here. So the next question I've prepared here is, maybe some trust issues when using cloud applications. And I think we already had discussed them and had brought them up. So I think there/ if someone would like to add here something, I would appreciate that. #00:25:07-0#

Participant #1: Maybe only that this leads typically to the point that even smaller companies like ours, we are typically looking for big providers where you can trust at least physical security that they have the manpower and the resources to do their job. And a very small data center provider maybe has then disadvantages here, due to smaller resources, lower resources. #00:25:38-0#

I: Yeah [Person]? #00:25:41-0#

Participant #2: Yeah. It just want to add, that's true. On the other end, most of the big ones are usually coming from the [Place], so that's then again the issue we have with our [Place] laws and the regulations you have been in the [Place] or in other countries. So this where the company's coming from, that is a big point in this trust that you have to keep in mind, due to the different regulation or/ I mean the [Place] have really different than we have in [Place], as well in [Place], for example, there is even really other regulations you have. And usually as a European company you’re not using a cloud in [Place], you try the best from this trust back from this side, then is to have something here in [Place] or at least in the [Place]. So that is definitely one big thing also. #00:26:39-0#

Participant #7: Yeah, I like to add something, from operation side. So I mean, a lot of stuff is right now going into the cloud, everyone is going to cloud, it's a lot of stuff is outsourced to clouds. So from operation side, we are getting more and more dependent on cloud providers. And I mean, they are right now with [Organization], [Organization] and [Organization], three big companies running, I don't know, more than 80 percent of all cloud centers. I don't know exactly, but as we are dependent on this, I mean, if they want to get more profit of it and we are dependent on it, we don't have another option then. This could be a trust issue in far future, but could be. #00:27:39-0#

Participant #4: Yeah, I think there is a more fundamental trust problem with cloud computing, because there usually is no way for any customer of a cloud service to independently encrypt or secure otherwise their own data. You can only trust the provider that they are doing everything they can, everything they deemed necessary, everything they deem worth the cost to protect your own data. But other than trust them and maybe money is off or any data leaks, you have no control over your own data once it's in the cloud. #00:28:22-0#

Participant #2: That I would not completely agree. You also have possibilities on your layer to encrypt data without trusting it. But of course, it's much more complicated. That you have to take a lot more effort. And also at as most of the time you also have then from time to time less comfort, but you have also the possibility for you to lose something to encrypt very/ and usually you'll see what kind of data you have and how important they are. And there you have to usually decide between different levels how to trust, but definitely you can also on your side encrypt things. #00:29:04-0#

Participant #4: Take, for instance, this Team's meeting we can't encrypt anything there, it's just a recording now somewhere wherever it is recorded. And well, we can switch to Chinese or any other language, but it's not an encryption we have at our hands. So if you use this for a discussion about company secrets, like most companies using Teams do, they have no control whatsoever about this type of information. [Organization] says we encrypt everything end to end or whatever, it's not open source. We can't prove it that they do, we can only trust them. #00:29:47-0#

Participant #2: Yeah. I somehow agree. Sorry but I just/ because, I mean, you could encrypt here this chat. We could use it, but then we would have much more, much less comfort. I mean, we could use some/ (uncl. #00:30:05-0#) we say we just don't speak no English, but instead we just do some, some special/ I know it's funny because you would never do, I agree. But you always have a layout where you can encrypt something, but you're absolutely right. That's a good example here in Teams. It will be, yeah, it is not an easy way to do, absolutely right. #00:30:29-0#

Participant #3: Additional to this thing that [Person] just said, also for simple things like data or data loss prevention, you can do this, but you have to do in the right way. And you have to know, all the more than 1,000 configurations and (uncl. #00:30:52-0#) to prevent, data loss prevention. So that's also a problem of trust, because it's not that trust side is also/ yeah, service side is the thing that you have to know what your possibilities are in the security, and to trust the company who's responsible for the service. So you also have to know what kind of trust level you can give to the company. It's not even that you trust them because it's a nice guy, but you have to trust them, because you know all the configurations, and not even the top management know already about it, but they have to know this from the configuration side, and that's, it's not usually processed (uncl. #00:31:52-0#) [Organization] or [Organization], or [Organization]. So most of the time it's okay, "That sounds nice from [Organization], let's take that, let's take out this". It's not even saying the configuration side and the data loss prevention is better on [Organization] or [Organization], or [Organization]. So it's the kind of trust like, you cannot avoid from that. You kind think about some stuff. #00:32:26-0#

I: Okay. I think from my point of view we talked a lot of trust here. It's pretty good. So then I would like to raise the next question here. And the next question is, is there a specific user group that is particular concerned with the issues of trust in cloud applications? So is there a specific group, or is it a more general problem? Why or why not? #00:32:57-0#

Participant #4: I think it's a specific user group mostly. Because, I don't know who said it, if you are a small company with no resources to properly maintain and secure your own data, loading your data into any cloud service will improve your security. And if you are a bigger company which should have the resources to secure your own data, you give that to the cloud operator and then you have to trust them. So it depends on the size or the resource pool you have available, whether trust is a big concern for you or not. If you're small, you have no other option and whatever they do it's better and better than anything you can do yourself. If you're a big, well, you have to make the trade off and weigh the consequences against each other. #00:34:15-0#

Participant #2: Yeah. I mean this question, I mean, it's not that easy to answer in the end. And from my point of view, everyone should be somehow concerned with issues of trust and cloud computing. But I mean, everyone is different, and of course the one cares more, the other one cares less about. So if I just see that general, of course, in the end, also the more knowledge you have then maybe you also are more concerned in this kind of things, because if you do not have any knowledge here, it is by the way also really, really hard to do something. You then just will trust or not, but it's hard to do anything, so if you do not have some background knowledge here. And/ so yeah, but not easy to answer that, answer that question. #00:35:17-0#

Participant #7: I think// #00:35:20-0#

I: Maybe trust one word yet. The intention is not to bring yes-no answers. But anyway, I know that the questions are quite broad. #00:35:30-0#

Participant #3: From my point of view, the bigger a company is, the more security layers in the company comes up and also that brings a level of trust to cloud computing company or to a service provider. So, so as big as the company is, so the specific group side, from my point of view is as big as a company is, then more trust should come from the security side or from the security department to the cloud computing. Because the technology side knows about technology and can provide a good solution in the cloud. But the security department should know what's good, what's bad, and that comes to personality. So some people are known that/ in [Place] we have some laws that are set up to where data has to live, and where not. So I think that should also be a discussion side that trust is not only the technology, that's also a view from the person who cannot, don't know about the technology behind that. So it's just more a personal view from one person in the whole company that is more than (uncl. #00:37:12-0#) that situation. #00:37:16-0#

Participant #6: Another question is, in addition to [Person] opinion, how is trust defined in that point of view? So trust can be, or trust is probably different for everybody. So there, of course there will be a person out there who just doesn't care about the trust issue, regarding the cloud computing, they can just say, "Oh, as long as it works, I'm fine with it. I don't care if someone is, could access it or not, could read it or not". And there are still people who will say, "Yes, of course I care about it because the data that I'm using or I'm working with is very sensitive. So the trust is very high priority in the cloud application". So I think I could not answer this question with, "Yes. There's specific user group or no, there's not a specific user group", because it just depends on the definition of that person that you are asking. And depending on that definition, the answer to that question varies differently. So I would say, yes, there are of course groups where they would say, "Yes, it is important and we have a big concern about that", and there will be groups who say, "No, I don't care about it". #00:39:01-0#

Participant #1: For me, I think it's simply clear, because there's just one group in my mind, it's the group of the cloud user or all of them. Because if you're using a cloud application, you do not just store some data, you store some information, not just information you provide, also other information like meta data. Metadata could also concern to other people who are not using the cloud system at all. And if you have/ for sure, you can have more sensitive datas, if you are a company who is something like, that's looking about innovative solutions, then you should think about if you're really able to use the cloud application. But if you want to give information to somebody, you should always care about some issues. #00:40:09-0#

Participant #6: Yeah, I think the/ you should, yes, definitely. But if/ where it should doesn't necessarily mean that everyone is doing this. So that's, therefore I would say it depends on the person and the people. Because by definition, if you say, okay, we have a group of people where we say, "Okay you, everybody here is using this cloud application. So, what do you think about trust? Or do you have/", and then you ask this question, maybe you think that everyone should concern or should think about the trust issue there, maybe because you work with clarifications and you know what issues there could be regarding those applications. But if you would ask someone new or someone who just, is just using it and is not working with cloud application and does not know how, what issues there there could be, I think that there, yeah, that they would have no clue about it. So yeah, should definitely, but if this is true, I think you cannot really say yes or no. #00:41:45-0#

I: Okay. Yeah, absolutely. As I said, the question is not meant to say yes or no, it's regarding opinions, regarding experience. So that's why they are quite broad and quite open. Yeah. So, all right. But the idea here behind that question just to bring it also up, is to figure out the environment where trust might be an issue. And, that's way the question is, is there a particular group? And we discussed it already. So the next question I would like to come up here, and this is already related also to that question and to the questions we had before regarding trust is, can you think of a technology or a methodology or something which highers trust, which is, what is important for you if it comes to trust? How high is the trust in an application to you, what makes an application trustworthy to you? Or which technology would be there for you, which you would say, "That can also be increased trust"? So how do you enumerate trust? #00:42:58-0#

Participant #6: I would/ maybe not necessarily a technology or methodology to increase the trust issue, but also that/ I mean, it is definitely important to implement or develop new technologies or methodologies so that the trust issue is increased for the people who are using it. But what is also important in my point of view is that people should also want to learn about trust, want to know about those technologies in order to be able to say, "Okay, I can trust this or I cannot trust this". So I would say that knowledge in general about those topics is also a way to increase trust, but also that the technologies and developments excel to increase the trust. So it is one, the task of the person who develops those technologies and methodologies, but also from the user point of view that the user is also willing to learn about those technologies so that, yeah, he or she can know more about it and also can decide, okay, maybe evaluate, "Okay, this is really good", or, "This is really bad because I know that this works like this and this". #00:44:46-0#

Participant #1: Yeah. One, technology to create trust, of course it's in general the blockchain. So, you can include data and you cannot change it afterwards anymore and replace it without having the history. So, technology could be using that in applications, to make sure that, to say that data hasn't been changed or has been changed and by whom. #00:45:24-0#

I: Yeah. #00:45:30-0#

Participant #2: From my point of view/ sorry// #00:45:32-0#

Participant #3: Go ahead. #00:45:35-0#

I: [Person] go, [Person], [Person] go ahead. #00:45:39-0#

Participant #3: From my point of view, I think simplify the cloud computing and the explanation of what we are doing there in this cloud, that that could probably be a solution to increase trust, because when you are simplifying complex strategies and complex things, yeah, simplify it down, then more people know what you're doing and more people can trust the operation that you do. So from my point of view, simplifying things is also a thing to increase trust in applications, know what you are doing. #00:46:25-0#.

Participant #2: Maybe on top of this also transparency regarding what you're using and how are you doing it. It's quite close to it, I would say. I mean, there are also from kind of technologies of course, I mean blockchain definitely is a possibility. There is also/ yeah, there are, I mean, in IT security and so on, there are some things like secure multiparty calculations, what you could do to increase trust. You could, of course you can also just use encryption on some type. It is a little bit that you then don't trust anymore, but you trust them, the algorithm of the encryption, what you could use to secure your data, what you're using there. So definitely there are a lot of technology, but as well not only technology, also process things, like simplifying transparency and so on what you can use definitely. #00:47:30-0#

I: I/ [Person] please. #00:47:36-0#

Participant #3: I think it's [Person]. #00:47:39-0#

I: [Person]? #00:47:40-0#

Participant #1: What also came to my mind was of course things like multifactor authentication. It's also technology that in the end makes you trust more in the application, because you think, "Okay, no one else, a second user needs a second/ if they would reach you, they would need another factor from you", so that's not so easy, and that's a very obvious thing for the end user, what first came to my mind. #00:48:11-0#

I: And I just want to add that everyone is knocking his head. So I think this is a complete (uncl. #00:48:20-0#) in that group, and also on the other topics, by the way, for the transcript, everyone had knocked his head. #00:48:26-0#

Participant #2: Yeah. I mean, I think all the things like you're using in IT security, I mean all the technologies you can more or less use to trust more. It's not only/ yeah, two factor authentication of course, but also to use up-to-date things from IT security. So there is definitely a lot of things. #00:48:47-0#

I: But that, that brings then the idea also of providing you with, on the one hand side probably with transparency, and on the other hand side also with the option of inter, or interacting with the system itself. So for example, bringing your own encryption algorithms to the system, would that also higher your trust or is this something you would say, "Okay, if they're using basic algorithms, I trust them"? #00:49:13-0#

Participant #2: I mean, to keep it short, whenever you can use something which is your own, of course that will increase your trust, because you haven't done something you especially choose, which you trust already. And if you can use this then on the (uncl. #00:49:34-0#), of course that will then improve this, definitely. Yeah. #00:49:39-0#

Participant #1: I don't trust if I would need to do that. #00:49:44-0#

Participant #3: Simpler applications or complex applications, like [Organization] cloud, there's a key wall that you can activate and put your own key to the application and work with this one, and there's just one thing of trust for the application, of course. #00:50:12-0#

I: But then you still need to trust the vendor, right? Or? #00:50:17-0#

Participant #2: Yes. #00:50:19-0#

Participant #3: You create your// #00:50:20-0#

I: How can you// #00:50:23-0#

Participant #2: It's cloud to cloud. So, yeah. Yeah, you have to trust [Organization], again. Yep. #00:50:32-0#

I: Yeah. But maybe/ I mean, I don't want to emphasize something or to push something in direction, but we have already hit some technologies like multifactor authentication or multiparty computation, we have heard the blockchain, I mean, those are all technologies which higher trust on the one hand side and can be somehow also combined, maybe, I don't know if that would be// #00:51:04-0#

Participant #2: Of course you can also do a combination. I mean, it's always the thing you should never only use one thing, you always should try to somehow have different things you can then, yeah, be sure. I mean, if you just have to trust one person, but instead if you have just to trust several ones and then if one is not good anymore, but you still, this is not reaching everything, that is of course a good idea definitely. And you should always use different levels and different layers of security. And yeah, that definitely is good. #00:51:47-0#

I: Someone with something to add to that topic here? Okay, then "pre last" slide. The question is, how could you evaluate whether an application is capable of increasing trust in cloud applications? So this is exactly where my question and my previous question was related to. So how could you measure trust and how could you measure whether an application highers the trust in the application for you or not? So how would you measure that, if someone provides you with an application and say that that application makes the cloud ten percent more trustworthy, how would you evaluate trust? Or how would you evaluate that application? So, on what point do you measure trust? #00:52:45-0#

Participant #3: Yes, more factors increasing the security, I think a level of trust will level up. So, [Person] just mentioned, it's not only one point, it's multiple points to increase the security. And from my point of view, security is the most thing for increase trust. So, so that's more, that's a/ as high as the security level and the less complex the security are, and it's related to me as a customer with simplify (uncl. #00:53:31-0#)that the level of trust will level up. #00:53:36-0#

I: So you would measure it somehow on simplification? Is it summarized correctly? #00:53:44-0#

Participant #3: Yeah. #00:53:45-0#

Participant #2: Again, a very hard question [Person]. #00:53:53-0#

I: If they would be easy, I wouldn't ask them. #00:53:56-0#

Participant #2: I mean, one thing what I would like to add here. I mean, trust always is some kind of individual. I mean, it is/ you definitely can use the survey to ask several persons, to ask, "Will this increase the trust of this application?", and you show what it's doing, increase the trust there, that you can definitely use. Because, yeah, as I said, it's always also an individual thing, because the word trust just is, there's always some individual thing. So it will be there by the way, also because of this, not easy to find something not like survey, but something to measure it will be not easy, I'm pretty sure. #00:54:43-0#

I: That's why I'm asking you, what you think. #00:54:45-0#

Participant #1: I think it's of course multi-factor based, so what I would do to, as trying to assess it, it's to define a set of criteria, for example, that also include the technological measures that you have taken to your application. We talked about, I don't know, the blockchain, the multifactor authentication, encryption technologies.

So you would say you have application A, you have this ten topics you need to assess, and it's not worth when nine of the topics are perfectly done, and one topic is totally messed up. So that, for example, the passwords are password for all your users for example, set by default, then it's still not a trustful application, because even though you have, I don't know, nine measures are very good, one is extremely bad, so it's not a linear thing, you can just add on top. So you need to be good in all criteria typically. And yeah, so it's a multifactor topic and you cannot be very bad in one, then you are still very bad. So you have to be good in probably all the topics and only then you're safe, and then you will have a high, very high trust. #00:56:04-0#

Participant #6: Yeah. I mean you could, I think [Person] mentioned it, you could, you should and could secure or have security technologies for each layer, for each level that you want to improve or something. However/ so you could use this as a checklist, so you could advertise it with, "Regarding this level, we have this and this, this, and this, and regarding that level we have that, that and that, and so on and so forth. But, I think as the most of you said that trust is individual and it is also an emotional thing, because if someone is saying, "Okay, those levels are more secure because we're using that or whatever we are using", but the other levels are not as protected/ I'll just call protected, than the other levels, then maybe someone could get the feeling that, "Okay, the first levels that I mentioned are the most important one for whatever reason. So this is enough", and the other levels is just an optional thing, and this is just like the cherry on top that if those levels are also protected. But for someone who wants a hundred percent full of trust feeling, it could be not enough. So it's/ it could be done with a checklist or with some criteria. But/ and those can also be very good and very, yeah very, very thoughtful. But if someone is not getting it or not feeling it because it's an emotional thing also, it could still be not good enough for that person, even though it is very good at that point. #00:58:14-0#

Participant #2: Yeah. What I would like to add is here, I mean, if you're really asking for criteria for some special application, if it's increasing trust, so I mean, what you could could use as a criteria is, is the application widely used? Is there a computer community behind this application? So is there someone who I'm already trusting who is already trusting this application? That is also good criteria what you could use. Is there/ you can also have a look, is there maybe even an open-source community? Is the source code open source? Is there a repository where there is also something going on? So is someone really working on this application and doing updates from time to time in a regular base? So this kind of criteria could of course already test somehow. #00:59:14-0#

Participant #6: And also maybe if there's something not very good, that there is a team or someone who's willing to fix it, and then telling the person, "Hey, we did an update and this and this, and this is fixed. So this is more secure". I think that this is also creating some more trust. #00:59:36-0#

I: Just to add here, because I think the question is getting somehow in the wrong direction, it's which measures or which topics are for you important. What do you think? What do you need? I mean, [Person] already, I think guided the question the right direction. It's if there's a, is there a community behind it, are there many committed? Is it frequently updated? Those are things which higher your trust in the application. There might be other, [Person] mentioned, for example the two factor authentication that's highering, or more security features which is highering his thrust in application? Or/ that's where this question is more or less going through. What are your criteria to evaluate whether you trust that application more or not? #01:00:18-0#

Participant #7: Yeah. Regarding the point from [Person], I wanted you to say the same. So if the application is highly used by a big open community and it's already, I mean, it's already improving itself all the time, this is a trustworthy application. And also, I mean, when we talk about standardization, so if we have, if this is certified by an independent community, so, okay it's regarding official criteria, for fitting this criteria, I'm trusting it more than if only the provider tells me, "Yeah, we are doing it the same way, but we are not certified". #01:01:10-0#

Participant #4: For me there's one additional criteria which could increase trust in an application, which is if it offers a possibility to use an independent, well, whatever, secret or a secret token, certificate or whatever which is independent from the cloud provider. If I can use my own means of encryption or security, that would allow me to be fairly certain that only I can use my data in the way I want to use them, and not any cloud provider who thinks they're doing a good job at encryption, and Joe hacker thinks, "Ha ha, you're not". #01:02:03-0#

I: Exactly. So this is more what the question was about. Sorry if that was misleading. So maybe one word, because our five minutes are leaving. We are five minutes before the end. We already talked about transparency, is there something which, which can maybe also/ is this also a criteria for you, higher the transparency or? #01:02:37-0#

Participant #2: Yes. #01:02:39-0#

I: That's why I'm not using that question. #01:02:42-0#

Participant #4: Yes, of course. #01:02:43-0#

Participant #2: Absolutely. #01:02:46-0#

I: Okay. So you see why I// #01:02:48-0#

Participant #1: I would like to add, yes, but for me as a customer, not for public. Because I would like to have transparency to me as a customer, not in the (uncl. #01:03:02-0#). That is also a thing like some companies mentioned, that they talk about the security issues way before they have patch. And I think that is the right way. On the customer side, I would like to have a solution before I have communication global wide. So they can tell me, "Okay, I got a security issue in my component and I will have a solution in the next 24 hours, and we will have a communication global wide to non-customers in the next four weeks so that you know as a customer what's going on, and everybody else know about this, but we have patched before this. That can also be a trust thing that they communicate like this. Some security guys are doing this, but some not. From my point of view communication to the customer first is way much better than communicate to everyone. #01:04:19-0#

Participant #2: I'm not sure if I would agree to this point. Because I mean/ sorry, I just, I mean, it's again, a discussion. So, the thing is, what I think is, where you're right, I agree, I also don't think it's a good idea if you post that there is a security issue and you exactly post to the whole world what exactly the issue is, and better even give a tutorial how you can go there and steal something or do something like this. And usually the big company is by the way also doing it, not that way, they are just doing that they get these things, then they are patching them, then they give everyone the possibility to all to install the patch. But then, so I think when you have the patch and you have something, then you can and should give it to everyone, not only to some special nice customers, because this would then from my side, even decrease the trust in this application, in this company. If that would only provide the things to the special great customers but not to me, because I think the security (uncl. #01:05:43-0#) patches should be always available for everyone. But yeah, you're absolutely right, the communication strategy which is used by the company, the vendor of the application of course, should be a good one. #01:05:59-0#

Participant #3: Nobody said it was easy. #01:06:01-0#

Participant #7: Yeah, just to add here something, I think regarding communication, trusting, it's not that easy to summarize. Because depending on the legal form of a corporation, if we think about limited corporation where you can buy stocks, I think from law side they are, they need to communicate to the community or to the public if they have any problems via ad hoc notifications to/ because they are, yeah, there are regulations from legal side for stock corporations. So I think it's not that easy to say that it would be nice just to inform the customers and afterwards the public. #01:06:54-0#

Participant #3: But I think in this point of view there is a way. There are ways around to work with the law, for sure. #01:07:06-0#

I: I just want to mention that we have only one minute left. So, would you like add something here? If not I already say, or just say thank you very much for your participation. I think I got the necessary input to continue here. We found a lot of opinions, which is quite good. I realized that the questions are not that easy, but I think that is the idea of the discussion, not making these questions too easy and bringing up own opinions. However, I will also have to evaluate the questions once again. Before we close here, we have of course the possibility to add something here, if you'd like. Otherwise, I would like to ask you to fulfill those surveys regarding the session, that I have an evaluation of that session. And if you have no questions anymore/ I'll just give you a few seconds to evaluate here.

Well, I think I should stop. So/ I mean the survey is also/ open up the discussion. Yeah, thank you again, once again thank you very much for the really good opinions. I got a lot of feedback, which I could now use for my PhD, there is a lot of valuable information. I'm really happy that also the buzzwords I'm looking for are all set. So I think I'm here also on a good direction. I would say thank you very much for you time, and if you have no, nothing to add, I would say/ #01:09:15-0#

APPENDIX B

Information phase	1. Welcome & thank you for the participation 2. Short introduction of the interviewer 3. Explanation of the guided interview method 4. Information about the interview process ▪ Several topic blocks with questions ▪ About 1h duration ▪ Always provide introductory information before questions to put the questions in the context 5. Note on video recording ▪ Writing in the postproduction ▪ No further use 6. Information on the use of the data ▪ For analysis and evaluation of dissertation only. ▪ Sociodemographic data narrowed down: job description, Curriculum vitae ▪ Anonymous use ▪ Declaration of consent & privacy policy via DocuSign 7. Request if there are still open questions/comments 8. Announcement for the start of video recording
Warm-up and introductory questions	Background knowledge and evaluation weight for this dissertation: ▪ Can you briefly tell me something about your professional background and your daily tasks? ▪ How long have you been employed and studying? Quantitative knowledge questions, please answer: ▪ I am a computer science expert (strongly agree, agree, neutral, disagree, strongly disagree) ▪ I am an information security expert (strongly agree, agree, neutral, disagree, strongly disagree) ▪ I am a cloud computing expert (strongly agree, agree, neutral, disagree, strongly disagree) ▪ I am a cryptography expert (strongly agree, agree, neutral, disagree, strongly disagree)
Main Phase	Introduce the three case studies (CompanyA, CompanyB, and CompanyC) to the interviewer. 1. Do you understand the case studies?

2. Do you think these cases are realistic (why/why not)?

I would now like to talk with you about the risk of cloud adaptation.

3. What can you tell me about risk management?
4. <Moderator explains risk management matrix>
5. <Ask if the interviewer understands the risk management matrix>
6. Do you think a risk management makes sense for the proposed use cases (why/why not)?
7. I would now like to present you with the following risks :
   - The risk is that the cloud application provider implements a contractually, not mutually agreed configuration. (transparency)
   - The risk that the implementation of compliance-driven configurations get delayed due to slow/manual processes(automation)
   - The risk of denying the implementation of a configuration in case of a dispute. There is the risk that one of the two contracting parties denies its responsibility to implement contractual agreements. (non-repudiation)

   Do you think those risks might occur on the described case studies (why/why not)?

8. I would now ask you to evaluate the qualitative risk of the three risks mentioned based on the case studies presented.

9. I would now like to briefly introduce you to another approach with which cloud applications can be configured. <explain results of RQ6>:
   - I have understood the approach (strongly agree, agree, neutral, disagree, strongly disagree)

10. I would now ask you to evaluate the qualitative risk of the three risks mentioned based on the case studies presented, assuming the Cloud Application provider would use the proposed Blockchain-based architecture.

	11. Now that you know the content of the dissertation: - Do you think the use of the blockchain makes sense at this approach (why/why not)? 12. We are slowly coming to the end of the interview. I would now like to come to the aspects of transparency, automation, and notarization. - Recall the approach presented and think about the issues of transparency, automation and notarization of cloud applications. Does the presented approach have an impact on those three topics (why/why not)? - Do you think the presented approach improves the transparency of cloud application configurations (why/why not)? - Do you think the presented approach can help to configure cloud applications in an automated way (why/why not)? - Do you think that the presented approach can help to investigate security incidents more easily (why/why not)? - Do you think the presented approach can help to identify responsible parties in a legally secure way (why/why not)? 13. Final question before we finish the main part. Overall, how would you evaluate the approach presented? Where do you see advantages, and where do you see the approach's potential for improvement or weaknesses? (or new risks upcoming?)
Closing Phase	14. We are coming to an end - Are there any other aspects you would like to bring in? 15. You have now heard all the questions and have joined me in my dissertation topic. In school grades, how would you rate your expertise in the area presented (1 - very good, 2 - good, 3 - satisfactory, 4 - sufficient, 5 - poor, 6 - insufficient)?
Closing information	Thanks for your openness, participation, and time <Outlook what will happen with the answers> <Transcription, anonymization, and evaluation> Thank you & have a nice day

APPENDIX C

CONSENT FOR INTERVIEW

I hereby give my consent to the use of the personal data collected during the following interview:

- *Date:*
- *Name:*
- *Trust in Cloud Applications and how to reduce adoption risks*
- *UCAM Catholic University of Murcia*
- *Thorsten Weber*

The data are collected in an oral interview recorded with a recording device. The orally collected data are written down (transcription) for data analysis, whereby the data are anonymized. Identification of the interviewee is thus ruled out.For documentation reasons, contact data that would allow the interviewed person to be identified later will only be made available to the reviewers of the scientific paper in a separate document. After completion of the project, these data will be deleted.The interviewee can object to the storage of personal data for documentation purposes. Participation in the interview is voluntary. The interview can be terminated at any time. Consent to the recording and further use of the data can be revoked.

____

First name and surname in block letters

____

Signature

____

Date, place

APPENDIX D

TRANSCRIPT INTERVIEW PARTICIPANT #1:

I: All right, then we will start with the interview [Person]. So, we are now in the warm up section, which means I need to get some background information from you, for later on. Yeah, weighting the evolution results. So based on your knowledge, I can say, "Okay, you are an expert in that area or you're not an expert, or less expert", so to say. So therefore my first question is, how long have you been employed and or studying? #00:00:40-0#

R: And or studying? #00:00:40-0#

I: So, how long have you been employed? #00:00:40-0#

R: I've been employed for a year now, I think. Not quite a year, I think it's currently eight months, I think eight months. Eight months. I've been employed for eight months, properly. I've done some minor jobs during my time as a student. But this is the first 40-hour a week job that I have. #00:01:10-0#

I: Can you briefly tell me something about your professional background? #00:01:20-0#

R: Yes. I'm a computer scientist. I studied computer science at the [Organization]. And I'm currently employed there as a research assistance with, as well as/ technically I think it's called PhD student in English, but in German it's a bit different. It's/ I'm both a research assistant and a PhD student. It's one program. So yeah, I'm looking to make my PhD there, so my doctorate thesis, I think it's called. Yeah, I've been, as I said I've been employed there for eight months and I hope to finish my thesis in the next three to four years. #00:02:00-0#

I: Okay. And can you tell me something about your daily tasks, your routines, what you are doing daily? #00:02:10-0#

R: My daily task in relation to my? #00:02:10-0#

I: Your profession. #00:02:10-0#

R: My profession, okay. My profession. So usually my working time is relatively flexible, but I usually start at, somewhere between nine o'clock in the morning or ten o'clock. And then I usually look at my mails, so my inbox. I try to find the most important task and I select. So I look at the e-mails and then I try to create a to-do for the day. So I sort the e-mails into important, the ones that I have to look at immediately, the ones that I might look at later, and the ones I don't have to look at, which are, I've read them once and then I can put them away. And the again, I also have a to-do list where I put down all my to-dos usually for the day that I have to, the things I want to accomplish this day. Unless I, unless there's some email where it's something very, that I have to do immediately, then I'm probably going to do that and then look at my to-do list. And then, the task I'm usually involved in, that is work at the chair regarding teaching, so I'm organizing the exercise sessions for (uncl #00:03:51-0#). So this usually/ and I have an assistant for that, a student assistant. I don't know if that's the correct English term, but let's say student assistant, who helps me with this. We are currently, we/ he helps me with creating the exercise tasks, and he's also the one correcting the tasks later on. And that's one of the things. So we're currently looking over the exercise sheets before we publish them, and then he corrects them, and then we have exercise sessions with the students where we go over the exercises and so on and so forth. So that's one part of my job. Then another part is, I'm currently working on, I'm currently developing a software for the chair, which is also in relation to the paper I'm currently working on. And also in a larger context related to my, to the project I was hired for. So, it's a [Organization] project. #00:05:00-0#

I: [Organization] means? #00:05:00-0#

R: [Organization], yeah. #00:05:00-0#

I: Is it// #00:05:00-0#

R: Yeah. So, I'm working there with/ in the context of that it's also probably going to be in my dissertation this topic. So that's something I'm working on. And usually there are meetings regarding, where I have to attend. And so I also have a calendar where I have all the important meetings, when I have a meeting I go there. Usually the calendar is really the one thing that structures my day at the most. If I don't have a meeting, again, I usually do either programming or working on the paper, or I'm thinking about how I want to structure my program, and so on and so forth, on the more theoretical side, thinking about the algorithm, how it works, trying to verify that it works so on and so forth. So that's also all the research part, aside from the teaching. And then there's also another thing that I'm currently working on, which is more, again, I help organize, what do they call it? Online lectures. They are not for students, they're for everyone to attend, presentations organized by the regional informatics society. And I/ there's a professor who organizes the lectures, which are guests lectures. So we get people, usually PhD or professors from other universities, that/ currently we're doing them on Zoom because of the pandemic, but we're probably going, might switch back to events that are both in person. So, I help organize that usually, that involves setting up the whole thing, recording, talking with/ recording, advertisement, everything. I'm kind of involved on that to make sure that it works out. And also I am the one who edits the videos and puts them on [Organization], at the channel of our chair. So that's also something that I'm involved in. Other things are like, I think that's also part of teaching, it's the bachelor master thesis of students I'm currently/ I have some students where I help them with their, I supervise their bachelor master thesis. So, we are also trying to integrate the work of the students into the overall project that I'm working on. And yeah, the whole thing is also/ so I'm also involved, the project has/ so technically I'm, I have this one project where I'm financed from, but I'm also working on the larger project that the chair's working on, which is like a software called (uncl #00:08:38-0#), which is the language work (uncl #00:08:39-0#) and so forth, and related software. And I'm also involved in that kind of. So// #00:08:40-0#

I: I think this is a very good picture of (uncl #00:08:46-0#). Okay. #00:08:40-0#

R: So yeah, it's mostly, it's a theoretical work to be done. So research, there is programming, there is teaching, organization. I have to do, I have to deal with my superiors and I also have to deal with students I'm supervising. So// #00:09:00-0#

I: I think this is a really, really amazing detailed. So I think this is quite good to understand where you're working. #00:09:10-0#

R: Just shorten it. #00:09:10-0#

I: Yeah. I will shorten it, no worries. So now to also this qualitative values you've provided us. I would like to get some quantitative results here. And therefore I'm using the Likert scale, you are familiar with the Likert scale? #00:09:30-0#

R: No, I'm not. #00:09:30-0#

I: Likert scale, we have five values, which is "strongly agree", "agree", "neutral", "disagree", "strongly disagree" to a statement. And I would like to, yeah, like to ask you to use that scale to answer the following four questions I will provide you, to just figure out how your knowledge is, based on quantitative values. Okay? #00:09:50-0#

R: Okay. #00:09:50-0#

I: So the first statement is, "I'm a computer science expert". And here I would like to have your statements evaluated based on the Likert scale. Do you strongly agree to that? Do you agree to that? Neutral, disagree, strongly disagree. #00:10:00-0#

R: I agree. #00:10:00-0#

I: Agree? #00:10:00-0#

R: There's still some stuff I need to learn. #00:10:10-0#

I: Okay. Absolute. "I am an information security expert." #00:10:10-0#

R: Neutral. #00:10:10-0#

I: "I am a cloud computing expert." #00:10:20-0#

R: Disagree. #00:10:20-0#

I: And, "I am a cryptography expert." #00:10:20-0#

R: Agree. Yeah, from the algorithmic side I have some knowledge about this. #00:10:30-0#

I: Okay. Yeah, perfectly. Super. That fits really good to that statics. You're through it here. Okay, cool. So that was the warm up phase. I think you've now become an overview about me, I've become an overview about you. And I would like now to enter into the main phase. #00:10:50-0#

R: Okay. #00:10:50-0#

I: And for the main phase, I already introduced you here with the three companies, company A, company B and company C, which I also call company A, company B, company C. So the first question I have here is, do you understand the case studies? #00:11:10-0#

R: Yes. #00:11:10-0#

I: Question two. Now again, quantitative values, and again a statement prepared where we'd like to have you asked in the Likert scale. "I believe that these are realistic cases from the business world." #00:11:20-0#

R: This machine/ tech/ per case study or? #00:11:40-0#

I: As you would like to answer it, yes. #00:11:40-0#

R: Okay. So I'm not quite sure about/ how far artificial intelligence is able to detect machine with failure at an early stage. I'd say, yeah, I think that there are some projects that are currently developing this, but I'm not quite sure if they're already in a phase where this is widely spread. So although/ I say yes. You know what, forget it, yes. #00:12:10-0#

I: Agree, strongly agree or? #00:12:10-0#

R: One second, the first one I'd say agree. The second one/ I go through the second one again, just wait. That's it again. Yeah, one second. I'd say strongly agree. #00:12:50-0#

I: Good. Alright, thanks a lot. And the cases presented always involve adapting a cloud application. How would you decide whether to adopt the cloud application or not? #00:13:00-0#

R: Depends on computing power, computing resources I need. If the computing resources are too great, are so great that I have to rely on a data center, then I would probably switch to cloud computing, because it also depends on how big my own// #00:13:20-0#

I: Sorry. I think I was misleading here. I mean, how would you decide on that cases if you were in the position of that cases and had to decide whether to adopt this cloud solution or not, how would you do that? #00:13:30-0#

R: Getting the first company I would, usually I would say yes, that I would adopt the cloud solution, because developing artificial intelligence software I assume the computing resources are quite high, and for a medium sized company, having the data centers themselves will probably be too much. For company B, I'd probably/ that's more difficult to say, but a company like B it's, I'm not 100 percent sure because for a company that is just like worldwide, like a worldwide player and this large, they could have their own data centers, and they probably have, they probably already have their own data centers and they could probably already outsource computing power at their own data centers. So using cloud services from other companies, I'm not so sure if that's a good idea. I'd probably say they have enough resources themselves, since/ oh no, it's a/ sorry, I'm wrong. This is a chemical company. Sorry. Then in case A and case B, yes. Case C, I don't know, provider C is/ I think/ okay. If you're looking at/ oh no, that's security. Right, I'm stupid. Sorry. I have to take into account the security. "Cloud computing is not that secure, regarding artificial data leakage/ this is attached to the shore on a personal computer. That's running up against system. If they (uncl #00:15:31-0#) look like to introduce a spot, it is extremely important to the company that the data is stored securely. Data leakage due to a hacker then could lead to economic and for and for the company. In this case, company A has chosen as a company (uncl #00:15:45-0#) it's certified according to//" #00:15:50-0#

I: Okay, maybe I ask the question differently. So the question I actually wanted to ask you is, all of these times, the companies try to adapt the SAS application, the new cloud application. And usually if you do something like that, if you adapt an external service, so this is like outsourcing the services, right? #00:16:10-0#

R: Yes. This is outsourcing. #00:16:10-0#

I: So the thing which companies are actually doing most often it's risk management. #00:16:20-0#

R: Yes. #00:16:20-0#

I: Have you ever heard about management? #00:16:20-0#

R: Yes. #00:16:20-0#

I: Have you ever heard about/ what can you tell me about risk management? #00:16:20-0#

R: Risk management is necessary. It's basically try to assess the potential risk with, that comes, in this case that comes with outsourcing regards to possible data leakages, possible, what's it called? Misuse of trust on the part of the company that you outsource, that you're outsourcing to, and so on. And so, it's tough. Especially, I think it's regarding customer data mostly, but also against internal data, customer data and (uncl #00:17:12-0#). So you have to make sure that the company (uncl #00:17:16-0#) that you are also seeing too as trustworthy, and that the company has, the company you're outsourcing to is able. That you/ not only that you know that they're trustworthy, but that they're also capable of, that they're capable of minimizing security risks. So a security leak or something, (uncl [#00:17:45-0#). So you have to also make sure that they're competent or not. I think in case study A, since they're both based in Europe and it's a limited liability company of one 180 million, I'd say in case study A that would be probably the right decision to make. In case study B, I'm pretty sure that's not a good idea. #00:18:00-0#

I: Let us/ sorry for interrupting you, because there are some steps involved and I would like to present also something, so we can do the risk management together. I just wanted to know, to make sure that you know what risk management is about. Then I understand you did. And I think also you agree, or do you agree to the statement that risk management makes sense in those cases? In these all three cases presented? #00:18:20-0#

R: It's absolutely necessary. #00:18:20-0#

I: Okay, perfect. #00:18:20-0#

R: At least in these first two cases. In the second case/ the third case it's not that, I think the data in the third case is not that sensitive. Since the online, since I see it's usually just some, it's probably just account management, I think the most data that get/ I think maybe if they, I think maybe the most data that gets stored is an address, and I'm not sure that the customer data for company C is that problematic to handle. So the risk assessed/ so I think in the case/ of course, you always have to do risk assessment. So yeah, I agree with that. I just say, I just think in the case of company A and company B, it's a lot more important for them. #00:19:20-0#

I: Okay, perfect. I would like now to present you following risk metrics. Please (uncl #00:19:34-0#). Do you see the risk metrics or do you understand that risk metrics first of all? Let me explain it thoroughly for you. So on the risk metrics, we have two values. On the one hand side, we have the probability that a specific incident occurs. And on the other hand side, we have the impact of that incident. So meaning, if an incident is certain and impact is really high, then the risk is very high. If we have an incident which has a really low probability and negligible impacts, or money in that case, then of course the risk is also low. #00:20:10-0#

R: I understand. #00:20:10-0#

I: So this is how to read that metrics, and I think you understand the metric. That's good. Now, I prepared that risk metrics in a generic case, meaning probabilities is always the same. So if you have a risk or an event with a high probability, higher than 90 percent for example, then it's called (uncl #00:20:37-0#) and those are the values for specific probabilities. So if your probability is below ten percent of an impact, or an incident, then it's called rare. It's unlikely if it's between ten percent and 30 percent, possible if it's between 30 and 60 percent, likely if it's between 60 and 90 percent, and certainly, or certain if it's bigger than 60, 90 percent. #00:21:00-0#

R: Yes. #00:21:00-0#

I: Okay? And also the impact, it's ne// #00:21:00-0#

R: Negligible. #00:21:00-0#

I: Negligible, if it's lower than ten percent of the yearly turnover of the company. So in that example here, what's the turn over of the/ 80 million I think. #00:21:10-0#

R: 80 million. #00:21:20-0#

I: And then of course it's negligible if it's below eight million. It's marginal if it's// #00:21:20-0#

R: Between ten and 30 percent, critical 30 to 80 percent, and catastrophic is above 80 percent. #00:21:30-0#

I: That holds for all the three case studies. So this means generic. Okay? Understood, I think. #00:21:40-0#

R: Yes. #00:21:40-0#

I: Okay. We talked here about that. Just/ okay. Now an open question here again, do you see any risks related to compliance topics? So policies set by a company that the cloud service provider must implement, like backup location, firewall configuration, design configuration, API setup. Do you see there any risks in the named three case studies? #00:22:10-0#

R: Yeah, of course. It's absolutely necessary that in the first/ data leakage should not occur and the company A is worried about data leakage. So in this case, we have to make sure that the security aspects are (uncl #00:22:38-0#). And I assume that the data is also valuable. So/ well, in the first case study the most important, the emphasis on storing the data security, so I would say access, access to the data has to be absolutely secure, which means/ but what were the points that you stated again? #00:23:00-0#

I: So it's compliance related topics, like backup location, firewall configuration// #00:23:10-0#

R: I would say firewall configuration is very important in this case. Backup location as well. I think all of them are important. Can you/ backup location, firewall configuration, the next is? #00:23:20-0#

I: Design configuration, so how does the design of the website looks like. #00:23:30-0#

R: The design of the website? The front end? I don't think that's that important. Although the company, as far as I know, here is relatively, has personal contact with its employees. So the front end design is probably not that important, considering that they're probably doing meetings in person and it's not handled on/ unless you're talking about provider. Are you talking about company or provider? #00:24:00-0#

I: I'm talking about provider. #00:24:00-0#

R: So provider is front end design. #00:24:10-0#

I: Yes. #00:24:10-0#

R: Yeah. Okay. Then that's important definitely, because provide A, if company A can only interact with provider A via online, so there's no personal contact between the two, then of course the website has to be, then the website design is important, so that company A doesn't accidentally use the wrong, select the wrong configurations, or select some sort of business contract that's not, that does not reflect their stated goals. #00:24:50-0#

I: I provided here three risks, which I would like you to, again, based on the Likert scale, I will tell you a risk and you can then tell me for each of the three use cases, whether this one you agree, strongly agree, neutral, or whatever that risk applies to that use case. Okay? #00:25:10-0#

R: Yeah. #00:25:10-0#

I: So the first risk is the risk that the cloud application provider, so the provider A, B and C, implements a contractually, not mutually agreed configuration. #00:25:20-0#

R: Yes. #00:25:20-0#

I: Do you understand that risk, first of all? #00:25:30-0#

R: Yes. I understand that risk. #00:25:30-0#

I: And second// #00:25:30-0#

R: The provider? #00:25:30-0#

I: The provider. #00:25:30-0#

R: Yes, okay. So, the second? What's the second? #00:25:40-0#

I: So first of all, do you, how would you rate that based on the Likert scale for all those three cases? Do you strongly agree that this is a risk which could occur to all of the three use cases or? #00:25:50-0#

R: Data/ "In this context company A has chosen. This company has an unknown/ It is limited to this sort of/ it says exclusive online (uncl #00:26:01-0#). This is/ so, regarding the Likert scale// #00:26:00-0#

I: The Likert scale just says whether you agree or strongly agree that this is a risk for this specific use. (uncl #00:26:14-0#) the risk. Just if this is// #00:26:10-0#

R: I strongly agree with this, this is a risk for case study one. "Company is/ sales on consultant services. So, there's always a consultant there. I would say neutral in this case, because there might be a risk depending on the competency of company B, but considering that they're actually talking to the employee, I think the list, the potential risks might be mitigated by that. So I'd say neutral on the second case. And at the third case, in the third case I'd say agree, if we're comparing the three. But// #00:27:10-0#

I: No, it's just whether you see that risk also in the use cases. #00:27:10-0#

R: In the use cases. So// #00:27:20-0#

I: In the case study, sorry. You see the risks? #00:27:20-0#

R: In the first strongly agree, I see the risk. In the company B I'd say neutral. And then company C I would say agree. #00:27:30-0#

I: Okay. Now coming to the rating of the risks, okay? And now again, I would like to ask you, not only to say whether you see that risk, also how you would rate that risk for the three use cases. #00:27:40-0#

R: In the first use case, I would say that the risk is very high. #00:27:50-0#

I: Because/ how would you? Just say how you would/ probability and impact? #00:27:50-0#

R: Probability and impact. #00:27:50-0#

I: Because you can be here or in very high. So// #00:28:00-0#

R: Okay. "So, considering that the company, that provider A sells exclusively online with all sales context and has headquarters and you//" So exclusively without sales context, I would say that the probability is likely, and the impact might be, I'm not sure if it's catastrophic or critical, because/ it kind of depends. So they are developed/ this is regarding/ so the problem is that provider A might implement the software service in a way that provider, that company A doesn't want it to implement. I would say that considering the size of the company, that is certified and so on and so forth, I would probably just say that it is a high. So likely and high. #00:29:00-0#

I: Likely and critical you mean? #00:29:00-0#

R: I would say critical. Because it could very well be that there is some sort of misunderstanding. #00:29:10-0#

I: For the second? #00:29:10-0#

R: For the second? I would say that we're having company B, that employ, the group employs 80,000 people and specializes in chemical plants. And the company B, it has its headquarters in India. Oh, can I// #00:29:30-0#

I: Do it. #00:29:40-0#

R: If I could go back to my previous answers I would say// #00:29:40-0#

I: It's your interview. #00:29:40-0#

R: //strongly agree, strongly agree and agree. #00:29:40-0#

I: Okay. #00:29:40-0#

R: And I would/ because/ strongly agree, strongly agree and agree. And then I would say likely and critical for the first. For the second I would say, that the/ okay, this company is going (uncl #00:30:22-0#) certified on supporting services, such as (uncl #00:30:27-0#). Yes. Okay, intrusion detection. So intrusion detection cases, I would say in the case of company B, I would say that it's also, that it's likely and catastrophic. #00:30:50-0#

I: So very high? #00:30:50-0#

R: Very high, yes. Although I would/ no, I would say possible and catastrophic, because they actually, they have consultants services. But considering that they headquartered in India, there might be problems with language barrier. So I would say possible and very high, because intrusion, detection, if something, if a case is misunderstood by them, then that might have dire consequences, considering they're also not, seemingly non-certified, so they might not be as trustworthy. So I would say possible and very high. "Companies and association of several farmers from one region", I would say possible and, possible and margin. So medium. #00:32:10-0#

I: Okay, thanks a lot. Okay, that was the first risk. The second risk I have here, and again, first of all I want you to say whether you strongly agree, so based on the Likert scale, and then again rate the risk if applies. The risk of the transparent and slow processing of configuration updates. So especially in terms of the planning of costs, so meaning that the implementation of configurations get delayed. #00:32:40-0#

R: Yes. The implementation of configurations get delayed. #00:32:40-0#

I: Compliance, we always talk about compliance. So for example, just to name an example, if you realize, "Okay, we'd like to store my data not anymore in Germany, but for example, in Spain." This is configuration change, and then the question is, is there a risk that this takes too long or there's a time problem with that configuration change? #00:33:10-0#

R: Yes. Considering provider/ so I would say, for company A, I would again say agree for company A. Company B I would say strongly agree, and company C, I would also say strongly agree. #00:33:30-0#

I: Okay, thanks a lot. And again, could you rate their risks? #00:33:40-0#

R: For company A, the risk I would say is possible and the impact might be high. (uncl #00:33:55-0#) is the impact critical? I have to think about. "If configurations are implemented too late, data storage, and they're using/" accounting, accounting data. I have to think about this. This is the important category, then new configuration. I would say possible and marginal in this case. #00:34:20-0#

I: Medium risk, right? #00:34:20-0#

R: Medium risk. Yes. Possible and marginal. In company case B risk I would say, "if configurations aren't inmplemented/" considering that they're doing sales on consultant, I would say unlikely. I'd say unlikely, but cric/ company B would be agree or not strongly agree. Agree, not strongly agree. I would say unlikely and critical. So also medium. In company C case, I would say likely, and I would say regarding the turnover, considering they're aiming to implement it only locally/ so I'm not sure. So they're trying to (uncl #00:35:52-0#) on the market and across the region via the internet. Depends on how much of the turnover would be via the internet. So my assessment is that the farmers selling via the internet isn't that high. So I would say likely and marginal, so high. As I assume likely and marginal. #00:36:10-0#

I: That's fine, perfect. And now I would like to prevent a third risk. #00:36:20-0#

R: Yeah. #00:36:20-0#

I: The third risk is that one of the parties denies the implementation of a configuration in a case of a dispute. So if there is a dispute, something happens, data leak or something like that, that one of the parties says, "Okay, that was not the configuration I made. So I am not guilty for that." Is that a risk you see in the three cases? The keyword here is repudiation. #00:36:50-0#

R: So, okay. The first company is certified and has its headquarters in Europe. So I would assume it's unlikely. Do you mean how much would it affect turnover if// #00:37:20-0#

I: They would deny it. #00:37:20-0#

R: They would deny it, the implementation. That question is kind of weird. #00:37:30-0#

I: Okay. #00:37:30-0#

R: Because if a problem happens, that would cause the catastrophic fall out. But then deny/ oh you probably mean that this could bring them in front of court. #00:37:40-0#

I: Yeah, exactly. #00:37:40-0#

R: Okay. So this makes sense. Yes, okay. So, okay/ so, they could be, the company A could be punished for something that provider A did if they denied. And I would say it's unlikely that that happens, but the impact of that would probably be catastrophic. So unlikely, but/ although is it unlikely? I would say actually, I don't think/ yeah, unlikely and catastrophic. #00:38:20-0#

I: That's fine. #00:38:20-0#

R: Although catastrophic could/ would it be catastrophic in the EU? You know what, let's say unlikely and critical. Not catastrophic, unlikely and critical. I'm not sure how, how large the punishments (uncl #00:38:44-0#) can get. #00:38:40-0#

I: So the case or the risk here, just to make it more, a bit clear. Imagine you have a firewall configuration, and now a hacker is able to get into your data. #00:38:50-0#

R: Yes. #00:38:50-0#

I: And now an investigation takes place, and your data is on the cloud provider. So the cloud provider needs to be open to you, otherwise you as a customer of the cloud, you are not able to see all the applied configurations. And the question is now, is there a risk that the cloud provider, or the application provider says, "I did not change anything and I do not provide you with the data from my cloud." #00:39:20-0#

R: Yeah, there is a risk, but what are the/ the risk, I would say, in this case, it's unlikely. The consequences of that risk/ I think for company A catastrophic, so unlikely and catastrophic now that I think about it. Because the reputation of company A is actually dependent on that, because of their personal contact with their customers. So yeah, it would be catastrophic. I would say it would be unlikely since the company, since provider is certified and has its headquarters in the EU. It's a least in Europe. Well, company B// #00:39:50-0#

I: It's EU, it's meant to be EU. #00:40:00-0#

R: Okay, that's important. So that's, that might be, so unlikely and catastrophic. In company B's case/ the network of company B, and we would assume that it has dealt with chemicals. I would say that this case is, let's assume that something happens, then the chances that a company that is not certified and not stationed, that is not certified and not stationed in Europe or the USA, I would say/ it's an India, but it has no certification. It's 20 millions, so it's not very large. Then I would actually say that it is likely that that happens. The cost for/ would I say likely? But there are two/ yeah, I would say they repudiated, I would say likely. And the impact, marginal or critical, that they would deny that this is their implementation. But in case A, now that I think about the case A, if it happens and they don't take, if they try to avoid blame in case A, would provider A do this? Would they try to deny their responsibility in front of court, that they didn't implement a certain service?

I think that would be difficult for company A, but it could be. Maybe I would/

kind of, is it possible? Yeah, I would still say unlikely, but maybe almost possible. In the case two I would say likely. But how are the costs if some hacker gets into the company? So I would actually say that, considering how large the company is, and that most of that, they only work together with the biggest companies, would I say critical or would I say marginal? I would actually say, I would/ I'm a bit pessimistic, I would say marginal. So// #00:42:30-0#

I: Too optimistic, right? #00:42:30-0#

R: Depends on what you're thinking about. If data leakage of something like that comes out and the company can get away with some stuff that's not/ let's say, legally gray, so yeah, marginal. #00:42:50-0#

I: Okay. So we have a high risk, right? #00:42:50-0#

R: A high risk, I would say. #00:42:50-0#

I: Second is also, and the third one? The third case? #00:43:00-0#

R: "(uncl #00:43:02-0#) corporation, but they deny." I would actually say, in the case of company C it's unlikely, and it's probably not negligible. #00:43:10-0#

I: (uncl #00:43:15-0#). #00:43:10-0#

R: So yeah, I would say no. #00:43:10-0#

I: Okay, good. Perfect. #00:43:20-0#

R: Sorry. I know it's taking so long. #00:43:20-0#

I: No, it's perfect. That's amazing, it's really great work. So, all right. So that was the more or less hard part, so to say. #00:43:30-0#

R: Yeah, difficult one. #00:43:30-0#

I: I mean, this is the time taking part. Think about a case study, get familiar with it, understand the risk and all this stuff. So now more or less followup questions will follow. Plus, I would also like to explain you my approach, which I implemented. And then we again have to rethink about the risks. Okay? So my approach I implemented is here, and I will explain you quickly how the approach works. So please ask me any questions if you do not understand (uncl #00:44:01-0#). So, I will go step by step through it. So, first of all, this is, the cloud picture here is the cloud, obviously. We have a cloud, this is in this case the [Organization] cloud, but that's not really important, or it's not as important. We have a blockchain application or we have a blockchain. #00:44:20-0#

R: Yeah. #00:44:20-0#

I: We have a customer wants to configure the application or the cloud application. So, the SAS application so to say. So, my approach says following, the configuration is not done directly to the cloud application itself, but the configuration is first encrypted. So the cloud consumer, the application itself, and the application provider create a common shared symmetric key. #00:44:50-0#

R: Oh, it's a metric. #00:44:50-0#

I: It's a metric. They using the Diffie-Hellman protocol for that, to create a common key. Based on that key configuration files are encrypted. #00:45:00-0#

R: And what is the protocol again? Defi? #00:45:00-0#

I: Diffie-Hellman. It's a key generation protocol. #00:45:10-0#

R: Yes, I remember. I can't remember the specifics of it. #00:45:10-0#

I: It's not important for that, but the (uncl #00:45:18-0#). #00:45:10-0#

R: That's a metric key, and the protocol for creating the symmetric key is cryptographically secure. #00:45:10-0#

I: Yeah, it's a secure protocol. So the protocol is not/ that might be any protocol. So just assume that they are able to create a shared symmetric key, okay? #00:45:30-0#

R: Share symmetric key// #00:45:30-0#

I: Using that key, they encrypt the configuration. Next step is, they start the encrypted configuration on the blockchain. The third, the second step is now, this is that step here, that the cloud application pulls the encrypted configuration from the blockchain and implements that configuration. #00:46:00-0#

R: Probably automatically. #00:46:00-0#

I: Automatically, yes. So there is no use (uncl #00:46:04-0#) at all, implements that configuration. In the next step, as soon as the configuration is implemented, it monitors the log files and sees whether the configuration was applied successfully or an error occurred. As soon as successful "applicated" or successfully applied, then a backup of the whole virtual machine is created through which the application runs, a hash read of that backup is created// #00:46:30-0#

R: Hash value. #00:46:30-0#

I: Yes, hash value, and dot on the blockchain. #00:46:30-0#

R: Okay. So if I understand correctly, the virtue/ we have on the cloud, we have the blockchain and we have the virtual machine. #00:46:40-0#

I: Yes, exactly. #00:46:40-0#

R: And the virtual/ okay, we have the virtual machine, we create a backup of the virtual machine or it/ and then we create a hash value? #00:46:50-0#

I: Yes. So we have to implement the configuration, we create a backup, and then start a hash value back to the block. #00:46:50-0#

R: What happens with the backup? #00:46:50-0#

I: That can either stay or be deleted. #00:47:00-0#

R: Okay. So we have the hash value, the hash stays and is put into the blockchain so we can check later on. #00:47:10-0#

I: Yes. #00:47:10-0#

R: Okay. #00:47:00-0#

I: Okay. So to sum it up, the configuration is written to the blockchain. The application itself pulls the configuration from the blockchain. As they share a symmetric key, it encrypts the configuration, implements the configuration, creates a backup, use the hash value of the backup, starts that hash (uncl #00:47:26-0#) back to the blockchain, and the cloud application consumer can see whether the application was successful or not. If not a successful application, it would be written to the blockchain that there was an error. #00:47:30-0#

R: So, yeah. Okay. So, and the consumer can of course check if there was an error by going to the blockchain. And the information is not made publicly available. So I mean, it is publicly available, but it is encrypted. So we assume that it is secure. #00:47:50-0#

I: Yeah. #00:47:50-0#

R: So, okay. Yeah, it makes sense. #00:47:50-0#

I: And all blockchain or written to the blockchain, in front of the blockchain, as you know are digitally signed, so they are traceable. #00:48:00-0#

R: Yes. #00:48:00-0#

I: Okay. So the first question here I have, did you understand, or I've understood that approach based on the (uncl #00:48:13-0#)? #00:48:10-0#

R: If I understand that approach? So, strongly. #00:48:10-0#

I: Okay. So you understood it. Okay. Now, back to the use cases we have here. Again, I would like now to again evaluate the risks with you. The first risk was the risk that a cloud application provider implements a contractually, not mutually agreed configuration. #00:48:30-0#

R: It's basically zero. So I would say strongly disagree. #00:48:40-0#

I: So that risk does not apply anymore? #00:48:40-0#

R: That risk does not apply anymore. #00:48:50-0#

I: And based on values again for A, B and C. #00:48:50-0#

R: For A, B and C? Okay. For A, I assume that they all/ question, is this the company or is this the provider? #00:49:00-0#

I: This one? #00:49:00-0#

R: Yeah, that's the company, I assume. #00:49:10-0#

I: That's a consumer. So this is the company, yes. #00:49:10-0#

R: So the comp/ okay. So, the risks/ if we assume that the blockchain is secure so enough people are working on it, and we assume that the/ yeah, I would say that implementing a feature that is/ I think about it. The configuration is automatically implemented in the virtual machine. The only/ it was not contractually agreed upon. The only way I could see that happening is if the configuration is not actually translated correctly into. So you write down the configuration in some way, which the companies A does it. Since it's through a blockchain, and the blockchain and the cloud application pulls it from the blockchain, seize the configuration, but interpret it in a completely different way, so that would be the only possibility. So I would say that it's, this is/ I would say disagree, but not strongly disagree because that could still happen if the implementation is completely unsound. So if the implementation is unsound, I would say disagree. Do I have to// #00:50:30-0#

I: The risk assessment again, yes. #00:50:30-0#

R: The risk assessments. So it's/ I would say that it is unlike/ what did I say for the impact? #00:50:30-0#

I: It was high at the beginning. I do not, did not write them with me. I just wrote the risks. #00:50:40-0#

R: Okay. I would say rare and catastrophic again. Because, so implements/ so this is implement a feature that they did not want? #00:50:50-0#

I: Yeah. #00:50:50-0#

R: So I would/ no wait, sorry. I am stupid. There was probably, I would say high, and I would say, I would assume that a company like this has some standard procedure, so I would say it's unlikely and the effects would be marginal. What's it marginal? I don't know. It's medium. That's the same in here. #00:51:20-0#

I: Okay, perfect. That's also fine if you just said the risks. And for the second case? #00:51:30-0#

R: For the second case, (uncl #00:51:40-0#) that's strongly implemented. Okay, they're using/ the company is not certified. So the problem is to ask, can they actually implement, translate the configuration that the user wants into the correct implementation?

And in this case, I would say the probability of this failing is unlikely, and the costs are still, would I say medium or high? I think I said/ did I say very high? #00:52:10-0#

I: Yes. Last one you said very. #00:52:10-0#

R: I would say also, I would say medium in this case. I'm not sure. I'm not quite sure if your approach it could still be wrongly used, incorrectly used. So I would say, yeah, I'd say medium. I'm going to be optimistic (uncl #00:52:38-0#). #00:52:30-0#

I: And the last one, the farming company? #00:52:40-0#

R: No. No. #00:52:40-0#

I: Okay. Then let's continue with the risk of transparency, low processes, with that approach. #00:52:50-0#

R: Transparency? #00:52:50-0#

I: No, the risk of slow processes that delay in applying the configurations of (uncl #00:53:05-0#). #00:53:00-0#

R: The/ since it's automatically applied it should be fast unless, the implementation is horribly inefficient. But I'd assume low, low. #00:53:10-0#

I: Thanks a lot. #00:53:10-0#

R: And you know what, make it, make it/ I would say in case, in case two I would still say, for the first question I would say give it a high, because the company is not such a (uncl #00:53:30-0#) Yeah, it's rather/ although they are 20, they make 20 million, I'd still say it's high. #00:53:30-0#

I: Last time it was medium for the first case. And for the second one, you had medium for the second risk, second company? #00:53:40-0#

R: No, I mean, first risk in second company, make that high. And then the case two it's all low. #00:53:50-0#

I: Okay, all right. #00:53:50-0#

R: I just, I'm kind of/ it's a company stationed in India that's not certified, so I'm kind of skeptical if they're going to do the implementation correctly. #00:54:00-0#

I: And third case, that someone denies having applied to configuration, the risk? #00:54:00-0#

R: It's basically, I would say all of them are low. Because the, this is/ the configurations are/ it's (uncl #00:54:25-0#), I would say no. Yeah. #00:54:20-0#

I: Okay. That's it. Thanks a lot. So, okay, we have that. Now we are nearly facing the end, so it's all good. So just/ so we are done with the risk assessment part here, just a few open, or just a few quantitative questions again. And again, based on the Likert scale, I have a few statements prepared and I would like for you to answer that question. And the question is now referring always to my approach, I proposed to you. And the question is, this approach moves the trust to the blockchain? Do you strongly agree? Agree? #00:55:00-0#

R: Agreed. I wouldn't say strongly agree, because again, the company has to also make sure that the configuration that is, is implemented. So, so the configuration of/ the customer writes down the stent correctly interpreted by the system. #00:55:20-0#

I: The next time, I think it makes sense to transfer trust to third parties (uncl #00:55:39-0#) describe case studies. #00:55:30-0#

R: It describes case studies. What do you mean by third party? I wouldn't call the blockchain a third party. #00:55:40-0#

I: That's what I would call it here in// #00:55:40-0#

R: Okay, you would call it. It makes sense to agree. You need something like this to make sure, yeah. #00:55:50-0#

I: I think the use of the blockchain as a trusted anchor makes sense. #00:56:00-0#

R: Agree. #00:56:00-0#

I: Could other trust building technologies such as web of trust or PKI also be used as trusted party? #00:56:10-0#

R: Can you tell me more regarding where both are trust? #00:56:10-0#

I: The web of trust means that you have a certificate, you create a private key for yourself, and you meet other peoples, and then you decide whether you trust their public (uncl #00:56:27-0#) or not. #00:56:20-0#

R: "Help other approach." So you're basically telling me, whether I trust the/ can I say whether, is this whether I trust the keys or whether I trust the company? Because that's two different things. #00:56:30-0#

I: The keys. #00:56:30-0#

R: The keys. But I mean, you could probably do it, like expand into, "Do I trust the company as well?" So yeah, basically a rating system kind of technically also (uncl #00:56:56-0#) would be, I think a good approach for this. And furthermore, if you have a key based rating system, then you could make sure that/ then you could say, I trust the key of the user who did this rating. So then you could make sure that this isn't a botch, would be my assumption. So I would say yes, web of trust yes. And the PKI was this what? #00:57:20-0#

I: There's the root certificate, and you trust the root certificate. And you trust everyone that root certificate signs again. #00:57:20-0#

R: Yeah. I would say, yeah. I would say strongly agree in this case. #00:57:30-0#

I: Okay. The use cases I presented to you, then they made sense for you? I think we already talked about that. So this is also fine. Do you think that these use cases reflect the scope of that architecture? Or do you think there are some further scenarios which are not covered here? #00:57:50-0#

R: Scope of the architecture? For the scenarios that would cover regarding the risks? #00:58:00-0#

I: Where this architecture could be used// #00:58:00-0#

R: Yeah. #00:58:00-0#

I: //but not named yet or// #00:58:10-0#

R: I mean, that this kind of architecture can be used in other contexts, I would say probably yes. So I agree. #00:58:10-0#

I: Okay. Okay, we are slowly coming to the end of the interview. I would like now to come to the aspects of transparency, automation, and authorization. We call the approach presented, this one, and think about the issue of transparency, automization and authorization of cloud applications. #00:58:40-0#

R: Yes. #00:58:40-0#

I: Does the presented approach have an impact on those three topics? #00:58:40-0#

R: Yes. #00:58:40-0#

I: And now again, I think the presented approach improve the transparency of cloud application configurations. Likert scale. #00:58:50-0#

R: Agree. I wouldn't say strongly agree, but because again the implementation is, might still be obscure. So the implementation of the cloud applies itself, but might still be problematic. You know what? Actually I'd say neutral, because the cloud application can just ignore the// #00:59:10-0#

I: Yeah, okay. #00:59:20-0#

R: It kind of depends, because you would assume the hash value changed. Yeah, I would say neutral because you can still, it might help but it might not necessarily help, because again, depends if the current application actually uses the configuration properly. Otherwise it could just store the configuration somewhere, not use it in its implementation, use the hash value and the stored valued changes the hash value. So you would see a change in the hash value, but the implementation is still, basically the same. And that's the same thing. And you couldn't actually look at this, because the problem is/ yeah, okay. So forget about it. Yes, we say, I would say neutral on this case. Second, what was the second one? #01:00:10-0#

I: Then there was the transparency question, does it have to make configurations transparent? #01:00:20-0#

R: Configuration, make configurations/ neutral. It makes the assumed configuration transparent, but not necessarily the actual. So let's say neutral. #01:00:30-0#

I: Do you think that this approach can help to configure cloud application in an automated way? #01:00:40-0#

R: Yes. #01:00:40-0#

I: So strongly agree or agree? #01:00:40-0#

R: It helps configurations in an automated way. I would say strongly agree. #01:00:40-0#

I: Do you think that this/ this question not here/ I think the presented approach can help to investigate security incidents more easily and to identify responsible parties in a legally secure way. #01:01:00-0#

R: Agree. #01:01:00-0#

I: You agree. #01:01:00-0#

R: Yes. The second one I would say, "Of course", but the first part of the question, perhaps. Again, depends on how the cloud application is actually using configuration, because the company A doesn't, can't really look into it, into the implementation itself.

They basically encode the encryption, sorry, encode the configuration, but it's still up to the developer of the cloud application to make sure that the cloud application actually adopts to that configuration properly. So I would say an agree, not strongly agree. #01:01:40-0#

I: But in the case of legal dispute? #01:01:40-0#

R: Yes. I would say agree. #01:01:50-0#

I: Then there's also not the possibility anymore for hiding something. #01:01:50-0#

R: No. The situation is not possible. Unless that, they would have to/ if they would say, "I have not implemented this", then they would also have to admit that they are, that cloud application is working properly, according to the configuration that is sent in as input. So, it makes repudiation a lot more difficult. #01:02:10-0#

I: Okay. So final questions. Do you want to add something? Do you have any topics, do you want to see if there are any advantages, disadvantages of the approach? Would you implement ot propose any improvements, weaknesses, or whatever? #01:02:30-0#

R: That would be prob/ I would, could/ the possibility of having some sort of verification or tests system for the cloud application that the consumer can, so that the consumer has as a way to verify, or at least test if the cloud application is working as intended. So, at the very least some sort of black box testing would be nice, which could also start the results on the blockchain if you want to. Or, I think verification might be difficult, but that would be the ideal case, that you have some sort of verification that the customer knows about what type of verification it is, and that the verification result can then also be stored on, will also be stored on the blockchain. So I would say automatic tests of verification that are transparent to the customer, how the tested verification work, and then this is stored on the blockchain as well. So that it would be my, something that I would add just to make sure that we can actually make sure that the configuration of the customer sends in, is then used by the application in the way that it was intended to, so properly. So, the application actually implements this configuration. This would be the one, like part of the current architecture where I would say that that would be necessary, or it would be a great benefit to this architecture. Yes. #01:04:20-0#

I: Okay. #01:04:20-0#

R: I don't/ I'm not sure if I have anything more to add. We could, so we could also use the previously mentioned web of trust or PKI in addition, to make sure that the companies that the consumer hires are trustworthy. So before they hire them, they could actually look into if this company is trustworthy. It's kind of like I said, I mean it's basically a certificate in some way or another, but it doesn't have to be from an official, something like the ISO or something. But basically user rating systems where you have the, where you have the private keys of the users are also, can be trusted or distrusted, so you can make sure that the user's actually real and not bots. So something along those lines could be used. It's not integrated into the architecture, but basically as a first step before deciding to buy the product// #01:05:20-0#

I: And dump the global application. #01:05:30-0#

R: The cloud application, yeah. #01:05:30-0#

I: Okay. Yeah. That's a really good hint. And now, as you have now heard everything, you have seen everything, you know everything, you have a big picture now, how would you rate your experience in that area presented in school marks, where one is very good and six is insufficient and so on? #01:05:50-0#

R: Regarding what? #01:05:50-0#

I: Regarding the whole topic we talked right now. Did you feel you familiar with that? Did you feel fine with that? Did you feel you're missing some knowledge here in that area? #01:06:00-0#

R: You mean, am I not so sure about this? #01:06:00-0#

I: What you said, are you sure about what you said or do you feel uncomfortable with what you said? #01:06:00-0#

R: I would say I'm relatively sure. Some points regarding risk assessments, I'm not quite sure if I picked the right value. So I would say, yeah, kind of. #01:06:20-0#

I: So in school rates? #01:06:20-0#

R: So my, how sure am I am about what I said? From one to six? #01:06:20-0#

I: Yes. #01:06:20-0#

R: Right. Okay. Two would be very, I'm very sure. #01:06:30-0#

I: Very good. #01:06:20-0#

R: And one would be very good. So very, very sure. Overall everything, I would say two. #01:06:40-0#

I: Okay, thanks a lot. Okay. Yeah, that was the closing phase. We are now closing information. Thanks for your openness, participation and time. As said, transcription will be the next step here, anonymization and evaluation. #01:07:00-0#

R: Yeah, maybe shorten the transcript. #01:07:00-0#

I: Thanks a lot [Person]. That's it. #01:07:00-0#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #2:

I: Okay, give me a second. I think it's starting. I will turn off this transcript. All right. So, I think we have a (unclear) #00:00:10-4#. It can start. And as I said, we start with a small warmup. And for the warmup session, I would like to get you a bit better known and also get your background a bit better known. To also weight your statements based on your background knowledge. So, the first question I have to you is, can you briefly tell me something about your professional background and your daily tasks? Just roughly. #00:00:39-5#

R: Sorry, again, I could - There was a disruption. I could not hear. #00:00:43-0#

I: Yep. Can you briefly tell me something about your professional background and your daily tasks summary? So, short version just about your background. #00:00:53-4#

R: Yeah. So, I'm working with (organization) and my daily task is to do some (unclear) #00:01:01-4# related to IT security testing of certifications. And also do some assessments regarding IT security. So, all in all like this IT, all in all it's related to IT security at the firm where I'm working. #00:01:16-5#

I: And have you studied or your professional background? #00:01:21-5#

R: Yeah. I completed my masters in computer science from (organization). And previously I studied my bachelor from Pakistan and also got a degree from U.K. (organization). #00:01:34-8#

I: So, your highest degree is a master, correct? #00:01:38-2#

R: Masters, yeah. #00:01:38-9#

I: In computer science. Okay. #00:01:39-8#

R: Yes. #00:01:40-4#

I: And how long have you been studying and how long are you employed right now? #00:01:45-6#

R: I am studying from 2000. Like also I just tell about the business? Then from 2013 - Okay. From 2000, I started my bachelor's in 2013. And in 2017 then did a job in (organization), so one and a half year and then started with the master. So, two and half years of masters. So, I completed master last year in 2021. And then again started working full time. And meanwhile I was also working as a part-time student when I was studying masters. #00:02:21-5#

I: Okay. So, all in all, I could say your background is computer science, and to be more precise, cyber security, is that correct? #00:02:31.5#

R: Yes. #00:02:32.0#

I: Summarized. Okay, good. Coming to the next. Now I have some quantitative questions. Quantitative means I would like to answer you - I give you a statement and I would like that you answered that statement with one of the five values; strongly agree, agree, neutral, disagree, strongly disagree. So, the first question or the first statement is; I am a computer science expert. #00:02:56-5#

R: Strongly agree. #00:03:01-5#

I: I am an information security expert. #00:03:07-6#

R: Strongly agree. #00:03:09-5#

I: I am a cloud computing expert. #00:03:13-0#

R: What was the third one? #00:03:16-0#

I: I am a cloud computing expert. #00:03:19-4#

R: Sorry, what was for? #00:03:21-6#

I: The second one or the options? Strongly agree, agree, neutral, disagree, strongly disagree. #00:03:28-5#

R: Agree. #00:03:29-0#

I: And last but not least, I am a cryptography expert. #00:03:34-2#

R: Agree or neutral. Neutral. Agree. #00:03:38-4#

I: Okay. Neutral or agree? #00:03:41-8#

R: Agree, yeah. #00:03:42.8#

I: Okay. Just that it's quantitative, so (laughs), it has to be one. Okay. That was already the warm up. So, I think we have a bit of background. We have your knowledge. And I think now we can enter the main phase. And I'm sure that will be easy for you. So, the task now is to read. I prepared three case studies and you have now time, as much as you need. I will send you the case studies in the chat. And I would like to ask you to read that case studies, first of all, check, if you can read. #00:04:19-8#

R: I don't see anything. Now I got it. #00:04:26-7#

I: So, take your time to read them. They're I think two pages. #00:04:33-6#

R: The file did not download. Open in browser. Okay. #00:04:44-3#

I: Can you read it? #00:04:49-8#

R: I just opened it. Yes, now I started reading it. So, I just have to read now, right? #00:05:06-0#

I: Mhm. Read and understand it as good as possible. #00:05:09-6#

R: Yes. I've read it. #00:10:04-8#

I: Okay. That's good. So, the first question, do you understand the case studies? #00:10:09-5#

R: Yes. #00:10:10-1#

I: Okay. Do you think these are realistic cases? #00:10:13-6#

R: Yeah, maybe. #00:10:15-8#

I: Yes, or maybe (laughter)? #00:10:17-9#

R: Yes, it can be. #00:10:20-4#

I: Okay. Now I would like now to talk with you about risk of cloud adoption. The first question I have is, can you tell me something about risk management? Do you have an idea about risk management, what risk management is and how it works? #00:10:40-1#

R: Yes. To identify the things that can happen and can lead to some disaster, to minimize that things or to handle the things is risk management. #00:10:53-1#

I: Okay. That sounds pretty good. I would like now to show you something. It's called the risk metrics. #00:11:00-4#

R: Okay. Can you - #00:11:03-2#

I: And I would - #00:11:03-7#

R: Just one time. Can you enlarge it? #00:11:06-8#

I: Yeah. #00:11:08-3#

R: Thank you. #00:11:10-2#

I: Is it okay? #00:11:10-2#

R: Yeah. #00:11:10-8#

I: Okay. So, this is a classical risk metrics, so to say, and it works as follows. So, you have on the left-hand side here, the probability of how probable a risk might be. And you have an impact how impactful the risk might be to your company. So, if you say we have a risk, which is rare, which is the probability is below 10 and is marginal in damage or in impact, then the risk would be rated as low.

If we have a risk that is, that probability is higher or below or higher than 90 percent, higher or at 90 percent to be more precise. And for example, the turnover per year is between, or the impact would be between that values here based on the turnover per year. So, in the case studies, you have always the turnover per year from each company.

And the impact would be between #00:12:10-3# that values, then it would be rated as very high, for example. So, this is generic in case of the turn over per year. So, for bigger companies this of course in absolute values more than for smaller companies. So, this is the basic idea here. The question I have to you is, do you understand that risk metrics? #00:12:32-1#

R: Yeah, I understand. #00:12:33-4#

I: Okay. Now, coming back to the cases we had, do you think a risk management makes sense for the proposed use cases? #00:12:46-5#

R: Yes. #00:12:49-0#

I: Okay. I would now like to present you with the following risks. And ask you whether that risks might be also risks that could occur in the case study presented. The first risk I would like to ask you whether that exists and also not only whether that exists, also, how you would rate it for the specific cases. Is the risk that the cloud application provider implements and contractually not mutually agreed configuration? #00:13:28-1#

R: Yes. #00:13:29-4#

I: I repeat it. The risk that the cloud application provider, so provider A, B and C in the use cases implements a contractually, so a statement which was not based on a contract, usually accrued. So that he or she, the provider implements something, a configuration. A configuration might be, for example, a backup application. A configuration might be anything which you can configure on the cloud application, which has not mutually agreed on. #00:14:03-2#

R: Yeah. Okay. #00:14:04-4#

I: So, let's go with that risk through the three use cases. Do you think this is a risk for the first use case? And how would you rate that risk if it is a risk? #00:14:18-4#

R: First of all, it'll be like negligible first for me for use case A. Because that is certified and has a huge turnover and is in Europe. So, I would say negligible and unlikely and negligible. Low. #00:14:42-9#

I: Unlikely and negligible, so the risk would be low. It’s okay. #00:14:45-7#

R: Yes. #00:14:46-0#

I: All right. Okay. The second risk. But you think the risk might exist, right? It might be a risk. #00:14:55-7#

R: Yes. #00:14:56-6#

I: The second risk. The risk that the implementation of a compliance driven configuration gets delayed due to slow manual processes. A compliance driven configuration is for example, the backup location again, or all the configurations you can do on a cloud application. #00:15:16-8#

R: Okay. That can be delayed, right? #00:15:20-3#

I: Yeah. That the risk that it delays due to slow or non-existing manual processes. So, to bring you an example, you, as a company realize, okay, the backup location needs to change. And now you need to get in contact with the cloud application provider and ask him to change the configuration. And the question is, do you see a risk that this gets delayed, that ask? So, the implementation of the configuration gets delayed. #00:15:49-4#

R: So, the company will ask the provider to change the location, right? #00:15:53-1#

I: Yes. #00:15:53-2#

R: For the use case A would be again low and like rare and negligible. #00:16:05-6#

I: Okay, so low. #00:16:09-7#

R: Yeah. #00:16:10-0#

I: Okay. And the last risk I would like to ask you is the risk of denying the implementation of a configuration in a case of dispute. So, there is the risk that one of the contractual parties denies its responsibility to implement contractual agreements in case of dispute. So, there might be a data leakage, and now there might be the situation that one of the parties says, "Okay, I did not say that." Or, "I did not configure that as it was configured," which led to that data leak. So, do you see that risk and how would you rate it? #00:16:49-7#

R: That would be a possible and negligible. #00:16:56-9#

I: Possible. So, also low? #00:16:59-2#

R: Yes. #00:17:00-3#

I: Okay. So, coming back to the second use case, so the second case study we had. So, that was all for the first case study, correct? #00:17:10-8#

R: Yeah, first case. Yeah. #00:17:11-6#

I: Now again, the risks for the second case study. The same risks, but now I ask you for the second case study. #00:17:18.7#

R: Second Case. So, can you repeat the risk? #00:17:21-6#

I: Yeah. The first risk was that the cloud application provider implements a contractually not mutually agreed configuration. #00:17:29-6#

R: Okay. That would be then possible and marginal. #00:17:43-2#

I: So, a medium risk, right? #00:17:45-0#

R: Yes. Just a moment. I have to read this one. I have to read something. #00:17:50-6#

I: Yeah, sure. #00:17:51-5#

R: Provider B right. It was provider B. #00:18:01-7#

I: Provider B, yes. #00:18:02-2#

R: I would say that it would then be - it would be critical obviously, and its possible. So, it would be high. #00:18:17-2#

I: Which risk, sorry? #00:18:20-4#

R: Possible and critical. #00:18:22-4#

I: For provider B at the first place? #00:18:25-2#

R: Yeah. #00:18:25-9#

I: Critical. So, it's high. #00:18:28-3#

R: Yeah. #00:18:29-6#

I: Okay. We are still at provider B. And now the second risk. This is the delay in implementing a configuration. #00:18:39-7#

R: Again, this would be then possible and marginal. Medium. #00:18:48-1#

I: Medium risk, okay. #00:18:49-0#

R: Yeah. #00:18:49-6#

I: And the third risk that one of the parties denies the implementation of a configuration in the case of dispute. #00:18:58-3#

R: Possible and critical. High. #00:19:02-0#

I: Possible and critical. High. And now we are doing it for the third use case or for the case study for the third case study. The first risk again, that one of the contractor parties implement something which was not mutually agreed on. #00:19:17-7#

R: So, it can be also from the company side, right. Mutual. #00:19:27-0#

I: Yeah. So, the provider implements. Sorry, I did not read the question correctly. It asks, the provider implements something which was contractually not agreed on. #00:19:35-5#

R: Okay. That would be rare, I would say. #00:19:39-5#

I: Which? Sorry, I just moved the mouse. #00:19:52-8#

R: Sorry, I - Because - Okay. After we will do that, we come to again, can we come again to provider A questions because - #00:20:02-6#

I: Yeah, sure. #00:20:03-3#

R: Okay. #00:20:0-.4#

I: You can always switch. As long as do the interview, you can update anything. #00:20:07-8#

R: Then for company C would be marginal and rare, so low. #00:20:17-3#

I: Marginal and rare, so low. Okay. We are the first risk at provide C, right? #00:20:24-0#

R: Yes. #00:20:24-8#

I: Okay. And you would like to update something for provider A at the first risk? #00:20:31-0#

R: Yes. That will also be, I would say marginal and unlikely. #00:20:35-9#

I: Marginal and unlikely. So, medium risk? #00:20:40-1#

R: Yes. #00:20:40-6#

I: I updated. Okay, coming to the second risk. I don't want to hurry you, so you have all the time you want. So, if you want to update something, just let know. The second risk is again, the risk that the implementation of compliance driven configuration get delayed due to slow or manual processes. And this is for provider C now. #00:21:09-2#

R: Then it's possible and marginal. #00:21:12-5#

I: Possible. So, it's a medium risk? #00:21:14-3#

R: Yes. #00:21:14-9#

I: Okay. And we had provider C and the third risk, the risk of denying the implementation of configuration in case of dispute. #00:21:26-8#

R: Critical and possible. #00:21:29-9#

I: Critical and possible. So, it's a high risk, correct? #00:21:34-9#

R: Yes. #00:21:35-5#

I: All right. So, that - #00:21:43-5#

R: Same for the provider A, critical and possible. #00:21:48-5#

I: Same for provider A. #00:21:50-8#

R: Yes. #00:21:51-4#

I: Critical and possible and critical, so it's high. Yes. Provider A, it's high for you, provider A? #00:22:00-5#

R: Yeah. #00:22:01-6#

I: So, I update from medium to high? #00:22:03-5#

R: Yes. #00:22:04-2#

I: Okay. I will just recap it, okay? #00:22:14-9#

R: Okay. #00:22:15-6#

I: The first risk you have for provider A high, for provider B high and for provider C low. #00:22:24-2#

R: Yes. #00:22:27-6#

I: The second risk, the speed of implementation. #00:22:31-7#

R: Yeah. Sorry? Yeah. #00:22:36-1#

I: It's okay? #00:22:37-2#

R: Yeah. #00:22:38-0#

I: Okay. The second one, the speed of implementation. You have for provider A low, for provider B medium, for provider C medium. #00:22:47-8#

R: Yes. #00:22:48-9#

I: And the third one, the third risk, denying in a dispute. You have for provider A low, for provider B high, for provider C high. #00:23:01-3#

R: For provider A for a will also be high. #00:23:04-4#

I: Okay. So, you're for all three high at the third risk? #00:23:09-3#

R: Yes. #00:23:10-0#

I: Okay. So, do you think those risks might occur in these described case studies? Yes. We had that already, right? #00:23:17.9#

R: Yeah. #00:23:18-7#

I: So, I already asked that question and we already evaluated it. Okay. I would like now to briefly introduce you to another approach with which cloud applications can be configured. This is - let me just show you that. Do you see my screen? Or let me just show it in a PowerPoint presentation. I think it's easier. #00:23:43-1#

R: This time of the day I'm a little bit off. So, if my answers are not (laughs) - #00:23:51-8#

I: All good, all good. No worries. So, let me show you the approach I want to show you. How do we do it? Yeah, we do it like this. I will share my screen again. And I will explain you the approach. And you are always welcome to ask questions. So, the idea of that approach is that we, first of all have a cloud. This is a cloud application. So, the cloud is the cloud. Within that cloud, we have two virtual machines as a test scenario.

In virtual machine one, a blockchain is running, but that could be any blockchain. So, don't think too much about the blockchain. That could be any blockchain. You can assume that the blockchain is secure. And we have a second scenario. In that scenario, we have a web server. And we do have a snort introduced intro #00:24:51-4# ideas (laughs). Detection section. Thanks a lot. And we have a cloud management script running here. I will explain you what that script is doing. So, the idea of that architecture is that a consumer, so in your case, that would be a company or whatever, the company A, B and C. They are the cloud application consumers. And we do have the cloud application provider. That would be provider A, B and C in your example.

Now the idea is that the application consumer and the cloud application provider and the cloud application itself create a mutually synchronized symmetric encryption key. You can think of they are doing a Diffie-Hellman key exchange to get a symmetric key. So, at the end, there is a symmetric key, which you said between the cloud application consumer, the provider and the cloud #00:25:51-5# application itself, they all have access to the same symmetric key. #00:25:54-8#

R: Same key. Yeah. #00:25:56-1#

I: Okay. Don't matter how they can get access to the key. They have the symmetric key. Now the idea is that the cloud application consumer uses that symmetric key to encrypt a textual descript or described configuration. So, a configuration, you can think of a JSON file, for example, as configuration. And they encrypt the configuration file with that symmetric key. Can you follow that idea? #00:26:26-3#

R: Yeah, I can follow. #00:26:27-4#

I: Now, the configuration, the encrypted configuration is written to the smart contract on the blockchain. You can follow that idea? #00:26:39.6#

R: Yep. #00:26:39-9#

I: Okay. Now the blockchain always creates new blocks. And once a new block is generated, the configuration or the input of a blockchain might change. And the cloud management script now monitors the blockchain for changes. If the cloud management script detects a change on the blockchain, it checks whether a start configuration of the blockchain has changed. So, it checks basically whether some of the parties, the consumer or the cloud application provider has changed the configuration on the blockchain. Can you follow that idea? #00:27:21.1#

R: Yeah. #00:27:21-8#

I: Okay. Now, as soon as it detects a configuration change, it pulls that configuration from the blockchain via smart contract. It encrypts the configuration as it has access to the same symmetric key and implements that configuration on the predefined application. In our case, the intrusion detection system. So, what the script would do is it would pull a configuration. An encrypted configuration from the blockchain would encrypt it, would read it and would implement it on the cloud application.

Besides implementing the cloud application or the configuration it read, it also monitors the log files of the application it needs to configure. So, in our case, the log files of the intrusion detection systems. And it monitors whether the configuration was implemented successfully or not.

If the configuration was implemented successfully, #00:28:21-6# so the first case, it triggers a backup of the virtual machine, of the whole virtual machine on which the application is running. #00:28:30-8#

R: In case of? #00:28:33-6#

I: In case of the configuration of the application was successfully implemented. #00:28:39-5#

R: Okay. #00:28:39-7#

I: It triggers the backup of the virtual machine. You can follow that idea? #00:28:45-7#

R: Yeah. #00:28:46-3#

I: It triggers the backup of the virtual machine, creates a hash value of the backup and starts that hash value back to the blockchain. #00:28:56-1#

R: Blockchain, yeah, okay. #00:28:57-7#

I: As a proof of implementation, so to say. #00:28:59-6#

R: Yes. #00:29:00-1#

I: Okay. That's the basic idea. Okay? #00:29:09-0#

R: Yes. #00:29:09-8#

I: So now, if for example at this boot might occur, you can always go back to the blockchain backup. Say, this is the hash which got approved, please have a look at it. So, you understand the idea of that approach, right? #00:29:24-4#

R: Yeah. #00:29:25-5#

I: So, this is now an architecture which a provider could provide to a consumer in case of implementing the application on his or her own. Instead of implementing on the provider side, the provider could also provide such an approach here for configuring the cloud application. Do you understand that? And do you agree with that?

#00:29:48-0#

R: Yes. Okay. Yeah, I got it, what you said, I think. #00:29:54-2#

I: What I would like now to do is with you, ask a question, first of all, as again based on the five values; strongly agree, agree, neutral, disagree, strongly disagree. I would like to ask you; I have understood the approach. #00:30:11-9#

R: Agree. #00:30:13-0#

I: Agree. I said you have always the possibility to ask questions if something's not clear. #00:30:18-6#

R: Okay. #00:30:18-7#

I: So, coming back to the risk assessment. Now, I would like to use that approach here. So, I would like to assume you that the providers of the case studies are implementing that approach here and (unclear) #00:30:34-0#

R: I don't know whether it's relevant or not. So, I have to assume this system as secure or possible of attacks, like - #00:30:44-9#

I: So, you can follow, you can assume following. You can assume that the blockchain is secure. So, you can assume that the blockchain itself, you can abstract from the blockchain. Based on the implementation, so meaning the cloud management script, you can make the general assumption as for example, on cryptographic functions. If you are in contact with other parties who are using cryptography, you also have to somehow rely on that they are correctly implemented the configuration of the encryption. But there might always be the risk that there's configuration error also in encryption functions. So, you understand this limitation? #00:31:29-6#

R: Okay. And so, I can assume that the blockchain is secure? #00:31:33-6#

I: Mhm. #00:31:34-3#

R: But the cryptography part, like the symmetric key could get leaks or something can happen? #00:31:40-0#

I: Also, not the symmetric key. Only that implementation of reading the configuration from the blockchain, implementing the right configuration in the cloud application, triggering a backup and performing a hash value of the backup. There might be the risk, of course, as always that there is a configuration error. That's implementation error. That it's not correctly implemented on the customer side. #00:32:10-7#

R: Okay. #00:32:11-6#

I: So, do you understand that? #00:32:14-4#

R: Yeah. Now I understood. The risk is in not correct implementation, but there is no secure key issues with the blockchain and the key. #00:32:30-2#

I: Exactly. Okay. So, it's - #00:32:32-8#

R: And one thing from the customer side to the provider, they will provide the configuration, right. So, it can be also be that they provided the wrong configuration, right? #00:32:44-5#

I: That the customer - Yeah, customer can also make a typo. #00:32:48-9#

R: Yeah, yeah. #00:32:50-0#

I: That's what you're asking, right? So, you can assume all these human errors, which might occur of course as a remaining risk, so to say. #00:33:06-9#

R: Yeah. Because then the dispute will occur. Otherwise, that dispute will not occur. #00:33:10-8#

I: Sorry? #00:33:11-9#

R: Then dispute will occur. Otherwise, dispute will not occur. #00:33:14-9#

I: Yeah. Okay. We will go through the risks or through the case studies. And again, I would now ask you again based on that approach. So, asset, the idea is not to abstract too much. The only thing we can abstract is really that the blockchain is secure. You can assume this is running on the theory in blockchain or whatever. So, this is the only thing. The rest is real life scenario, so to say. There might always be an implementation error. So, I do not want to abstract too much from real life. So, assume real life errors might also occur here, like in the other cases. #00:33:54-6#

R: Okay. #00:33:56-4#

I: It's really just the architecture at the end. Okay. So again, I would like to go through the risk with you. And again, asks you based on the - do you see the risks here? #00:34:10-0#

R: Yes, I can. #00:34:11-1#

I: And again, based on the three case studies, I would like to evaluate the risk using that architecture here. Let's go to task. So, the first ask is the risk that the cloud application provider implements a contractually not mutually agreed configuration using that approach. #00:34:34-6#

R: Say again? #00:34:36-4#

I: The risk that the cloud application provider implements a contractually not mutually agreed configuration based on the approach we have seen here. #00:34:48-1#

R: Okay. That will be - Last time it was medium, right? #00:34:57-0#

I: Last time it was high. #00:34:58-4#

R: High. Possible and critical, right? #00:35:02-6#

I: Yes. #00:35:03-9#

R: Yes, the same. #00:35:05-2#

I: For provider A, right? #00:35:08-9#

R: Yes. For provider A. #00:35:10-6#

I: For provider B? #00:35:11-6#

R: Yeah, same. #00:35:18-5#

I: So, it's also high? #00:35:21-1#

R: Yes. And again, for C. #00:35:24-3#

I: For C, we had last time, low. #00:35:27-2#

R: Contractually. Okay. That was marginal and rare, right? #00:35:34-7#

I: Marginal and rare. Yeah, exactly. #00:35:40-8#

R: For C. So, yeah, same. #00:35:44-6#

I: Okay. Coming to the risk that the implementation of compliance from configuration gets delayed. So, manual process delay. #00:35:54-7#

R: Last time it was medium, right. #00:35:57-2#

I: Last time the first one was low and then medium, medium. #00:36:01-4#

R: Yeah. I will go with the same. #00:36:04-2#

I: Same? #00:36:05-3#

R: Yeah. #00:36:06-3#

I: And the risk of denying the implementation of a configuration? #00:36:15-2#

R: It'll also be the same. Medium. It was medium, right? High or medium? #00:36:19-9#

I: Last time, it was high, high, high. #00:36:22-1#

R: High, yeah. #00:36:23-2#

I: Okay. So, everything the same? #00:36:25-0#

R: Yes. But I want to update for the first one. For the first risk for provider A would be high in both cases. #00:36:38-4#

I: That's what we had. #00:36:42-1#

R: Yeah. #00:36:43-3#

I: So, basically the proposed approach did not change anything, right? #00:36:48-4#

R: Yeah. #00:36:49-0#

I: Okay. Can you also describe why? #00:36:52-5#

R: Because again, the architecture. Because I was assuming the process, not the architecture when I was thinking about the risk. Like I was also assuming the turnover and like how much they're running and like where they're located. So, I was more focusing on from like company culture as compared to the architecture they are following. #00:37:27-6#

I: So, in summary, just to keep it here? #00:37:37-5#

R: Yeah. Because it's not like a comparison between one system to the other system. It is just a comparison of, of course I didn't know about what they're actually using. But still I know. But the risk are same because the metrics on which I like assume the risk are not based on the architecture, but on the company's culture and location and their turnover. #00:38:04-1#

I: Okay. So, now as you assume it on the processes or on the architecture itself, the processes. You don't see any differences in that architecture and the regular architecture they are using right now? #00:38:22-7#

R: Yeah. Because again as you said, there could be a human, like the possibility of the contextual changes could be there. And the last risk is that they deny something could be from their generic companies' policy that they don't want to add something. Or they want to delay. Like delaying also is not dependent on the architecture, you know, it's on the people. Like how was the process of the company to develop or release something? They might take a lot of time. It does not depend on the architecture. #00:39:00-0#

I: Okay. Maybe we can then also go through the third risk we had here, the denying and implementation. Maybe you can quickly describe why you think this approach here does not protect from denying an application of configuration. #00:39:17-3#

R: Can you repeat the risk again? #00:39:20-7#

I: Yeah. The risk of denying the implementation of configuration in the case of dispute. So, if for example - #00:39:27-4#

R: Yeah, sorry, sorry. So, yeah, in that case it'll be low, sorry. In all cases. #00:39:35-2#

I: Okay. So, it reduces the risk here? #00:39:39-7#

R: Yes. #00:39:40-1#

I: Okay. And the speed of the process did not change, right? #00:39:46-8#

R: Yes, the speed of the process did not change. #00:39:49-0#

I: And the risk that the cloud application provider implemented a contractually not mutually agreed configuration? #00:39:55-8#

R: Yes. Because that could be initially something is done and before the dispute, right? So, that could lead to some mistake. But they cannot deny it if they have done some mistake. #00:40:10-0#

I: Okay. All right. So basically, we have a change in the third risk of denying, right? #00:40:17-1#

R: Yeah. Because blockchain, yeah. #00:40:19-6#

I: Okay. All right. That was it here. Okay. (person) now that you know the content of the dissertation, do you think the use of the blockchain makes sense at this approach? #00:40:36-9#

R: Yes. #00:40:38-2#

I: Can you think of other use cases where the proposed architecture might be used? Or do you think, I ask the question differently, the proposed case studies are wholesome, so covering a broad area of use cases? #00:40:57-9#

R: The second question, whether it is covering every area or not, right. I think because the first question, the second delay is I think is, I don't know, like what's the purpose. Yeah, that also makes sense to add something which is not related to blockchain. Like delaying something, you know, has nothing to do with blockchain. So, I would say that discovering, yeah. Discovering. #00:41:37-3#

I: Do you think that this approach here also creates new risks? So, it's not only mitigating a risk, also creating new risks or do you - so #00:41:48-7#

R: Yeah, I can, this second take. Can you open the architecture if you can? #00:41:55-7#

I: Sure. Always. #00:41:57-5#

R: But isn't it subjective, like to say that whether it opens new risk or not? #00:42:11-2#

I: That's the idea in qualitative survey. #00:42:14-7#

R: Yes. I would say yes, because I would say then the risk would be then, further would be like the handling of blockchain itself would be a risk for the provider then. #00:42:33-5#

I: Okay. Which approach would you prefer as a customer? #00:42:38-3#

R: This one. #00:42:42-3#

I: Okay. All right (person), I think we are coming slowly to an end of the interview already. I would now like to come to a few aspects here, but give me just a second. If we talk about transparency, automation and notarization of configurations. #00:43:13-3#

R: The last one was? #00:43:14-9#

I: Notarization. Notarize. #00:43:17-0#

R: Okay. #00:43:18-3#

I: Do you think the presented approach has an impact on one of those three topics? #00:43:23-4#

R: Yes. #00:43:26-6#

I: Transparency, automation and notarization? #00:43:28-7#

R: Yes. Yeah, all. #00:43:30-7#

I: Okay. And do you think the percentage approach improve the transparency, the automatization and the notarization of cloud configurations? #00:43:40-0#

R: The second one is automatization, right? #00:43:43-2#

I: Automatization. Yeah. #00:43:44-6#

R: Yes. All. Yeah, of course. #00:43:51-7#

I: Okay. Do you think the presented approach can help to investigate security incidents more easily? #00:44:03-8#

R: But so here, I don't have to think about blockchain, but not, and the architecture, right? (unclear) #00:44:17-1#. Yeah, it can. Yeah. #00:44:20-8#

I: Okay. And we already discussed it but I asked the question for being wholesome. Do you think the percent approach can help to identify responsible parties in a legally secure way? #00:44:38-0#

R: Yes. #00:44:38-7#

I: Okay. That's also - we already talked about the advantages, disadvantages, potential for improvements. Would you like to add anything? #00:44:51-8#

R: To the cases or? #00:44:57-0#

I: To the cases, to the questions, to anything. Would you like to add anything? Would you like to change something? Would you add some risks? Would you criticize it? You can do now whatever you want on that approach. #00:45:08-8#

R: No, I like that approach. And maybe you can make - but yeah, you already said that is the nature of interview. That there are some things which are not to affect. So, I, like I agree with the approach. Yeah. #00:45:32-3#

I: Okay. #00:45:32-9#

R: Right now, nothing in my mind to change. #00:45:36-1#

I: That's good. (laughter) Now you have heard everything here. You have all seen all the questions. You've joined me in this dissertation topic. Now you know everything I wanted to ask you. In school grades, how would you rate your experience in the area presented, from one to six, where one is a very good and six is very bad? #00:45:58-9#

R: How it is presented? #00:46:00-7#

I: How you would rate your experience in the presented topic? #00:46:05-7#

R: One to six. So, I have to what, have to grade my experience? #00:46:12.3#

I: Yeah. Your experience. Now you have heard everything. You have seen everything. And if someone comes to you, how would you rate yourself as an - #00:46:21-2#

R: (laughs) Five. Yeah. Assuming not six. #00:46:27-5#

I: So, based on school grades, how would you say? #00:46:35-3#

R: Oh, okay. Sorry. I'm not on the German. You are on the German. #00:46:44-1#

I: I'm on the German system. Yes. #00:46:45-4#

R: Sorry (laughs). I'm on my school system. I'm sorry. The five, six is the highest. Sorry. #00:46:51-1#

I: Okay. (laughter) So, (unclear) #00:46:55-4#. So, we agree both on two, right? #00:47:02-5#

R: Yes. #00:47:02-9#

I: Just for the transcript. Okay, thanks for the openness, participation and time set. The thing will now be transcripted and evaluated. And having that said, I would stop the recording now. #00:47:19-5#

R: Yeah. Thank you. #00:47:20-9#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #3:

I: All right, so let's start. So first and foremost, thanks for participating. Before we start the interview, as already explained, I would like to start with the warm up, and introduction phase. And during that phase, I would like to get you know better. So the first question I have here is, could you please provide me some background information from you? So can you briefly tell me something about your professional background, and your daily tasks? Really short version of it. #00:00:52-09#

R: Yes, for sure. I'm working for now more than one and a half years as a DevOps Engineer. Back then I studied Mechanical Engineering, but already had a focus on Software Engineering. And then I switched my profession to DevOps engineer, and I'm mostly responsible for, in my daily task, for Server Cloud Administration. Providing our software to our customers, and monitor that our software is working in the way it should work. #00:01:29-11#

I: And regarding your professional background, and also your study background, how long have you studied? And which degrees do you have, and how long are you working? #00:01:40-21#

R: I studied, Mechanical Engineering started in 2012. And my Bachelor's degree in 2016, and my Master's degree in 2018. And since summer of 2019, I'm working, but as a DevOps engineer, since September 2020. #00:02:04-37#

I: Okay, thanks a lot. So that was the qualitative part. Now some quantitative questions. And for that case, I will present you with a statement, and I'll ask you to say either, "strongly agree, I agree to that statement, neutral, disagree to the statement, or strongly disagree to that statement." So the statement, the first statement I have here prepared is, I am a computer science expert. #00:02:29-63#

R: I agree. #00:02:32-98#

I: I'm an Information Security Expert. #00:02:36-36#

R: Neutral. #00:02:39-26#

I: I'm a Cloud Computing Expert. #00:02:42-40#

R: I agree. #00:02:44-14#

I: And I'm a Cryptography Expert. #00:02:48-06#

R: I disagree. #00:02:51-58#

I: Okay. Alright, that's already the warmup part. So I think we have now a good overview about your background, and your knowledge. So the next thing I would like to do is, step into the main phase. And for that, I would like to send you a case study, or to be more precise, three case studies, and would ask you to read them briefly. Give me a second. I send them to you. So take your time for reading them. They are a bit longer. So it's a (noble? #00:03:24-48#) race. Let me just see. Just to have some issues in sending documents. One second. Okay, it's not sending. I will send it via email, okay. #00:03:50-76#

R: Sure. #00:03:51-74#

I: It's a PDF document. Think you have received it. #00:04:23-06#

R: I will synchronise. Yip. Okay, I will read it. #00:04:27-06#

I: Yeah. Take your time. They are a bit longer. #00:04:35-88#

R: Okay. #00:07:43-06#

I: Okay, good. So first question here. Do you understand the case studies? #00:07:47-57#

R: Yes. #00:07:49-62#

I: Second question. Do you think those case studies are realistic? #00:07:53-28#

R: Yes. I think they are realistic. #00:07:57-32#

I: Good. Now I would like to talk with you about the risk of cloud adaption. So adapting a cloud application. So first of all, and here the question is, what can you tell me about risk management? Do you have any knowledge about risk management? #00:08:14-06#

R: I would say my knowledge is basic. So to identify risk, to adapt strategies, to potential risk, and also procedures for risk management. I know, but I'm not that kind of expert. #00:08:33-19#

I: That's okay. I would like to show you following metrics. Give me a second. It's called the Risk Metrics. Let me just know if you see it. So you see it? #00:08:46-28#

R: Yes. #00:08:47-80#

I: I will also send you that metrics soon, after that I explained it to you. So the basic idea of the Risk Metrics is that we have on the one hand side, the probability that a risk occurs, and on the other hand side, the impact it might create on the company if the risk occurs. On the left-hand side, there are the percentage values of how likely it is that a certain risk appears. So red for example means that the probability is below 10%. And on the impact side, we have the amount of money the company will lose due to that risk. You see here that these are relative values. So as bigger a company as bigger also the absolute values of impact, which the company loss. And this is calculated based on the turn-over per year of the company. So small companies, of course, for them it's more difficult to lose already a small amount of money, and for bigger companies, it's not that huge issue to loss a bit money. I think that's clear to understand, right. And based on probability and impact, you can then determine the risk. Okay. So the question here is, do you understand the risk management metrics? #00:10:06-90#

R: Yes, but to be honest, I've seen it also beforehand, so I know it. #00:10:13-55#

I: That's good. And do you think the risk management metrics makes sense for estimating risks? #00:10:22-13#

R: I think in general it makes sense. But, for example the impact, when we see for this critical impact, between 30% and 80% of the turnover, it's a very high amount. So I think it could be more specific in some cases. #00:10:45-88#

I: Let's stick with that numbers here. I'd keep that in mind. I noted it down, but in general, I think you're fine with that metrics if you continue, or are there any concerns on your side? Okay. #00:10:59-13#

R: No. #00:10:59-66#

I: Now I would like to present you three risks. I will send you first the metrics. Give me a second, that you also have it on your side. Yeah, I think it makes sense to send it. All right, should receive it. So you can open it because now, and I think this is only consequence, I would like to provide you with three cloud adaption risks. First, I would like ask you whether you think those risks are realistic. And second, I would like to ask you to rate the risk I present you. Okay? #00:11:58-13#

R: Yeah. #00:11:59-09#

I: And I would like to ask you to do it for case A, B and C. So we start with case A. I will present you three risks, and would ask you to rate those risks based on case A. Then we go to case C, and then the same risk for case B. And then we go to case C, and the same risks for Case C. So this is how we will start now. And the first question, and all the questions are related to cloud adaption, is the risk that the cloud application provider, so provider A in that case, implements a contractually, not mutually agreed configuration. A configuration in that case might be for example, a backup location, a firewall configuration, or anything you could configure based on the customer wish. So first question, is that realistic, that risk for you? #00:12:57-13#

R: In case A, as the provider is certified, I would say the risk is unlikely, or more rare. #00:13:12-97#

I: Yeah. And the impact so that we can... #00:13:17-40#

R: The impact, if it happens is, while maybe even catastrophic, or critical. So I would say probability unlikely, and impact critical. So the risk itself is medium. #00:13:41-63#

I: Okay. Now I would like to present you a second risk. The risk that the implementation of compliance (ribbon?

#00:13:50-13#) configurations gets delayed due to slow, or manual processes. So you have a configuration change on customer side. You tell it to the company, the provider, and now it gets delayed due to manual, or due to a slow processes. #00:14:07-33#

R: Sorry. I would say this risk is possible, and the impact would be marginal. So the risk itself is medium as well. #00:14:27-13#

I: And last but not least, the risk of denying the implementation of a configuration in a case of a dispute. So if there is a data leak, for example, and one party does not say he, or she implemented a configuration as agreed on, so denying the configuration. So it's clear what I mean with that? #00:14:54-14#

R: Yeah. I think for me, it's clear. I would say the probability is unlikely, and impact is critical, again. #00:15:10-78#

I: So it's a medium risk here, right? #00:15:13-49#

R: Yes. #00:15:13-55#

I: Okay. So that's it already for the first part. So let's step to the second case study, and do the same again. I will, if you want, read the risks again. #00:15:23-99#

R: Yes please. #00:15:25-55#

I: So we are now at the company B the [Organisation]. And here, the question is, the risk is that the cloud application provider implements a contractually not mutually agreed configuration. #00:15:42-73#

R: I would say the risk is possible, and the impact is potentially critical, or more marginal. #00:16:00-04#

I: So we are medium, right? #00:16:01-40#

R: Yes. #00:16:03-32#

I: So the second thing. The risk that the implementation of compliance driven configuration gets delayed due to slow, or manual processes. #00:16:12-96#

R: Probability likely, but impact, how do you say it? #00:16:22-30#

I: Negligible. #00:16:23-96#

R: Yeah. So risk medium. #00:16:26-98#

I: Negligible. Medium. And the risk of denying the implementation of a configuration in a case of a dispute? #00:16:36-63#

R: Here I would say probability also likely, and impact marginal. #00:16:45-19#

I: So it's a high risk here, right? #00:16:47-17#

R: Yeah. #00:16:48-15#

I: All right. And now coming to the case C. So companies C, and here again, the three risk questions. The risk that the cloud application provider implements a contractually, not mutually agreed configuration. #00:17:06-29#

R: I would say possible, and the impact would be negligible. #00:17:18-54#

I: So it's a low risk, right? #00:17:21-15#

R: Yes. #00:17:21-97#

I: So the second risk. The risk that the implementation of compliance driven configuration get delayed due to slow, or manual processes. #00:17:31-83#

R: I would say probability is rare, and then the impact is negligible. So low risk. #00:17:43-03#

I: Okay. Last but not least, the risk of denying the implementation of configuration in a case of dispute. #00:17:48-91#

R: I would say unlikely, and also negligible, so low. #00:17:57-58#

I: Okay. Low. All right. So, we are half-through. So as said, this is now a comparison of two approaches. We have the classical cloud configuration approach, we just had right now. And now I would like to present you the approach I developed during my PhD thesis. And would ask you to ask questions if you do not understand that approach, or if any questions. Let me just share the approach. I have it here as a PowerPoint presentation. Give me a second. So I hope you will see it now. #00:18:38-29#

R: Yip. #00:18:40-70#

I: That's good? So let me quickly start with pointing out the crucial elements here. So on the one hand side, we have the application consumer. This might either be the client of the company, or that might also be the application provider. So someone who wants to configure the cloud application, it's that person here. Clear so far? #00:19:11-19#

R: Yip. #00:19:12-39#

I: We have the cloud environment here. So you can think of any cloud environment you would like to, for example, [Organisation], or whatever you can think of. And on that cloud environment, we have two components. We have on the one hand, and this is just a demo case here, a blockchain. And this is the only assumption you can do during the whole interview that the blockchain is secure. So we are using a secure blockchain, you did not need to think about 50+ attacks, or whatever. So you can assume that the blockchain will be secure. And this is the only assumption I asked you to do. And we have on the other hand side, a virtual machine running. On that virtual machine, we have two servers running, or one web server running, and one intrusion detection system running. An intrusion detection system that monitor's traffic, and triggers an alarm as soon as it sees unusual traffic. Now, the idea of the whole architecture is as follows. First and foremost, there is a symmetric key. You know what a symmetric key is? #00:20:17-89#

R: Yip. #00:20:19-39#

I: So there is a symmetric key shared between the cloud application consumer, so the company in our cases. The provider has that key, and that key is placed on the cloud application itself, so at the virtual machine. The symmetric key itself is created using the Diffie-Hellman protocol. So you can also think here that this protocol is implemented correctly and safe. So this is again, something you can assume, that this key is created safe and secure. Now, the idea is to configure this intrusion detection system via the blockchain. And let me explain you how that works. So in the first phase, the person who wants to configure the cloud application, writes down a configuration, as used in a configuration file, you can think of a JSON, a text document, or whatever, and encrypts that text file using the symmetric key, she or he has access to. In the next step, he or she writes that encrypted configuration to the blockchain via smart contract. So now on this blockchain, there is an encrypted configuration start. In the next step, the cloud management script, a script running on the cloud application detects the change of blockchain, that a new configuration was stored on the blockchain. Then it pulls that configuration from the blockchain, and decrypts it because it has access to the same symmetric key as the consumer here. Let me just switch here. Now, the decrypted configuration is available on the cloud application. I think you can follow, right? I step always in to ask whether you can follow. #00:22:24-01#

R: Yip. #00:22:25-07#

I: Okay. So now the decrypted configuration is available on the cloud application. In the next, the management script implements that configuration on the to configure application, so in our case, the intrusion detection system. It knows where to write that configuration file, and just writes it through. Additionally, it monitors also the lock file of the intrusion detection system, and monitors whether the implementation was successful, or not. If the implementation was successful, it triggers a backup of the virtual machine via the cloud management. So as soon as it detects, okay, it was successful, it triggers a backup of the whole virtual machine here. You can still follow that idea, right? #00:23:22-89#

R: Yes, yes. All good. #00:23:24-85#

I: Okay. So this is how it looks like. This backup is then pulled into the virtual machine, and hashed. So the hash value of the virtual machine backup is created. The virtual machine backup itself is then again deleted from the virtual machine, and the hash value, which was created, is written back to the blockchain. And this is also then seen as the proof that the configuration was successfully implemented on the cloud application side. Meaning the cloud consumer has now the possibility to contact the blockchain, and get the latest hash value from the blockchain. The idea is now, in a case of a dispute, someone can say, "Okay, this is the hash value from the last successful configuration. Please show me the backup of that configuration. And we will investigate whether the actual configuration was implemented or not." So this is the overall idea of that architecture. Here again all the steps. The question I have here is, have you understood this approach, and based on the Likert Scale, and also on qualitative value. The first question is, have you understood it? #00:24:41-64#

R: Yes. #00:24:43-49#

I: And on the Likert Scale, strongly agree, agree, neutral, disagree, strongly disagree? #00:24:47-89#

R: Agree, as I'm not an expert of blockchain. #00:24:55-50#.

I: But that's fine. Okay. Now, assuming we are now implementing that approach for adapting to cloud application from the use cases we have seen before. So now we assume that approach here is provided by the cloud application providers from the use cases I should you. And now surprisingly, we are doing again the risk assessment, okay. Based on having that approach in mind. I will again share my risks with you. And please let me know if you need anything shared, or known. There's... #00:25:41-81#

R: All good. #00:25:42-53#

I: There's no issue just yet. Okay. So we are starting again with company A. And I again, ask you to assume we have implemented the percentage approach. And now I would like to ask you to evaluate the risk that the cloud application provider implements a contractually, not mutually agreed configuration. #00:26:05-69#

R: The probability is, in this case, I would say rare, and the impact is critical, maybe. So I would say medium.

I: Then we are continue with the second risk. The risk that the implementation of the compliance driven configuration gets delayed due to slow, or manual processes. #00:26:49-02#

R: The probability in this case, I would say is unlikely, and impact negligible. #00:27:03-64#

I: So it's low, correct? #00:27:05-53#

R: Yes. #00:27:06-51#

I: I just repeat the values that I have it also on the transcript. #00:27:09-63#

R: Yeah, all good. #00:27:11-45#

I: Okay. The risk of denying the implementation of a configuration in case of a dispute? #00:27:17-03#

R: Probability rare, impact negligible, so risk low. #00:27:26-64#

I: Going to the second case. So the [Organisation], so company B, and again ask you to evaluate the risk that the cloud application provider implements a contractually, not mutually agreed configuration. #00:27:42-64#

R: The risk is unlikely, and the impact is marginal. So medium risk. #00:28:00-77#

I: Medium risk. And the risk that implementation of compliance driven configuration gets delayed due to slow, or manual processes. #00:28:10-18#

R: Probability possible, and impact negligible, so risk low. #00:28:20-40#

I: So we have here low risk. And the risk of denying the implementation of configuration in case of a dispute? #00:28:27-43#

R: Probability unlikely, impact negligible, so low risk. #00:28:37-64#

I: And now we are doing it surprisingly also for the third one. So you need the risks or? #00:28:46-04#

R: Nope. #00:28:48-43#

I: Okay. So first risk I would say is probability unlikely, impact negligible. So low risk. The second risk, was the manual delay, right? #00:29:06-90#

I: Exactly. #00:29:08-13#

R: Probability rare, impact negligible, so low risk. And the third one, I would also say probability rare, and impact marginal, low risk. #00:29:23-59#

I: Alright. Okay. That's it already for the risk assessment. Now that you know the content of the dissertation, and all we talked about, do you think the use of the blockchain makes sense at this approach? #00:29:43-47#

R: I think in general, it makes sense if you have case studies as you provided. When you have software provider, and you can use this as a monitoring of if requirements are fulfilled. I think then it's a quite good approach if you are providing software in your own company. So developing it on your own, it maybe is a bit over load, but in general, it's a quite good approach. #00:30:26-43#

I: All right. Now we are slowly coming to the end of the interview. I would now like to come to the aspect of transparency, automation, and notarisation. And here again, no qualitative answers. So you can express yourself as you want, and recall the approach presented. So the approach I presented you from the dissertation. And think about the issue of transparency, automatisation, and notarisation of cloud applications, and their configurations. Does the presented approach have an impact on one of those three aspects, or topic? #00:31:08-44#

R: For sure. I think, automation, as you have seen in the approach, you have the symmetric key, and then the blockchain is automatically talking, or connecting to the second virtual machine. The backup is done automatically, the hash value. So it's definitely has a big impact on automation. And I would say this is a quite good approach, and the automation was very good. What was the second notification? #00:31:50-79#

I: Transparency. #00:31:51-31#

R: The transparency itself is also affected, but I think in case of that you have the changes in the configuration done via the symmetric key. Then it depends on if it's somehow locked, which user changed it. And for example, you said there's an application manager user. This could be also a technical user, then it's hard to track down from who the changes come, if it is falsely done. But in general, as we have then the backup, and if the backup on the VM equals the configuration, the hash values written down to the blockchain, the transparency itself is given of all changes. And the third one was? #00:32:58-15#

I: The third one was not a recession. So the traceability, or the non-repudiation so to say. That someone is not able to say, "I did not do it." That's repudiation means to say, "I didn't do it." And non-repudiation is a computer science, or security principle of not being able to say. "It was not me." That's what it's described as, non-repudiation. #00:33:20-99#

R: Okay. Yeah. That's the same what I did, told you about, the answer before. So if we have maybe one only technical user, which can be accessed by multiple people, then it's possible. But in general, I would say as we can see the changes in the blockchain, the hash value, the changes in the configuration are traceable. #00:33:54-83#

I: Do you think that deeper centered approach can help to investigate security incidents more easily? #00:34:02-65#

R: Yes. I think as in the approach is shown that it's only possible via the symmetric key. And if we then have changes in the configuration, which are not done by the application manager via the blockchain, we definitely can see it directly in the VM itself, so that changes are made potentially, and not written back to the blockchain. So we can directly track down changes in the text to verify in the blockchain. #00:34:47-77#

I: Thanks a lot. And last question here, do you think the percentage approach can help to identify responsible parties in a legally secure way? #00:34:57-59#

R: Good question. I would say yes, as we have the direct traceability from when changes are made. So I think then it is possible to track down which changes are made, and when. And if the changes fulfil the requirements, so then it is possible to track down this to further requirement's when company /. For example, in this use case studies, when company A contacts the provider A, and say, "We want to have this requirements fulfilled." They implement it, and the implementation changes are not the way the requirements are defined. Then you can track down that the requirement are not fulfilled due to the changes written into the blockchain. So I would say definitely it's possible. #00:36:10-47#

I: Okay. So that's the final question though. So the final question is not a question directly, but it's giving you the word. So asking you, would you like to add something here? Would you like to add any advantage, any disadvantage? Would you maybe also emphasise a new upcoming risk? Would you something improve? Do you see any weaknesses? Do you want to add something in conclusion? #00:36:35-91#

R: Nope. I think it's a quite nice approach. In general it will be then interesting to see it in production mode. This is right now research, and then to see this implemented into production mode, and see the advantages of it. And maybe then also, to track down disadvantages. For example, if we talk about costs, having a second VM, having automation tools running to do this. Maybe then as I already mentioned, you need to verify costs against the advantages, and if you can track down with a lower approach the same then it needs to be verified again. But in general, very interesting topic. #00:37:37-24#

I: And now the final question, now that you have heard everything here, and join me on the dissertation topic. In school grades, so one is very good, six is insufficient. So you know the German school system, or the European school system. How would you rate your experience in that area I presented you? And how would you rate your statements you made today? #00:38:04-52#

R: It's not that easy. I would say school grade, two in topics of cloud applications, and cloud administration, and then into, for example, this encryption topic, blockchain, it's more between three and four. #00:37:37-24#

I: Okay, that's it. Thanks for your openness, participation, and time-set. The outlook is now the transcription of this interview. I will anonymise it, and I will use it for an evaluation. With that said thanks a lot. And I will stop recording. #00:38:51-87#

(End of Interview)

TRANSCRIPT INTERVIEW PARTICIPANT #4:

I: So, welcome to the interview. And as said, the information phase is finished. We started recording and we are soon entering the warm up and introduction phase. And there I prepared, as I said, qualitative and quantitative questions. So, first of all, to get a bit you better known and also to get your background. And the question is, can you briefly tell me something about your professional background and your daily tasks? #00:00:37-0#

R: Sure. Yeah. So, my background is - I studied computer science in (organization). And afterwards I worked several years as a software developer in a small company in (place). And now since six years, I'm the CTO of medium sized company or medium, I don't know. It depends on the definition. Around about 70 employees. And as CTO, I'm mainly responsible for the - We are a software development company and I'm mainly responsible for the overall technical tasks in our company. So, for software development mainly, but also for other things like IT/ITSEC and DevOps task, for example. #00:01:30-6#

I: And can you quickly also name the highest degree from university or from school you have? So, your highest education degree. #00:01:40-3#

R: I'm a "Diplom Informatiker", so that's my master. Then diploma and it's (unclear) #00:01:49-3#

I: Okay. All right. Thanks a lot for introducing yourself and providing us a bit background here. And as said, now I would also like to ask you some quantitative questions. So, I will provide you with a statement and I ask you to say strongly agree, agree, neutral, disagree, or strongly disagree. The first statement I have here is; I am a computer science expert. #00:02:10-3#

R: Yeah, that I would strongly agree. #00:02:14-4#

I: I am an information security expert. #00:02:17-7#

R: Yeah. I would agree. #00:02:20-6#

I: I'm a cloud computing expert. #00:02:22-9#

R: Agree. #00:02:25-7#

I: And I'm a cryptography expert. #00:02:28-9#

R: Also agree. #00:02:30-6#

I: All right. That's it already with the warm up. So, we have a (laughs) quite good background. And having the warm up and introduction phase finished, we will enter into the main phase. And for the main phase, I already provided you with three case studies; company A, B, and C to be more precise. And the first question I have here is, do you understand the case studies? #00:02:53-3#

R: I would say yes. #00:02:55-1#

I: Okay. And the second question here, do you think the cases are realistic? #00:02:59-6#

R: (laughs) That's a good question. But I would say overall yes. Why not? So, this definitely could be things which seems to be realistic. Yes. #00:03:11-3#

I: Okay. Then continuing here, I would now like, and this is also part of the aim of my dissertation, to talk about the risk in adopting cloud applications. So, it's now about risk of cloud adaptation. And before we start with risk and, or discussing the adoption risk, I have the question, whether you can tell me about something about risk management or even an idea about what risk management is about. #00:03:39-5#

R: Now in parts of cloud management or overall risk management? #00:03:44-7#

I: Overall risk management. #00:03:46-5#

R: I mean, risk management is an important thing. You have to do in a company. And so, in the end, you have to define what kind of risks are there for your company. And then you have to manage this and to think about measurements you do to minimize in the end the risks you have. Or to decide also, sometimes you also decide not to do anything because the risk is not high enough or something like this. So, that's in the demand. And what you have to do on management side. #00:04:20-9#

I: Okay. perfect. That's amazing. I would like now to present you a graphic here or a picture and ask you whether you have seen something similar like that? Or if you are aware of the concept of a risk metrics. #00:04:36-3#

R: Yeah. #00:04:37-4#

I: So, we have the probability here. And the probability, how probable. Probability it is that a risk occurs and we have the impact. So, in monetary value, so in money values. And what it means for the company if the risk arises. During that study or during that interview, we will use that risk metrics here. And as we have different case studies, this risk metrics is a bit of generic. Meaning we are talking here about that negligible is 10 percent of their yearly turnover and so on. So, we are having here relative values. But at the end, of course, we are talking about absolute values, depending on the use cases. Okay. I think you have understand it, is that correct? #00:05:21-3#

R: Yes, definitely. #00:05:22-5#

I: Okay. And now coming back to the cases we had and here is the question. Do you think it makes sense to do a risk management when adopting cloud applications, from a business perspective? #00:05:40-4#

R: Absolutely. It makes sense. Yes (laughs). #00:05:43-2#

I: So, you would also say that in the presented case studies, it would make sense to do the risk assessment, right? #00:05:50-9#

R: Definitely. Yeah. #00:05:53-4#

I: Good. And this is what we would like to do now. So, I would like to ask you now to do the risk assessment of the cases presented. However, I already prepared three risks for you, which I would like to present to you, and would like to ask you to rate on. And I will also share here my screen again. So, the risks are - let me just know if you see it. So, we have three risks and three cases. So, at the end we should have nine ratings.

So, for each, the case, we rate all of the three risks. The first risk is that the cloud application provider implements a contractually, not mutually agreed configuration. And a configuration, you can think of, for example the configuration of how often that backup will be made. Or in the case of intrusion detecting system, which case will be detected. So, that is something you can think of a configuration. #00:06:53-4# So, something which configures the cloud application.

The second risk is the risk that the implementation of the compliance driven configuration, so for example a backup configuration, gets delayed due to slow or manual processes. So, the company decides that there's some backup change in the frequency. And now they need to communicate it to the company. And that there's a risk of delaying that.

And the third risk is in the case of a dispute. So, if there's a fight or there's a data leak and they go to court. That one of the parties says he did not implement something which was implemented so that they deny an implementation. So, do you understand those three risks? #00:07:38-5#

R: Yep. #00:07:40-3#

I: Okay. Do you see them also as risks? #00:07:42-9#

R: Yes. (laughs) The risk is there. The question now is how high is the risk? #00:07:54-6#

I: Exactly. This is what I would like to do with you now (laughs). So, the risk assessment. You can either do the risk assessment if you say maybe the probability and the impact of all of the three risks. Or you can also name it directly the risk, and I will write it here, such that you see it also. So, for the first case, for company A. The risk that the cloud providers or provider A implement the configuration, which was not agreed on. #00:08:22-7#

R: How high is this risk. So, in case A we have a medium-sized company. And they won the provider A, was a bigger company, right? Yeah. 130 million turnover. Already ISO 2700 certified. No sales contact and headquarters in Europe. Wow. So, the first thought would be that this risk is not that high here. I mean, we have a little bit better company. So, a lot of turnover. They have a certification of ISO 2700, which 001, which is of course good. #00:09:22-5# Headquarters in Europe also seems to be a thing where I would say is trusty and sounds fine so far.

So that the cloud application provider implements a not a great configuration. I see, to be honest, the risk low that they do it. And also, I think that also the impact for our company A in the end is not that high, I would say. I mean, it depends of course, on what exactly (laughs) thing is done there. But you told in the beginning that something like for example backup is not right configured. Things like this. #00:10:19-7#

I: Firewall is not configured. So, compliance application. So, the company itself sets itself compliance requirements. For example, they do not want to open port 80 or whatever. And that one of these compliance requirements is not implemented on the provider side. #00:10:37-4#

R: Yeah. That's then of course, if this - I mean, first of all, I think it's rare the probability. And the impact I think could be now of course different things in there. If security things like port are not configured the way they should be, you can of course have then the risk that you have a text there. But yeah, I would (unclear) #00:11:12-6# let me shortly see what we are doing. People in developed artificial intelligence software. #00:11:19-0#

I: So, they want to adapt a bookkeeping system. So, I think configurations errors would be for example, that it is open to the public or whatever. #00:11:29-4#

R: Yeah. Could be of course. I mean, I don't think that it would be then an impact if we now see it like in this metrics that then directly 80 percent turnover would be always. I would say, I could be then of course the - if this is then in the public, this is of course not a good thing definitely. But I don't think that then, let's say after, the customers will go away. But yeah, let's then maybe say it's marginal. I would say from the impact we have. So, we are overall there, they're still in low from the metrics I would say. Yeah. #00:12:20-3#

I: Okay. Then we do it for the second risk. So, the risk that the compliance driven configuration gets delayed due to slow or manual processes. #00:12:30-5#

R: But this is, I mean, that's now in the company itself, the process is too small, not for the provider, but (unclear) #00:12:42-3#

I: So, for the provider. So, for example, the company A decides that they now need a new backup strategy because one country left, EU for example. And now they communicate that to the provider and the provider is in charge of changing it. #00:12:56-5#

R: For me, it sounds like, at least from what I see here in the texts, is that the provider, that you can configure things directly online. I mean, you don't have a direct sales contact, so it looks like that the things will be configured online. And so, I don't see that this then will take long time. So, usually as such provider, usually you have it that this is then directly done. So, I would see this definitely as a rare risk. And also, the impact is, I mean, it's then even - could be that you're then due to this have small time where something is not configured the right way. Of course, then you could. There could be an attack or something like this. But in the end, I think it's close to the first risk, I would say. I would still also say it's low. #00:14:12-4#

I: So, low, correct? #00:14:14-1#

R: Yeah. #00:14:14-8#

I: And the third risk. That one of the parties denies, in the case of a dispute denies the implementation of a configuration. #00:14:24-4#

R: Risk of denying the implementation of configuration in case of a dispute. That's a good question. I mean, in the end, I'm just thinking now what kind of thing it could be that a company is denying to implement in a configuration. Which makes issues for me or for this company then in the end. And so, I don't know. I don't see that many things which could be denied #00:15:24-7# due to a dispute.

So, (laughs) here I would also say low. One thing is what I now have to say, unfortunately, (laughs) because I know read again in the text. It is that there are data leakage due to a hacker attack, could lead to economic and for the company. That if I now read this, I have to say that I thought (laughs) you have to maybe then go for all the things from low to medium. Because then the impact is just higher than I thought. So, I would also here say that the probability is still rare. But then I would go for all the kind from all the things that it is more critical in impact. And then I would change it maybe to medium. #00:16:26-6#

I: Is it okay if I change it here? #00:16:28-3#

R: Yeah. #00:16:28-6#

I: Okay. So, I change it, okay. #00:16:30-8#

R: It makes then more sense to go to medium because then the impact is then definitely higher. But here, risk deny implementation. I would then even here say that this is - This I would still say is low because I mean, in the end then it is really like I want to do a configuration, but the company don't want it. Then I'm knowing that this issue is there and that's for the other two guys we had before is not the case. But here I can then also do other things. I could completely stop this here or pause, freeze it, go to another company. So, that I would then definitely put in low. #00:17:19-1#

I: Okay. So, just to make it clear, you can always adjust the answers you had. Also, if we are further with the interview, if you decide you want to change something, it's your interview so to say (laughs). #00:17:31-1#

R: Yeah, okay. #00:17:31-9#

I: Okay? #00:17:33.4#

R: That's good. Good to know. #00:17:35-0#

I: (laughs) So that was the first one. And going to provider B and we’re doing exactly the same now for provider B. Or for the case B sorry, not for provider B. #00:17:46-6#

R: Yeah. Company B and provider B as case B. So, let me shortly look over again to the company. And especially to the provider they have chosen. Based on company's bid policy of choosing lowest price of three offers, provider B was selected. 20,000 million turnover. So, that's now a little bit smaller provider than we had in the first certifications. And I mean, Google ratings. That's of course maybe not (laughs) the best thing you should choose for such a provider.

Provider base. That's exclusively by sales and consultant service. And headquarters is in India. Good. Let me also shortly show what we want to put here to the cloud. #00:18:59-3#

I: Intrusion detection system. #00:19:01-0#

R: Intrusion detection. Okay. I mean, I would now definitely put in the probability a little bit higher. As how it is written now in this case study, the overall trust in this company for me is then in the provider, not in the company. So, in the provider would be lower, to be honest, than it was in the first one. I mean, we have this - We don't have any certificates. I mean, let's not - The only thing which matters, but of course it helps if someone has an ISO 27001. Of course, it's also like choosing a company just by price and Google rating. Google ratings can be #00:20:01-0# completely wrong. You can even buy them. So, it's for me, not really a good measurement so that this is a trusted company.

You have, of course then sales and a consultant service where you can directly talk to. But yeah, I mean, that's a little bit harder. And then you also have like headquarters in India. Nothing is wrong with India. But of course from side of law and legal things, it's always for a company - Company B is the Europe one, right? Yeah. Always a little bit easier and better to have than also a company from Europe where you then can better go with the legal things and so on. #00:21:01-5#

So, the risk that the cloud application provider implements a contractually not mutually agreed configuration. As I said, I would go here definitely to higher probability. But I would still not go to something like the very big ones. I mean, it doesn't make that much sense also for this company to not implement. So, it's not like that I now directly say, okay, this provider seems to be some evil guy or something like this. But of course, I mean, the risk is a little bit higher here. So, I would go then maybe to the, not to rare, but then to, maybe to possible.

That could be then maybe the thing I would go here. #00:22:01-2# Because I mean maybe they just do not do it because they want it. But there is something not right implemented, whatever. So, we can go here maybe to possible. The question then is how hard would this be for this company? We are a global player. And intrusion detection (laughs). If this is not working, that would be of course not good. Because it's there to find something which is not working. But if the mechanism to find it is already not working, that's of course not that good.

The risk could maybe be marginal. I would say also, not say that it is. But yeah, the impact could be critical then. So, we are here then, we have something between medium and high (laughs) I would say. #00:23:05-2#

I: (unclear) #00:23:05-7#

R: I know I need something between (laughter). #00:23:08-6#

I: No, I need one of those. #00:23:15-8#

R: Yeah. So, if I then now compare it to the first scenario, then I would go now higher. So, I would go then too high. #00:23:28-1#

I: That's okay. #00:23:31-7#

R: Yeah, this risk that implementation - That's the thing. I mean, I don't know that much about this provider. But as I said, usually you do the configuration directly online and there is usually not that much delay time for things like this. But that's a little bit more maybe biased by my experience about this kind of providers definitely. So here, I mean, the impact for me here is more or less. Could then also be definitely critical, but it's a probability I see not that high. So there, I would stay then at medium, that's pretty like this. #00:24:28-1#

I: So, at which parts are here? #00:24:32-0#

R: Yeah, unlikely to critical, I would them somehow say. The risk of denying the implementation case of a dispute. Impact. I mean, again, the impact, if they're denying, you know it, you can then also change. But on the other hand, you cannot stop the intrusion detection. So, I mean, you can stop, but then you of course have direct risks. So, change here is then – Then the impact I would say is maybe more critical. So, I would then also go to medium overall as we would be then also like unlikely to critical. I would more so let's say. Or maybe even rare to critical, but those would result in medium. #00:25:40-0#

I: Last but not least. The third provider. #00:25:44-7#

R: Company C. #00:25:45-8#

I: Company C, the farmers. #00:25:47-7#

R: The farmers. So, and the provider, let me shortly recap the provider. They already, they took it because they have other license. And the service is free. Oh, nothing comes for free, but yeah (laughs). Have an annual turnover of a lot of money. And stock companies, global corporation, with headquarters in USA for the (unclear) #00:26:12-4# software exclusively online.

So, it's a consign service, can be booked against additional payment. Provider C certified according to all current worldwide certifications. That is fantastic. All worldwide certifications. Okay. Of course, what is then already interesting, why are they doing it for free? Whereas that's of course what you learn in the first directly thing, because makes it a little bit, yeah. #00:26:50-2#

I: The use case should mean that is included in the license. They already have that. #00:26:56-1#

R: Okay. #00:26:57-4#

I: It's misleading. #00:26:58-7#

R: So yeah, then that makes then more sense (laughs). Yeah, you're right, as they already have other license. Okay, good. I mean the provider seems to have all those certifications. That's definitely a good thing. It's a big company.

Headquarters in the United States. Of course, that's, again, Europe is always a little bit better for German or Europe company as the legal rights than a Europe based. Which is better for other companies than it is if it's in the United States. The customers, young people and what they're doing exactly. Now here, the website, right? #00:27:52-9#

I: Mhm. #00:27:53.7#

R: Number of goods thrown away. So, good about to expire (unclear) #00:27:56-9# online. And they want to sell the goods and want to have a system then, which is good to adjust and so on and so on. I mean, here, the risk is that cloud application provider plan, a contractor, not mature, agree to configuration. Definitely again, rare. And even if you do impact, what could then happen? What would be the worst? I mean, they are selling their goods there. What would be the impact you could do if you make an attack here because something is not configured the right way? #00:28:53-1#

Yeah. What could happen? I mean, you could somehow sell the things for less money. You could delay. But I don't see that there would be an impact which is that catastrophic in the end. I mean, if you're a farmer, you have some goods, selling it from time to time. If there is an attack, I don't see that there is now an - could be an impact, which is then more than marginal in the end. It's small farmers' company. I don't see that there is - I mean, you have then customers, young people, I don't know. And usually, I don't see that the impact for this would be very high or critical or whatever. So, I would put it more or less to marginal and rare. #00:29:53-1# Then we are in a low risk here.

And again here, why should it be a delayed slow manual process? I mean, it seems to be a provider which is completely automated in the selling process. Everything can be good. But I don't see that there is a risk. That's definitely rare. And again, the impact is also still marginal. So also low, I would say. The risk of denying the implementation of a configuration in case of a dispute. This is, I mean, okay, you have then a company in United States, so legal things could be worse than it would be in Europe. But still, the probability #00:30:53-3# has to come to this point.

And then yeah, I still see it rare. And definitely here also, the impact is not that high if they're not doing some stuff. I mean, you can also change then. I mean, that's what I say or stop for, I don't know. Yeah, of course. I mean, what would be then the worst? You have to do a change, go to someone else if you have the issues. And then the website would not be online for, let's say one, two weeks. But then you're still not on a big impact. You can lose then the money for some weeks. And also losing then some more customers as you have some trust. But I don't see it more than negligible (laughs). So, I would also go here for low. #00:31:48-6#

I: All right. Perfect. #00:31:51-0#

R: I don't know if it's perfect, but yeah. #00:31:53-6#

I: No, it's your interview. (laughs) I said there is no correct answer. That's why we are doing the interview, to get opinions on that. All right, so now I presented you more or less the general architecture we have in the cloud environment. And how it works more or less in the current situation. I would like now to present you my approach I developed during that PhD. And then we go again through the risks. And based on the newly proposed approach, we, again rate the risks. Okay? #00:32:29-6#

R: Nice. #00:32:30-7#

I: So, the first thing I will do is share a small presentation with you. And I will explain it very shortly and slowly so that you have the chance to follow it. And please ask questions if something is unclear on the process itself. So, first of all, you see the overall architecture here. And to say the core idea here is to bring it on the point then do the configuration via the blockchain. So, the core idea is that the cloud application provider, the consumer and the cloud application itself share is a common symmetric key. So, they can create it via the Diffie-Hellman protocol. They can create a shared symmetric key via the blockchain.

Each transaction during the process of creating the symmetric key is digitally signed, which protects from the man in the middle attack. So, you can assume that the man in the #00:33:30-3# middle attack is not possible here. Further thing you can assume here is that the blockchain is secure. So, you can abstract from having the 50 plus attack or whatever. It is really about the approach itself. It's not about whether the blockchain might be not secure. So, the idea, the overall idea is here now that the consumer, so the one who is using or wants to configure the cloud application, encrypts the configuration. You can think of a configuration as a JSON file, as a text file or whatever, depending on the cloud application, encrypts that configuration and stores it, encrypt it to the blockchain.

The cloud application itself, which is hosted in the cloud. Obviously, it's a cloud application, (laughs) has a backend script, so to say, which pulls the encrypted configuration from the blockchain. And encrypts the configuration and implements the configuration #00:34:30-9# based on the redefined application you would like to configure. In that case, it's an intrusion detection system managed by Snort.

So, the configuration is now read into the application you would like to configure, and it's implemented based on that script. The script furthermore, and I have also here some arrows. Sorry, I forgot to show you the arrows. Not a rose, arrows. We, we, we pulled the (laughs) - Yeah, we pulled it and we implemented it now. Now the script not only implements that cloud configuration, it also monitors the cloud application for success of failure. So, it has an access to the log files of the application. And watches whether the application was implemented successful or not.

Assuming the case it is implemented successful. So, we can see in the log file that a configuration was implemented successfully, then the cloud management script #00:35:30-4# does the following; it triggers a backup from the cloud application. So, from the VM here. It triggers that on the cloud application provider. So, you can think of, for example, Microsoft Azure, Google Cloud or whatever. And on that they trigger a virtual machine backup. Then a hash value of that backup is created. And start back to the blockchain as a configuration confirmation.

And now the person who set the configuration is also able to pull out that hash value. And in case, for example, a dispute, they can say, “Okay, this is the hash value of the configuration which was implemented. Please show me the backup of that file.” And then they can recreate that backup. That's the idea of the overall architecture here. Have you understood it? #00:36:24-2#

R: Yeah. #00:36:24-8#

I: Any questions? #00:36:26-5#

R: So far, not. #00:36:29-6#

I: Okay. Then let me just see, have you understood the approach? And have you understood the approach on quantitative values or strongly agree, agree, neutral, disagree, strongly disagree? #00:36:40-7#

R: I would then go with agree, I would say, yeah. #00:36:47-2#

I: Okay. All right. So now we are assuming we've implemented that approach for configuring cloud applications. I would now again ask you to rate the risks based on the three cases we had. So, how would you like to see it? (laughs) Should I keep it here or as you would like to have it, I can present it to you. #00:37:13-5#

R: Maybe, yeah, as we had before. So that, I mean, where we already put in the risks we had. This view. Oh, that's fine. So, one question now. I mean, now say the providers are still the same? #00:37:34-5#

I: The providers are still the same. And there might be the risk that the providers also did not really correctly implement that approach. (laughter) So, for example - Yeah, no. You should not assume that this is 100 percent correct. So, that risk always remains. So, you can really assume it as a real-life scenario. For example, it's also not always ensured that the cryptographic algorithm is correctly implemented. So, that should be the area where you do the risk assessment. #00:38:05-0#

R: Yeah, because now I have to see what changed. So, in the end, in the risk end. I mean, we have the risk that the cloud application provider implements a contractually not mutually agreed configuration. The risk then, the probability could be lower maybe. Because, I mean, in the end you can better check (laughs) what is in. But as you said, still, it could be that you check it, but it's not really implemented like this. But it seems to at least gives a little bit more trust here regarding to this probability. The impact I think is not really changing, right.

I mean, in the end, if the bad thing #00:39:05-3# happens, then the impact is still there. I mean, yeah, you can then go and say, "That's a good thing. I'm not the guilty guy." And could try to get something back from the provider or whatever with your hash value system where you can directly say, "Okay, but this was what we agreed. And I can prove that this was what I put in." But in the end, if something happens, it happens. And I mean, we had there this sentence, the data leakage due to hacker attack could to economic and for the company. So, the risk impact, I would say is the, especially then for the first one, the same. Maybe the probability can go a little bit lower.

So, we had, #00:40:05-3# I think, before something like critical impact, but still where the impact is still critical. So, I think I can here not go lower overall to medium, which would stay. Maybe then we can in the second one definitely go - No, I mean sorry, for the second - #00:40:33-0#

I: Provider B? #00:40:33-6#

R: Provider B, yes. Because there we were before at possible critical. And I would then say, okay then this possible maybe goes a little bit lower. We are on unlikely. So, we would go here maybe then for medium. And for the other one, we would stay for a low. Because lower than low (laughs), it's not possible in this colour. #00:40:56-5#

I: It's true. All right. So then those are the risks. Going to the manual processes. #00:41:05-0#

R: Yeah. The risk that the implementation led you to a slow manual process. I mean, this process, what you now presented, seems to be completely automated. So, there is not - I mean, it doesn't look - If this is shown from the company that this is their approach they're doing, this would not fit to a manual configuration afterwards. So, I would go here definitely from the probability again, it's definitely rare for all these guys. And therefore, I would then - nevertheless, as the impact here for the first one still is critical, still medium. The second one, I would then go to low and low. Medium and low.

I: And we have here low. #00:42:01-3#

R: Mhm. #00:42:02-5#

I: All right. And - #00:42:04-5#

R: Yep. Sorry. #00:42:06-1#

I: The third one please. #00:42:07-9#

R: Denying the implementation. It looks like that, I mean, from the approach you showed, it's like that there is the configuration. It's done. And as you said, you can even afterwards also say, if there is a dispute, you can completely see what was happening and so on. So, I mean, here we can then - But I already here also on low, medium, low in this.

I would then discuss denying. Maybe we can then go to low, low, low to make it also a little bit - But I mean, I cannot go - The risk is definitely not increasing. That's the first. Maybe also the first one thing I can say beside. I mean, definitely the risk on all of these three risks, the probability is definitely not increasing. #00:43:07-0# It's decreasing. The question is, if this is also now due to the risk metrics doing then an impact. I mean, I'm here now already on low. As I said, lower than low is not possible. So, the only question still is then for company B. Well, before on medium. The impact would be hopefully then a little bit less critical. Let's go to low, low, low (laughs). #00:43:41-8#

I: It's a statement, yes? #00:43:43-7#

R: Yes. That's a statement. #00:43:44-8#

I: Okay (laughs). So, low, low and low. All right. Thanks a lot. #00:44:02.0#

R: You're welcome. #00:44:02-7#

I: So, we have finished the risk assessment and we are coming slowly to an end now. But there are still some questions we quickly need to go through. But I do not need to share my screen anymore because the questions are open. So, the question I have here is, do you think that the use of the blockchain makes sense at the presented approach? #00:44:23-8#

R: Yes. I mean, I already - I have to go by (unclear) #00:44:30-3# scale, right? #00:44:31-9#

I: Oh, no. It's just an open question. #00:44:33-4#

R: It’s open question. Okay. Then it's a yes. As I also already mentioned, I mean, it is definitely not increasing the risk. So, the probability will decrease because we have a full automation. We can be sure that something, and we can also afterwards prove that a configuration was done by our site. So, it's not that the provider then can say, “It was not like this.” So, you have a nice history, which is provable of which configuration you had. So, it definitely makes sense. Yeah. #00:45:14-8#

I: So, you already answered a lot of my further questions. So, we talked about the optimization. You talked about notarizations of proving. One thing, it's open, its transparency. Do you think that has an influence on the transparency? #00:45:27-2#

R: Yes (laughs). I would say yes. Because yeah, as I said, I mean, you have - The thing is due to the reason that you afterwards have approved as a company that the provider, that you did the configuration it would, I think, then also lead - It’s more transparent from my point of view. Because then - Otherwise you, as I said, you can then - The other, the provider can then go and, “Yeah, it is not like this and it is - ” They have this commitment now to do it and this leads, from my point of view, also to more transparency. #00:46:14-9#

I: Okay. Then final question. And this is the question where the word is on your side. Do you want to add something? Do you want to add some advantages/disadvantages? Do you want to raise some new risks? Do you want to improve something? Do you want to name some weaknesses? So, the last word is on your side. #00:46:32-6#

R: Add anything here? To think about from my point of view, I do not have not that much what I could here, to be honest (laughs). I mean, looks as a promising approach definitely. Now the short track, I don't have now anything really to add. #00:47:05-6#

I: Okay. And now the really last question. Now we have heard everything. You have seen everything. You have seen the topic of the dissertation. In school grades, in German school grades where one is very good and six is insufficient, how would you rate your overall experience in that area? And how would you rate your statements you made today? #00:47:24-7#

R: What do you mean exactly by this question? #00:47:31-0#

I: So, how sure you are with your statements you made. Are you sure confident with what you said or you are not that confident with that? #00:47:39-7#

R: Okay. And confident would be then very sure would be a one? #00:47:43-9#

I: Yeah. #00:47:44-4#

R: One to six you said? #00:47:45-5#

I: Exactly. #00:47:46-1#

R: I would go with a two then. #00:47:51-3#

I: Okay. So, we are at the end. Thank you very much for the openness, for your time. And as said, the next step will be the transcription, the anonymization, and the use for the evaluation. And having that said, I will stop the recording. #00:48:08-9#

R: Okay. Thank you. #00:48:10-4#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #5:

I: All right. Let’s start the interview. Okay. So, as said, this interview is divided up into several blocks. We are now in the warm up and introduction phase. And during that phase, the aim is to get you know, a bit better. So, what I would like to ask you is if you could briefly tell me something about your professional background, and your daily tasks, such that we have a background from your knowledge and your doings. #00:00:43-3#

R: Okay. So, my name is (Person). I studied computer science at the (unclear) #00:00:51-4# I finished my bachelor and my master (unclear) #00:01:02-4#

I: Degree? #00:01:03-4#

R: Degree, yes. So, currently, I’m having a master of science there. Currently, I’m working at the (Organisation) and I am responsible on my - my work is called Software Architecture DevOps. And so, I am basically responsible for my institute, everything regardings the architecture and the infrastructure of the institute, and also regarding yeah, that everything runs a little bit smoother regarding the computer science stuff, and also helping the colleagues in some projects. So, also, some scientific stuff. And yeah, and I’m also responsible for our own cluster at our institute. #00:02:07-2#

I: Mhm. And since when you are enrolled? #00:02:09-7#

R: February ‘21. #00:02:14-8#

I: So, more than a year? One and a half year probably? #00:02:18-6#

R: Yeah. #00:02:19-0#

I: - round work, okay. Mhm. All right. I think that gives us a good background and good overview about your knowledge. Now, I would also present you some quantitative questions. So, I will ask you or give you a statement. #00:02:34-5#

R: Mhm. #00:02:35-4#

I: And I would ask you to give an answer to that statement based on strongly agree, agree, neutral, disagree and strongly disagree to that statement. #00:02:47-7#

R: Okay. #00:02:48-8#

I: So, this is a Five-point Likert Scale called. #00:02:52-2#

R: Mhm. #00:02:52-6#

I: And you have to just pick one of the five values based on how you would rate that statement I give you. Okay? #00:02:59-9#

R: And common values in-between are not allowed? #00:03:03-6#

I: That’s correct. #00:03:05-4#

R: Okay. #00:03:06-2#

I: So, I will give you now the statement. I am a computer science expert. And now I ask that this is the statement, and now I would like you to rate that statement, do you strongly agree to that statement? Do you agree to that statement? Do you-, are you neutral to that statement? Are you disagree to that statement or are you strongly disagree to that statement? #00:03:27-6#

R: That depends. (laughs) Agree. #00:03:43-0#

I: Mhm, perfect. I am an information security expert. #00:03:48-3#

R: Agree. #00:03:53-0#

I: Mhm. I’m a cloud computing expert. #00:03:56-5#

R: Agree. #00:04:00-3#

I: Mhm. And I'm a (cryptocurrency?) #00:04:02-7# expert. #00:04:03-4#

R: Neutral. #00:04:15-4#

I: Okay. That's it. That's it. It's your interview. You can always change something. There's no right or wrong answers. Everything is fine. It's just to get a bit background of you later on if we get some answers from your side, we can then relate the answers to how you rated yourself. That's the whole idea. There's no right or wrong answers here. That's it already from the background. So, I think that helps a lot to understand the background, your knowledge and everything. So, thanks a lot for that. And now I would like to enter into the main phase. The main phase is all about the case studies I've showed to you. So, in the case study, you have learned about company A, B and company C. And the first question I have here is do you understand the case studies? #00:05:03-9#

R: I think so. #00:05:07-7#

I: Mhm. And do you think that the cases are realistic? #00:05:12-9#

R: I think there's no definite yes or no answer. I would say it sounds quite realistic. #00:05:32-6#

I: It's possible, right? #00:05:36-2#

R: It's possible, yeah. #00:05:37-5#

I: Mhm. Okay. That's fine. Fine. Okay. Now, that we have clarified the cases, we have deci/-, or you have seen them, you have understood them, which is quite good. The question is now, or not the question, now, the task is now I would like to talk about with you about risk management and about the risk of adopting cloud applications. And the first question I have here is do you have already some experience in risk management? #00:06:06-2#

R: In theory. #00:06:09-1#

I: Excuse me? #00:06:11-0#

R: In theory, I have experience. So, in the, during my studies, I had, yeah, I have learned something about risk management regarding software project management. And also, risk management regarding security. #00:06:33-6#

I: Mhm. #00:06:34-5#

R: Yeah. #00:06:37-5#

I: Okay. I want to show you now a risk matrix. And let's have a look, if you have seen that before, and that's not-, no, if you have not, I will explain it to you. This is the risk matrix I would like to show you. Just let me know if you see it. #00:06:53-3#

R: Yes, I do. #00:06:56-1#

I: Okay. Have you ever seen such a risk matrix? #00:06:58-7#

R: Yes, I have. #00:07:00-2#

I: Okay. So, the basic idea of the risk matrix is to rate a risk based on two values, based on the probability of the risk and the impact of it for a company. The probability is here on the left-hand side and is divided into five points. It can rare, unlikely, possible, likely or certainly. So, the risk might be certainly, but still even though if the risk is really, really probable and really, really highly likely, there might be still the fact that it is not really important for the company. That the impact of it, is not really high for the company. So, then we would say the risk is still high, as it's quite certain but negligible.

There's the other case for example if the risk is possible but still negligible so it's not really high damage for the company, then the risk would be low. And this is how this risk matrix is to see. So, #00:08:00-1# if a risk is quite likely, and the damage would be really high for the company so the impact of that risk would be really high, then it's a very high risk.

Now, this risk matrix here is generic in terms of the absolute values on the impact. This is due to the case that you have three case studies. And for a smaller company, a damage, an absolute damage from for example, one billion is different than an absolute damage for a bigger company. And therefore, we have here some relative values, based on the turnover per year, which a company does. So, if the company does 80 million a year on turnover, then a damage below eight million would be negligible for that company. If it does 800,000 or eight billion, then of course ten percent of that turnover would be negligible. #00:08:56-9#

R: Mhm. #00:08:57-9#

I: Is it clear the idea of the risk matrix? #00:09:01-8#

R: Yeah. #00:09:02-7#

I: Okay, good. (…) So, just to make sure you understood that risk matrix, right? #00:09:13-7#

R: Yeah. Yeah, I do. #00:09:16-0#

I: Okay. That's what we will now use to rate some risks. So, during the studies, during the preparation and doing the creation of that dissertation, I identified three adoption risks. So, three general adoption risks. And based on the three adoptions risks and the provided use cases, I would like now to ask you to rate the risks of the risk I present you. #00:09:45-6#

R: Mhm. #00:09:46-8#

I: Okay? So, let me quickly present the risks to you, and explain also the risks to you. And you have always the possibility to ask if something is unclear. #00:09:56-3#

R: Yes. #00:09:57-5#

I: Okay? #00:09:58-0#

R: Okay. Mhm. #00:09:58-8#

I: So, you've seen the three case studies, case and company A, B, and C. #00:10:03-7#

R: Mhm. #00:10:04-4#

I: And they all want to adopt the cloud application but on different use cases. So, for example, company A would like to adopt the cloud application for a bookkeeping system. Company B would like to adopt it from intrusion detection system, and Company C would like to adopt it for a new web application. And they all have different providers. #00:10:25-5#

R: Mhm. #00:10:26-3#

I: So, the first provider is a cleaning company and it's an ISO certified company from Europe. The second one is an India company, which has a good Google rating. #00:10:37-5#

R: Mhm. #00:10:37-9#

I: And the third one is a big American company, which provides its service in license of the company already has. (…) Okay? (.) And now, there are three risks I would like to tell you like, and I would like for us to ask you whether you understand that risks. So, the first risk is, the risk that the cloud application provider, so, provider A, B and C implements a contractually not mutually agreed configuration. And a configuration, you can quite think of as a broad term, a configuration might be the backup location, the configuration might be a firewall configuration, the configuration might be (deport?) #00:11:26-6# configuration. So, everything you can technically configure, you can think of a configuration. And mutually agreed means that some party in that case the provider does it without the knowledge of the company who is asking for that service. So, is that risk clear? Any unclears, or if you understand a term not correctly, you can also in German of course, I will translate it. #00:11:55-6#

R: Mhm. Configuration can be anything. Right? #00:12:06-3#

I: Mhm. Anything you can think of technically configuration. #00:12:09-5#

R: Yeah. Okay. (Neil?) #00:12:11-8# and then it's clear. #00:12:14-1#

I: Mhm. #00:12:15-1#

R: So far. #00:12:15-4#

I: The second risk is the risk that the implementation of a compliance-driven configuration and a compliance-driven configuration is again something which - you know what compliance means? So, compliance means something the company itself, sets itself as rules. So, for example, the company says I do not only want to stop backups in Spain as an example. And compliance-driven configuration would be then that the configu/-, the backups are configured such that they are in Spain. #00:12:45-7#

R: Yeah. #00:12:46-8#

I: Other example of a compliance-driven configuration could be for example the company says it only wants to accept HTTPS traffic. #00:12:53-6#

R: Mhm. #00:12:53-9#

I: Then the compliance-driven configuration would be a configuration on the firewall at only HTTPS traffic is allowed to pass the firewall. So, everything the company sets itself as a rule can be seen as compliance-driven configuration. #00:13:07-9#

R: All right. #00:13:08-6#

I: Okay? #00:13:09-7#

R: Mhm. #00:13:10-3#

I: And the risk here is that the compliance-driven configuration gets delayed due to slow or manual processes. So, you can think of the example of the UK, they left the EU and the compliance requirement could be that they got some SP stored in the EU, the European Union. #00:13:29-0#

R: Mhm. #00:13:29-7#

I: And now the compliance-driven change would be to say, okay, please do not store. Please provider do not store any configurations anymore in the UK but store them in another European country. #00:13:41-9#

R: Mhm. #00:13:43-4#

I: And there might be the risk that this has to be done manually, so, they have to call the provider, the provider has to send the consultant or provide a consultant. And the consultant then needs to provide that information to the cloud application administrator. The cloud administrator-, the cloud application administrator needs to implement it. So, that is the risk explained here. #00:14:05-5#

R: All right. #00:14:09-2#

I: Okay. So, a delay in changing a configuration. There might be also that the company changes its colour. They say okay, we are now red instead of blue. And again, this configuration change also needs to be implemented in the cloud application, and there might be again a delay in that. #00:14:26-7#

R: So, the risk in the second one is always from the company itself. It’s not depending on some service from another company as per anything, right? #00:14:39-5#

I: That’s highly-, #00:14:41-6#

R: Or is it-, or does it depend on the context? #00:14:46-9#

I: It depends on the provider. So, whether the provider implements that configuration fast or not so to say. #00:14:53-7#

R: Okay. #00:14:55-1#

I: So, if you tell it to the provider and how the provider will then treat that configuration trait. #00:15:00-6#

R: Okay. But nothing else but the provider? #00:15:02-9#

I: Mhm. Exactly. Mhm. #00:15:04-3#

R: Okay. #00:15:04-7#

I: Okay. And the third risk, I think this is the most understandable here is the risk that in the risk of denying the implementation of a configuration in case like a dispute. So, if there's some data leakage for example and the topic goes to court, then one of the parties says I did not configure that. I, it wasn't me, I have no documents about that. We do not have any emails or whatever about the configurations. It was not our side made the mistake. #00:15:40-4#

R: Also, with the provider, right? #00:15:46-0#

I: Exactly. Either the provider or of course also the company itself asking for the service. #00:15:52-4#

R: Mhm. #00:15:53-2#

I: So, they go on to say that we did not say that. The provider could say ay, they have never heard about that. #00:15:58-3#

R: Okay, Okay. So, we only have two parties, the company or the provider? Okay. #00:16:02-7#

I: Ja. Mhm. Okay? #00:16:06-1#

R: Yeah. #00:16:07-0#

I: So, the question here is do you understand that risk? #00:16:11-2#

R: Yes. #00:16:15-0#

I: Okay. Good, good. Then I would say we start and we rate the risks based on the use cases. So, we take the first use case company A. #00:16:28-8#

R: Uh-huh. #00:16:30-0#

I: And we take the risks that the cloud application provider, so provider A (.) might implement the configuration, which was not mutually agreed on. So, provider A decides to implement any configuration which they did not talk about with the company A. #00:16:48-6#

R: Mhm. #00:16:49-9#

I: And I would now ask you to take the risk matrix here and to go through it. Is it probable, how probable it is, and what might be the damage of the-, for the company A here? If such a risk would occur. (7) And please let me know if any is unclear. #00:17:15-5#

R: Mhm. Can I think loudly? #00:17:18-4#

I: Ja, sure. #00:17:19-4#

R: So, one aspect point regarding if something did not go as planned or as agreed on, it is important to know that company A is headquartered in Europe and the provider is also headquartered in Europe because the law in Europe is a different one regarding you know, in the United States for instance. #00:17:48-8#

I: Mhm. #00:17:49-8#

R: So, that would minimise a little bit the risk in comparison to okay, company A is in Europe and provider A would be in United States or Manila. #00:18:03-5#

I: Mhm. #00:18:04-4#

R: So, (4) the law would hold there and since company A is a certified and provider A is also certified on the same, with the same number, the same letter, I think that the agreement there is quite clear since they have the same standards. (…) But there's also the possibility. You never have 100 percent safety or agreement or yeah, security that everything works 100 percent. #00:18:50-2#

I: Mhm. #00:18:50-8#

R: So, (4) but I would say the first risk for company A or for scenario A, I would-, (5) the probability would be possible. #00:19:18-9#

I: Mhm. Really? #00:19:20-3#

R: Yes. For my opinion. And if that happens, then it always depends on what the configuration is. #00:19:34-4#

I: Mhm. #00:19:35-3#

R: If there is some configuration where there is sensible stuff that was made without the agreement from both sides-, #00:19:46-9#

I: Mhm. #00:19:47-6#

R: - then it is, even though it is possible throughout on the lower side, it can be still critical. #00:19:56-0#

I: Fantastic. One rule of plan in risk management, you should always expect worse case scenario. #00:20:05-3#

R: Yes. So, always think with the factories on top if anything happens. #00:20:10-4#

I: Okay. #00:20:11-3#

R: So, I would say, (..) it is-, since I just said it could go-, it could be in the direction critical, I would definitely rate it in the probability possible and the impact to critical. #00:20:30-2#

I: Okay. That is a high risk. #00:20:31-6#

R: It's a high risk. #00:20:33-0#

I: All right. I'll write it down such as we have an overview here. #00:20:36-0#

R: Yeah. #00:20:36-8#

I: Okay. The second question-, // #00:20:39-5#

R: The second. So, now for scenario B, right? #00:20:42-4#

I: Ja. As you want to. Either we can (unclear) #00:20:45-9# risk to the first case or we can go as you want. #00:20:50-5#

R: Okay. Then let's do it for A completely first. #00:20:55-1#

I: Mhm. Ja. #00:20:55-9#

R: The risk implementation of compliance (unclear) #00:20:59-8# that always can happen. I mean, there is even if you have the perfect plan for anything, there is always a small risk or a small factor that anything goes sideways. So, it could be a ve/-, even if it's a small thing like yeah, just like something stupid that it could get delayed. It always depends again on the implementation as the product, or the implementation for the product at the end. (…)

So, since it always can happen that anything like that works or happens, my thought is the slower we are at the end in our project, the more money it would cost the company at the end. So, the probability is, it is always possible that anything goes wrong, but regarding to the point, to the fact that the slower we are in our plan, the more money it would cost us, I would-, and also, it depends on how much money it would cost us. The longer, of course, the more money. But since the company is (…) money-based, something between high and very high. (..) I have to decide for one. Right? #00:23:06-2#

I: That's true. Yes (laughs), the quantitative value. #00:23:09-4#

R: Okay. I would say very high. #00:23:16-9#

I: Mhm. All right. #00:23:18-2#

R: The risk of denying the implementation of a configuration-, #00:23:24-1#

I: In case of a dispute. #00:23:26-4#

R: Dispute. What does-, #00:23:34-7#

I: Dispute means a fight and disagreement in-, #00:23:42-1#

R: Okay. So, if there are some, yeah, okay. (.) If they're fighting or something, yeah? #00:23:51-8#

I: Exactly. #00:23:52-8#

R: The risk of denying the implementation. Is that a point that is in their contract somewhere (.) noted? #00:24:05-9#

I: You mean the configuration itself? #00:24:09-4#

R: Mhm. #00:24:10-5#

I: You can assume that the basic configurations are defined so that the company for example only wants to stay in Europe and you can also assume that most things are at least discussed but not part of the contract. #00:24:29-0#

R: Okay. #00:24:30-9#

I: So, you can assume that this is a cloud application as many applications that no details are in the contract but service level agreements for example. #00:24:41-2#

R: Mhm. Okay. There's the same risk that I see in the third risk like the second risk. So, if |(..) provider A denies to implement the configuration, (.) then company A will delay with their product at the end, what they want to have in order to work more efficiently or whatsoever. So, the slower we are, or whatever disruption we have, the more money it will cost us at the end. How likely it will happen where company A has ISO standard and provider A has the same ISO standard. So, I imagine that they have (.) some common same understandability for each other and for the requirements that company A wants to do. (…) So, I would rate it-, (4) I mean, it's a small risk regarding the percentage or the probability is quite slow I imagine. But if it happens, then the impact would be very high. So, I would-, (..) I would put it (4) factor it, so, I would say high. #00:26:33-6#

I: Mhm. Okay. And ja, doing the second one. So, exactly the same. #00:26:41-3#

R: Okay. So, let's say company B is in Europe? #00:26:50-8#

I: Yes. (.) All the companies are in Europe. #00:26:55-8#

R: All the companies are? #00:26:57-0#

I: Ja. Ja. But the providers are different. #00:26:58-9#

R: Okay. So, it also doesn't really matter the product of the company that they're doing, right? It's just important to know where the company is and who the provider or where the providers is. #00:27:12-2#

I: Mhm. #00:27:13-1#

R: Okay. So, (…) provider B is not in Europe. (4) Provider B has no ISO certification. (9) So, the law is different there regarding company in Europe versus Asia. #00:27:53-1#

I: Mhm. #00:27:54-0#

R: No, (7) I would say very high. #00:28:07-5#

I: Okay. (unclear) #00:28:12-6# The second, the third risk. #00:28:16-0#

R: The second risk. (9) I think the constraints are the same. So, if there are-, if there's any stop in our plan or any delay we have, it doesn't matter where the provider is, either, I mean, it is easier to (.) handle the delay if it is in the same area or place. (..) But a delay is always expensive the longer the delay is. So, I would also say here it is, it holds just the same, very high. #00:29:14-5#

I: Okay. But risk is? #00:29:23-4#

R: It might sounds a little bit cliché but I think if you find one provider in India, (.) there, I think that if provider B is denying it that company B can find another provider in India if they would want that to have in India since they are working quite fast. So, I would say, and (..) this company is also making more money in comparison to company A. So, I think that company B has-, can pay more or better (.) if they hire someone new. So, I think that the risk here is medium. #00:30:24-4#

I: Mhm. Okay. (…) And we go to third case. #00:30:30-3#

R: So, C is also new. But C is making the smallest amount of money per year, right? #00:30:38-3#

I: Yes, ja. (..) It’s a collection of farmers. #00:30:42-7#

R: (laughs) It’s a collection of farmers. And company C? #00:30:47-6#

I: It’s a huge American company. #00:30:51-4#

R: American company. (..) Okay. So-, #00:30:55-7#

I: U.S. company to be more precise. #00:30:59-4#

R: Yeah, yeah, yeah. In the USA. So, the risk complication if there’s anything unmutually agreed, (.) the same case here, the company is new and the provider is in the United States so with also different one. (5) I would also say very high. #00:31:27-2#

I: Okay. #00:31:28-3#

R: The risk, that implementation gets late due to the-, so, this company is making the least money per year. It would cost them even more in comparison to the annual income or annual making, in comparison to the-, to company A and B. So, if I would put it here very high, then it would not be really comparable to company A and B. (.) So, I would probably now that I see C in comparison with A and B-, #00:32:20-0#

I: Mhm. #00:32:20-8#

R: I would say C is very high. #00:32:23-4#

I: Mhm. #00:32:24-1#

R: And the other two are high. #00:32:27-3#

I: All right. Give me a second. (…) Okay, updated. #00:32:34-1#

R: Yeah (laughs). And the last one, (4) deny (unclear) #00:32:44-0# okay, so, I’m quite sure that if they are not happy or the company in use A is denying implementing (.) a configuration, I think that they also would be able to find another provider to do it. However, again, the longer the project runs, the more expensive it will get. (.) And here, (..) taking, well, again, taking the annual turnover into account, it would (8) be very high. #00:33:42-1#

I: Mhm. Just to compare, to verify that the risk here, this is here in the case of dispute. So, for example, if a data leakage or whatever occurs, that one of the parties says it was not me who implemented that. I think this is how you understood it, right? (..) Or how did you understood that risk? #00:34:06-9#

R: Regarding the dispute, I understood it that there is, there weren’t anything wrong. #00:34:16-3#

I: Mhm. #00:34:17-1#

R: No matter what, it was a data leakage or yeah, anything else was leaked. And fighting about who or yeah, who did it and what was leaked and how severe it is. #00:34:34-7#

I: Okay. #00:34:35-5#

R: And now they’re in a fight and that’s why they’re delaying everything. #00:34:40-0#

I: Mhm. #00:34:40-6#

R: So, that’s how I understand it. #00:34:42-8#

I: Mhm. Okay. Perfect. Okay. So, that was the first round so to say. #00:34:49-9#

R: Mhm. #00:34:50-6#

I: And in the second round, and first of all, thanks a lot for rating it of course. The second round, I would like now to present you the approach I developed during the PhD. #00:35:02-4#

R: Yeah. #00:35:03-2#

I: And explain it to you quickly. And this is in architecture, and let me just share my screen for that case. (.) So, I hope you already see it. It’s a PowerPoint, and you will see there some arrows jumping up-, #00:35:20-6#

R: Mhm. #00:35:22-0#

I: Jump back, so, okay. I hope you see it. Sorry, there was (unclear) #00:35:26-7# so, second, just have to go here. Okay perfect. So, you see there the architecture? And let me quickly explain it. So, everything starts here at the consume, at the cloud application consumer. The cloud application consumer can either be the customer, so company A, B or C. Or the provider, provider A, B and C. (.) Both have the opportunity or the possibility to configure a cloud application. #00:35:59-4#

R: Mhm. #00:36:00-1#

I: And in that scenario, here in the presented scenario, we have three parties. So, the consumer, the provider, and the cloud application itself. #00:36:11-4#

R: Mhm. #00:36:13-3#

I: The cloud application is the applications from the cloud scenarios you have seen. In the concrete example here, it's an intrusion detection system, and to be even more precise, it's a Snort intrusion detection system, which should be configured either by a consumer or by a provider. #00:36:31-7#

R: Yeah. #00:36:33-6#

I: Okay? And you have always the possibility to interrupt and ask questions. #00:36:38-8#

R: Mhm. #00:36:39-7#

I: Okay? #00:36:40-1#

R: Mhm. #00:36:40-4#

I: So, we have three parties, and all of the three parties share a common shared symmetric key, encryption key. (.) This is created and this is not really important but for your interesting, I can explain it to you. This is created during, using the blockchain. So, they store their public Diffie-Hellman values on the blockchain and receive the public Diffie-Hellman values from the other parties. So, it's a three-party Diffie-Hellman protocol. #00:37:15-2#

R: Mhm. #00:37:15-9#

I: You can also think of creating the shared symmetrically on a different way for example, via multiparty computation or whatever. But in that case, it's created using the Diffie-Hellman protocol. And you can assume that the creation of the symmetric keys is secure and man-in-the-middle is not possible. So, you can assume that they have a shared symmetric key. #00:37:40-2#

R: Mhm. Okay. #00:37:42-3#

I: You could further assume that the blockchain is secure. So, 50 plus likes or whatever are not possible. We abstract from the concrete use case as a block chain. We just use the blockchain and assume it is secure. #00:37:56-6#

R: Mhm. #00:37:57-7#

I: Okay. (.) Now, the idea is that the consumer, so, either the provider or the company take a configuration and you can think of a configuration as for example, as a text file, as a JSON file, as an XML file or anything you can write down in a document. And they use their symmetric keys and encrypt the configuration. Okay? You can follow that idea? (5) So, they decide they would like to configure a cloud application, and now, take the configuration, they would like to implement, write it down. #00:38:40-0#

R: Mhm. #00:38:40-8#

I: And encrypt it. #00:38:42-1#

R: Yeah. Okay. #00:38:43-6#

I: Ja? Then they sent the encrypted file to the blockchain, using the (unclear) #00:38:49-8# the blockchain. #00:38:51-1#

R: Yeah. #00:38:52-9#

I: Meaning now, the encrypted configuration is stored on the blockchain. #00:38:56-0#

R: Yeah. #00:38:59-2#

I: Okay? In the next step, the cloud management script. So, you can think of a backend script from the Snort applications or from the intrusion detection system has one script, which just monitors the blockchain. It monitors the blockchain for changes. #00:39:18-3#

R: Mhm. #00:39:19-1#

I: That can either be pull or push request. So, we can either see every ten seconds whether a new block came through. #00:39:25-3#

R: Mhm. #00:39:25-8#

I: Or the blockchain itself says hey, there's a new block. Have a look at this. #00:39:29-2#

R: Mhm. #00:39:30-1#

I: So, what the script is doing, it monitors the blockchain and checks whether new configuration files get implemented on a smart contract on the blockchain. #00:39:40-6#

R: Mhm. #00:39:42-3#

I: As soon as it detects that new configuration, new encrypted configuration on the blockchain and more precise on a smart contract, it pulls that new configuration, encrypts the configuration as it has access to the symmetric key, (..) implements that configuration on the application which should be configured so you can think of in Snort for example, the configuration is just a text file. So, it overrides that text file. #00:40:10-6#

R: Mhm. #00:40:11-6#

I: And monitors the lock files from the intrusion detection system in that case. So, it monitors the lock files of intrusion detection system, whether the configuration was implemented successfully or not. #00:40:24-2#

R: Mhm. #00:40:24-9#

I: So, it's not (dusted?) #00:40:25-9#, it rides in the configuration files whether a configuration changed has occurred and whether it was successful or not. #00:40:32-6#

R: Mhm. #00:40:33-4#

I: So, this is what happens here. So, in the third step, configurations are implemented and lock files are monitored. #00:40:40-7#

R: Yeah. #00:40:42-1#

I: As soon as it detects a configuration implemented successfully, the script or the cloud management script to be more precise, triggers a backup of the virtual machine on which the cloud application is running. So, the whole virtual machine on which the cloud application is running gets backup. #00:41:03-4#

R: Mhm. Okay. #00:41:04-6#

I: Okay? (.) Then that backup is used and the hash value of the backup is created. #00:41:11-9#

R: Yeah. #00:41:12-7#

I: The cryptographic hash value to be more precise. #00:41:15-1#

R: Yeah. #00:41:15-9#

I: And that cryptographic hash value is written back to the blockchain. #00:41:22-4#

R: Mhm. #00:41:23-6#

I: As the proof of implementation. #00:41:25-9#

R: Yeah. #00:41:27-6#

I: Which means now, the hash value of a virtual machine which has successfully implemented a configuration is stored on the blockchain. #00:41:38-6#

R: Mhm. #00:41:40-2#

I: And the idea is now in case of a dispute for example-, #00:41:44-0#

R: Yeah. #00:41:44-8#

I: - can take that hash value and ask to provide the responding or the corresponding backup and investigate it. #00:41:54-9#

R: Mhm. #00:41:56-1#

I: So, in case of a dispute, you go to court, present their last implemented hash value, so, the proof of implementation and present the backup. #00:42:05-0#

R: Mhm. #00:42:07-6#

I: And they can be investigated as the hash value is unique, you can check each configuration was implemented based on that hash value. #00:42:16-7#

R: Yes. #00:42:17-7#

I: Okay? #00:42:18-9#

R: Mhm. #00:42:20-7#

I: Everything which you have seen here, happens automatically. So, there is no person in-between who is checking something. Just because that question came also up in the past. #00:42:29-4#

R: Okay. Okay. #00:42:30-9#

I: Okay. That's it already. #00:42:33-2#

R: Yeah. #00:42:37-9#

I: Does it make sense? Do we understand it? #00:42:41-9#

R: I understand it. My question is that this (..) constructional architecture is a possible solution if we are having a dispute. #00:43:01-1#

I: So, this is a solution which providers can use as an alternative architecture for configuring their cloud applications. So, this could be used for configure for example an intrusion detection system, but you can also think of that the configuration file is for example a web server configuration file or an ERP configuration file or whatever. So, it's-, #00:43:30-1#

R: Yeah. #00:43:30-2#

I: - generic in terms of application you configure. #00:43:32-5#

R: Yeah. No, no. The architecture that is, that I understood. My question is, (4) is there a, because we just spoke of the risks and you just mentioned one example that if there is a dispute-, #00:43:53-6#

I: Mhm. #00:43:54-2#

R: - you can use the unique hash value and then retrack it and then see who was doing what and what's whatever. So, for the risk, if we would have a dispute, then this architecture could be a solution on how to manage it. #00:44:14-5#

I: Mhm. #00:44:15-4#

R: So, my question would be what, or how does this architecture apply to the other tools or will you come to that? #00:44:24-6#

I: To which other tools? #00:44:28-9#

R: To risks, so, if the, what was it? If the other-, if we are having a delay-, #00:44:37-8#

I: Mhm. #00:44:38-9#

R: - self-, self-made rules and the other risk was-, #00:44:45-3#

I: Transfer, just there's one that someone implements a configuration. #00:44:51-9#

R: Yeah, yeah. #00:44:52-1#

I: Which was not mutually agreed on. So, the thing is now, (.) I would like you to assume that we are using that configuration. #00:45:02-0#

R: Mhm. Okay. #00:45:03-4#

I: And I would like to ask you if you think that this configuration or this architecture changes something in the risk of those three risks. #00:45:14-8#

R: Okay. Okay, okay. Maybe that will answer my question. #00:45:18-6#

I: Okay. (laughs) Let me just know if any questions are there. Okay? So, we will clarify them-, #00:45:25-0#

R: Yeah, yeah. #00:45:25-6#

I: - I'm quite sure. Okay? So, the next task is now, as you, or the next question first of all, is have you understood the presented approach? And here, I again need a strongly agree, agree and neutral, a disagree or a strongly disagree. #00:45:41-4#

R: I agree. #00:45:45-1#

I: Okay. (..) So, now, as said, we are assuming that the cloud application providers, so, the providers in the scenario you have seen providing their cloud application using the proposed architecture. So, now, the application gets configured via the blockchain, as described. #00:46:08-6#

R: Mhm. #00:46:09-3#

I: And what I would like to ask you now is again, go through the risk with me, and again rate if there is a change in risks. #00:46:17-4#

R: Well, of course, there will be (laughs). #00:46:21-8#

I: Okay. So, the first question is now again, we are the company A, we are at the risk that the cloud application provider implements a contractually not mutually agreed configuration. And here I ask you, do you see-, or how do you see the risk? (…) Using now the budget-based architecture. #00:46:47-6#

R: Can we start with the last risk maybe? #00:46:55-8#

I: Absolutely. As you want. #00:46:57-3#

R: So, risk of denying implementation (unclear) #00:47:00-7# configuration (…) in case of a dispute. In case of dispute regarding the question who's responsible for what and how or what created this dispute, I would say since we can backtrack the work of the provider or the company that has been done, I would say the risk is lower. But regarding in their loss or the risk management itself, there is still a risk because if we would have a dispute and we can backtrack it and know at the end who's responsible for what, who did what? We would have an answer to, #00:47:57-6# maybe to clarify it or who has to pay what if it goes to court or something like that. However, the project will still be delayed.

So, (4) we have-, (.) we know how to solve the issue, if we would go into a dispute or go to court. If we will find out that we are not responsible for the dispute but the other party, then we will probably win at court. So, yeah. There will be less money lost, but still there would be money lost. So, #00:48:57-3# (14) Mhm. Okay, the last one, I mean, it always depends. I would like to go half step lower on the risk. There are no half steps in this matrix. So, (11) for company C I would say from very high, it can go to high. #00:49:45-6#

I: Mhm. #00:49:46-6#

R: I mean, company B is doing the most money of them all. (…) So, (5) but there would still be losses. Company A I would say since they are also doing quite money, it can go to medium. #00:50:18-6#

I: Mhm. #00:50:19-7#

R: But yeah, in comparison to that, I, to have the, (..) the scales to correct, I would have to go to low there. #00:50:37-3#

I: (unclear) #00:50:40-3#

R: Yes. #00:50:50-9#

I: Mhm. #00:50:52-0#

R: Yes, low. It can be the-, maybe I would change my mind later but for now, it's low. #00:50:57-8#

I: Okay. You can always change your mind. // #00:51:00-2#

R: Mhm. The risk of implementation of the compliance during configuration get, delay the intrusion processes. (…) Yeah. Taking your architecture into account, (.) if we do not or if the company does not know which compliance-driven configuration slows the project down, it can be backtracked again via the unique hash (5) to see what causes the slow process. (..) But still, it would, and after it is found and hopefully resolved, hopefully the project will go on the-, go further with the right pace so that it can still be finished in time depending on how long it would take to detect this slow or body compliance-driven configuration that slows the project down. (4) But still, there would be still money that goes away. (5) I think I will leave it like that. #00:52:36-3#

I: Mhm. And (unclear) #00:52:39-5#

R: Yes. #00:52:46-9#

I: Mhm. #00:52:48-0#

R: For now (laughs). #00:52:51-3#

I: All good. And this one. #00:52:58-6#

R: What-, I mean, with the architecture, (.) since we can backtrack it, and every step of the implementation or during the implementation is documented, we will have the security to always go back and try to look what went wrong. So, or at what point it went wrong so that one can understand why one landed at that point where the project is right now. (6) The risk is a little bit lower since we have the security point that we can always do the detection work since we have it documented or since we know what was done in what step during the implementation. (6) But the money is still-, (…) so, the last one for company C, I would say it is still very high (..) because the company is making the least of money and both the company and provider they are still in a different area. #00:54:47-2#

I: Okay. #00:54:48-6#

R: Company A and provider A are in the same areas. So, I think this will be easier to find it. And then if they found what went wrong and if there will be-, since it is contract and in the worst case that if it also goes to court, (..) that law holds pretty clearly since they are both in the same area. So, I think it can go to medium. #00:55:30-0#

I: Mhm. #00:55:31-2#

R: Since we have more or clear evidence what was the point that was implemented even though they did not agreed on. #00:55:42-0#

I: Okay. Okay. #00:55:43-1#

R: B, (12) since this company is having a lot of money (.) and they can track it and have the evidence pretty clear, I would say it can go to high. #00:56:17-1#

I: Mhm. (unclear) #00:56:21-7#. Okay. You have still the possibility if you want to change something, you're always free to change. #00:56:29-9#

R: Yeah. Yeah, let me think about it. (14) The risk of denying, so, the last risk, risk of denying the implementation (4) of configuration in case of dispute. (9) Yeah, I think I will leave it that way. #00:57:20-8#

I: (unclear) #00:57:24-7# (laughs)

R: Yes. #00:57:30-9#

I: Okay. Okay. Then I close that state. Okay? #00:57:36-6#

R: Mhm. #00:57:37-1#

I: Good. So, that was the risk assessment part. And now only smaller questions follow as you have already extensively explained all your steps. So, I think I have seen how you rate the aspects of the transparency, the aspects of the authorisation. Also, how you rate the case of dispute. So, I think that's clear. Except, you would like to add something on your rating. #00:58:11-9#

R: No. #00:58:13-8#

I: Okay. And there is another question which is open on my side, is now you have seen the approach, you have seen that the blockchain is used and the question here is do you think the use of the blockchain makes sense at this approach? #00:58:28-5#

R: Regarding the risk management. #00:58:33-4#

I: Regarding the usage, whether it makes sense to use the blockchain in that case presented to configure cloud applications. #00:58:44-7#

R: I would say yes. #00:58:54-3#

I: Okay. #00:58:56-4#

R: Do I-, okay. #00:59:05-0#

I: You create something if you want. #00:59:06-8#

R: I would say yes because since it is a cloud application, or data that we trust this application, where the server of this application, of this cloud application is depending on the company, it is know where they are. But however, there always can be something happening to the servers. It doesn't matter if it's, if one cable is not correct in the server or there is a thunder or I don't know, a flood or anything like that and everything goes, goes away. Hopefully, (..) the data on the server is backed up somewhere so the data (.) is not lost. But it is still good that this data is secured regarding the encryption of the data because if they would get lost or if they would get leaked in any way, that can also always happen that the intruder does not really have any information other than the hash. #01:00:28-9#

I: Mhm. #01:00:29-9#

R: So, the blockchain security in that case or security in general, I would always recommend. #01:00:38-0#

I: Mhm. Okay. Cool. That's it more or less. I have a final question here for, in the main part. And the final question is, overall, how would you evaluate the presented approach? Where do you see some advantages? Where do you see some approach, approach for potential for improvements or weaknesses? Do you see any upcoming risks or more or less the question is would you like to add something? #01:01:06-8#

R: I think that the approach of the architecture can be good help for companies who are quite new or who are not so familiar with cloud application or also security. So, that there's a, some sort of let's say a standard. If the architecture would be a standard, and a new company would just look around and try to learn about it and say okay, this is our standard and this standard already provides us with the blockchain, which will fulfils this security part and yeah, maybe other parts regarding, okay, what about the backup of the data. And how is the-, is the traffic between the user and the cloud application and so on. So, I think that standards or architectures like that can always help since - I'm not quite sure if there are already a lot of standards out there regarding cloud application or not. But if not, then definitely, and if yes, if there are already some standards there, and this is an add-on on those standards, then it still a yes. #01:02:44-7#

I: Mhm. Okay. Cool. We are at closing phase. So, the closing phase means there's only one last question. And now, you have heard all the questions from my side, you have joined me in the dissertation topic. Now, in school grades, how, and we're talking about German school grades where one is very good and six is insufficient. In school grades, how would you rate your experience in that area and how would you rate the statements you provide today? (.) So, are you sure about them? So, are you very good with them? Are you say, okay, this was good? Would you say it was insufficient, that was poor, sufficient satisfying, good, or very good? #01:03:35-8#

R: My answers? #01:03:37-5#

I: Mhm. Mhm. #01:03:38-5#

R: I could always reason why I would decide to what I decided. #01:03:51-0#

I: Mhm. #01:03:51-4#

R: So, what was it? How I would grade my answers and how I would grade my? #01:04:01-4#

I: Your answers, so, how would you rate your answers you provided here? #01:04:05-7#

R: (laughs) Pretty good. (laughs) Yeah. I would give me a solid two. #01:04:18-5#

I: Mhm. Okay. #01:04:20-0#

R: Plus, or anything. #01:04:20-8#

I: Okay. All right. that was the closing phase. And now, the closing information is thanks a lot for your openness, for your participation, and also for your time. The next step from my side is now the transcription, the anonymisation and the use of that conversation for the evaluation of my approach. Having that said, I would stop the recording. #01:04:42-8#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #6:

I: All right. Let's start with the interview. Thanks for participating to that evaluation interview. Before we start, as announced, I would like to start with a warmup and introduction phase. During that phase, I would like to get you know a bit better. And therefore, my first question to you. This is an open question. Can you briefly tell me something about your professional background and your daily tasks? #00:00:36-8#

R: Yeah, sure. I'm a IT professional for over 15 years. I started my professional with network and server system knowledge, and continued with software development. So far, I'm a test analyst for a bigger software consulting company and develop and test bigger kind of application. #00:01:10-9#

I: And just to have it also here in a written form, your educational background. Can you briefly tell me something about that? #00:01:21-8#

R: Yes. I have the A level education, a apprenticeship as IT system electronic. And I have not finished bachelor study. #00:01:36-5#

I: And you have 15 years of professional experience. That's correct. #00:01:42-0#

R: More or less, yes. 15. #00:01:45-4#

I: Okay, amazing. Good. So, those were the open questions. And as already introduced, we have also some quantitative questions. And there, I already explained strongly agree, agree, neutral, disagree, or strongly disagree to the statements I will provide you. So, the first statement I have here is, I am a computer science expert. #00:02:08-8#

R: Agree. #00:02:14-7#

I: I'm an information security expert. #00:02:19-2#

R: Agree. #00:02:23-2#

I: I'm a cloud computing expert. #00:02:26-5#

R: Neutral. #00:02:27-7#

I: I'm a cryptography expert. #00:02:31-0#

R: Disagree. #00:02:34-0#

I: Okay. Amazing. All right. That's it already, the introduction phase is over. We know you really very, very good now. So, hopefully I think we can start with the main phase. And for the main phase you already received the case studies. In the case study, you have read about company A, B and company C who want to adopt the cloud application on different use cases. The first question I have here is, do you understand the use cases? #00:03:05-7#

R: I do. #00:03:07-4#

I: Okay. And do you think those are realistic use cases? #00:03:11-9#

R: In the most cases, I think yes. #00:03:16-0#

I: Okay, perfect. Okay. Having that discussed and seeing that the use cases seem to be quite realistic so to say, I would like now to talk about the risk of adopting cloud applications. And that's why I would like to tell you, or to discuss you about risk management. And here, my open first question is, have you ever heard about risk management in the area of computer science? #00:03:46-9#

R: Yes, I have. #00:03:48-7#

I: Do you have any experience? #00:03:51-1#

R: Yes, for sure. There are a lot of risk in development, for example. Applications can be really risk fuelled by some mistakes or also by getting new technologies and open some dangerous or more or less dangerous risk. And they are also risk by creating some environments like network environments. And also, in the progress of developing or also in the use of normal, the use of data. For instance, if employee doesn't matter about his password, it is also dangerous as when you develop or deploy a very weak software. #00:04:55-8#

I: Okay. Amazing. Have you ever heard about the term risk metrics? Do you know what a risk metrics is? And I can also show you one, maybe you've seen it already, if not heard the term yet. #00:05:09-1#

R: I have one in my mind with four parts, maybe it's the same. Okay, there are some more parts (laughs). #00:05:18-5#

I: So, the basic concept is probably always the same. So, you have the probability on the left-hand side, and you have the impact on the right-hand side. And during the risk assessment we do now during the evaluation, I would like to use that risk metrics here. And therefore, I also explain it quickly to you. So, as already said, there are two factors influencing a risk. Those are the probability; how probable a risk is that it occurs. And on the other hand side, the impact the risk creates on your company. So, there might be risks which are super seldom occurring, so they're super rare, but they create a catastrophic damage on your company. And then we would classify that risk as a medium risk.

If we have a risk which suddenly appears, so it's really, really sure that this risk will occur, but it's negligible. So, it's really, really, really #00:06:18-8# low damage. It's only really a small amount of money damage. Then it's still a high risk, as an example here. And this is how that risk metrics works. We have the probability of how probable a risk is. And this is always subjective. So, there is no clear guidance on saying, okay, this starts 30, 50 or 60 percent. This is out of your experience where you need to rate it.

And the same holds also for the impact. So, you need to rate it based on your experience. There is no clear guidance whether a catastrophic damage will occur or a marginal damage. So, this is how that metrics works. And the question is now from my side, do you understand that metrics? #00:07:04-6#

R: I get it. Yeah. #00:07:05-9#

I: Okay. One last comment here. This metrics here is generic in the term of impact. That means you see here the impact is measured in percent based on the turnover per year. So, you have three different use cases. They have different turnovers per year. So, (unclear) #00:07:29-2#. And of course, for a bigger company a negligible damage is different, absolute value than for example, for a smaller company. That's why we use that generic term here. So, if you say here 10 percent, then it's always 10 percent of the specific use case turnover, which is then the impact amount. Is that clear? #00:07:5506#

R: Yeah, it is. #00:07:57-0#

I: Okay. That's good. All right. So, I think you've understood the risk metrics. Now, the question that I have here is, do you think a risk management makes sense in the proposed use cases? #00:08:15-4#

R: Totally, yes. It makes sense because every situation needs to be analysed regarding any risk. #00:08:26-5#

I: Now I would like - Sorry, did I interrupt? #00:08:31-2#

R: No, no. I just thought about if I have to agree or explain it with my own words. No, everything is fine. #00:08:41-6#

I: Okay, perfect. Now I would like to present you three adoption risks. So, if you want to buy a new cloud application. There I identified for my PhD three risks. And I would like you, or ask you to rate the percentage use cases based on those three risks. So, I give you three risks. And I would like to ask you to go through the use cases and give me a risk value for all of the three risks from each use case. So, in total, at the end, we should have nine risks, three in each of the three use cases. So, it's two times three, it's a bit confusing. But I think we will get it together. I will share my screen. And I will share the screen in a way that you see on the left-hand side the risks and on the right-hand side, the risk metrics such we can use it.

I hope you can read it. And I will also explain you the risks shortly. So, the first risk #00:09:41-7# I have on my side is the risk that the cloud application provider, so provider A, B and C implements a contractually not mutually agreed configuration. Meaning the provider A implements, for example, a backup location, which was not agreed on contractually. They say, okay, we, for example, implement a data storage location, not only in the agreed storage location, but also an additional location, for example. So, they configure something which was not mutually agreed on. Do you understand that risk? #00:10:23-4#

R: I hope so. Yeah. #00:10:25-0#

I: Okay. Please let me know if any questions arise. It's really crucial to get the risks. So, a configuration in that sense means anything you can think of configuring. That could be, for example, a backup application. This can be a firewall configuration. And this can be also for example, the configuration of an intrusion detection system, the configuration of the layout from a web application. So, everything you can configure, you can think of in configuration. The second - #00:11:01-4#

R: Sorry. But it excludes some user data or employee data, or is it also included? #00:11:12-9#

I: The configuration itself means, for example the - How to describe it better. #00:11:22-2#

R: Just technical configuration data or? #00:11:25-3#

I: So, everything you can technically configure in the cloud application. Okay? #00:11:30-1#

R: Okay. Yes, I get it. #00:11:34-0#

I: The second risk is a process related risk. So that the risk that the implementation of a compliance driven configuration. So again, compliance driven configurations are the configuration we just discussed, for example, backup storage location, firewall configuration, or whatever. Gets delayed due to slow or manual processes on the provider side. So, the risk says, for example, you realize as a company that you would like to change the backup location. Now you need to communicate that change to the provider. And the provider needs to implement that.

And there might be the risk that you first have to go through a consultant. The consultant then needs to bring it to the cloud application, DevOps or whomever is maintaining it. So, the administrator of the cloud application. And he, or she then implements the configuration. That's meant by that risk, that it doesn't delay in configuring.

And the third risk, I think this is the most clear one #00:12:34-0# then, is that one of the parties denied to have a configuration implemented in case of a dispute. So if, for example, a data leakage occurs and the case goes to court, then the risk that one of the parties says, "Okay, this is not what we said we would like to have. This was not contractually agreed on what was configured." So that one of the parties just denies to having done something which was not agreed on. So, do you understand that also, that risk? #00:13:06-4#

R: Yes. #00:13:07-8#

I: Okay. I hope the risks are understandable. Please let me know if something is unclear on the risks. Because my next question is exactly, do you understand the risks? (laughs) #00:13:17-9#

R: I do, yes. I understand them. #00:13:21-6#

I: Do you think that the risks are realistic? Do you see those risks for the three cases? #00:13:28-0#

R: The last one in total, I think. I try to get some example for the second one. And I'm not really sure if the first risk can be really that dangerous, but yes. Can, for sure. Everything can be possible. #00:13:47-8#

I: (laughs) Yeah. That's the point where with risks. The question is always how high the risk at the end will be. And that's what we are now trying to figure out (laughs). So, this is your task now, to figure out. And therefore, I would like to start with the case A, so company A, with company A. And here, I would like to ask you the first question and ask you to evaluate the risk that the provider A implements something in the cloud application, which was not contractually agreed on. #00:14:24-8#

R: Okay. Let me check the text again. #00:14:28-0#

I: Yeah, sure. Take your time. #00:14:31-9#

R: Just jump over again. All right. Okay. First, I just want to exclude because the lowest seems to be not the best choice. Because they have a high security need to store the data. If configuration data are stored separately without any knowledge of the company, they cannot set up some processes to keep it also stored or keep it in mind. So, I think it's also not the highest risk. Because first the provider seems to be as secured as possible. And it's not really, really so likely that backup systems backup or backup configuration data are hacked mainly. #00:16:31-9#

I: You can think of the configuration as everything they did. That might be also that they configured the application wrongly, that it's now accessible from the public side, for example, instead of only from internal side. So, in any case, a configuration. That's not only about a backup. Sorry for being misleading here. #00:16:49-8#

R: Okay. That gives a bigger range as well. But I would set it to a high risk, I think. Yes. #00:17:04-6#

I: High risk. I will note it down here because we will later on need it again. Then should we stay at provider A and go to the second risk. So that the risk, that manual process (unclear) #00:17:25-7#

R: Machine, yes. Likely. They use machines and manufacturers of larger enterprises, so they need to set up some things, I think. I would also give it a high, high level. #00:18:06-8#

I: Please take your time. So, no one is pushing you. And the third risk, that someone denies it in the case of dispute. #00:18:18-2#

R: Well, misunderstandings are quite normal. And even if there was any danger to the own company. But there are contracts and I think often contracts are not that, how do you say in English, abstract bar? #00:18:50-0#

I: Deniable or? #00:18:51-5#

R: Deniable. Maybe, yeah, deniable. Not really deniable. So, I think it's more a medium, medium one. #00:19:00-6#

I: Okay. Now we go with the second company, with company B. Yes. #00:19:10-3#

R: All right. Okay. I think it's very high. Do I need to give a explanation for that or is it - #00:20:15-5#

I: If you want. It's your interview (laughs). #00:20:17-2#

R: (laughs) I think it's why just because the provider doesn't seem secure. I guess they don't want to spend such money for the security. Just one point. And I think it's very high. #00:20:38-7#

I: Okay. Good. The configuration gets delayed. #00:20:46-7#

R: Yeah. It's low risk. Set it to a low risk. And dispute. Okay, regarding the metrics, I would say high. #00:22:01-2#

I: All right. Maybe it's a good idea to just name the probability and the impact you're thinking of. It makes it also more transparent. #00:22:11-2#

R: Okay. To all of them, or just to -? #00:22:14-5#

I: Just the last one or the last two ones you decide on. #00:22:17-3#

R: Okay. I think for the high risk, I would say it's likely. But how do I put pronounce it, marginal. #00:22:30-3#

I: Marginal. #00:22:30-8#

R: Marginal. All right. Yes. And the medium one I choose, got delayed - What did I choose? #00:22:46-0#

I: For delay, for the second one you've chosen? #00:22:50-4#

R: Low. I was confusing right now. Yes, I was choosing. It was negligible (laughs). #00:23:00-8#

I: Negligible, yeah. #00:23:02-3#

R: Negligible, sorry. And possible. #00:23:05-3#

I: Perfect. All right. Amazing. Okay. And now you're an expert on rating (laughter) so you can continue with providers. You know it's really good. It's really, really good. So, I think you got it. #00:23:19-1#

R: Thank you. Okay. Two weeks ago. Yes, I would give it to a low risk. #00:23:56-0#

I: Can you name the - #00:24:03-0#

R: Yeah. I would say it's unlikely and negligible. Configuration. (unclear) #00:24:18-1# is also low, but let check that with the metrics. I think it's. I think it’s rare and negligible. #00:24:36-3#

I: All right. It's low risk. #00:24:40-0#

R: So, sorry. Sorry. Would give it the low to the last. #00:24:48-6#

I: Ah, to the last one? #00:24:49-2#

R: Yeah. To the last one. Sorry. #00:24:51-1#

I: And to the second one? #00:24:52-0#

R: Delayed. #00:24:55-1#

I: Delayed risk, yes. #00:24:56-5#

R: Delayed. I think, well, (unclear) #00:25:09-1# margin. Give it a medium. Possible and marginal. #00:25:24-7#

I: Possible and marginal. All right. Perfect. Amazing. All right. So, we are halfway there, so to say. (laughs) But I see you're doing really good. And I see that you have rated the risk really understandable. So, we had that. I'm just checking the interview guide. Now I would like to briefly introduce you the architecture I developed during my PhD. And here again, please let me know if something is unclear on that architecture, on the idea of the architecture. #00:26:12-1#

R: Okay. #00:26:13-2#

I: And I will there again, share my screen with you. Give me a second. This is a really, really short PowerPoint presentation (laughs). So, it's just, I think it's easier to understand having a PowerPoint presentation. So, the approach itself contains of three participants. That's on the one hand side, the consumer. Whereas a cloud application consumer can either be the provider of an application or the consumer of the application. So, the customer of an application. So those be both.

And the third party involved here is the cloud application itself, which is obviously hosted in the cloud. Otherwise, the cloud application would maybe a bit misleading here. So, those are the three parties more or less involved in the whole architecture. And all of those three parties share a common shared secret key. They have a symmetric #00:27:13-3# key together. They are creating that symmetric key via the Diffie–Hellman key exchange protocol.

It's not mandatory that you definitely need to understand the details of the protocol, you just need to know that they have a shared secret key. They have a symmetric shared key together. Furthermore, we do have the blockchain in our approach. And here is the only assumption you can make, that the blockchain itself is secure in this case. So, you don't need to think of 50 plus attacks or whatever. You can think of that the blockchain itself is secure. We abstract from the blockchain a bit.

Now the idea of configuring the cloud application, which is in our case here, an intrusion detection system, or to be more precise Snort intrusion detection system is as follows. And please always interrupt #00:28:13-2# me if I'm too fast or to unclear. The aim would be that you understand that architecture.

So, the idea is that the cloud application consumer would like to implement a new configuration. And you can think again, of a configuration as a text file, as a JSON file, as an XML file or whatever any configuration might look like. Clear so far? #00:28:41-6#

R: Yeah. #00:28:42-8#

I: Now, what the consumer does is it encrypts the configuration with the symmetric key it shares with the three parties. It then uses the encrypted configuration and puts it to the blockchain encrypted. So, on the blockchain is an encrypted configuration now. And of course, this is all digitally signed via their private keys as blockchains work.

In the next step, this cloud management script here comes into place. The cloud management script you can really think of as a part of an application, as a part of a cloud application. So, as a backend part of a cloud application. And this script detects changes on the blockchain. So, all the time a new block comes to the blockchain, this script detects such changes. This is done either via a pull mechanism. So, meaning it, every few seconds, pulls whether a new block was created on the blockchain. #00:29:42-6# Or via a push mechanism the blockchain says all the time, "A, there's a new block, please be aware of that."

So, those might be the mechanisms. But it's still not important how that detection will be done. You can assume that this is possible to do. Now, the cloud management script detects that there's a new block on the blockchain. And then monitors the blockchain, whether there's also a change configuration stored on it. So, it monitors whether the configuration, which is stored on the blockchain for the cloud application got changed during the new block, which were attached to the blockchain. Is it clear so far? #00:30:24-6#

R: Yes. #00:30:26-0#

I: So, more or less, it does monitor the blockchain for new blocks, for new configurations. Then it takes that configuration, if it's a new one, decrypts the configuration and writes it to the cloud application it configures. You can think of writing a configuration into an application like it's overwriting a text document. So, it's not for example, the text, it's a textual configuration. And it implements a new text file into the existing configuration. So, just overrides the text file more or less, to describe it on a real easy way.

And it's not configuration itself, is nothing else but text which describes at which cases an alarm should be created. So, what this script does is more or less it overrides a text file on the cloud application. Furthermore, so additionally, that cloud management script also monitors the log files of the cloud #00:31:26-3# application it configures. So, it watches the log files and checks whether the configuration was implemented successfully or not. So, Snort says, "Okay, I have a new configuration," or Snort says, "Oh, there was a configuration error." Okay, understandable, right? #00:31:44-5#

R: Yes. #00:31:45-3#

I: Now we assume the cloud management script detects that the configuration was implemented successfully. Then in the next step, it triggers a backup of the virtual machine on which the cloud application is running. It takes that backup and creates a hash value out of the backup. So, it hashes the backup it has just created and recently implemented the configuration. #00:32:17-2#

R: Without encryption. #00:32:18-8#

I: Without encryption, yeah. Now it takes the hash value of the backup, of the created backup and writes it to the blockchain. So, now on the blockchain is the hash value of the virtual machine having the latest configuration implemented. So, as soon as the configuration gets successfully implemented, it creates a backup. It takes the hash value and stores that hash value to the blockchain. And that's it more or less (laughs).

So now what we have is we have a cloud application configured based on the configuration which was set on the blockchain. And we have written back a hash value of a virtual machine having a successfully implemented #00:33:18-1# configuration. So, the idea is now, if for example, dispute occurs, you can go to court and say this is the latest hash value from a configuration which was mutually agreed on, implemented. Please show me that backup matching to that hash value. And you can then investigate that backup and see which configuration was implemented during the creation of that hash value. And none of those parties can now deny that a specific configuration was not implemented. As the hash value matches to the backup and the backup contains the whole virtual machine. So, what the hash value at the end is, is a fingerprint of the agreed-on configuration. Any questions to that? #00:34:19-4#

R: There were some, but you continued and then the question was answered. #00:34:25-9#

I: Okay. (laughs) That's good. Just talk as long as possible to solve all the questions (laughs). That's a good approach. No. So, now I have a question actually, and this is, again, an answer I would like to hear from you on strongly agree, agree, neutral, disagree, strongly disagree. And this is, have you understood the approach? #00:34:50-1#

R: Agree. Yep. #00:34:53-2#

I: Amazing. Okay. And now I think it's not surprising that we, again go through the risk management process. And we again take now the provided case studies. But we are assuming now that the provider is having implemented that architecture here and is configuring the cloud application based on that architecture here. And now I, again ask you to provide me with the risk assessment. And I share my screen here, so we have the same conditions as before. All right. So, then we start with the provider A. #00:35:37-0#

R: So, company A. They are saying implements a contractually and mutually agreed configuration. (unclear) #00:36:28-1# May I give a question to you? #00:37:02-2#

I: Yeah, sure. #00:37:02-7#

R: Do we expect that the stored configurations are also encrypted? #00:37:21-9#

I: The configurations are encrypted. #00:37:23-6#

R: Okay. Here in the example for the first. Not for your explanation. Not in your explanation of your work. I mean, for the first situation, if the provider implements a contractually not mutually agreed configuration. Is this one also encrypted or not? #00:37:50-6#

I: So, everyone, so the provider, it is encrypted, yes. But the provider, the consumer and the cloud application has the key to the encrypted file. So, those are the three parties who can encrypt it. #00:38:05-6#

R: Company A. Okay. I would go down here to the medium risk because it's likely negligible. #00:38:50-4#

I: And then we go to the automation, to the manual process. So, just because that question came up in the past time, this is everything is automated. So, there's no manual process in between. Because that question came a few times already, so this is already an answer to your question, which might come up. #00:39:10-9#

R: Okay. (laughs) I think we can go down to low in this case. #00:39:23-7#

I: And the third risk? #00:39:27-4#

R: In case of a dispute, could it be a risk? Not possible. You explained it. I would give it a low as well. #00:39:42-2#

I: Okay. Amazing. And now we go - If you have any understanding issues, but I think you understood it as (laughs) far as I got it. So, if anything is unclear, just let me know. #00:39:55-8#

R: Okay. I'm just thinking about any examples or maybe there are some something I haven't seen so far. And that's why I'm just a little bit slow. #00:40:07-0#

I: No. Take your time. So, the company B company. #00:40:13-1#

R: Company B. We set it too high. I set it too high. And delayed because it's automated. And even if it takes a bit of time, yeah, I can't go more down. So, it's low. #00:41:31-4#

I: Yeah. That's true (laughter). And the next one. #00:41:36-1#

R: The disputable is also low. And you can also put it to the third company because I do not see any possibility yet. #00:41:48-6#

I: That's good. #00:41:49-3#

R: - to a higher - Company C. (unclear) #00:42:11-7# Delayed. There were two networks, right, two virtual machines. #00:42:33-8#

I: You can assume that the blockchain is secure. So, you can also think of a dedicated blockchain. Don’t care about that. #00:42:45-4#

R: Okay. Give it a low. Yeah. #00:42:51-4#

I: I think it’s good. #00:42:54-8#

R: Yeah, it looks good. #00:42:56-6#

I: So, you're happy with your answers? #00:43:00-2#

R: I think so, yes. #00:43:02-8#

I: That's good. #00:43:04-3#

R: It looks more or less good because of the first one, medium and high. Maybe I'm too carefully, but I keep it like that. #00:43:18-6#

I: Amazing. Cool. Good. Then we are done with the risk assessment and are nearly done with the interview. Just a few let's say outgoing questions here. You've seen that this approach has used the blockchain. And the question I have here is, do you think the use of the blockchain makes sense at this approach? #00:43:40-6#

R: It makes, yes. Totally. #00:43:43-7#

I: Okay. And based on your risk assessment, do you think that the approach I presented to you has an influence on the transparency of configurations on the automization of configurations and, or on the notarization? So, on the digitally signing of configurations? #00:44:07-0#

R: Transparency, yes. What was the second one? #00:44:15-3#

I: Automization. #00:44:16-8#

R: Automization, okay. I think it's also possible without blockchain. And third part was usability? #00:44:29-8#

I: Digitally sign in, notarization. #00:44:31-4#

R: Digital signing blockchain. #00:44:33-9#

I: It's not related to blockchain. It's just whether that approach has an influence on notarization. #00:44:42-0#

R: Ah, okay. Ah, sorry, sorry. Say again, please. #00:44:50-5#

I: Yeah. Do you think the presented approach has an influence on the digital signing of configurations? So, do you think it influences how configurations are implemented, so to say? #00:45:03-6#

R: You've uses Diffie-Hellman and blockchain. I'm not really sure. I do not have any - #00:45:19-3#

I: Okay. That's not a problem. #00:45:20-4#

R: Okay. (unclear) #00:45:2206# the answer. #00:45:24-0#

I: Yeah, sure. So, there is no need of answering everything. It's way more valuable if you could just answer that way 'I'm sure' than just answering everything and being not sure. This is always something I had also to mention. The final question and then we are already through is, would you like to add something to the whole approach you see? Would you like to comment something? Would you like to mention any advantages, any disadvantages? Would you maybe also make aware of an upcoming risk due to the newly implemented approach, which was not discussed here? So, the stage is more or less yours. Would you like to add something? #00:46:05-0#

R: Okay. I think it's a really good combination of blockchain and cloud system to use the blockchain to increase the security. And the security parts as well with the cloud system. And if you have the possibility to increase the dispute-ability, the authentication, the encryption, for example, it should be used. Definitely if the implementation is really realistic in combination, in the view of spending of the money you can use. It must be compared. And for that reason, I think it's for the just the first view, really, really good. #00:47:11-4#

I: Okay. Amazing. You already nailed it quite good. This is a research example. I totally agree to the fact that you say, okay, of course in real life, it also has to pay money. Or it should not be more expensive than (laughs) having the regular one. Because at the end, the price is also deciding. I think that's what you wanted to say, right? #00:47:34-0#

R: Yeah. #00:47:34-6#

I: Okay. Perfect. All right. We are in the closing phase. In the closing phase, there's only one last question. And now that you have heard everything, so you know, the topic, you have seen all the questions, you have heard all questions. Based on the school marks, based on German school marks, so one is very good and a six is insufficient, how would you rate your experience? And more precisely, how would you rate your statements you gave today on grade? So, are you quite confident with what you said or are you totally unsure with what you said? #00:48:12-5#

R: Well, I have some experience regarding cloud system, regarding blockchain and security. But in fact, I often, I think I cannot overview everything. And also, not in general. And I think even in that short time, it's needed to analyse special parts, much, much more in detail. And therefore, I think for my spontaneous answer, it's a really good three. #00:48:47-9#

I: Okay, amazing. So, it's a satisfactory three. Perfect. So, we are in the closing. So, thank you very much for your openness, participation and time. As said, the, the next steps for me will be the transcription, the anonymization, and then the use of your statements for the transcription. And having that said, I stop the recording. #00:49:12-3#

R: Okay. #00:49:14-2#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #7:

R: You might had the transcript (unclear)#00:00:05-6# started. #00:00:06-8#

I: Yes. Recording has started. #00:00:10-6#

R: (Foreign language)#00:00:11-6#. #00:00:15-1#

I: Ja. Recording is running. We are in the interview. #00:00:18-6#

R: Okay. #00:00:20-3#

I: Ready to go? #00:00:22-0#

R: I am. #00:00:23-5#

I: Alright. Ja. Welcome to the interview, and thanks for participating. As already introduced in the info phase, this is now the second phase of the interview, the warmup phase. And during the warmup phase, I would like to get you known a bit better. And therefore, I prepared a few questions I would like us to answer you. Anyway/. #00:00:54-9#

R: I understand. #00:00:56-2#

I: Good. So, for the information here and for having it also in the interview documented here, can you briefly tell us something about your professional background and your daily tasks? #00:01:11-1#

R: I started my professional life 15 years ago as a systems administrator. And I have been working since then in different roads as a systems administrator and as a technical consultant. I worked both in government positions and in oh, what is it called? Damn. #00:01:47-1#

I: Public sector or? #00:01:49-5#

R: Ja. Public and private sector. Private sector that is the word I was looking for. Ranging from companies with 15 employees to companies with over 80,000 companies. And my work is mainly focused on infrastructure, more specifically email and security topics. #00:02:16-2#

I: Great. Can you also a bit tell us about your professional background, so your educational background? #00:02:26-5#

R: My educational background, I completed German Abitur. I started several attempts at attaining an university degree, but I did not finish any of that. And I completed, now it is difficult to translate that into English. #00:02:51-4#

I: The apprenticeship or what are you looking for? #00:02:58-3#

R: Ja, whatever the system is called, how we train for jobs in (Place). #00:03:07-0#

I: The dual education system? #00:03:08-8#

R: Dual education system yes, and finished as (foreign language)#00:03:12-1#. #00:03:14-8#

I: So, professional computer scientist, so to say in a dual system? #00:03:20-7#

R: Yes. #00:03:21-9#

I: For an international area. Okay. Amazing. And I think that already provided good background information about you. And as I already said, and we have also some quantitative questions here, and therefore I would like to provide you with a statement and like to ask you to answer that statement either with strongly agree, agree, neutral, disagree, strongly disagree to that statement. Okay. So, the first statement I have here prepared is, I am a computer science expert. #00:03:56-0#

R: Strongly agree. #00:03:59-9#

I: Okay. I am an information security expert. #00:04:05-0#

R: Agree. #00:04:09-3#

I: I am a cloud computing expert. #00:04:14-0#

R: Agree. #00:04:15-6#

I: And I am a cryptography expert. #00:04:19-5#

R: Neutral. #00:04:22-7#

I: Alright. That is it already. So that was already the warm up phase. So, I hope it is now warm, and we can enter into the main phase. So, thanks a lot for providing that information so far. And I said, this is background information, and this is used also to relate your statements with your background information. So just that you know also why we are making that. So, I would now like to enter into the main phase. And during the main phase, we do evaluation of architectures. The evaluation is based on a risk management approach.

So, the first question or the first thing I have here on my to-do list so to say on the guided interview list, and this is the introduction of the three case studies. And I think you already read the three case studies. So, you are already familiar with Company A, Company B and Company C, and their respective providers. The first question I have here is, do you understand the case studies? #00:05:28-2#

R: Yes, I do. #00:05:31-0#

I: Okay. And do you think the case studies are realistic? #00:05:35-4#

R: They are, yes. #00:05:38-2#

I: Okay. Amazing. Alright. Now as said, I would like to talk with you about the risk management of cloud adoption, cloud service adoption. And the first question I have here is, can you tell me a bit about your knowledge in risk management, or do you have any experience with risk management? #00:06:01-4#

R: My experience is more on the practical no, on the implementation side. In this role, I have been asked some questions regarding risk management, but I did not have to manage it in a larger capacity. #00:06:26-1#

I: Okay. Let me just quickly show you the following risk management metrics and see whether we can figure out if you understand it, or if I can explain it quickly to you. Give me a second. And here we are. Let me just know is it a bit small for you probably? #00:06:47-3#

R: No, no. It is okay. #00:06:49-2#

I: Okay. So, have you ever seen such a risk management metrics? #00:06:54-3#

R: Yes. #00:06:56-3#

I: And otherwise, I will explain. So, do you need a quick explanation or is it clear? So on the left hand side, we have the probability values. So, if the probability of that risk is for example lower than 10%, we would say it is rare, the probability. And on the X axis, we do have the impact of the risk. So, this is based on money on euros to be more precise. Now, as we have three case studies with different sizes of company, I made the impact more generic, meaning here are not absolute values written here are relative values.

So that means for smaller companies of course at the end, an absolute value would be smaller value negligible than for example for a bigger company. I think it is understandable why I have taken relative values here. Ja. And to build the risk now, or to rate the risk, you have to take the likelihood and the impact. And then based on the two values you have chosen, you can then figure out the related risk. I think it is understandable, right? #00:08:09-0#

R: Yes, it is. #00:08:11-8#

I: Okay. So, this is the question here, have you understood the risk management metrics? #00:08:18-4#

R: Yes, I do. #00:08:20-3#

I: Good. Now coming back to the case studies we have discussed or you have seen, do you think risk management makes sense for the proposed cases in general? #00:08:33-0#

R: Absolutely. Yes. #00:08:36-0#

I: Adapting cloud applications to be more precise. Good. So, I see it as a yes. Now during my PhD, I have identified three major risks in cloud application adoption, which are related to compliance based configurations. Let me quickly explain that to make it a bit clear. So, I think cloud adaption is clear. So, a company would like to adapt the cloud application, an application which is hosted in the cloud. Now, what a compliance driven configuration is, is something you can think of for example, a company itself sets itself some policies, some rules.

For example, they say, “I do only want to stop backups in (Place).” Or, “I do not want to open other ports than port 80 on my firewall, for example, or port for 443 to be on the secure side.” So, those you could think of compliance driven configurations, so based on compliance requirements, those configurations are set. Is that so far understandable? #00:09:53-9#

R: Yes, it is. #00:09:55-6#

I: Okay. Now, I have three risks here which might, or which ja, you can tell me that, which in the best case to say should hold for the presented use cases. And those risks are, and I will present you them, the risks that the cloud application provider, so Provider A, B, and C, I can also make it bigger if you do not that Google cloud provider/. #00:10:24-2#

R: No, it is okay. It is okay. #00:10:24-6#

I: That is fine. Okay. So that cloud application Provider A, B C in the respective use cases or case studies implements a contractually, not mutually agreed configuration. So that the provider implements a configuration that was not discussed on. Do you understand that risk? #00:10:47-4#

R: Yes, I do very well. Yes. #00:10:50-0#

I: Okay. The second risk, the risk that the implementation of a compliance driven configuration gets delayed due to slow or manual processes. You can think of now as the (Place) left the (Place) and a compliance requirement could be that backups should only be stored in (Place) countries. Now they need to change the storing of backups from (Place) back for example to (Place) or wherever. And this is a change in compliance requirements.

And now of course, the company needs to contact the cloud application provider and ask them to change the storage location. And here the question is, is there a risk or how do you see the risk that this gets delayed due to manual processes? #00:11:46-4#

R: Okay. Yes. #00:11:49-0#

I: It is clear. Okay. And the third risk is the risk of denying the implementation of a configuration in the case of a dispute. So, if there is a data leakage for example, and something goes to court that one of the parties says, “Whoa, that was not what we agreed on, or that was not what we implemented.” #00:12:08-9#

R: Okay. Ja. #00:12:12-8#

I: So, this is what dispute means? #00:12:16-1#

R: Ja. #00:12:17-4#

I: Okay. Ja. So, those are the three risks I would like to talk with you. And the first question here, do you think those risk might occur in the described case studies I presented to you? So, do you think these risks are realistic to ask that question maybe in a different way? #00:12:37-1#

R: The first one, most definitely. The second one, let me look. Yes. That might occur. Well, it will occur. And the third one, yes. That might also happen. #00:13:07-3#

I: Okay, perfect. So, then as we see all these three risks I would now ask you also to go through the case studies to the three case studies and rate all those three risks on the three case studies. So at the end, we should have nine risks determined. Three times three, for each case study all the three risks. Okay. And I would say we start with

Case A and/. #00:13:38-6#

R: And rate it according to your metrics. #00:13:39-9#

I: Exactly. According to the risk metrics. Ja. #00:13:42-0#

R: Okay. Case A, medium sized, headquartered in (Place). Okay. #00:14:02-0#

I: So, you can either say the probability and the impact and then the risk, or you just say the risk as you would like. I noted down here that you have it available. #00:14:14-3#

R: Ja. Just let me think about it in a moment. #00:14:18-8#

I: Ja, sure. Take your time. #00:14:19-9#

R: Okay. The first risk, not mutually agreed configuration, I think it is. I guess I need one clarification. Not mutually agreed. That is not meant by well, according to the terms of use, there have been some explicit agreements written down between Company A and Provider A. But there are also some terms of use for the services of Provider A, and the not mutually agreed configuration would be in accordance with those terms of use or would they violate them? #00:15:54-3#

I: You could think of, they are in terms of use, so they discuss it. Or the provider and company discuss it. However, there might be for example a misunderstanding or something misleading so to say, so it might violate it or not. #00:16:18-7#

R: I have got a quite specific use case in mind, and that is where the provider well, they are constantly optimizing their own services, and activate or deactivate some features in their service. They do this as outlined in their terms of use, but they do not seek explicit consent from the customers. So that would be according to your risk. #00:16:48-5#

I: Ja, exactly. That would be the case. So, there might be now a configuration on the customer side, which was not before and might now violate the compliance requirements of the company or this part of it. #00:17:03-6#

R: Okay. I would rate this risk as unlikely to occur and well the impact both companies are quite sizeable, so they usually do know what they are doing, and I would rate the impact as marginal. #00:17:32-9#

I: So, it is a high, right? #00:17:35-0#

R: Greater than ja, exactly. #00:17:37-8#

I: Okay. How would you like to proceed? Would you like to go from case to case to case with the first risk, or would you like to go with the three risks to Case One, to Case A to Case B and to Case C? #00:17:49-8#

R: By case study. First all three risks for Case A. So, the risk of the implementation of compliance within configurations delayed, the probability is possible, impact could be anything from legible to catastrophic. But again, both companies are sizable quite sizable and therefore probably skilled. So, I think it is again, marginal impact and that would be a medium. #00:18:50-2#

I: And last but not least? #00:18:56-0#

R: So, to clarify this one, that would be the case if well something happens and Company A would sue Provider A for negligence or whatever. And they dispute that they ever took that configuration like, “We never put your data in an (Organization). #00:19:26-8#

I: Exactly. #00:19:27-8#

R: Okay. That I would count as rare. Well, what would be the impact? Again, the impact could be anything, if in violation of GDPR and Company A would be sued for 10% of that turnout. Ah, what is 10%? Oh, it is marginal. Okay. So that gives it a no risk. #00:20:14-0#

I: Alright. I think you have the flow now. Let us continue with the second case study. #00:20:23-0#

R: Okay. Second case global player, one big one, the Provider B. The Google writing. Okay. Not mutually agreed upon configuration. In that case, I think that is quite likely a limited liability company. (Unclear)#00:21:23-1# by sales and headquartered in (Place). Okay. So, there is no face to face contact between those two. And in those circumstances that could go a lot wrong. So that would be could you scroll up the risk metrics please? A critical impact. And we would get to a higher risk in that case again. #00:22:00-7#

I: And the second one, the delay? #00:22:06-7#

R: Again, likely I cannot decide between marginal or critical, but both result in a high risk. So that is taking it as high. Denying the implementation of the configuration yes, again that is likely I would rate it again as a high risk. #00:22:40-6#

I: Alright. That runs good here. So, this third case study. #00:22:49-1#

R: The third case, the small ones with local provider. Was it local? No. #00:22:57-6#

I: Local farmer. #00:22:59-1#

R: Quite the opposite. The global provider. Okay. The risk of cloud applications, not mutually good configuration that is so to say certain and therefore the result in a high risk, whatever the impact may be. #00:23:18-9#

I: Just to inform you, if you are uncertain, you can either be high or very high, right? #00:23:27-3#

R: Oh, indeed. Okay. I guess, because it is a global player, they would not do anything on purpose critically impacting their customers, but there might be the case that the customer is not aware of the consequences from one of those changes. And I guess that is mostly in the negligible or marginal region, so I stay at high risk. #00:24:04-9#

I: Okay. And the automated process, the manual process, sorry. #00:24:13-8#

R: That is rather unlikely. Unless they ever get the idea of changing their provider, and it is certain. Well, though it is unlikely and what might be the impact of that? At this level, there is not much manual processing and a lot of automation. So, I guess the impact would be negligible. So, we have the low risk. #00:24:47-8#

I: Alright. Okay. #00:24:51-2#

R: The number appreciation that will not happen here. Again, everything is automated. So, this is rare. Although in this case, the occurrence might be rare, but as the company see is a very small company and little things might add up to large amounts for them, large amounts of money for them. It could have particular catastrophic impact. So, the risk is a medium one. #00:25:31-0#

I: Alright. That was really good. And that was already the most part so to say. Now is again, a bit listen part, and I will explain you my architecture for configuring cloud application. Yes, exactly. So, now I would like to explain you the configuration or the architecture for configuring cloud applications I developed during my PhD, and then we do again the same risk management here. So therefore, let me just show you that picture here.

And I hope, and let me just share it here, you can read it. And always if something is unclear, just let me know, I will clarify open questions. Okay. So, can you see it? #00:26:25-0#

R: I can see. I have to scroll a little bit, but it is clear, ja. #00:26:31-2#

I: So, the first thing is we have three parties in the proposed approach. The first party is a consumer, a person who wants to consume a cloud application. The second party is a provider of a cloud application. And the third party is the cloud application itself. Is that clear? #00:26:58-1#

R: Yes. #00:27:00-0#

I: Ja. Now what they do have, and this is something they create in advance via the blockchain, and this is the more or less only assumption you can do here because others ask me that question already also, whether they can assume that the blockchain itself is secure? And you can assume that the blockchain, so a text like 50 plus or something like that will not occur, and there will be a secure blockchain. You can assume that. So, you do not need to care about the blockchain itself, the security of the blockchain.

So, what happens is that those three parties first mutually create a symmetric encryption key together via the Diffie–Hellman protocol. Therefore, each of the three parties creates a Diffie–Hellman value, stores it to the blockchain, and takes it from the other parties from the blockchain. And doing that is a more or less three party Diffie–Hellman protocol for creating symmetric keys. Okay. Do you understand that? #00:28:01-9#

R: Yes. #00:28:03-5#

I: Okay. So at the end, the cloud consumer, the provider, and the cloud application itself have access to a shared symmetric key. Now assume that for example, the cloud consumer would like to configure in cloud application. Therefore, the cloud consumer takes that configuration, and you can think of a configuration as for example a (unclear)#00:28:30-9# an XML file or whatever a configuration of the application might look like, takes that configuration and encrypts it with the shared symmetric key, clear? So, I will always stop and then ask whether it is fine for understanding. Okay? #00:28:53-3#

R: Ja. That is okay. #00:28:54-3#

I: Alright. So, the consumer takes that configuration, encrypts it, and stores it on the blockchain via a smart contract, encrypted stored on the blockchain or the configuration. Now, on the cloud application itself, and this is the part here, the cloud application itself has a cloud management script. And you can think of the cloud management script as in back end application of the cloud application, which should be configured.

So, there is a script which monitors the blockchain, monitors the blockchain for changes in the smart contract and monitors whether a new configuration gets implemented into the smart contract, which it monitors. The monitoring itself to answer that question can be done on two ways, either on pulling or on pushing, meaning the monitoring either can be done every 10 seconds, #00:29:54-8# checks the smart contract whether an update has been created, or the blockchain itself pushes the information, if there is an update please have a look.

So, we do not need to care about how the monitoring mechanism is done. You can only assume that also this can be done. So, what the cloud management script does is it monitors the blockchain for changes of new configurations. And as soon as it detects the configuration, it downloads that configuration from the blockchain or to be more precise from the smart contract, and as it has access to the symmetric key, it encrypts that configuration.

In the next step, it stores that configuration in the path where the cloud application itself stores its configurations. So, in the case here, we for example talk about an intrusion detection system as a concrete example. And storing the configuration means just it overrides the text file and implements the configuration, which was originally stored on the blockchain encrypted. Is that clear so far? #00:31:07-3#

R: Yes, it is. #00:31:09-1#

I: Okay, good. In the next step, it monitors the lock files of the cloud application. In that case, the smart application or the intrusion detection application and monitors whether the configuration was successfully implemented. If the configuration was successfully implemented, the cloud management script triggers a backup of the virtual machine on the cloud provider side. So, what it does is more or less it triggers a backup from the virtual machine on which the cloud application is running. Clear? #00:31:45-7#

R: Ja. #00:31:46-7#

I: Okay. In the next step it takes that trigger, the backup creates the hash value, the cryptographic hash value to be more precise of that backup and stores the hash value back to the blockchain as the proof of configuration change, so to say. Now, the cloud consumer, so that person here who you originally initiated the configuration change has the possibility of also downloading that hash value.

So, if for example now there is this pool or something like that, the person can take that hash value and can ask for the backup fitting to that hash value and can investigate then so legal departments, for example, can investigate then whether or which configuration was implemented based on the provided hash value on which both parties agreed on. Is that understandable that approach? #00:32:49-5#

R: Yes, it is. #00:32:51-2#

I: Okay. That is already all I wanted to show you. And this is the general architecture idea. And if there are any questions later on, please let me know. And also, if you have right now any questions to that, please let me already know. If not, I have also some questions prepared here. #00:33:13-7#

R: Okay. Then start with your questions. Mine will follow, I think. #00:33:20-3#

I: Alright. Okay, perfect. So, the first or the only question I have here is, and this is again a qualitative and a quantitative question. So, first the quantitative question. I have understood the approach. And here again, I need a strongly agree, agree, a neutral disagree, strongly disagree. #00:33:41-6#

R: Agree. #00:33:46-0#

I: Okay. Would you like to ask something to that approach? This is my second question. #00:33:53-9#

R: I might get back to that question, but at the moment, no. #00:34:06-2#

I: Okay. Now I would like again, now ask you to assume that the providers in the case studies are now providing their services using the architecture I just showed you. So, they are configuring their application or their cloud application now via the approach I showed you. And based on that assumption, I would now like to ask you to again do the risk assessment. Alright? #00:34:43-1#

R: Alright. #00:34:45-0#

I: Let us do it. We do it as same as before. So, same conditions here. We start with Case A and the Risk One. #00:34:56-6#

R: Okay. Not mutually agreed configuration. That should not happen if everything works as designed. #00:35:11-8#

I: So, this is also something because that question came up also. So, what you not should assume is that the configuration gets perfectly implemented. So for example, if you have encryptions configured, there might also be implementation error. So, there might always be of course a residual risk of not having the correct implementation. So, this is something you should not abstract off. #00:35:36-3#

R: Okay. But it is still a rare occurrence. As long as I follow do not do your own crypto. So, it should be rare. Let us phrase it that way. It should be rare. Is it low or is it a medium risk? Based on my previous assessment, I took the impact as marginal, so that would give me together with a rare probability, a low risk. #00:36:26-0#

I: And to ask that information because others ask also that question, there is no intention of having someone in between who is doing any manual work on that approach? #00:36:45-2#

R: Ja. That would have been part of my assessment to state that there is by design no manual component in implementing the configuration. But there is still an element of automation, and that could be slow due to whatever. Again, the probability I would rate as rare. Again, a low risk, because the impact would be marginal unengaged. #00:37:30-0#

I: Okay. And the third one. #00:37:32-8#

R: Just a side note, try to tell (Person) that 10% of his turnover is negligible. Deny non-repudiation again, probability should be rare or non-existent. The impact, if anything on that scale could happen could be catastrophic, but what are we talking with Case A? Big and big. Okay. Again, a low risk. #00:38:23-6#

I: And I think you already could assume what will come now. Do it for case B. #00:38:31-2#

R: Oh, I am not prepared for that. Global player and Uber rating, here comes into play, do not assume that implementation is perfect, especially the crypto part. That is a question I could ask. Is the implementation of the blockchain and of the web application, is that the responsibility of the provider or the company or any third party?

#00:39:13-4#

I: Yes. So, everything which is on the blockchain is of course verifiable. So, even though if the provider implements it on the block, ja. #00:39:24-2#

R: You said the blockchain is the definition trustworthy. So that part is okay. Now, I take the question back. #00:39:36-0#

I: And the application for configuring would be basically a decentralized application, so something accessing the blockchain, which you could also then verify. #00:39:43-8#

R: Okay. In that case, I might have made an error in my previous assessment because this design does not prevent anyone from doing any not mutually agreed configuration. It just makes it impossible to hide. So, if the client is not vigilant and does not verify what is written in the blockchain, the provider could get away with doing anything that is not mutually agreed upon. Okay. But they got a Google rating of 4.3 based on 400 ratings. That is a start. #00:40:52-1#

I: As I said you can always update your risk. So, this is not set in stone. #00:40:57-5#

R: Ja. But together with the sizes of the companies involved in Case study A, I remain at low risk. So, for Case study B I think the probability that something not mutually agreed upon happens is a bit higher. So, it is in the possible range, but that it is very viable and detectable that they did it, the impact would not be too harsh. So, we get a low risk again. #00:41:45-5#

I: And the automatization for the manual process here, second risk for the second case study? #00:41:58-8#

R: Almost the same justification as for the first risk. And therefore again, a low risk. Probabilities higher than Case study A, but that does not change the risk that much that it would be a medium or even a higher risk. Okay, risk C, third risk. #00:42:25-9#

I: Yes. #00:42:27-5#

R: Again, that they try to do that. The company with that shade of gray, one to 50, I do not know. I would think they are likely to do some or try something like this, but they will not succeed. So, the impact will be negligible. That gives them medium risk. #00:43:03-0#

I: Alright. And surprisingly, we are now with the third case study. #00:43:12-8#

R: Okay. My lovely kibbutz victim to a global player, but not mutually agreed upon. The probability remains at likely to certain. Is it 90% or below? Okay. Likely I think, so this gives a medium risk. #00:43:50-4#

I: You get it. Alright. And the second risk? #00:43:57-7#

R: That is rare and negligible impact, so low. #00:44:05-8#

I: And the last one? #00:44:09-9#

R: Non-repudiation. Again, low. #00:44:19-6#

I: Oh, that was wrong, pardon. So, you again have the possibility of course to again, go through the risks and update any risk if you want. Just let know. #00:44:36-4#

R: And let me think about my last assessment. #00:44:38-7#

I: Ja, sure. Take your time. #00:44:40-7#

R: Because I rated the impact as negligible, but an association consisting of seven farmers might not be text savvy enough to do all that verification thing with the blockchain. Or is it implied that this is some easy to do task? #00:45:12-8#

I: So, you can assume that there might be a smartphone application on which they can do the configuration. So, there might be a beautiful UI UX. #00:45:21-9#

R: There is no beautiful UX. Okay. So, the design is for not that tech savvy persons. #00:45:36-5#

I: Yes. So, you can assume that the big company is able to provide a nice looking interface. #00:45:46-5#

R: As demonstrated again and again in the past. I remain with my previous assessment and this is a low risk. Okay. So, you may proceed. #00:46:04-7#

I: Okay. So, it is your final decision here? #00:46:07-2#

R: It is final. #00:46:09-2#

I: Okay. Alright. Then we are good to go. So, I do have another open question here. And the question is, what do you think about the use of the blockchain in that case? Does it make sense for you? #00:46:27-2#

R: With the implied trustworthiness of the blockchain? Yes. So, if the implementation is bulletproof and there are no known as of yet flaws in it, yes. That makes sense. Because it enables both parties to verify or assert what they did was agreed upon. #00:46:56-4#

I: And if you now think of maybe also other trust and generating approaches, like web of trust or PKI, could that be alternative approaches for that instead of using the blockchain? #00:47:12-3#

R: Cool. Let me think about this a second. Okay. In the case of a PKI we would not have a blockchain, so we would have some third party vouching for integrity of the participants, but there would not be any common element not of trust. But there would be no trustworthy storage for the decisions for the smart contract. Now at the moment, I do not see that PKI or web of trust would be a substitute for this. #00:48:08-5#

I: Okay. That is fine. I mean, you are also provided here an argue for, so I think it is as always you can also think about it, do not feel any pressure. #00:48:24-6#

R: Ja. I do think about it. Perhaps you could define web of trust a bit more. I think I have an understanding, but I am not sure if it is the same. #00:48:39-5#

I: So, in the web of trust, you generate your own private and public key and you meet other peoples or at least get in contact with other peoples, and add at their public keys to your trusted key store, and you can rate their public keys whether fully trust, half trust. And then if you have for example, two keys, you have trust, you can also assume that it is a fully trust, so to say. #00:49:04-7#

R: Okay, no. It would not be an option here either with the same justification as for the PKI, because we might end up with trustworthy certificates or keys or whatever, but we have no common storage or no common secure storage for our smart contract. #00:49:28-0#

I: Okay. We are slowly coming to an end of the interview. And now that you have seen and I think we already discussed a lot of, just a few questions here. Do you think the presented approach improves the transparency of cloud application configurations? #00:49:54-0#

R: Assuming that the implementation would be truly according to that design? Yes. That would have this transparency. I cannot see any currently available cloud service doing this, but if they would do it, it would improve transparency. Yes. #00:50:35-0#

I: And also the same question for automization. Do you think the percent approach can help to configure cloud application in an automated way? #00:50:46-8#

R: It helps because they have to, there is no other way. Yes. #00:50:55-7#

I: Okay. And do you think the percent approach can help to investigate security incidents more easily? #00:51:04-1#

R: Absolutely. Because of the inherent capabilities of a blockchain. #00:51:11-5#

I: And do you think the percent approach can help to identify responsible parties in a legal secure way? #00:51:19-8#

R: Ah, that is a good one. I am not sure at the moment. I need to think about it because we are within symmetric encryption key here. #00:51:49-9#

I: That is correct. So, the configuration itself is symmetrically encrypted, but just for explanation if you store something on the blockchain, you need to digitally sign it. So, each storing on the blockchain is also related to digital signature. #00:52:07-2#

R: Ah, okay. Ah, here comes PKI again. Okay. In that case, if it is digitally signed and blockchain is temp proof, then yes. Whatever your question was, I answer with yes. #00:52:26-9#

I: So, do you think the presented approach can help to identify responsible parties in a legal, secure way? That was the question. #00:52:34-4#

R: Yes, I do. #00:52:35-0#

I: Okay. Perfect. Alright. Final question in the main phase. Now, you have seen everything and you have evaluated the approach. And now again, the word is on your side so to say on the last question. Do you see any advantages to the approach where it could be improved? Do you see any disadvantages where it could be improved, and any advantages for the current existing approaches? That is how I would like to ask the questions.

Or do you see any new upcoming risks using that approach? And you can also discuss it with me if you want. And if you have nothing to add, you can also say it is fine. So, it is/. #00:53:23-8#

R: Again, I need some second to think about it. #00:53:27-6#

I: Ja, sure. #00:53:28-2#

R: The disadvantage I see with this approach disadvantage it relies on the services provided by the web application to be able to put into a single container like a classic hardware computer, just as an abstraction into (unclear)#00:54:21-0#. And then you can take your snapshot and create the hash in case of any services not compartmentalized in that way, like email services from large, very large providers who do not have your own compartment in that service as a customer that I think it would be difficult to implement it in this way.

Again, any currently existing cloud provider I know would have a hard time implementing this. But I think some of them deliberately designed their services to be divided into smaller pieces. So, the solution might not be viable for any generic cloud service. So, the first part of the question was what advantages, you know what I could improve or what I think could be improved on the design? #00:55:57-2#

I: Ja. So, any improvements or weaknesses, so to say. #00:56:00-2#

R: Weaknesses. For that assessment, I would need to think about a lot longer. On your drawing of the design, you included specific techniques like python and power share. #00:56:33-4#

I: Ja, exactly. This is just to make an abstract architecture more tangible. So, there is no generic implementation you need to think of. This is just how it could be that you have an imagine of how it could look like. #00:56:50-1#

R: Okay. But the design is, what would you call it? Technology agnostic or whatever. Can take any technology you like as long as it adheres to the specifications. Okay. #00:57:07-1#

I: Exactly. #00:57:08-0#

R: Now I am sorry, I have no improvements to make at this point. #00:57:15-9#

I: That is also fine. Do you see any new risks with that? #00:57:25-5#

R: One risk is my battery is running low. It is at 10%. The warning for 20% came 50 minutes ago. So that is enough time, I think. Any new risks? No, I think the risks remain broadly the same. As a customer, I have to rely on the provider that they are able and willing to implement this design according to the letter, with intent. This is the same risk we have. Ja. Okay. Ja. #00:58:17-4#

I: Alright. I definitely do not want to interrupt you, so. #00:58:20-1#

R: No, I cannot think of any additional risks at the moment. Maybe if you finish your dissertation and do a startup after that, I sue you because whatever risk occurs to me. #00:58:38-4#

I: Okay. I think we can close the main phase with that, right? #00:58:46-2#

R: Okay. #00:58:47-5#

I: We discussed everything here. We came to end. You had opportunity to bring in your thoughts. So, now you have heard really all my questions, you have joined me in the dissertation topic. In school grades, how would you rate your statements you have provided here during that interview? Do you think/. #00:59:11-3#

R: My own statements? #00:59:12-0#

I: Your own statements? Yes. Do you think you were you verbal with what you said or are you totally unsure with what you said? And that rating please in school rates, German school rates, between one is a very good and six is insufficient. #00:59:29-8#

R: I would rate it, I guess two. #00:59:37-9#

I: Okay. That was my closing question. So, thank you very much for your openness, for the participation, and your time. As said, the outlook will be that this will now be transcript, anonymized, and used for the evaluation of my dissertation. Thank you very much. I will stop the recording. #00:59:59-9#

R: You are very welcome. #01:00:01-3#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #8:

I: Welcome to the interview of the evaluation of my PhD. Thank you for your time. Let's start. So, before we start with the evaluation, I would like to get you a bit better known and therefore, I have some background questions for you, and you can answer them as widely as you would like to answer them, or you can also just briefly answer them. The first question is, can you tell me something about your professional background and your daily routines? #00:00:42-0#

R: Well, thanks for having me [Person]. And I'm a computer science student, graduate student from [Organization]. I've just completed my master's thesis and focused my studies on the last semesters in high-performance computing. Well, usually from a daily perspective, I'm waking up, making coffee, eating something for breakfast, and then going on my computer to work a little bit on my personal projects. Some scripting, nothing very huge and searching for jobs currently. #00:01:27-0#

I: Good, thanks a lot. And can you in a bit more detail explain to us what you studied in detail and what was your master's thesis about? #00:01:39-0#

R: I'm in the department of performance computing, I've studied mainly on, the main interest in this research area is the field of performance modeling. My master's thesis was about trying to predict or creating a model for performance prediction for the (uncl.#00:02:01-0#) vector processor architecture that is widely used (uncl.#00:02:06-0#) in high performance computing, but a traditional vector computer processor architecture often used in previous computations that differs significantly from general (uncl.#00:02:19-0#) architectures, for example, that is the main process architecture in nowadays computations or nowadays computing in general, also amongst the consumer products. The prediction was performed on a mathematical model, that should be precise in theory, but lacked some preciseness in the terms of performance predictions due to some currently unknown constraints that are given and imposed by a translation from different architectures to each other. The master's thesis contained a mathematical approach that is analytically precise, but, on the other hand, as already mentioned, lacks some background information, some model information that could have been filled with artificial intelligence or machine learning, but that was not employed under the thesis at all. #00:03:18-0#

I: Right. Do you want to add something or it's fine? #00:03:24-0#

R: I'm fine with the explanation or the short overview. It is more or less also the same or similar to what I've done in my previous seminar thesis and also my bachelor's thesis on a different level, of course. #00:03:43-0#

I: Okay, yeah. Thanks a lot. It's really interesting topic, to say. Besides that qualitative, I also have some quantitative questions. Meaning, I give you a statement and I would like to get, and I would like to ask you to answer that statement with one of the five answers. The one/ the five answers are strongly agree, agree, neutral, disagree, strongly disagree. So, I will give you a statement and ask you to provide an answer for the statement based on the five values I provided you. Okay? #00:04:19-0#

R: Okay. #00:04:20-0#

I: So the first question I have, your first statement here is "I am a computer science expert." #00:04:27-0#

R: I agree. #00:04:29-0#

I: "I am an information security expert." #00:04:33-0#

R: I neither agree nor disagree. #00:04:40-0#

I: So it's neutral, right? #00:04:41-0#

R: Neutral. Yes. #00:04:42-0#

I: Okay. "I'm a cloud computing expert." #00:04:44-0#

R: And neutral again. #00:04:46-0#

I: And "I am a cryptography expert." #00:04:50-0#

R: I do not agree. #00:04:53-0#

I: Disagree? #00:04:54-0#

R: I do not agree. #00:04:56-0#

I: Yeah, that means disagree, right? #00:05:00-0#

R: Disagree. Yeah. #00:05:02-0#

I: Okay, perfect. Yeah, perfect. That was already the warm-up and introduction part. So, having that part completed, we are directly entering into the main phase. And in the main phase, the three case studies are the most focused one or the ones we are just talking about now. So, the first question I have here is, do you understand the case studies? #00:05:28-0#

R: Yes. I understand the case studies, but I would like to hear a small recap on them, because it has been some time since I have read them. #00:05:38-0#

I: So, the first company, company A is a mid-sized company, it makes about 80 million on turnover per year. And it's ISO certified led by a female CEO. This company would like to implement an accounting system based on a SaaS software, Software as a service cloud application. Now, this company gets an offer from provider A. The provider A makes a yearly turnover from about 180 million euros, it's a limited liability company, in Germany you would say GmbH, and is certified according ISO 27001. The company/ provider A sells exclusively online without sales contact and has its headquarters in Europe. So, it's a headquartered company in Europe, provider A. Company B is a huge chemical company, which produces mainly for chemical and for pharmacological industries. This company would like to/ this company is more or less victim to hacktivism. So they have a lot of hacktivism ongoing and outside and people who do not like what they are doing. Therefore they would like to implement intrusion detection system. This intrusion detection system should be based on again, a SaaS application and should be offered by the cheapest company available. So, they make an offer, "Ausschreibung" we would say in Germany, and based on that they take, from three offers they take the lowest price and would provide it to the company who has the lowest price in implementing this (uncl.#00:07:34-0#) detection system, which is company B. Company B is hosted in India and company B is not certified at all, but it has a Google rating of four, three from one to five stars. So, in average four to three stars. Company C, company C are farmers. They are producing goods. They would like now, not only sell their goods on a market, but they would also like to sell their goods online. In that case here, it is like/ these are goods which get bad really fast, and bad quality. So they need to sell it quite fast. Therefore they would like to have an online website and on that the website, they would like to be very flexible and adjust the website, based on their needs and based on the products they have right now to sell. And therefore, they would like to have a website as said, based on a SaaS again, and here company C offers them a free SaaS application, free website based on the contracts they already have and using that contract or this SaaS application, they would like to sell their goods. The company C is a huge company based in the USA and is certified based on all existing or all current usually provided certifications. Yes. So this is the rough overview about those three. Understood? #00:09:09-0#

R: Yeah. I'm fine with that. I would like to proceed from scenario to scenario and not rating all in a row. It would be easier to recap. #00:09:25-0#

I: Okay. Just give me a second, okay? #00:09:27-0#

R: Okay. #00:09:28-0#

I: Before we start rating, the first question I have is, have you ever heard about risk management? Because we would like now to do risk management here. You already mentioned that we are going to rate them, but have you any experience with risk management? #00:09:46-0#

R: Not from a professional point of view, but we attended the lecture/ I've attended the lecture of, what was it named? Software Project Management, or something like that in 2019. Risk management was one of the topics that was covered there, in which the risks were correlated to the potential outcomes or possible consequences to estimate damages to/ damages or profits, either way to a company. #00:10:26-0#

I: Also we have this risk metrics here. This is probably something you've then seen already in the lecture. So, a risk is basically depending on two factors, on its probability, how probable is that a certain risk arises and how big is the impact if that risk arises. So if you have a, for example, a low probability that risk arises and low impact from the risk, then the risk is not very high, it's low. However, if you have a high probability for a risk and also a high impact, impact, meaning on financial perspective, then of course it's a very high risk. And based on that, we do usually risk estimation or risk management. And I think this is also what you just mentioned. #00:11:15-0#

R: Exactly. #00:11:15-0#

I: In that risk matrix, I think, you quite fast get it. If a risk is the probability is below ten percent then it's called rare. If it's higher than 90 percent we call it certain, and everything between here is named as written here. Furthermore, if a risk is from financial perspective, lower than ten percent of the yearly turnover of a company, then we call it negligible and so on and so forth. So I think the idea of the risk metrics is clear. Just to confirm, is it clear? #00:11:48-0#

R: It is clear. #00:11:48-0#

I: Okay. So the question I have here is, did you understand the risk management metrics? #00:11:56-0#

R: From my perspective, I understand the metrics. #00:12:00-0#

I: Okay, perfect. Do you think risk management in the scenario I described here, so adopting a cloud application, do you think risk management makes sense? #00:12:11-0#

R: Well apparently, if one has to estimate and to analyze in which areas possible risks and possible impacts in the business of companies are positioned, then the risk management analysis using the risk of risk analysis metrics can help to identify those risks on, not to identify, but rather to identify the impact and in which areas a special focus has to be put on, when designing special services or performing certain decisions. #00:13:05-0#

I: Okay. Yeah, fine. So based on that, we, I identified in my thesis or in my PhD thesis dissertation, three risks, which from each of those cases could occur. And I would like to explain you those three risks quickly, okay? #00:13:25-0#

R: Yeah. #00:13:27-0#

I: So the three risks we would like to analyze and to rate are, the risk that the cloud application provider implements a contractually, not mutually agreed configuration. Then we have the second risk, the risk that the implementation of compliance driven configuration gets delayed due to slow or manual processes. And last but not least, the risk of denying the implementation of configuration in case of a dispute. Those are the three risks which are, got identified during the PhD and which will be considered during the PhD. And I would like now to ask you to rate those three risks based on the risk metrics and based on the scenarios and on the architecture you've already seen here. No, not on the architecture. Sorry that was not correct. I need to cancel that. I just want you to answer the risks based on the case studies presented here. Okay? #00:14:31-0#

R: Okay. #00:14:31-0#

I: So we start with the first risk and then// #00:14:37-0#

I: Okay. The first risk was, the cloud application provider implements a contractually not mutually agreed configuration. Well, the risk is always given, I suppose. It is from the probability likely. Possible to likely, I would suppose. Even if the contract especially lists all the points that were agreed on, upon the contract, in German in the so-called "Pflichtenheft", then there are some degrees of freedom the developers and the implementers can proceed to realize the implementation. So it is possible, I think possible, not likely but possible that the agreed contract, the/ sorry, I think/ the contractually mutually agreed configuration may slightly differ, so it is possible. And from the impact point of view, I would say it depends in which context of the configuration is altered. When it comes to legal regulations, for example, in medical terms, medical regulations, then the impact of small differences from the specification can have a very high impact, a critical impact, but in other points, for example, in (uncl #00:16:44-0#) web pages, when, for example, an image is delivered before, whatever, JavaScript or something like that, the page might break or could break, but the impact is not that high, especially from the point of view when considering profit margins or liability. #00:17:11-0#

I: So at the end, it's high for you, right? #00:17:16-0#

R: It is. It is high, yes. #00:17:16-0#

I: Okay. #00:17:18-0#

R: It is possible a marginal to critical, have a marginal to critical impact. So I would rate (uncl #00:17:26-0#) the worst case scenario a high, high risk. #00:17:29-0#

I: If you want we can also go faster through it, if you would like to explain it for sure, but you don't have to explain it in that detail if you don't want to. #00:17:39-0#

R: Okay. #00:17:39-0#

I: That was for company A, right? So the first risk was the high, and now we come to company B. #00:17:50-0#

R: Company B, global player, head (uncl #00:17:52-0#). Yeah, there I would rate, as mentioned before, depending on the department in which this specification has made chemical products, have a very high security clearance. So this, the probability could be lower, potentially be lower that the specification is added. But on the other hand, the impacts on small deviations from the specification have a very high impact, a critical impact on the risk is high, very high. Yeah. With respect to the risk metrics. #00:18:51-0#

I: Yeah. And the third one, company C? #00:18:55-0#

R: What was it? Farmers from (uncl #00:18:58-0#). Okay. Well, for farmers the security may be not that of a problem. Yeah. For selling some goods locally, I would suppose deviations may occur with respect to the initially agreed configuration, but the impact might not be very high or not critical. So it is still a high risk that if something goes wrong, then it may impact the business or the pharma corporation or the pharma association to a not severe, but also not a mild impact, still a high risk. Yeah. #00:20:07-0#

I: Okay, amazing. That was it already for the first risk. And I think we are good on track. So, I would say we immediately continue with the second risk. The risk that the implementation of compliance driven configuration gets delayed due to slow or manual processes. So a configuration change occurs. And now the question is, is there a risk that this might cause damage for, or is there the risk for the companies? And if yes, how high is that risk? And we start again with company A, as you already did perfectly. #00:20:45-0#

R: Yeah. Well, if there are delays in delivery or in, yeah, delivery/ let me think about that for a moment. It delays, especially for companies with services. Okay, well again, if/ I would say that this still depends on the domain in which the company resides in. But on the other hand, delays always have a moderate to high impact depending on the contracted failure clauses or "Vertragsverletzung Klausel" in German. I think so, delay is always a high risk, if a delay occurs. #00:22:13-0#

I: So for all the three cases, you mean? #00:22:16-0#

R: Yeah, it is always high. Sometimes delays cannot be circumvented, they simply occur to some (uncl #00:22:30-0#), unforeseen consequences, that can always happen and is always a high risk in every kind of business. #00:22:36-0#

I: Perfect. Then I take here high, high, and high for all three scenarios, right? #00:22:12-0#

R: Yeah. #00:22:48-0#

I: And last but not least we are having an incident or something happened and now it goes to court. And the question is now, how would you rate the risk that one, or the provider in that case, denies to having implemented something or denies that something was configured as (uncl #00:23:11-0#), or as it says here, "The risk of denied implementation of a configuration in case of dispute."? So there's dispute and someone says, "No, that was not what we discussed on. That was not how we agreed on." #00:23:24-0#

R: Yeah. So, in principle there's a contract in which specifically contracts/ the agreed upon configuration. So the contract already contains the specification, and it's also a hint if not the absolute, the proof that something is not right, because both parties have agreed and signed the contract. If some party overread something in the contract, then it is in the fault of the contractor that has (uncl #00:24:19-0#) signed the contract because of not understanding, in case of not understanding or not fully being aware of what the contract is about. But the implementation, if there's something implemented/ I have a question once again, if you're allowed into this scenario, the risk of (uncl #00:24:45-0#)implementation, then the contract is given, they have both signed and understood was what was written in there? #00:24:53-0#

I: Yeah. #00:24:54-0#

R: All right. So the implementation is then delivered and the party that has to implement denies that the implementation was done by fault.#00:25:11-0#

I: So, usually if you are buying a SaaS application or software service application, you are not negotiating every single configuration step. You are more or less negotiating SLA, so software license agreement, soft, service level agreement. Sorry. So you say, for example, the service needs to be delivered 99 percent a year, or you agree on where the configuration or where the service should be delivered from, so they provide a location and so on. But you do not negotiate. for example, (uncl #00:25:49-0#) should be open or whatever. So technical configurations are not negotiated during a contract, as the contracting negotiating partings usually do not have that experience to negotiate that. So those are things which will be later on either configured by a request from the client, or the company or the provider itself does it automatically or by default configurations. #00:26:13-0#

R: Okay. So if I understand this correctly, the, I call it call the parties license. So if you agree the license of the contract that implements, or should, it's called to implement this specific service, contracts some subservice providers and has no full control over the implementation itself. Am I right? #00:26:41-0#

I: That's a scenario from the possible scenarios. You're right. #00:26:46-0#

R: Okay. So, from that point of view, if the/ how did I call them? The licensee/ the implementer. If the implementer uses, for example, a center, computing center based on the specification, for example, in Germany, but the computing center has some own configuration that cannot be circumvented, but fulfills in graph or in the frame of the contract the specification, then yeah, the implementer has no, only to a certain degree influence on the specific configuration as you already mentioned. So if there are any differences in configuration and the implementation, the specific implementation on hardware basis, for example, is not done by the implementer himself, then there might be a moderate to high risk that this could be the case. It is likely, it is possible. It is likely if some hyper vendors, hyper providers, compute cluster providers for example, have a specific configuration that do not fully match the specifications from a technical point of view. Then it is likely that deviance/ and if you could open the risk matrix once again. Yeah, in case of, for example, if the computing center can provide GPUs, but do/ for GPU computing, for example, but does not offer the latest configuration of the latest generation that was requested or was intended to be used by the contractor for developing, for example, on the latest technology, then there can be a critical impact. So a likely, from the likely possibility and the critical impact there's a high risk that something is not as it should be. And especially also in court, there's a high risk that either of the parties could be right, given right. Yeah. #00:29:32-0#

I: Okay. So your ratings are? #00:29:40-0#

R: There's a high risk. (uncl #00:29:44-0#). #00:29:44-0#

I: That's for company A, right? #00:29:46-0#

R: That's for company A, for hundred employees. Yeah, AI company, I think it was. #00:29:53-0#

I: The ratings for company B and C? #00:30:01-0#

R: Global player. Chemical products is, again, a high security department, high security clearance department. So, any deviance may cause a huge amount of, well/ how to call it in English? In Germany is "Strafzahlung", if there's something wrong. So it is not only a high risk, but a very high risk if something is not as contractually mutually agreed. And in case of court, there might be a very high "Vertragsstrafe", "Gerichtsstrafe or Strafzahlung" if something is not, from that point or from the change of configuration, not implementing or denying. Very high risk of losing a lot of money, possibly also the allowance to enter some markets. #00:31:11-0#

I: And company C? #00:31:15-0#

R: Yeah. Again, from, solely from the metrics it is a high risk. It is likely that someone can deny a configuration if the contractor itself, himself, the implementer himself uses some subcontractors or subservices. And from that also/ selling locally. (uncl #00:32:00-0#). I think/ yeah, I think if the farmers or the pharma association also has some contracts they have to fulfill, then the outcome or the risk that they are facing in court may be also high. #00:32:38-0#

I: Perfect. I think then we are through it already, right? #00:32:47-0#

R: Yeah. #00:32:48-0#

I: Then// #00:32:49-0#

R: From the initial scenario. #00:32:50-0#

I: Yeah, the initial scenario. Then I would like to provide you with the advanced architecture or the, not the advanced architecture, the architecture developed during my PhD. So as a short summary of the architecture, in the architecture itself we have three parties. It's the cloud application consumer, the cloud application provider and the cloud application itself. The cloud application consumer and provider are more or less the same persons but having different private keys, so they act as the same role so to say. The cloud application consumer is able to note down its configuration he or she would like to set on the cloud application, based on regular (uncl #00:33:37-0#) codes. So for example, you can think of a JSON file. He or she can then start this configuration file on the blockchain. On the application, or to be more precise on the virtual machine in which the cloud application runs, a script called cloud management script runs this script regularly/ do you hear me? #00:34:01-0#

R: Yes, I hear you. #00:34:03-0#

I: Okay. This script regularly monitors the blockchain for the changes. If it detects that the configuration was changed on the blockchain, it downloads that configuration, it encrypts that configuration. I forgot to say that this configurations of course stored encrypted, the encryption keys created between the three parties via the Diffie–Hellman key-exchange protocol, so they all have the same symmetric key without knowing the key of the others. Using the decrypted configuration or the decrypted configuration is then started into the cloud application by the cloud management script. You can think of Linux, everything is a file so to say, so also the configuration is a file. And that file is then started in the config folder of the cloud application. The cloud application is then implemented such that it uses the newly set configuration and follows that configuration. If everything is fine, so if the lock file of the cloud application says, "Okay, new configuration was successfully implemented", the cloud management script detects that and also triggers and backup of the virtual machine in which the cloud application is running. It then creates the hash value of that virtual machine, and starts the hash value on the blockchain such that every user, so the cloud application consumer and provider has the chance to contact blockchain and see the latest successfully implemented hash value of a virtual machine. That's the basic idea. #00:35:37-0#

R: Okay. #00:35:38-0#

I: Okay. So based on that architecture, again, we go back and I would like to ask you now to, again, rate the risks described here. So the risk of implementing a contractor and not mutually agreed configuration, slow manual processes, and the configuration case of dispute, based on the three cases we do have here.

Okay, understood? #00:36:03-0#

R: I understood. #00:36:04-0#

I: Okay. So first, before we go into it, maybe the question, have you understood the approach I've presented to you? And here again, strongly agree, agree, neutral, disagree, strongly disagree. #00:36:16-0#

R: Strongly agree. #00:36:18-0#

I: Perfect. So, and then I already spoiled it a bit, I would like you to do the risk assessment again from the three companies, based or assuming we have the architecture I presented you here, implemented, or the provider have implemented the architecture I just presented to you. Okay? #00:36:39-0#

R: Yeah. So, from the first scenario, "The risk that the cloud application provider implements a contractually not mutually agreed configuration." Well, the possibility also exists in all scenarios, but due to the blockchain implementation that is responsible to automatically configuring, if I understand correctly the service, then the blockchain as a contract record always contains the correct implementation, also foreseeable or viewable, reviewable by both parties. So the possibility exists, but due to the blockchain any change made on the blockchain is visible and can therefore be, what you say, can be verified. So the impact is not that high anymore. And if it is possible, I do not know whether this is the case, but one can or could always play back or replay a successful or correct configuration because the blockchain is one way recorded, if I understand technology correctly. So all configurations that are correct can still, can always be replayed. #00:38:19-0#

I: True. #00:38:20-0#

R: So, due to the fact that still there's the possibility that not mutually agreed configuration is deployed, it's still possible. It is not a high risk anymore because of the backup possibilities. But I would rate at medium, especially in the case if the change or the not neutrally agreed configuration isn't detected immediately. #00:38:45-0#

I: For all three scenarios, right? #00:38:50-0#

R: For all three scenarios. Yeah. #00:38:52-0#

I: Okay, perfect. That was already the first risk. So the second risk, the slow or manual processes. #00:38:58-0#

R: Yeah, slow manual processes. As mentioned before, on the first risk analysis, it is always the case that things can happen, things that cannot be foreseen. So it is still a high risk. For example, if the technology or the redundancy of your approach does not work because of some of failures or whatever, then if there are at down times, if there goes something wrong, it goes wrong. It is always a high risk that something can go wrong. Yeah. So high for everyone, for every party. #00:39:37-0#

I: Okay. And last but not least, we go to court and someone denies to have implemented something. #00:39:45-0#

R: Well, denial is not possible in the case of blockchain. Because this is clearly recorded, clearly noted who made a change on the blockchain. It cannot be deleted afterwards, the blocks are fixed. So the blockchain is the proof that something was utterly wrong or everything is contracted. So there's a lower risk. #00:40:09-0#

I: All the threes, right? #00:40:12-0##00:40:13-0#

R: All the threes, especially in court. The blockchain is the proof that either one party misbehaved or whether they behaved correctly. #00:40:23-0#

I: All right. That's it more or less already for the risk assessment. And the next question I have here, and I think you already answered it during your explanations, do you think the use of the blockchain makes sense in this approach? #00:40:42-0#

R: Well, especially in, with respect to the liability or the denial of having implemented something, the blockchain really is a help, it can help keep track of all changes as a non-modifiable record. So it makes sense, especially from the legal point of view. From the automatic configuration, I'm unsure whether it would be vet of a benefit. Especially, also I do not know how much performance implications the blockchain calls may have on the overall application or service performance. I cannot foresee a model of that right now. So it is a bit unclear to me which impact this might have, but an automatically configuration is always, especially if the service should be scalable, a very good approach. See, for example, the use of IPv6, IPv6 configures the address basis automatically from the host's perspective rather, but rather than being configured by a centered entity or network of centered entities due to the scalability issues with the older IPv4 address basis. So from a scalability point of view, blockchain or a record unified, distributed unified, automatic configuration is also a benefit. #00:42:16-0#

I: Correct, thanks a lot. And having a few last questions, I mean, you already answered that the point of optimization, and I understood that you're not really sure, and you also think that it's also a kind of a process question also not only a technical question, but also a company internal process. But other questions I do have is, do you think the provided approach here improves the transparency of cloud application configurations? #00:42:47-0#

R: By the transparency, the transparency will be provided for sure, because both parties are all involved parties in the contract if I understand your architecture correctly, are able to review the blockchain. So each change and each configuration can be seen and can be evaluated and verified by each party. So the configuration is transparent. You have, you do not have to rely on the word of the implementer that specific configuration is made. You do not have to trust them anymore. You can trust on the configuration itself because it is recorded on the blockchain. #00:43:36-0#

I: Perfect. And do you think the percentage approach can help to investigate security incidents more easily? #00:43:47-0#

R: Yeah. Once again, from that point of view also, because the configuration is presented on the blockchain. The server, if they are working as intended and also applying the configurations as intended, then it can be assumed that the server follows strictly the configurations that is written to the blockchain, and therefore configuration issues, not implementation issues, but configuration issues could be identified on the blockchain. If, for example, a bad compiler or malicious compiler compiles code in a way that you always have a backdoor in some code for example, some program for example, then the configuration on the blockchain will not have either. At some point there you have to trust that at the lowest level, in the dependency degree, the leads or the notes are trustful and trustworthy, that they're working as intended. And from that point of view, if they are working as intended, and if you trust the notes themselves, then security can be more easily investigated based on this approach. From my view. #00:45:00-0#

I: Perfect, thanks a lot. So final question before we finish the main part. Overall, how would you evaluate the presented approach? Would you like to add something? Do you want to see something in future? Do you have any potential? Do you see any potential for improvements or any weaknesses? So to summarize it, the word is yours. Would you like to add something to that branch? #00:45:26-0#

R: Now, let me think for a moment. #00:45:33-0#

I: Yeah, sure. #00:45:33-0#

R: Well, I suppose that the blockchain would not grow (uncl #00:45:40-0#) like, for example, some value transactions like Bitcoin also. Because the blockchain, once again if I understand correctly, is not (uncl #00:45:51-0#), is not deliverable or blocks of content or records are fixed or are existent forever. It can be the case in some years, if extensively used, that the blockchain grows from a storage perspective, that is just a storage limitation, that the storage may be the limitation for using the approach. But in contrast to the Bitcoin, for example, as mentioned earlier, the/ currently I do not see why this could be the case, especially if in sometime in the future the technology might change again, that the block blockchain has or remains in a (uncl #00:46:46-0#) handleable size, a reasonable size to be handled. That was my only remark. But I think, this would only apply if the configuration of the approach would be unified, unified used on a global scope for all corporates, corporates and associations. For a single association or single corporation this should not be a limitation, I think. #00:47:22-0#

I: Okay, cool. Thanks a lot. And that's it more or less. I have a final question and then I would like to close that. So you've now heard all the questions and have joined me in my dissertation topic. In school grades, how would you rate your experience in that area presented and how would you rate the answers you have provided here? #00:47:51-0#

R: Can I hear the question once again, please? #00:47:56-0#

I: Yeah. So you provided a lot of statements and you said a lot, and you have heard a lot from my side, you have learned a new architecture, we discussed a bit the architecture. In school rates, how confident are you with the answers you provided? So in school marks. So from one to six, European school or German school. #00:48:17-0#

R: Okay. In German, I would say one minus to two plus. In American or English, A minus to B plus I think, would be the quality of my answers. #00:48:31-0#

I: Okay. #00:48:31-0#

R: With my background in computer science. #00:48:33-0#

I: Perfect, thanks a lot for your openness, for your participation and time. As already mentioned, the next step will be the transcription, the anonymization and the use for the evaluation. And having that said I would stop the recording, and thank you very much for your time. #00:48:53-0#

R: Thank you also for being here. #00:48:55-0#

(End of Interview)

TRANSCRIPT INTERVIEW PARTICIPANT #9:

I: (Foreign language) #00:00:02-0#

R: Ready for take-off. #00:00:06-9#

I: Yes. So, welcome to the interview where recording started, and I think we can already start through. So, as already explained, the interview has several phases, and after the information phase, we are now in the warm up and introduction phase. And during that phase, the aim is to get you a bit better known. And therefore, I prepared some questions. I have prepared some qualitative and quantitative questions. So, we start with the qualitative questions where we would like to hear about-, something about you. And this is also the first question I've written down here. Can you briefly tell me something about you, your professional background and your daily tasks? #00:00:50-0#

R: Of course, my name is (Person), I'm working in the field of IT security for around about twelve years now. Before that, I made an apprenticeship at (Organisation) for three years. And yeah, (Foreign language) #00:01:10-7#. After that, I joined a company who did, you know, some tasks in the field of information security, where I worked as a consultant in the field of telecommunications mainly.

And in the year 2019, I joined (Organisation) as consultant, sorry, as specialist for data leakage preventions. Means that all the traffic that was outgoing from the bank was scanned by all the servers and analysed by the rules that we have got written. I was the one who wrote the rules, administered #00:01:50-4# the infrastructure, made some kinds of internal management. And after that, in April this year, I followed some colleagues of mine who founded a company and made, are doing a lot of information security stuff again, mainly building information security management systems and yeah, some minor tasks of awareness. #00:02:15-7#

I: Amazing. (laughs) No question stayed open. So, we know how long you're working in cyber security on the working area. We know your professional background. So, so perfectly answered that question so to say. All right. So, I think we have already a lot of qualitative background. And now, as said, also some quantitative statements, and here as already explained in advance, I prepared some statements, and I would like to ask you to answer that statement with a strongly agree, with agree, with a neutral, with a disagree and with a strongly disagree. All right? #00:02:53-3#

R: Yeah. #00:02:54-0#

I: So, the first statement is I am a computer science expert. #00:02:57-3#

R: I would agree on that. #00:03:00-3#

I: Mhm. I see. I'm an information security expert. #00:03:04-9#

R: I would strongly agree with that one. #00:03:07-2#

I: Mhm. I'm a cloud computing expert. #00:03:10-1#

R: Two of five, that was, the one below neutral was? #00:03:19-2#

I: Disagree. #00:03:20-5#

R: Disagree. Okay. #00:03:22-1#

I: Okay. Disagree. And I'm a cryptography expert. #00:03:27-7#

R: Neutral. #00:03:29-8#

I: Amazing. That's it already. So, this is already the background, the scope is clarified. We know what you did, we know your background, we know your skillset so to say for that focus area here. So, the warm up phase is from my side ended. And we would directly go into the main phase. In the main phase, we will compare, or we will have a look at the case studies I already shared with you, you read through. And here, my first question is do you understand the case studies? #00:04:01-6#

R: I think so, yes. #00:04:04-0#

I: Okay. This is an open question, so, you can-, this is not yes or no. If you have any questions, you're always welcome to ask. Let me know if something is unclear here. Okay? #00:04:16-6#

R: Of course. #00:04:17-1#

I: And the next question is, and this is just again an open question. Do you think these cases are realistic? #00:04:24-7#

R: Let me just have a short look again at those cases. I think that the first case regarding company A is a realistic case. I think the case around company two is also a very realistic case, and I would say that the case around company C is also a realistic case. #00:05:15-5#

I: Okay. So, you think all the cases are quite realistic, right? #00:05:19-2#

R: Yes. #00:05:19-6#

I: Okay. Now, all of these cases have one thing in common. They would like to adapt the cloud application. All right? The companies all would like to adapt a cloud application from different cloud application providers for different use cases. And usually, if companies adapt cloud applications, what they do or if they adapt new software, they do a risk assessment. So, do you agree with that? #00:05:45-0#

R: Absolutely. I already did some of those risk assessments in the past. #00:05:50-8#

I: And that's exactly the next question I had here. What can you tell me about risk assessment, do you have any experience on that area? #00:05:59-1#

R: Yes. It was a task I did several times while working as a consultant and I did several times working for (Organisation). What-, you mean generally what I know about those things? #00:06:13-3#

I: Yes. So, what is your impression about risk management? What do you know about risk management? Do you think it's realistic, it's needful, it's useful? Have you ever performed it? So, these are the open questions here. #00:06:24-6#

R: Yes, I performed it several times. I think it's really needful due to the fact that's when you give data to other companies you want to ensure that those data is, yeah, stored secure. There are I think several dimensions that matter there. On the one hand, it's the security and talking about security, I mean, the confidentiality, integrity and availability of the data I give to another company. On the other hand, there is the thing about compliance where we need to make sure that we obey to local laws due to the fact that we're here in Germany in a highly regulated country.

So, one last sentence, I, and I think that often, or my impression often was when performing those audits, that's the part with the compliance #00:07:24-8# was the focus. Due to the fact that that's the company doesn't or that the management-, but for the management, it isn't important what IT security means with the data they give to other companies. The impression I had always doing those reviews was that compliance is the thing that matters, and if anything happens to the data and the management can say, 'Hey, we did everything we can and we did perform all those audits and so on', then things are really fine. So, my personal impression was that most of the time when data was stored at other companies, the security level lowered by that and that this is the fact everybody in the company was aware of and those reviews took place to make sure that the compliance factor I mentioned is in place. #00:08:16-4#

I: Great. So, thanks a lot for that impression and then those experience on your side for providing that. That's really, really great. Now, I would like to go or continue with your experience of risk management and also perform a risk management but before we do that, I would like to show you a so-called risk matrix. And we will have a look at whether that sounds somehow familiar to you or whether you have seen that before. So, this is the risk matrix we would like or I would like to use for that evaluation here. And the first question is have you ever seen such a risk matrix? #00:08:57-6#

R: Yes. I have seen such a risk matrix before. Regarding the impact, I always found concrete numbers and not some kind of percentage. So, this would be a question here how-, #00:09:13-0#

I: Exactly. This is also a question I always answer or I always explain if I present that because you're right, this is not usual. So, first of all, maybe start with probability as I think these are quite sure. So, first and foremost, this is a 5.4 matrix so we have five probabilities and four impact factors. There might be other metrics 3 point-, 3.3 or 3x3 matrix, 5x3 five matrix. There are many different matrix out there. So, please be fine with the 5.4 except you say this makes no sense. Then of course-, #00:09:50-5#

R: It's absolutely okay for me. #00:09:51-6#

I: (laughs) Okay. There is, as you probably know, not the matrix. So, on probability we have these five different probabilities. We have a below ten percentage, we have in-between ten and 30 percentage. We have in-between 30 and 60, so 60-90 and we have more than 90 percent probability that a certain risk will occur. Now, coming to the impact and you're totally right, that this is a bit strange that there are percentages. But this is due to the case that we have different case studies and this matrix should map to the case studies and the ten percent or the percentage here are always relative values to the turnover the companies do per year. So, for a small company, the absolute value would be smaller than for example for a bigger company. And to use that matrix for all the three cases I used here relative values. So, if you-, #00:10:51-9#

R: Yeah. #00:10:52-0#

I: - think of ten percent in the case A is of course a different absolute value than for example in case B. #00:10:57-1#

R: Okay, yeah. I see. #00:10:59-0#

I: Okay? Make sense? #00:11:00-6#

R: Makes sense. Makes sense, again. Yeah. #00:11:02-9#

I: Okay, great. And ja, I mean, what to say else here, probability in relation to impact provides us then the risk we see with a certain topic. Okay? #00:11:18-5#

R: Yeah. #00:11:19-5#

I: Okay. Anything to add here? Any questions? Anything unclear? #00:11:24-2#

R: No. #00:11:25-4#

I: Do you understand the risk matrix? So, this is the-, #00:11:28-4#

R: Yeah. #00:11:28-5#

I: - official question here. (laughs) #00:11:29-9#

R: I think so. #00:11:30-6#

I: (laughs) Ja. As always, be, feel free if you're-, if you have any, any questions. So, now, the thing is I would like to present you now three compliance risks. The topic itself is about compliance and you, you already mentioned compliance is one of the important topics. And I prepared here three compliance topics. I will first explain you the compliance risks I identified. And then we can quickly or shortly discuss whether they make again sense for you, whether they are clear for you, all right? #00:12:05-7#

R: Okay. #00:12:06-6#

I: And having the risk matrix and the risks known, we will then perform the risk management. So, it's straightforward so to say. (laughs) #00:12:15-4#

R: Okay. #00:12:16-3#

I: All right. So, here we do have three compliance related risks. And I will explain them quite quickly to you. The first risk is that the cloud application providers, so, provider A, B or C, implements a contractually not mutually agreed configuration. Now, the question might be okay, what is a configuration? And in the case here you can see a configuration as everything which is related to compliance. So, for example, the backup location of your cloud application. For example, in the intrusion detection case, the rules which the intrusion detection system configures. So, everything which relates to configuring something compliance-based is a configuration. Okay? #00:13:06-5#

R: Yeah. #00:13:07-4#

I: So, the first risk is that the provider implements something which was a configuration which was not mutually agreed. To bring here an example that for example a backup location, out of Europe is implemented which was not agreed on. #00:13:21-1#

R: Okay. #00:13:22-0#

I: That would be one example, of course. And you can think of others for sure. #00:13:26-9#

R: Okay. #00:13:27-2#

I: The second risk is that the implementation of a compliance configuration gets delayed due to some slow or manual processes. Again, we stay with the backup case, I will stay with that case if it's okay for you. So, imagine the case that we are in the past made our backups also georedundant in the UK. Now, the case comes in that UK leaves the EU, the European Union, not the EU, it's still in Europe. #00:13:57-4#

R: Yeah. #00:13:57-5#

I: But the (laughs) European Union. Now, we need to contact our cloud application provider and tell them, please do not do any-, store any backups anymore in the UK as it is not anymore Europe and it's not anymore compliant with the GDPR. So, please-, #00:14:14-0#

R: Yeah. #00:14:14-3#

I: - change that. And the risk is that the provider maybe due to many requests or whatever, delays that or it loses that or it does not do, or he or she does not do it. This is the risk here. #00:14:25-8#

R: Yeah. #00:14:26-7#

I: Okay? The delay intake. Now, the third and last risk, and this is a risk related also a bit to the topic of forensic. And the risk of denying the implementation of a configuration in a case of dispute. So, imagine there is a data leakage or whatever, and now it goes to court. And one of the parties at court says that is not what we agreed on, this is not what we set up, this is not what we meant to have. This was not how we wanted to have it. It's not our fault. #00:14:57-6#

R: Yeah. #00:14:58-4#

I: And this is that risk here. These are the three risks we will look at. Do you understand that risk? #00:15:06-0#

R: Give me a second for the third risk. #00:15:08-4#

I: Sure. #00:15:08-4#

R: I would like to read it again. #00:15:10-1#

I: Ja, sure. #00:15:11-0#

R: Denying the implementation would-, I'm kind of example guy, so, let's say we have got a firewall? #00:15:27-7#

I: Yes. #00:15:28-5#

R: And we say ports 22 was open and-, #00:15:33-8#

I: Ja. #00:15:34-2#

R: - it was contractually reach on that port 22 is closed. #00:15:38-6#

I: Yes. #00:15:39-3#

R: Are we till in exa/-, or in risk number three in this case? #00:15:44-2#

I: We are in risk number three at this case, yes. That would be an example but then you-, that would be so to say, a positive example of that case. But to bring also a negative example with your example you brought in, there is port 23 open and/or 22, and there is no paper documentation of that. There are only for example, unsigned emails or there's only telephone where this was agreed on. So, there is no clear contract available in that case. #00:16:18-4#

R: Yeah. #00:16:18-5#

I: And now it comes to court and the person who implemented that says this is what person A, B, C or whatever said we should do because there was some compliance change or whatever, and we quickly needed to change it for example. We needed to change it, not necessarily quickly but we needed to change it. And now the thing is, there's a dispute on that. One person says that was intended to say, to do so and the other person says that was not what we said. #00:16:46-9#

R: Okay. #00:16:48-8#

I: Is that clear? #00:16:50-2#

R: So, does it mean that in this case we say we don't have some kind of SLA for this parameter? #00:17:01-2#

I: Mhm. Exactly. So-, #00:17:03-9#

R: So, company-, #00:17:06-2#

I: Ja. #00:17:07-1#

R: Sorry. So, company A would say, which is the one that got hacked, they say we always leave port 22 open and the company B which the data was stolen says how could you date to leave port 22 open. It has to be closed until it's found (best practice?) #00:17:23-3#

I: Exactly. So-, #00:17:25-9#

R: Okay. #00:17:26-2#

I: That would be in that example but also for example, if an SQL injection is possible, then the question is of course how is the data stored? Is it hashed? How is it hashed and so on? This is usually something you do not necessarily contractually agree on. This is something which exists, is somewhere maybe also written. But at the end, if a dispute comes up, there might be, ja, where need to be discussed then. #00:17:56-0#

R: Okay. #00:17:56-5#

I: So, these are the topics here. That something which is maybe not necessarily contractually agreed which occurred and data leakage for example comes to court and then creates a dispute. #00:18:10-2#

R: Understood. #00:18:11-8#

I: Okay. So, this is more or less meant here not necessarily something you can say hey, there it's written, we did it. So, in case some, ja, parallel talks took place and they are not documented or not well, not, not, non-reputable documented so to say. This is maybe also a bit better description of that risk. #00:18:35-0#

R: Okay. #00:18:35-5#

I: Okay? Further questions? #00:18:39-0#

R: No further questions. #00:18:40-7#

I: Good. Then I would say, your task and this is why you are here is to go through the case studies, A, B, C and take the risk number one, or let me stop a second, we start with case study A and do all the three risks for case study A. Then we go to case B, we go all the three risks based on risk matrix for case B and then we go to case C and we do, go through all the risks on case C. Such that we in the end have made risks starting from case A. So, this is-, sorry, I had to organise myself. (laughs) All right? #00:19:18-7#

R: All right. #00:19:19-9#

I: It would be nice if you could name how you rate the probability and the impact. If you don't want, if it's for more or less something you do out of your stomach, and for you, marginal or critical is somehow unclear and you just want to provide high, it's also fine. But just name this one risk, it's not necessarily the risk you need to say. But it would be as transparent as possible so to say. #00:19:42-8#

R: Okay. #00:19:43-6#

I: So, we start with the case A, case study A, how likely do you think that the provider A implements a configuration which was not mutually agreed on? #00:19:55-4#

R: Yeah, let me just skim again over-, #00:19:59-3#

I: Sure. You have all the time you need. #00:20:00-7#

R: - over it. Okay. #00:20:01-7#

I: And you can also ask questions for sure. #00:20:09-2#

R: One question appears regarding the risk matrix and the probability. #00:20:33-7#

I: Ja. Mhm. #00:20:34-7#

R: The, regarding the likelihood of an incident-, #00:20:38-0#

I: Ja. #00:20:38-7#

R: - are we talking about some timeframe here? Or because I would say it is within one year. #00:20:46-8#

I: See, different-, ja, in one-year timeframe. #00:20:48-2#

R: One year? Okay. So, I think regarding the impact, this is an easy one due to the fact that it says that the impact would be catastrophic. So, looking at 80 percent of the revenue is catastrophic. Of course, perhaps it might be critical but I would stand to catastrophic here because also a loss of 30 percent or more could, of the turnover could turn out to catastrophic impacts. But I would say at this point, let's assume it's catastrophic and it's more than 80 percent of the turnover. #00:21:48-4#

Let me just have a look. Yeah. If the company has some kind of ISO 27 certification, which means they were able to, yeah, write some, write some last documentation and regarding the ISO certifications, I saw by and myself, this doesn't mean too much. It means a little bit but it doesn't mean too much. So, I would-, I would just-, this is the company or the tools provider A, which is a company with lots of turnover 180 billion so, I would suppose that they are running some serious IT stuff. And due to the limited information received in this, in this paragraph, I would tend to say that it is some kind of, I would tend to say it's unlikely. So, we have got catastrophic and we have got unlikely, so, we would have a high risk here. #00:22:51-2#

I: Mhm. Great. Perfect. Exactly, this is how we should do it. And I would say we did-, this is more or less also up to you how you would like to do it. You want to go from provider, from case to case or do you want from risk to risk? (laughs) So-, #00:23:07-0#

R: Let's go from risk to risk. I think this is better. #00:23:09-1#

I: Okay. Mhm. Okay, ja. That's always dependent on the participant. So, I'm totally flexible with that. Okay. The second one is the implementation of compliance during configuration gets delayed due to slow or manual processes. #00:23:22-0#

R: Yeah. I would say the impact is marginal. #00:23:36-1#

I: Mhm. Ja. Ja. #00:23:38-1#

R: Looking at a timeframe of one year because here it, of course it always depends. You could have cases that are catastrophic, you could have cases that are much below but this is just a lucky guess here saying it's marginal due to the fact that those risks here really depend on which laws you're breaking, thinking on some kind of Brexit scenario here, I would say if one or two years after the Brexit, if you still host some servers in the UK which shouldn't be there, yeah, it's some kind of marginal in the worst case I would think just from the experience I saw. And I would say this is something which is unlikely due to the fact that some things like Brexit or something else don't come from one day to another. So, at this point, I would say, it's medium, tending, tending to the low direction. #00:24:39-0#

I: Tending is unfortunately not possible (laughs). So-, #00:24:43-9#

R: Yeah, and then-, #00:24:44-8#

I: - you stick to? #00:24:45-7#

R: Then here, it's-, my stomach tells me it's low, but looking here at the numbers I would say it's medium so let's-, let's stay at medium. #00:24:56-8#

I: And that something is-, the thing happened due to something which was not necessarily written down or which is maybe, in Poser written down and it's interpretable and now, someone says this is not how we said it, or this is how that mis meant. #00:25:21-3#

R: Yeah. I, looking at the impact, what could happen, we could have some kind of data leakage et cetera. So, we are again at catastrophic, at the impact. We have got, if I remember it correctly, we had just online sales. Is that correct? We didn't have any contact to any sales person. So, I would say we are not, not really sure where exactly but I would say I'm definitely at very high. Yeah. #00:25:55-7#

I: Mhm. Okay. Mhm. Okay. Amazing. That's exactly how we should do it. So, let's continue (laughs) with that flow also with the case B. #00:26:05-7#

R: A. #00:26:07-9#

I: Sorry, B. #00:26:08-4#

R: I just would skim it for a second. #00:26:14-1#

I: Ja, sure. #00:26:15-5#

R: Okay. #00:26:54-9#

I: All right? #00:26:56-0#

R: Yeah. So, let's start with the first one. That they have agreed. So, sorry I have to just re-skim again here. #00:27:24-0#

I: Ja. Sure, sure. Take your time. #00:27:25-4#

R: The passage. Yeah, okay. So, second, second try. #00:28:34-3#

I: Mhm. #00:28:35-5#

R: Yeah. I have to think about this one for a second. #00:28:48-4#

I: Ja, sure. #00:28:49-4#

R: So, regarding the impact. Perhaps, I'm looking at that in a really pragmatic way saying that if we have got some activists that are trying to hack us, from things that I've seen on these stages of attack, I would say most of the attacks were more or less harmless. So, I would say we are here at the negli/-, how do I pronounce this word correctly? #00:29:43-2#

I: Negligible. #00:29:44-5#

R: Negligible, thank you very much. Yeah, I would say we are at negligible. So, regarding the impact, the probability at this point, we have got a small company with no certification. So, it's yeah, kind of, kind of, yeah, it's come to, (Foreign language) #00:30:07-3# and due to that I take one in the middle saying it's possible. #00:30:20-9#

I: Mhm. #00:30:21-7#

R: And so, we come out in low risk. #00:30:23-5#

I: Mhm. All right. And number B. Risk number two, not number B, sorry. (laughs) #00:30:35-9#

R: Yeah. Yeah, just a second. Do we have any compliance screening things in this scenario? Do we assume in scenario B that the company has to implement passwords? #00:30:59-4#

I: Yes, yes, yes. You can assume that. That this company is so huge that it has also some compliance-driven, compliance-based configurations. #00:31:08-3#

R: Yeah. I would still-, looking at the funds that (Organisation) is giving to banks in Germany, I would say we are still at the negligible. #00:31:23-3#

I: Mhm. #00:31:24-0#

R: Here because we are far under ten percent. We are talking about some millions in worst case I would say. It's of course possible that this happens here and I would say it's due to the fact that I don't know anything about the company. Yeah, and about their turnover and the Google rating, I would say I have to stay in the middle and say possible so we would be at low-risk schedule. #00:31:49-4#

I: Mhm. Okay. Ja. Mhm. And last but not least, the denying risk. #00:31:55-3#

R: Yeah. As mentioned in the first, at the first risk, I don't think that for company number B anything will happen by misconfiguration, where an impact would be higher than ten percent. We are staying at neg/-, ne/-, #00:32:13-7#

I: Negligible? #00:32:14-8#

R: Could you tell me again? Negligible. #00:32:16-0#

I: Yes. #00:32:16-7#

R: I hate this word. Negligible, and at this point, I would also say that this is-, let me just a look. They have got sales and consultant but execution is done in India. So, at this point without wanting to be a racist, I say it's very likely just from empiric evidences I've seen in those cases. So, we are at medium here. #00:32:46-1#

I: Mhm. You can also, if you want to think a lot about India, I mean, yes, it's India here but you can also think of East-, #00:32:59-3#

R: Yeah, I would say it at any other country in the world too, I think. #00:33:02-1#

I: Ja (laughs). #00:33:03-6#

R: We were looking for a smaller, yeah. #00:33:05-1#

I: That's the topic here. #00:33:06-9#

R: Yeah. #00:33:07-2#

I: Okay? #00:33:08-1#

R: Okay. #00:33:08-9#

I: Okay. Then let's go to the third. #00:33:10-7#

R: Okay. Let me just skim that again. #00:33:14-4#

I: Mhm. Sure. #00:33:15-3#

R: Okay. Yeah. #00:33:28-6#

I: Mhm. #00:33:29-4#

R: At this one, I would like to start with the probability. #00:33:45-5#

I: Mhm. #00:33:46-4#

R: And here, I would say this is something which is unlikely from my view. And regarding the impact, I would say it's negi/-, #00:34:05-4#

I: Negligible. Okay. #00:34:07-5#

R: Negligible. (laughter) I would say here. This is, yeah, it's something which is, which I would say we're at low here. #00:34:16-3#

I: Mhm. Okay. #00:34:17-2#

R: The second one, yeah, give me a second please. #00:34:28-8#

I: Ja, sure. #00:34:29-8#

R: Yeah. We're talking here about some-, a business case which is at risk if I read it correctly. And looking at the probability that something like that happens at a global player, I would say this is unlikely because normally from my empiric evidences, the SLAs are really fixed there, and the impact I would say in the worst case it's marginal so I would say we have got a medium risk here. #00:35:19-2#

I: All right. Yup. We are here. #00:35:22-5#

R: Yeah. #00:35:23-3#

I: Third one. #00:35:26-3#

R: Yeah. (laughs) Yeah, let me think about this one a second. I would say it's low because the probability that something like this happens is really low. They must be out of mind if they try to sue a global player because of some configuration changes. And the probability that's because of, and this is something happens, which would be marginal, I think. #00:36:26-9#

I: Okay. So, at the end, we're here at a low risk. Right? #00:36:31-0#

R: We're at low. That's right. #00:36:32-1#

I: Okay, perfect. Amazing. That was more or less the hard part. Now, comes the fun part (laughs). #00:36:38-0#

R: Okay. #00:36:39-1#

I: And as said, we're following or I follow a comparison of architectures. You have seen now or you rated that based on the existing architecture, existing processes. And what I wanted to show you now is the architecture I propose here in my dissertation. #00:36:58-3#

R: Yeah. #00:36:58-4#

I: And this is the image of it and I will quickly go through it. And if you have any questions, please let me know. This is an example case here. So, this is the example implementation // #00:37:10-3#

R: Sorry to interrupt. Could you just zoom in a little bit? #00:37:12-9#

I: Sure. Sure. Sure, sure. This should not be the limitation factor. So-, #00:37:16-9#

R: Great. Thanks. #00:37:17-6#

I: So, (laughs) I think it's better, right? So-, #00:37:20-0#

R: Absolutely. #00:37:20-7#

I: In the case, so, first and foremost again here, this is a concrete application of the architecture otherwise, it would be quite difficult to show it in an architecture diagram. It might be impossible, it's hard to explain and even harder to imagine how it might work. So, please ask direct also from the concrete case if necessary. The basic idea and this is where everything starts is with the cloud application consumer. So, someone who would like to use the application or would like to be more precise to configure the application, compliance-based. #00:37:55-9#

R: Yeah. #00:37:56-6#

I: And a compliance configuration you can think of as for example, a textural file, as a JSON file, as an XML file, whatever you can somehow textually represent which can then translate for a computer application. Okay? #00:38:13-6#

R: Yeah. #00:38:14-2#

I: Now, the thing starts with a cloud application consumer and as said, the cloud application consumer can either be the person who buys that application or the one who provides the application. So, it could also be consumer here. So, both parties can configure that application. #00:38:32-1#

R: Okay. #00:38:32-6#

I: Third, and this is the third party here is the cloud application itself. So, at the end, my architecture sees three participants. The consumer, it's the provider and the application itself. Whereas the provider and the consumer can both configure the application. #00:38:49-7#

R: Yeah. #00:38:50-2#

I: Okay? Now, those three parties, they share a common symmetric key. This key is arranged due to a Diffie-Hellman key exchange blockchain based. So, everyone starts his Diffie-Hellman value due to the blockchain in a smart contract, digitally signed, pulls out the Diffie-Hellman, the public Diffie-Hellman from the other parties. Performs Diffie-Hellman computation. Stores back (laughs) the Diffie-Hellman value, takes the other Diffie-Hellman values from the other parties and do it again the Diffie-Hellman computations such that at the end, everyone can create its own symmetric key, and all the key exchanges are digitally signed due to the storage on the blockchain. #00:39:32-3#

R: Yeah. #00:39:33-1#

I: Okay? So, important here at the end, the three parties involved in that approach, do have the same symmetric key. And this is just a side note here. If they want, they can also perform that protocol again to get a new one. So, this is not something set in stone. But at the end, and this is important, everyone has the same symmetric key in that set up. Now, the person who would like to configure the cloud application takes the configuration and encrypts that configuration with the received symmetric key or with the generated symmetric key to be more precise. #00:40:09-6#

R: Yeah. #00:40:10-2#

I: Encrypts that configuration and stores it again digitally signed on the blockchain via a smart contract. Now, the cloud application comes into place. On the cloud application itself, there's a script called the cloud management script. And you can think of a backend script which runs on backend of the cloud application itself. And the aim of that script is more or less three things. First thing is to monitor the blockchain for configuration changes. So, as soon as it detects a configuration change on the blockchain, it pulls out the configuration from the blockchain and decrypts it as it has also access to the symmetric key. Okay? #00:40:52-2#

R: Understood. #00:40:53-1#

I: Did you? Okay, that's good. The next step is it takes that encrypted script, encrypted configuration sorry, (laughs), it takes that encrypted configuration and implements it for the application it runs for. So, for example, in the case of intrusion detection system and to be more precise, in the Snort case, it would override the Snort configuration. It would stop the application, it would override it and would restart it to be absolutely precise here.

In parallel, it would also monitor the log files of the application. So, it would go through the log files step-by-step in the-, and monitor the logfiles for a result meaning whether the implementation of the configuration change was successful or not. Assuming the implementation of the configuration was successful so it's not again starting and says okay, configuration could be implemented successfully, in that case, the configuration script, so, this one here, triggers a backup of the virtual machine on which the intrusion detection system is running on the cloud provider, from the cloud provider. #00:42:02-4#

R: I haven't understood that one. It triggers the backup? #00:42:04-2#

I: Ja. #00:42:04-7#

R: What does that mean? #00:42:05-7#

I: It starts the backup-, #00:42:08-1#

R: It performs the backup? Okay. #00:42:08-7#

I: It forces the backup. #00:42:09-5#

R: Okay. The backup process is great, yeah. Understood. #00:42:12-3#

I: Ja, okay. Mhm. Okay. Ja. Good question. This is also represented by this disk (laughs). #00:42:18-3#

R: Okay. #00:42:18-8#

I: So, there is a backup initiated from the virtual machine on which the application is running. Okay? #00:42:27-4#

R: Yeah. #00:42:27-9#

I: And the hash value of that backup is built. So, backup created, hash value of the backup built. Imagine, the configuration was already successfully implemented. So, the hash value is the hash value of a backup which already has a successfully implementation of the configuration received. Okay? #00:42:49-5#

R: Yeah. #00:42:49-7#

I: This, keep in mind. Now, what that script does, and this is the third action, the third, the first action was monitoring the blockchain, second action was implementing the cloud configuration and configuring the backup. And the third thing is now it writes that hash value it created back to the blockchain, as a kind of proof of configuration work. So, it says okay, this is to prove that everything works well. Here is the new hash value. In case of an error, it would write an error to the blockchain. Okay? #00:43:20-8#

R: Okay. #00:43:21-3#

I: Now, I assume that everything works well. Now, everyone in that configuration has the possibility of going to the blockchain and see the latest hash value. The assumption is now in a case of a dispute, so, something went wrong or there’s something unclear, you can take the hash value and as the provider for the backup, go to court and have a look on the backup based on that hash value and then investigate that hash value, that backup. Okay? #00:43:49-8#

R: Yeah. #00:43:49-9#

I: This is the underlying assumption here. #00:43:52-5#

R: Understood. #00:43:54-8#

I: Good. The only thing you can assume here and you should not consider under the risk management is this thing of the blockchain. Did the blockchain gets attacked by a 50 plus attack or whatever? So, you can assume you can choose whatever blockchain you would like to take on. #00:44:11-7#

R: Okay. #00:44:12-5#

I: And whatever blockchain you would think of and if you want, you can also use a private or one somewhere distributed on your own network. So, please assume from any blockchain attacks. This is the only assumption I ask you to do. #00:44:24-7#

R: Okay. #00:44:25-3#

I: All right? Other assumptions like that there might be an error in implementing the case or in the architecture, whatever, you cannot, ja, abstract from. So, this is-, should be a realistic risk assessment now. So, anything else which can go wrong might go wrong. #00:44:42-9#

R: Okay. #00:44:43-8#

I: So, as // case also. The only thing really, I ask you to assume is that the blockchain is secure. #00:44:48-0#

R: Okay. #00:44:49-1#

I: Okay? And having that said, I would now ask you again to go with me through the three risks and see if something changes, if providers would provide their approach based on that architecture. #00:45:03-5#

R: Yeah. Do we assume at this point-, #00:45:07-6#

I: Ja. #00:45:08-1#

R: - that we are - saying we are at court, do we assume that for example company, sorry, provider C, which is a global player grant us access to their blockchain or is this-, sorry, not blockchain, to their backups or is it a risk we have to keep in mind here? #00:45:27-7#

I: You can think of that this is something you can also contractually negotiate, to say, okay, I always would like to have backup access or I always would like to receive the backup as soon as the configuration gets implemented. So, this is something which can organisationally be solved. #00:45:43-3#

R: Okay. Okay. So, and now we take this architecture in mind and see if any of these risks would-, #00:45:52-8#

I: change or? #00:45:54-7#

R: - become si/-, would change? Okay. #00:45:55-8#

I: Exactly. Or stay the same. So, we do exactly the risk assessment again essentially. #00:46:01-4#

R: Yeah. #00:46:01-6#

I: Are we clear or any questions to that? #00:46:07-4#

R: I think it's clear here. #00:46:09-1#

I: Okay. Mhm. I try to make it such that you see the risks, the architecture and the risk matrix. I hope that works for you. Is it okay? #00:46:23-8#

R: Yeah, that works. So, the first-, I think that the first case, please correct me if I'm wrong. #00:46:38-4#

I: Mhm. #00:46:39-1#

R: But from my assumption would be that nothing changed because in risk one, and this is a question I would like to ask you at this point, we assume that something is implemented by an end user's port or something like this, and something is misconfigured by (unclear) #00:47:03-7#

I: Mhm. Ja. #00:47:05-6#

R: So, I think // this is nothing any, any software like, or any architecture which is in the picture below could prevent. So, I would say at this point, all the three risks stay the same for me. #00:47:23-3#

I: Mhm. Okay. Mhm. Just as a-, this is not something to buy if you were just to clarify that. #00:47:36-9#

R: Yeah. #00:47:37-6#

I: You do have-, so, all the three participants do have the possibility to see the configuration at least. So-, #00:47:44-1#

R: Okay. #00:47:44-4#

I: Ja. I mean, they have all access to the blockchain and can see the configuration. But you're right. I agree to that. That they cannot-, as soon as implemented, they cannot prevent it from being, taking place. #00:47:58-2#

R: Yeah, and I would stay at this point at the risks due to the fact that if both or does it mean, sorry-, #00:48:06-9#

I: Ja. #00:48:07-7#

R: Does it-, does it mean this is also something for my understanding right now-, #00:48:13-1#

I: Mhm. #00:48:13-6#

R: - does it mean that in scenario one, with all this architecture, I wasn't able to see the configuration and now I'm able to see the configuration? Is there a change? #00:48:23-2#

I: Yes. So, in case one, there might be that the cloud application provider has some additional or some configurations implemented you are not aware of. They might be-, wherever they came from-, this thing is you never know all the configurations or there might be always hidden configurations so to say. So, you do not-,

#00:48:45-4#

R: Yeah. #00:48:45-5#

I: - have the possibility to go to the cloud provider and let you show all the configurations implemented. This is what, what is meant here. Now, the second thing is all configuration. So, it's-, it is not possible to configure the cloud application except you, you of course violate that architecture without going through the blockchain. #00:49:05-5#

R: Yeah. Okay. That means, just for the clarification again, that in scenario one, sorry, let me just read again-, #00:49:17-6#

I: Ja. #00:49:17-7#

R: - through first. So, at scenario one, we spoke before without the architecture. Maybe we would say the cloud provider leaves port 22 open. #00:49:31-1#

I: Mhm. #00:49:31-7#

R: And nobody in my company, when I'm the customer of the cloud provider here, then nobody in my company or even, I think it was company A, nobody in company A was able to see it. No? I'm as for example, the boss of company A, I'm able to say hey, some guys from the IT please review the architecture. #00:49:56-7#

I: Ja, exactly. This is the difference. #00:49:58-1#

R: Okay. Yeah. #00:49:58-6#

I: This is the difference. #00:49:59-2#

R: No, no. No, I understand the scenario. Okay. Thanks, thanks for clarifying that. So, we said before that the impact would be catastrophic. So, it's something where I would say it would make sense from my perspective if I'm in the leadership team of company A, it's of course an incentive to have some very close review running on this process. So, we said that we are, or that the impact would be catastrophic. We said that something like this happens is unlikely, and due to the fact that I would still say it's-, due to the fact that all those configurations are really complex, I would say at this point, I would like to stay at high due to the fact that I don't think if it's so complex that someone is able to find those, yeah, some vulnerabilities in this one. So, I would like to stay at this one for company A. #00:51:03-3#

I: Mhm. #00:51:03-8#

R: Looking at company B, we are already at low and at company C, it would-, we are also at low due to the fact that there aren't any IT guys who could have a look at it. If I see the scenario correctly. Looking or going back to company B, I would say we have got a global player here who will have some really good IT guys. We were already at low. So, we can't get any deeper here. But as far as I remember, I said that I'm not at the lowest point of low. So here, we can't change the risk but I would say we could go here regarding the probability. If it wasn't low before, I'm not sure right now, then we would be at the lowest point right here I would say that. #00:51:56-1#

I: Okay. Mhm. I keep it at low, okay? And remark that it is not getting higher (laughs). #00:52:03-1#

R: Yeah. I would tend to-, I would tend to see this one lower or also we are already at low. #00:52:08-5#

I: Exactly. #00:52:09-3#

R: Yeah. I think, and at C, I think it stays the same due to the fact that there are no IT guys implemented and we have got some farmers, what should they do with some configuration. #00:52:22-0#

I: Okay, perfectly. Exactly. That's how we should proceed (laughs). #00:52:27-3#

R: Okay. #00:52:28-2#

I: All right. And let's go, I think now we went differently than at the beginning-, #00:52:34-5#

R: Yeah. #00:52:35-2#

I: And now we just go, stayed at the first risk and went through all the cases. Would you like to continue with that or? #00:52:41-6#

R: Yes. #00:52:41-6#

I: Okay. #00:52:42-4#

R: I would love to do it that way. #00:52:43-2#

I: Ja, mhm. Now, we have the slow or manual processes. #00:52:46-4#

R: Yeah. Give me a second to think over this please. #00:52:51-7#

I: Sure. Sure, sure, sure. #00:52:52-7#

R: I would stay-, I would stay at the exactly same risk levels as we had before here. #00:53:51-9#

I: Yes, okay. Yes. And last but least. #00:54:05-7#

R: Yeah. #00:54:07-0#

I: And again, take your time. #00:54:13-2#

R: Yeah. I would say that we are at all the three points here. Or let, let me, sorry. I know weekend is near but let me-, #00:55:29-8#

I: All good. Take your time. (laughs) #00:55:31-5#

R: Let me, let me think about this one for a minute please. #00:55:34-9#

I: Your answer is more important than the weekend. #00:55:38-0#

R: Thought that you would say something like this. So, I was taking my time here. #00:55:44-7#

I: Ja, definitely, definitely. #00:55:46-6#

R: I'm not exactly sure where we are standing at this risk matrix here but I would say in all the cases in this model, we are here at low due to the fact that we say we have got the small scenario where the cloud provider denies access to some logs as far as I underst/-, sorry, through the configuration or where some side statements were given. And at this point, everybody can see the configuration at any time. So, I would say we have got a minimised risk that anybody couldn't deny saying that some implementations were done here. So, at all three points, I would say we're at low, right here. #00:57:10-0#

I: Ja. I write it down. Okay? #00:57:11-8#

R: Yeah. #00:57:12-7#

I: All right. Now, we have the time to rethink everything, if you want. #00:57:19-9#

R: I think we are done with this one. #00:57:23-4#

I: Okay. That is amazing because then we are nearly at the end. #00:57:28-5#

R: Okay. #00:57:29-1#

I: And before we come to the end, actually, I forgot one question to ask but I think this is not necessarily very important. Based on a quantitative scale, again, strongly agree, agree and so on, and the statement, I have understood the approach. How would you answer that question? #00:57:47-5#

R: Fully understood. So, strongly agree. #00:57:49-9#

I: Agreed. All right. Perfect. We did the evaluation. So, okay, do you think the blockchain makes sense in this approach? Can you think of other architectural components or trust-enhancing mechanisms which could be placed there? #00:58:04-8#

R: Yes. I would think on a PKI infrastructure. #00:58:08-9#

I: Mhm. And the storage of the-, so, for example, now the application, the configuration is stored on the blockchain, how would you realise that with a PKI infrastructure? #00:58:21-8#

R: I would sign the requests that are made and would provide this or those on the, this over with the signature. So, here in Germany, as far as I remember, we have got a (Foreign language) #00:58:35-6# which is some kind of equal to signing a document and I would use this one to sign this group that makes the changes for example or the configuration which is applied or the backup, whatever makes sense most. I think this would-, but I would have to look at this more closer to make one statement but-, #00:58:55-9#

I: Ja. #00:58:56-1#

R: - signing some kind of configuration of this group and providing this one to all the participants would make sense here too, I think. #00:59:03-9#

I: Mhm. Via email just sort of storage, it's just interesting also to know that, where would you store the configuration then? #00:59:11-1#

R: For being able, I won't really care. I don't know how confidential this has to be. If we would confidentiality is interesting here, put it on Dropbox. If confidentiality is or if confidentiality matters here and I would think that it matters, I think there are several ways. You could do it by email, you could do it in the browser, perhaps, yeah, you could use some of the PKI infrastructure already implemented in the browser. Not sure about that. I would have to think about this one later on but I wouldn't say that this is the real important thing here due to the fact that if we have a closer look at the configuration for doing some audits, if the confide/-, sorry, if the integrity which matters here most from my point of view is broken, then they would, an alarm would trigger. And so, I wouldn't say that this is the most important thing here but thinking of some kind of yeah, storage, thinking of a website, whatever, I think, as long as the integrity is done or is (Foreign language) #01:00:20-9#

I: Mhm. Okay. Ja. Okay. So, thanks also for that. And now, as we are slowly coming to the end of the interview, I would ask you to recall again a bit what all we discussed. And I mean, we already discussed about some topics. Based on the topic of transparency, do you think that that provided approach here has an influence of transparency related to configurations, transparency in the sense of making it transparent who configured what? #01:00:54-5#

R: Of course. Having some kind of audit trail makes things more transparent. That's the reason why all auditors I know who performs here his audits, for example, like (Organisation) once in an audit trail and through, it's one of the key requirements for example, German insurances, for German banks to have some kind of audit trail where you can see who did at which time which changes? So, I think in case of transparency, it really matters there. It, of course, it depends again, which company you have. So, looking at company C and going back to the use cases-, #01:01:34-2#

I: That's true. #01:01:34-8#

R: I don't think that's-, I don't think that company C really needs some kind of audit trail. Because if they have got some-, yeah, some, if they get hacked, if they have got some data loss, they have got serious other problems, and there are certain farmers without any It knowledge. So, I don't think that it's really important for them to have an audit trail if they have got several other problems. #01:01:56-5#

I: Ja. #01:01:57-3#

R: When we have got to look at company B, I think we just said that there are several regulations. If they have got some kind of-, if they've got some kind of data leakage for example, then at this point, it could happen that some regulator or whoever is coming to the company and says, "Hey, we would like to see your audit trail." And this is the one where this approach, or however, if you drive a blockchain with PKI, however, this approach makes things more transparent. And if some regulator is standing in your house and asking you, 'please provide me an audit trail', and you're not able to, this is some kind of really bad situation in this point. So, I think having an audit trail however, which method you choose makes absolutely sense. #01:02:42-5#

I: Mhm. Related to automisation or automising processes, do you think that that approach has an influence on that? #01:02:49-9#

R: What-, what approach? Do you mean the blockchain approach or the? #01:02:54-2#

I: The architectural approach including the blockchain now. So, saying it has the provided architecture here, and influence on the automisation of implementation of configurations. #01:03:05-7#

R: I wouldn't say that this is some kind of huge impact it has there. It's-, it depends of course, like always, but I would say that this is something where I think where the program must have got their (unclear) #01:03:23-0# processes and I would say this is some kind of process you could put in before implementing the configuration change. So, from an IT perspective, I don't see this huge impact here. #01:03:35-2#

I: Mhm. And last but not least, the question of notarisation or integrity protection of providing integrity to a configuration. How would you rate that one or how do you see that one on that approach? #01:03:49-6#

R: Are we still assuming that the blockchain is safe? #01:03:55-5#

I: Yes, yes, this is the basic assumption. Ja. #01:03:58-8#

R: Yeah. Could you just say again the phrase, or the question? #01:04:05-7#

I: So, the question was do you think the presented approach can help to investigate security incidents more easily? Or do you think the presented approach can help to identify responsible parties in a legal secure way? So, we are talking about integrity. #01:04:23-1#

R: Yeah. I would both answer with yes. If we assume that this, all those measures we take here are safe, then of course, it would help us to, yeah, to structure integrity. #01:04:39-6#

I: Okay. Thanks a lot. Final question and then (laughs) you are free so to say, as always in an interview, the last stage is on your side. And the question is overall, would you like to add something to that approach, to the evaluation you made, to anything? So, to say the last stage is yours now. (laughs) #01:05:04-1#

R: Yeah. Give me a second. #01:05:18-5#

I: Ja, sure. #01:05:19-4#

R: I would think that one of the biggest challenge is to make the things that happen at the blockchain level transparent. #01:05:45-7#

I: Mhm. #01:05:46-4#

R: Because thinking on German courts for example, there are people working who don't have to do too much with IT. And of course, you can take people there, good at. However, who are able to yeah, make assumptions and at this approach, I think if you're able to realise something like this, this would help as we saw at the risk rating a huge impact on our risk matrix. This is one thing. And in our example, here, we are assuming that the blockchain is safe and that things that are happening there are transparent. And I think those are the real big challenges. I suppose that you're working on theories about that in your dissertation. So, I think this is the one where I would say or this is the main question here, how do we get this one transparent? How do we get it safe? And if this challenge is solved, then we are here, or this, I think this dissertation would have a really huge impact. #01:06:59-8#

I: Okay. So, ja, thanks a lot for that statement and for that rating. We are at the end of the questionnaire. And I would also stop here and provide you a last and final question. Overall, now you have heard everything here, you joined me in the dissertations topic, you answered, you provided some really qualitative statements, some good statements so to say. And the question on my side is now how would you rate your experience overall in that area? How would you rate your statements based on school rates? So, would you say everything you said you strongly agree, or a very good, a good, a sufficient, a satisfactory, sufficient, poor or insufficient? So, how would you rate overall the statements you provided here today? #01:07:51-4#

R: Yeah. I would say we are-, could you say again the marks I could give myself here? #01:08:02-9#

I: School marks in German schools? #01:08:05-5#

R: School, okay. I would suppose I know what I'm talking about here. So, I would say we are at, yeah, talking about, so strongly agree. #01:08:15-9#

I: Okay. So, very good? So, sorry, school marks based on your school system, one is very good. #01:08:23-1#

R: One, I would say we're talking about one here. #01:08:25-3#

I: Perfect. Thanks a lot. Thank you for your openness, for your time, for the participation here. As said, the outlook is now that everything will be transcripted, anonymised and used for the evaluation of my architecture. Having that said, I would also stop the recording here. #01:08:42-0#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #10:

I: All right. We are starting the interview. Now, the interview is started to be more precise. Welcome and thanks for participating to the interview. Before we start with the main phase, I already introduced that we will start with a warm up and introduction phase. And the aim of that phase is to get you known a bit better. And therefore, my first question to you is, can you briefly tell me something about your professional background and your daily tasks? #00:00:38-5#

R: Yeah. Sure, of course. My name is (Person) and I'm a Team Lead of Collaboration Solutions at (Organisation). So, my responsibilities are coordinating a team who are responsible for the complete M365 stack. So, in terms of security, collaborations, and the products like SharePoint, OneDrive, Teams and the complete mail structure for around 15,000 people in Europe. So, my daily business is coordinating these teams and always I like to pronounce. So, according, like the team structure, the team building and the facing of technology where we want to build or what we want to build. Right now, we are moving from onsite securities and onsite, or on prime services to cloud services since a year and a half. And you know, that's my daily task. Anything else from background, what I did before or? #00:01:53-6#

I: No, no, that's amazing. That's amazing. #00:01:56-0#

R: (laughs) Okay. #00:01:56-2#

I: Ja. Just maybe your educational background. So, school starting or apprenticeship and such. #00:02:05-4#

R: Just school and then I, yeah, went to military for more than eleven years. And after that, I spent three years in consulting with team sizes more than 80 people. #00:02:21-8#

I: Mhm. Perfect. #00:02:23-4#

R: As a project lead. #00:02:24-4#

I: Amazing. Ja, in fact, that also gives us a bit information about your professional lifetime or career in years. Perfect. So, to summarise that, you have more than now let's say 15 years of experience in working? #00:02:40-3#

R: Hmm, yes, more than 15 years. Right, yeah. #00:02:45-3#

I: Ja, okay. (laughter) That's amazing. Okay. Good. All right. I think from everything, we know your background, and as already introduced at the beginning, I do have also some quantitative questions where I would like to give you a statement and ask you to answer that statement based on the values strongly agree, agree, neutral, disagree, strongly disagree. All right? #00:03:13-5#

R: Mhm. #00:03:13-9#

I: So-, #00:03:14-8#

R: Okay. #00:03:14-8#

I: - the first statement is I am a computer science expert. #00:03:18-4#

R: Agree. #00:03:20-1#

I: I am an information security expert. #00:03:24-6#

R: Agree. #00:03:26-2#

I: I am a cloud computing expert. #00:03:29-7#

R: Strongly agree. (laughs) #00:03:31-8#

I: And I am a cryptography expert. #00:03:36-5#

R: Hmm, not that much. So, what-, what's between agree and not agree? (laughs) #00:03:44-1#

I: Neutral. #00:03:45-6#

R: Neutral. So, I would like to answer the question with neutral. #00:03:49-6#

I: Okay. Amazing. Ja, thanks a lot. This is already the warm up. And I think we are warm (laughs). So, we can immediately enter into the main phase. And for the main phase, I already introduced you three case studies. So, company A, company B, company C. And the first-, #00:04:09-8#

R: Yeah. #00:04:10-0#

I: - question I do have here is do you understand the case studies? #00:04:13-7#

R: Of course. (laughs) #00:04:14-7#

I: Okay. Do you think the cases are realistic in those case studies? #00:04:20-3#

R: Yes, of course. #00:04:21-9#

I: Okay. And now, I would like to talk with you about risk of cloud adoption. So, we're talking about adopting cloud applications. And as already mentioned, I would like to talk about the risk of cloud adoption. So, the question here is do you have any background in risk management and what can you tell us about risk management? #00:04:48-6#

R: Yes, I do have some skills, and this I would like to have and also experience. I also mentioned that I have more than three years spend in project management as a project lead of a security project. So, that means, security phone, mobile security phones and a governance construct. And therefore, we have a lot of security experience in this. So, I have done a lot of risk management in case of, yeah, security. #00:05:23-5#

I: Okay. Great, cool. Now, I would also like to show you a so-called risk matrix on which we would now like to evaluate or to estimate risks. #00:05:38-8#

R: Mhm. #00:05:39-6#

I: And here the question is have you ever seen a risk matrix before and have you ever worked with a risk matrix? #00:05:45-5#

R: Yes, I do have. #00:05:46-7#

I: Okay. So, we have here a risk matrix in a format of 5x4, which is as common as other matrix 3x4, or 3x3. So, the thing is we have five values here in the probability and we do have four values in impact. And as said, and as you have already seen, the probabilities are on the left-hand side, we have probabilities below ten percent called rare, probabilities between ten and 30 percent, we call unlikely. We have probabilities between 30 and 60 percent, we call that possible. Between 60 and 90 percent, we call likely and more than 30 percent risk, 90 percent or more probability we call certain.

On the other hand side, on the x-axis, we do have the impact, so, how many money would result if the-, or would be needed to spend or would be lost to be more precise if that risk occurs or takes place. And here-, #00:06:51-8#

R: Mhm. #00:06:52-0#

I: - we do have negligible, which is if the turnover per year is below ten percent. So, we had the case studies with turnovers and if ten percent of the yearly turnover would be the impact of the risk, then we would say this is negligible for a company. And using that logic also for the other values ten to 30 percent, 30 to 80 percent, and 80 or more percent. I think as I understood you correctly, this is fine, right? #00:07:19-9#

R: Yeah. Got you. #00:07:21-3#

I: Okay. Good. Do you think risk management makes sense for the proposed use case or do you think risk management makes fence for adapting cloud applications in these three case studies? #00:07:39-0#

R: Of course. Sure, you have to do this in case of every implementation of any secured, any IT, any using of IT, you have do a risk (analysis?) #00:07:52-4#

I: Mhm. Now, the topic of my thesis or of my dissertation to be more precise is based on compliance driven risks. And compliance-driven risk means everything is so compliant, so, just for explanation is companies do set themselves rules or get rules also from government. So, there are some certain rules which governments need to follow on. And compliance-driven configurations are now if you adopt a cloud application and you adjust the cloud application based on the rules you set yourself. These are compliance-driven configuration. So, to bring you also an example on that, if you for example, say okay, my backups need to be stored in Spain, then this is a compliance requirement, all backups need to be stored in Spain in a compliance-driven configuration is now, if you configure the cloud application such that it stores backups in Spain. Mhm. Okay? #00:08:49-6#

R: Sure. (laughs) #00:08:50-4#

I: (laughs) Okay. So, my dissertation is as said on the compliance-driven configurations and the aim is to configure cloud applications, compliance-based. So, therefore, I would like to present you three risks and we rate the risks on the use cases, on the case studies. And let me just share my screen and then we go step by step through the risks. And I would ask you to rate the risk as you think they are on the specific cases. Okay? #00:09:25-3#

R: Mhm. #00:09:26-3#

I: Always interrupt me if anything is unclear. Okay? #00:09:31-9#

R: I will do. #00:09:33-2#

I: So, we are the first case in the case study, where we have that software company which would like to adopt an ERP system for their company. And they are doing highly critical stuff. So, if they get hacked, that would be a super mess. However, they adopt the cloud servers from an ISO-certified company, which is based in Europe. So, I think this is the summary of case A. And now, the risk which I would like you to ask and to rate on is the risk that the-, that the cloud application provider, so, provider A in the case study implements a contractually not mutually agreed configuration. So, that the cloud application provider sets a configuration which was not agreed on so to say. #00:10:30-0#

R: So, first of all, that is not good (laughs), if the provider (laughs) is so, is set in a test or in a RFP sets or when did this happen? Or did it already happen or it’s just a risk that we are planning on? #00:11:00-6#

I: Depending on the case study-, #00:11:04-6#

R: Yeah. #00:11:05-2#

I: This is a new provider so, we-, #00:11:08-8#

R: Okay. #00:11:09-0#

I: - they do not have any experience with that provider. #00:11:11-3#

R: Okay. Yeah. Okay. That’s what I just want to-, #00:11:14-0#

I: Mhm. #00:11:14-4#

R: - confirm (laughs). #00:11:15-5#

I: Ja. #00:11:16-6#

R: So, in case of that, usually as a customer, I get to try on a-, #00:11:31-0#

I: Control? #00:11:32-0#

R: - control my external partner. I am responsible to give them all set ups or compliance I would like to set up-, #00:11:49-4#

I: Mhm. #00:11:50-2#

R: - before. So, it’s much better for my company, from company A, it’s well-based and it’s all done. So, that will probably every time happen, and when I onboard a new provider, I would like to say that it’s not that high that that could be happening. So, (laughs) maximum unlikely. #00:12:15-4#

I: Mhm. #00:12:16-3#

R: And if this happens, that will be a mess. It could be critical at least, because another catastrophe, not that critical but I think that could be critical and unlikely because I don't think that that will be-, I am, I am worried. ISO

27001:2019. So, in fact, so my company is already based on how the process will be done in the provider, so, all this will be already proceed and all this has been done. I don't think that can be possible. Unlikely and critical, medium at least. #00:13:14-5#

I: Okay. Medium. #00:13:15-9#

R: That will be my answer. #00:13:17-5#

I: All right. Great. (laughter) Ja, I think you have the flow, that’s exactly what we are doing now. (laughs) So, we stay with provider A, okay? #00:13:29-6#

R: Mhm. #00:13:30-5#

I: And the next question is the risk that the implementation of a compliance-driven configuration gets delayed due to slow or manual processes. I can also provide you here and okay, I think you already got it. (laughs) If you need an example just let me know. #00:13:51-7#

R: (laughs) That is very possible. Every new, every impacted, a new provider can be, they promise you everything from we will do this until tomorrow, and four months ago, you think about ah, that should be done last month. So, there is the category high, that will happen. That is not a risk, that will happen in my point of view. So, from - I can be happy and will be not happen but I would like to say 60 to 90 percent so likely and a possibility. And there is not that impact because I am planning, if I am a set up company, I would like to have a proper planning. So, that the plan is not set in place and one day after the whole group will be implemented. So, likely and (laughs) ten percent neg/-, #00:15:11-6#

I: Negligible. #00:15:12-3#

R: Yeah, right. #00:15:13-7#

I: Okay. I will take negligible and write here medium. Okay? #00:15:17-4#

R: Yeah, please. #00:15:18-4#

I: Okay. So, and last but not least, the risk of denying the implementation of a configuration in case of a dispute. So, imagine a data leak occurs, if data leak happens, and now the parties go to court. And the court needs to clarify whose fault was it that the data leakage could arise due to a wrong configuration. And now, the question is how high is the risk that one of the parties will say that was not me, that was not how we agreed on. So, acts more or less opportunistically. #00:16:02-7#

R: So, the company or the provider I would like to pay for his job is already certified. So, he will definitely say wasn’t my fault (laughs) every time. So, that is true. And I have seen this before. So, that will happen. So, I’d say it’s high risk. But maybe I don't understand it right. #00:16:43-8#

I: Mhm. #00:16:44-4#

R: Is the question that it will be possible that he will say it wasn’t my fault? Or is the question how possible will this that we are getting to-, yeah, during one of these cases I would like to go to the judge. #00:17:13-8#

I: The question here is if, if already something happened-, #00:17:19-1#

R: Okay. #00:17:20-4#

I: That some of the party says no, that was not my fault that this happened. #00:17:25-8#

R: Every time. #00:17:27-7#

I: Excuse me? #00:17:30-0#

R: Yeah, every time. So, nobody would say in this case because they have a high value of classification and they would like to take care of the data both sides. So, both are companies with one of this, the company I am in, who do the risk analysis, I have to avoid the situation at least and searching for a good company who can provide this. And if I would like to, yeah, get this risk down, so, I would like to minimise this risk, that is what just happened in my head, I have to search another company but this is not a risk who I can minimise with another company but just happened. (laughs) Because the good company will say, no, it wasn't my fault because they have to stand up for a good security company. And they don't get in place with oh, no, we did a big mistake. All my other customers would like to, I don't know, I would like to say this is critical. Going on another intake, likely, yeah, it's likely that certain, certain in the possibility. But certain in the possibility but the business case is not that high because I'm right. (laughs) That it's their fault. So, I'm winning for the judge. But (laughs) maybe now I would like to go with high, so-, #00:19:43-2#

I: Ja, okay. #00:19:43-6#

R: So, certain and yeah. #00:19:45-4#

I: Yup. All right. That was for company A. Now, let's continue with company B. You remember the case? So, company B is a big huge, huge chemical company, which picked the cheapest of three offers for an intrusion detection system. The intrusion detection system itself is maintained by an internal IT department. So, they outsourced all their services except the maintains of the services so to say. And now, they would like to have a sub-contractor which support them in the intrusion detection area. Therefore, they picked the cheapest out of three offers. #00:20:26-8#

R: Mhm. #00:20:27-2#

I: And that offer is placed in India and has a Google rating of four to three stars out of 400 ratings. #00:20:35-2#

R: Okay. A, therefore, it is very possible that they misunderstood my compliance configurations. I see this in the past on my own. So, I would like to say this will happen. (laughs) Therefore, it's very likely. And how much impact will this have on my business value or the finance, I think that it will be high. #00:21:19-9#

I: Mhm. #00:21:20-5#

R: But yeah, and thinking about critical I or maybe not, so-, #00:21:28-6#

I: Ja. The-, #00:21:32-4#

R: That doesn't matter okay. High. (laughs) #00:21:34-1#

I: No, no. No, no. Because if you're in critical it's very-, #00:21:37-4#

R: I think it will be high. Yeah, yeah. I think that it will be likely but maybe not so it's high, high, so, it doesn't matter, you know, matrix, so, it's high. #00:21:50-2#

I: Exactly. Mhm. The risk of that the implementation of compliance configuration gets delayed due to slow or manual processes. #00:21:59-7#

R: If they get the comp/- no, if they get the configurations, that will be done, that will be done fast, that will be really done fast. I have seen this before. But you know, with some typos but I just mentioned before, but it will be done. (laughs) So, it is-, I would like to go with low at least. I would like to go with low. So, it's, yeah. #00:22:36-3#

I: Okay. Ja, it's fine. #00:22:39-4#

R: Yeah, on point. (laughs) #00:22:40-5#

I: Ja. (laughs) #00:22:42-2#

R: So, it will be (raw?) #00:22:42-9#, it will, really, really raw but I'm in the right to say the company or the company and that from my point of view, it is not done-, has not been done in the right time. So, they will be delivered but there are mistakes in for sure. (laughs) #00:23:07-6#

I: It will-, #00:23:09-1#

R: So, that will be done but you know, but yeah. #00:23:12-1#

I: This falls then also under the category of manuals, slow manual processes. So, for example, if you bring up a configuration, they said it-, said that in configuration, however, you realise that there's an error and it needs again to be redone, this is still the process. So, this is more or less the maintain or the adjustment process. So, do you see-

, #00:23:38-1#

R: No, then let me switch to medium in the matrix. We have to switch to medium. #00:23:43-2#

I: Mhm. See the whole until it's all rightly configured. #00:23:47-1#

R: Yeah. #00:23:47-4#

I: Yes. Please. #00:23:48-2#

R: Yeah, but it's too rare and the possibility, it's unlikely, between unlikely and rare in my vision. And therefore, it can be much more critical because the run time will be longer. So, it can be critical but unlikely but it can be happening. #00:24:05-7#

I: Mhm. So, we are at medium, right? #00:24:07-5#

R: Yeah, medium. #00:24:08-5#

I: Mhm. And last but not least in case of a dispute that some of the parties will deny a configuration. #00:24:15-8#

R: That's high. Let's take this very high. Let me watch through the matrix-, #00:24:24-8#

I: Ja. #00:24:24-9#

R: - and-, #00:24:25-4#

I: Take your time. #00:24:26-4#

R: - get my, (laughs) get my - that's very high, between, because I think they are in the, in the country out of Europe. So, we have to agree where our or where our judges will have set up. And that can be a discussion that takes a long time. And if this happened, it's a, would be a mess. I mean, 400-ish people have said that Google will be a good customer. So, (laughs) I would like to go with possible and catastrophe, my God. #00:25:33-0#

I: Catastrophe. #00:25:34-4#

R: Yeah. I would like to go with very high. #00:25:35-5#

I: Ja, exactly. So, that's fine. All right. And now, the farmers, so, the case C. #00:25:45-0#

R: Mhm. Well-, #00:25:50-0#

I: So, now the question is that this big company implements something which will then-, #00:25:54-6#

R: Can we go to down on the (laughs) that's the case up here. So, I just have to // I just have to watch out where, what the provider was doing just-, #00:26:12-7#

I: Ja. Sure, sure, sure. Take your time. #00:26:15-2#

R: What the provider wants, so, where the-, what did the provider C already (unclear) #00:26:24-0# okay, yeah, yeah, okay. Yeah, okay. No, no, no. I would like to go with-, it can be possible but don't interrupt my money. So, I would have to go low. #00:26:39-4#

I: Mhm. #00:26:40-7#

R: In this case. The risk and the implementation of the compliance-driven risk. So, they just want to have product but a lot of people in this case from a customer point of view, provider can implement in this case like, you know, pretty fast. And I don't think that that will be a mess. (laughs) So, they deliver a product. So, it's going fast. So, I would like to go also low. #00:27:22-8#

I: Mhm. #00:27:23-5#

R: - in here. So, it can be possible, but it will be (raw?) #00:27:28-3# but the money is maximum in the money now case. So, they don't spend that much time on it. There will be no much delay at least, I think. The risk of implementation (unclear) #00:27:44-8# they will lose (laughs) sorry. (laughs) it's minimised, so. It's high. It's high. #00:28:02-3#

I: All right. I think we have the first round so to say. So, this was more or less the risks from the current architecture, cloud architecture we know, and which we all are aware of. Now, I would like to propose you the architecture I developed during my PhD. And then we do exactly the same. So, we do again the risk assessment here. All right? I explain you the architecture based on a concrete implementation case as it is an architecture and explaining an architecture without a use case is quite (laughs) quite generic. That's why here we do have a use case. The use case of an intrusion detection system. Okay? #00:28:56-6#

R: Yeah, mhm. #00:28:57-9#

I: During that archi/-, or with that architecture, first and foremost, we do have three participants. We do have a cloud application consumer. This is a person who uses the cloud application. We do have a cloud application provider. This is the person who provides the cloud application and we do have the cloud application itself, as an independent, you can see it as a technical user. Okay? #00:29:27-8#

R: Okay. #00:29:28-4#

I: So, those are the three participants of that architecture. Now, what they are doing at the beginning of the architecture and this is shown here also as step one is they use a Diffie-Hellman protocol, which is a protocol for creating symmetric shared key. So, what they are doing is, they are using the blockchain for sharing symmetric, or for creating a shared symmetric key. Everyone starts his public Diffie-Hellman value on the blockchain and uses that public Diffie-Hellman value and does create a shared symmetric key. So, every one of those three participants at the end has access to the shared symmetric key. #00:30:10-5#

R: Okay. #00:30:13-4#

I: I will always stop after an explanation step to see-, #00:30:17-3#

R: (laughs) Okay. I got you. (laughs) #00:30:18-6#

I: - whether I lost you or not. Okay. #00:30:22-8#

R: Yeah. #00:30:23-0#

I: But that's, that's amazing. #00:30:24-1#

R: No loss man. (laughs) #00:30:26-0#

I: This is the first thing. So, the first thing is now all three participants have access to the same symmetric shared key. In the next step, the person who would like to configure the cloud application, let's assume the cloud application consumer would like to configure the cloud application, uses a configuration, a configuration you can think of as a text document, as a text file, as a JSON file, as an XML file or whatever, whatever structure you can think of but at the end, you can bring it back to text format. Okay? #00:30:59-0#

R: Mhm. #00:30:59-8#

I: Now, the cloud consumer writes down his configuration based on a text file for example, and encrypts that text file with a shared symmetric key. Hmm? #00:31:13-6#

R: Mhm. #00:31:14-6#

I: Okay. Next step, and this is again, this step here. He or she, so, the person who would like to configure the cloud application starts that encrypted configuration on the blockchain. In the next step, the cloud application, so, now a case to intrusion detection system, uses an extended backend script, the so-called management script. This, you can think of as a python script-, #00:31:44-1#

R: Mhm. #00:31:44-5#

I: - which runs in the background. That script monitors the blockchain for changes. So, that script monitors whether something changed on the blockchain. As the cloud application consumer start configuration on the blockchain, this cloud management script will realise that and will download the configure-, the encrypted configuration from the blockchain. Having access to the symmetric key, it is able to encrypt, to decrypt the configuration and is able to get the plain text of the encrypted start configuration. #00:32:21-8#

R: Mhm. #00:32:23-3#

I: Ja. A question or still clear? #00:32:27-8#

R: No, no, no, no. #00:32:29-1#

I: All fine? #00:32:31-1#

R: I got you fine, yes. #00:32:32-0#

I: Okay. Okay. In the next step, as this cloud management script now has access to the encrypted, so, to the decrypted, sorry. To the decrypted configuration, so, to the plain text to be more precise, it uses that configuration and overrides the existing application configuration. So, you can think of in Snort, the configuration is nothing than a text document. And if you just replace that text document, you have implemented a new configuration. Huh?

Beside overwriting the configuration of the application, the cloud management script also monitors the log files of the cloud application. In that, or using that, it is possible or able to see whether the configuration was implemented successfully or not. Now, we assume the configuration was implemented successfully. So, it's overwritten, restarted and in the log files we see it's fine, it's working. Now, the idea is as soon as the cloud management scripted text, okay, everything worked fine, it triggers, it starts, it initiates a backup from the virtual machine on which the cloud application is running. So, the whole virtual machine on which a cloud management script is running and the application, so, the intrusion detection in ours, in our case gets backup. Okay? #00:34:08-0#

R: Mhm. #00:34:08-6#

I: That backup is then used and the hash value out of that backup is created. #00:34:15-4#

R: Mhm. #00:34:17-8#

I: That hash value is then written back to the cloud application, to the blockchain-, #00:34:24-1#

R: Mhm. #00:34:25-1#

I: - as proof of implementation. Now, the idea is in case of for example a dispute and someone says, this was not what we implemented or agreed on, // on the configuration you take the backup, which you could maybe agree on downloading, you take the hash value and say, "Hey, this is the hash value you confirmed on the blockchain. Please show me the backup corresponding to that backup and now we can investigate that. And having that said, this is more or less (laughs) the architecture I wanted to present you. So, the configuration is more or less done by encrypting a text file or-, #00:35:02-9#

R: I have one question before I forget. (laughs) #00:35:04-4#

I: Ja, sure. Sure, sure, sure, fire up. #00:35:06-7#

R: Why? Why don't you do a backup before updating the plain text message to the server? #00:35:14-1#

I: I mean, you do have already a backup. I mean, and initially you could do a backup, so, you could set up the system, you could make a backup. And then follow up in the // (unclear) #00:35:29-8#

R: I mean, your process, you already described the process-, #00:35:32-7#

I: Ja. #00:35:33-3#

R: - which one we run. So, in case of a backup. #00:35:36-1#

I: Ja. #00:35:36-8#

R: So, if I did my backup and the change on the config doesn't happen that often I think-, #00:35:43-6#

I: Ja. #00:35:44-1#

R: So, in case I have a backup of a configuration that's more than one year old, maybe I did a backup or did an update or something like this, and these guys haven't done your job. (laughs) So, in my point of view, I think if you implement a backup before updating the configuration, you have a clear backup what was, yeah, per hour or two hours old. So, after that, you're doing all this, you can having a, yeah, two hours of backup and with the same structure and the same backend structure also. So, maybe just a (unclear) #00:36:37-8# proven (laughs), proving the concept. (laughs) #00:36:42-9#

I: Ja, sure, sure. I mean, the thing is (laughter) at the end, you need or the thing is to prove the implementation of a configuration. It's not necessarily the point in time and depending on which you agree on. I mean, there might be, and every second the change which tremendously change everything. So-, #00:37:08-9#

R: Yeah. #00:37:09-3#

I: - doing a backup one minute before, or two minutes before or ten hours before wouldn't change the overall concept of it. I agree. #00:37:17-1#

R: No, no, no. No. #00:37:18-4#

I: That it would be more likely or easier to investigate at the end-, #00:37:25-8#

R: Mhm. #00:37:26-1#

I: But at the end, in both cases, the implementation of the configuration gets hashed. #00:37:32-2#

R: Yeah, yeah, yeah, sure. #00:37:33-8#

I: And this is the point here. #00:37:35-1#

R: Yeah. #00:37:35-7#

I: Though from a practical perspective, I really agree with what you said. #00:37:40-1#

R: Yeah. Nice. (laughs) #00:37:43-6#

I: Ja. #00:37:44-4#

R: Our bias (laughs). #00:37:45-5#

I: You just have to use it. (laughs) #00:37:48-7#

R: Yeah. #00:37:49-0#

I: All right. So, coming back to the risk management and to the use cases we just discussed, and now, we are assuming that we are using the architecture I proposed to you here to configure the cloud applications. I would like again to do the risk assessment with the three cases you already investigated, we already discussed. So, provider A, provider B, provider C. We assume-, #00:38:21-3#

R: Mhm. #00:38:21-5#

I: - you know provider A, provider B and provider C are implementing the proposed approach. And we would like to do now the risk assessment here. A quick disclaimer, there is, as always in life nearly nothing you can assume, except that the blockchain here in that case is secure. So-, #00:38:45-5#

R: Mhm. #00:38:45-7#

I: - please do not assume that any 50 plus attack or something like that take place. Please abstract from the blockchain security in that case. #00:38:54-5#

R: Mhm. #00:38:55-4#

I: Beside that, you can even not assume and this is also in cryptography or wherever that the provider 100 percent correctly implemented it. So, that might also be a risk (laughter) (which remains?) #00:39:08-8#. And having that said, I think that hopefully answered your question if there was one. #00:39:17-7#

R: I can run through this point at least. But I would like to quick thing about. So, assuming technology on architecture like I have seen in your case right now, it's much more trustful I think, it was a presentation start with this. So, first of all, I think that-, I think that breaks up some trust feeling in my mind so (laughs) I just say okay, using this, that kind of architecture. So, not nice and I do understand this as a customer. That's also a point. But I think that will be minimise some risk in some cases. So first, we're running through case A, correct? #00:40:14-8#

I: Mhm. #00:40:15-2#

R: Case A? #00:40:15-6#

I: Ja, yes please. #00:40:16-8#

R: In this case, this will go risk (unclear) #00:40:27-5# improving the (unclear) #00:40:28-8# so, we need to think about what the-, it doesn't change on the technical side, it only change on technical side. But I will have to go down on low on this because I think if the provider can implement technology (unclear) #00:40:58-2# team, I too get them that he knows what he is doing and yeah. (unclear) #00:41:12-4# Yeah, that depends more on my point of view on the, on my company A, company. #00:41:25-3#

I: It's company A. #00:41:27-9#

R: Yeah, with company A. #00:41:29-1#

I: Ja, it's company A. #00:41:29-3#

R: So, that's on my company A. So, I think I'm surprised or so in the matrix, I would like to think that it's still possible if this happened. It's, that's still medium. Sorry. #00:41:53-2#

I: Mhm. #00:41:53-6#

R: Still medium. #00:41:55-0#

I: Fine, that's fine. You can rate whatever. It's your interview (laughter) so you can rate however you want. (laughs) And the risk of denying the implementation of configuration in case of dispute. #00:42:08-5#

R: It's still expensive. I would like to go into, go down to unlikely and critical. So, I would like to put medium point, point. Company B. #00:42:31-7#

I: Yup. #00:42:32-2#

R: I don't trust this (unclear) #00:42:36-9#. I stay with high in this case. No. #00:42:46-7#

I: The process? #00:42:50-0#

R: And in this case, I would like to go up. #00:42:54-2#

I: Mhm. #00:42:55-0#

R: Why? (laughs) If a company who I'm not trusting presenting a complex structure architecture, I am not that peaceful that they can implement it in a good, yeah, in a good, good configuration. And also, I probably have to hesitate with some delays and all this. And with-, so, I would like to go up with high at least. #00:43:37-8#

I: Okay. #00:43:38-9#

R: Because I think the structure is too complex for a provider that came from India and have 400 Google ratings. Sorry for that. (laughs) #00:43:57-3#

I: So, can you rate here on the risk matrix that? #00:44:02-7#

R: Yeah. It's like I said before, I go with the answer before possible, and minor, and then I would like to go with likely because I think it's much more possible. And still the money is minor also, go, went up to high. #00:44:29-0#

I: All right. Then let's do that. And here, in the case of dispute. #00:44:37-7#

R: Yeah, still very high. #00:44:42-2#

I: Mhm. All right. And last but not least. #00:44:49-8#

R: Yeah. It's still low. #00:44:53-4#

I: Mhm. #00:44:54-2#

R: Because the provider we are searching is set up and just a little. Next one-, #00:45:04-9#

I: Yes. #00:45:05-6#

R: - also, low. And in the last point, I would like to go down on medium because I think the possibility is lower, the catastrophic is still there (laughs) but it depends on the matrix to medium. #00:45:27-6#

I: Cool. So, you're fine with that? #00:45:38-6#

R: Yeah. #00:45:40-1#

I: Amazing. #00:45:42-2#

R: When you say that (laughs) #00:45:47-3#

I: So, let me just check. Okay. There was some stuff-, ja, I forgot of course one question. Question nine was forgotten. So, now I repeat it. And this is actually after I presented you the architecture but I think (laughter) you already answered that question also during the presentation. So, the question is again quantitative, and I would like to ask you or provide you with the statement, I've understood the approach. #00:46:24-1#

R: Yeah, that (laughs) I did. #00:46:27-0#

I: So, strongly agree, agree, neutral, disagree, strongly disagree? #00:46:30-7#

R: Sorry. Agree. #00:46:32-5#

I: Okay. Perfect. We did the evaluation and now that you have seen the approach and you have also with risk management made some risk management with it, I do have the question, do you think the use of the blockchain makes sense at this approach and yes, why or no, why not? How could you maybe replace it? #00:46:56-6#

R: First of all, it's the first time, I've seen this case. So, I haven't seen this before. Second, I do think that that will make sense because it improves the security of the architecture and the way of communication, the communication ways at least. So, I can do this on different way of communication in case of I communicate with B and 2. So, all this makes sense for me. #00:47:28-1#

I: Okay. And now, also, that we are slowly coming to the end of the interview, I would again emphasise three topics which we maybe quickly can also discuss. If we are recalling the presented approach here, do you think the presented approach improves the transparency of cloud application configurations? Do you think that approach makes cloud configurations more transparent? #00:47:59-4#

R: No. (laughs) I don't think so. #00:48:03-9#

I: Mhm. #00:48:04-7#

R: So, it increase the complexity. And every time you increase complexity, much more people don't understand the structure. #00:48:13-0#

I: Mhm. Okay. #00:48:14-3#

R: So-, #00:48:14-3#

I: Ja, that's fine. Anything to add or? #00:48:19-1#

R: No. #00:48:19-6#

I: I don't want-, I don't want to interrupt you. Do you think the presented approach can help to configure cloud applications in an automated way? #00:48:27-7#

R: I do think so. Because all these processes that would mean I only explain the architecture sounds for me like an automating process. That's why I thought about the backup doing before in. #00:48:44-7#

I: Ja. Okay. And what do you think about the presented approach, whether it can help to investigate security incidents more easily? Do you think it can help to investigate security incidents more easily? #00:49:00-6#

R: It depends on the investigation team. But yes, I think we're doing a lot of documentation in this architecture at least in the blockchain where all processes have been documentated. So, yes, I do think the investigation can be much faster. #00:49:32-1#

I: Mhm. Okay. And the last but not least, do you think that the presented approach can help to identify responsible parties in a legally secure way? So, in case of a dispute, help to identify a responsible person? #00:49:52-1#

R: Sure, because documentated. And so, yes, it can be improved this. #00:49:58-5#

I: Mhm. All right. Those were my final questions, but before we finish the interview, now, it's actually the time on which you are free to also propose your ideas. You're free to also bring in here, your thoughts on whether that approach has some improve, need for improvements, some weaknesses or maybe you also see some upcoming risks which you would like to mention at the end. So, more or less summarised, now it is that the stage is yours and you can comment and bring up some other thoughts on that approach. #00:50:40-1#

R: Yeah. First of all, I think that's a good study. And I already did my thought on the backup. And I think it's not bad because I, first, enter this, the question with do this architecture (is no longer?) #00:51:06-9# complexity. So, I don't, I answered with no and I don't think that's bad. I think that's even good because we need some human understanding to build a complex architecture, what cannot be easily hacked. And for that, we have to improve our processes and many ways probably also more automative. But I think in this case, we implement things like the blockchain where we're documentating a lot of things in a way that can't be changed without a log. That's the best way for investigation, and sounds good. #00:51:58-4#

I: Amazing. So, if you have nothing to add, we are in the closing phase of the interview. And during the closing phase, I would like to ask you to recap all your questions you provided here or your answers you provided here. I provided the questions. And (laughter) I would like to ask you to rate your experience and the quality of your statements based on school marks. So, based on school marks in European or in German school, would you say the statements you provided, you're an expert in that area and the statements you provided were very good, good, satisfactory, sufficient, poor, or insufficient, which would be a six and a very good would be a one. A good would be a two, a three would be a satisfactory, a four would be a sufficient, a five would be a poor, and a six would be insufficient. #00:52:52-4#

R: Yeah. So, my own answers I have to rate, right? #00:52:58-8#

I: Mhm. Ja, exactly. #00:52:59-9#

R: Okay. #00:53:00-2#

I: So, now that you've seen everything and what do you think the statements, how would you rate them? #00:53:05-4#

R: I'd say two. #00:53:07-9#

I: Mhm. Okay. Then thanks a lot for your openness for the participation and your time. As mentioned, as an outlook here, what happen will next is that it will be transcript. It will be anonymised and it will be used for the evaluation of my PhD. Thank you very much and I will stop the recording. #00:53:33-0#

R: Thank you, bye. #00:53:34-5#

(End of interview)

TRANSCRIPT INTERVIEW PARTICIPANT #11:

I: All right. We are starting the interview. Now, the interview is started to be more precise. Welcome and thanks for participating to the interview. Before we start with the main phase, I already introduced that we will start with a warm up and introduction phase. And the aim of that phase is to get you known a bit better. And therefore, my first question to you is, can you briefly tell me something about your professional background and your daily tasks? #00:00:38-5#

R: Yeah. Sure, of course. My name is (Person) and I'm a Team Lead of Collaboration Solutions at (Organisation). So, my responsibilities are coordinating a team who are responsible for the complete M365 stack. So, in terms of security, collaborations, and the products like SharePoint, OneDrive, Teams and the complete mail structure for around 15,000 people in Europe. So, my daily business is coordinating these teams and always I like to pronounce. So, according, like the team structure, the team building and the facing of technology where we want to build or what we want to build. Right now, we are moving from onsite securities and onsite, or on prime services to cloud services since a year and a half. And you know, that's my daily task. Anything else from background, what I did before or? #00:01:53-6#

I: No, no, that's amazing. That's amazing. #00:01:56-0#

R: (laughs) Okay. #00:01:56-2#

I: Ja. Just maybe your educational background. So, school starting or apprenticeship and such. #00:02:05-4#

R: Just school and then I, yeah, went to military for more than eleven years. And after that, I spent three years in consulting with team sizes more than 80 people. #00:02:21-8#

I: Mhm. Perfect. #00:02:23-4#

R: As a project lead. #00:02:24-4#

I: Amazing. Ja, in fact, that also gives us a bit information about your professional lifetime or career in years. Perfect. So, to summarise that, you have more than now let's say 15 years of experience in working? #00:02:40-3#

R: Hmm, yes, more than 15 years. Right, yeah. #00:02:45-3#

I: Ja, okay. (laughter) That's amazing. Okay. Good. All right. I think from everything, we know your background, and as already introduced at the beginning, I do have also some quantitative questions where I would like to give you a statement and ask you to answer that statement based on the values strongly agree, agree, neutral, disagree, strongly disagree. All right? #00:03:13-5#

R: Mhm. #00:03:13-9#

I: So-, #00:03:14-8#

R: Okay. #00:03:14-8#

I: - the first statement is I am a computer science expert. #00:03:18-4#

R: Agree. #00:03:20-1#

I: I am an information security expert. #00:03:24-6#

R: Agree. #00:03:26-2#

I: I am a cloud computing expert. #00:03:29-7#

R: Strongly agree. (laughs) #00:03:31-8#

I: And I am a cryptography expert. #00:03:36-5#

R: Hmm, not that much. So, what-, what's between agree and not agree? (laughs) #00:03:44-1#

I: Neutral. #00:03:45-6#

R: Neutral. So, I would like to answer the question with neutral. #00:03:49-6#

I: Okay. Amazing. Ja, thanks a lot. This is already the warm up. And I think we are warm (laughs). So, we can immediately enter into the main phase. And for the main phase, I already introduced you three case studies. So, company A, company B, company C. And the first-, #00:04:09-8#

R: Yeah. #00:04:10-0#

I: - question I do have here is do you understand the case studies? #00:04:13-7#

R: Of course. (laughs) #00:04:14-7#

I: Okay. Do you think the cases are realistic in those case studies? #00:04:20-3#

R: Yes, of course. #00:04:21-9#

I: Okay. And now, I would like to talk with you about risk of cloud adoption. So, we're talking about adopting cloud applications. And as already mentioned, I would like to talk about the risk of cloud adoption. So, the question here is do you have any background in risk management and what can you tell us about risk management? #00:04:48-6#

R: Yes, I do have some skills, and this I would like to have and also experience. I also mentioned that I have more than three years spend in project management as a project lead of a security project. So, that means, security phone, mobile security phones and a governance construct. And therefore, we have a lot of security experience in this. So, I have done a lot of risk management in case of, yeah, security. #00:05:23-5#

I: Okay. Great, cool. Now, I would also like to show you a so-called risk matrix on which we would now like to evaluate or to estimate risks. #00:05:38-8#

R: Mhm. #00:05:39-6#

I: And here the question is have you ever seen a risk matrix before and have you ever worked with a risk matrix? #00:05:45-5#

R: Yes, I do have. #00:05:46-7#

I: Okay. So, we have here a risk matrix in a format of 5x4, which is as common as other matrix 3x4, or 3x3. So, the thing is we have five values here in the probability and we do have four values in impact. And as said, and as you have already seen, the probabilities are on the left-hand side, we have probabilities below ten percent called rare, probabilities between ten and 30 percent, we call unlikely. We have probabilities between 30 and 60 percent, we call that possible. Between 60 and 90 percent, we call likely and more than 30 percent risk, 90 percent or more probability we call certain.

On the other hand side, on the x-axis, we do have the impact, so, how many money would result if the-, or would be needed to spend or would be lost to be more precise if that risk occurs or takes place. And here-, #00:06:51-8#

R: Mhm. #00:06:52-0#

I: - we do have negligible, which is if the turnover per year is below ten percent. So, we had the case studies with turnovers and if ten percent of the yearly turnover would be the impact of the risk, then we would say this is negligible for a company. And using that logic also for the other values ten to 30 percent, 30 to 80 percent, and 80 or more percent. I think as I understood you correctly, this is fine, right? #00:07:19-9#

R: Yeah. Got you. #00:07:21-3#

I: Okay. Good. Do you think risk management makes sense for the proposed use case or do you think risk management makes fence for adapting cloud applications in these three case studies? #00:07:39-0#

R: Of course. Sure, you have to do this in case of every implementation of any secured, any IT, any using of IT, you have do a risk (analysis?) #00:07:52-4#

I: Mhm. Now, the topic of my thesis or of my dissertation to be more precise is based on compliance driven risks. And compliance-driven risk means everything is so compliant, so, just for explanation is companies do set themselves rules or get rules also from government. So, there are some certain rules which governments need to follow on. And compliance-driven configurations are now if you adopt a cloud application and you adjust the cloud application based on the rules you set yourself. These are compliance-driven configuration. So, to bring you also an example on that, if you for example, say okay, my backups need to be stored in Spain, then this is a compliance requirement, all backups need to be stored in Spain in a compliance-driven configuration is now, if you configure the cloud application such that it stores backups in Spain. Mhm. Okay? #00:08:49-6#

R: Sure. (laughs) #00:08:50-4#

I: (laughs) Okay. So, my dissertation is as said on the compliance-driven configurations and the aim is to configure cloud applications, compliance-based. So, therefore, I would like to present you three risks and we rate the risks on the use cases, on the case studies. And let me just share my screen and then we go step by step through the risks. And I would ask you to rate the risk as you think they are on the specific cases. Okay? #00:09:25-3#

R: Mhm. #00:09:26-3#

I: Always interrupt me if anything is unclear. Okay? #00:09:31-9#

R: I will do. #00:09:33-2#

I: So, we are the first case in the case study, where we have that software company which would like to adopt an ERP system for their company. And they are doing highly critical stuff. So, if they get hacked, that would be a super mess. However, they adopt the cloud servers from an ISO-certified company, which is based in Europe. So, I think this is the summary of case A. And now, the risk which I would like you to ask and to rate on is the risk that the-, that the cloud application provider, so, provider A in the case study implements a contractually not mutually agreed configuration. So, that the cloud application provider sets a configuration which was not agreed on so to say. #00:10:30-0#

R: So, first of all, that is not good (laughs), if the provider (laughs) is so, is set in a test or in a RFP sets or when did this happen? Or did it already happen or it’s just a risk that we are planning on? #00:11:00-6#

I: Depending on the case study-, #00:11:04-6#

R: Yeah. #00:11:05-2#

I: This is a new provider so, we-, #00:11:08-8#

R: Okay. #00:11:09-0#

I: - they do not have any experience with that provider. #00:11:11-3#

R: Okay. Yeah. Okay. That’s what I just want to-, #00:11:14-0#

I: Mhm. #00:11:14-4#

R: - confirm (laughs). #00:11:15-5#

I: Ja. #00:11:16-6#

R: So, in case of that, usually as a customer, I get to try on a-, #00:11:31-0#

I: Control? #00:11:32-0#

R: - control my external partner. I am responsible to give them all set ups or compliance I would like to set up-, #00:11:49-4#

I: Mhm. #00:11:50-2#

R: - before. So, it’s much better for my company, from company A, it’s well-based and it’s all done. So, that will probably every time happen, and when I onboard a new provider, I would like to say that it’s not that high that that could be happening. So, (laughs) maximum unlikely. #00:12:15-4#

I: Mhm. #00:12:16-3#

R: And if this happens, that will be a mess. It could be critical at least, because another catastrophe, not that critical but I think that could be critical and unlikely because I don't think that that will be-, I am, I am worried. ISO

27001:2019. So, in fact, so my company is already based on how the process will be done in the provider, so, all this will be already proceed and all this has been done. I don't think that can be possible. Unlikely and critical, medium at least. #00:13:14-5#

I: Okay. Medium. #00:13:15-9#

R: That will be my answer. #00:13:17-5#

I: All right. Great. (laughter) Ja, I think you have the flow, that’s exactly what we are doing now. (laughs) So, we stay with provider A, okay? #00:13:29-6#

R: Mhm. #00:13:30-5#

I: And the next question is the risk that the implementation of a compliance-driven configuration gets delayed due to slow or manual processes. I can also provide you here and okay, I think you already got it. (laughs) If you need an example just let me know. #00:13:51-7#

R: (laughs) That is very possible. Every new, every impacted, a new provider can be, they promise you everything from we will do this until tomorrow, and four months ago, you think about ah, that should be done last month. So, there is the category high, that will happen. That is not a risk, that will happen in my point of view. So, from - I can be happy and will be not happen but I would like to say 60 to 90 percent so likely and a possibility. And there is not that impact because I am planning, if I am a set up company, I would like to have a proper planning. So, that the plan is not set in place and one day after the whole group will be implemented. So, likely and (laughs) ten percent neg/-, #00:15:11-6#

I: Negligible. #00:15:12-3#

R: Yeah, right. #00:15:13-7#

I: Okay. I will take negligible and write here medium. Okay? #00:15:17-4#

R: Yeah, please. #00:15:18-4#

I: Okay. So, and last but not least, the risk of denying the implementation of a configuration in case of a dispute. So, imagine a data leak occurs, if data leak happens, and now the parties go to court. And the court needs to clarify whose fault was it that the data leakage could arise due to a wrong configuration. And now, the question is how high is the risk that one of the parties will say that was not me, that was not how we agreed on. So, acts more or less opportunistically. #00:16:02-7#

R: So, the company or the provider I would like to pay for his job is already certified. So, he will definitely say wasn’t my fault (laughs) every time. So, that is true. And I have seen this before. So, that will happen. So, I’d say it’s high risk. But maybe I don't understand it right. #00:16:43-8#

I: Mhm. #00:16:44-4#

R: Is the question that it will be possible that he will say it wasn’t my fault? Or is the question how possible will this that we are getting to-, yeah, during one of these cases I would like to go to the judge. #00:17:13-8#

I: The question here is if, if already something happened-, #00:17:19-1#

R: Okay. #00:17:20-4#

I: That some of the party says no, that was not my fault that this happened. #00:17:25-8#

R: Every time. #00:17:27-7#

I: Excuse me? #00:17:30-0#

R: Yeah, every time. So, nobody would say in this case because they have a high value of classification and they would like to take care of the data both sides. So, both are companies with one of this, the company I am in, who do the risk analysis, I have to avoid the situation at least and searching for a good company who can provide this. And if I would like to, yeah, get this risk down, so, I would like to minimise this risk, that is what just happened in my head, I have to search another company but this is not a risk who I can minimise with another company but just happened. (laughs) Because the good company will say, no, it wasn't my fault because they have to stand up for a good security company. And they don't get in place with oh, no, we did a big mistake. All my other customers would like to, I don't know, I would like to say this is critical. Going on another intake, likely, yeah, it's likely that certain, certain in the possibility. But certain in the possibility but the business case is not that high because I'm right. (laughs) That it's their fault. So, I'm winning for the judge. But (laughs) maybe now I would like to go with high, so-, #00:19:43-2#

I: Ja, okay. #00:19:43-6#

R: So, certain and yeah. #00:19:45-4#

I: Yup. All right. That was for company A. Now, let's continue with company B. You remember the case? So, company B is a big huge, huge chemical company, which picked the cheapest of three offers for an intrusion detection system. The intrusion detection system itself is maintained by an internal IT department. So, they outsourced all their services except the maintains of the services so to say. And now, they would like to have a sub-contractor which support them in the intrusion detection area. Therefore, they picked the cheapest out of three offers. #00:20:26-8#

R: Mhm. #00:20:27-2#

I: And that offer is placed in India and has a Google rating of four to three stars out of 400 ratings. #00:20:35-2#

R: Okay. A, therefore, it is very possible that they misunderstood my compliance configurations. I see this in the past on my own. So, I would like to say this will happen. (laughs) Therefore, it's very likely. And how much impact will this have on my business value or the finance, I think that it will be high. #00:21:19-9#

I: Mhm. #00:21:20-5#

R: But yeah, and thinking about critical I or maybe not, so-, #00:21:28-6#

I: Ja. The-, #00:21:32-4#

R: That doesn't matter okay. High. (laughs) #00:21:34-1#

I: No, no. No, no. Because if you're in critical it's very-, #00:21:37-4#

R: I think it will be high. Yeah, yeah. I think that it will be likely but maybe not so it's high, high, so, it doesn't matter, you know, matrix, so, it's high. #00:21:50-2#

I: Exactly. Mhm. The risk of that the implementation of compliance configuration gets delayed due to slow or manual processes. #00:21:59-7#

R: If they get the comp/- no, if they get the configurations, that will be done, that will be done fast, that will be really done fast. I have seen this before. But you know, with some typos but I just mentioned before, but it will be done. (laughs) So, it is-, I would like to go with low at least. I would like to go with low. So, it's, yeah. #00:22:36-3#

I: Okay. Ja, it's fine. #00:22:39-4#

R: Yeah, on point. (laughs) #00:22:40-5#

I: Ja. (laughs) #00:22:42-2#

R: So, it will be (raw?) #00:22:42-9#, it will, really, really raw but I'm in the right to say the company or the company and that from my point of view, it is not done-, has not been done in the right time. So, they will be delivered but there are mistakes in for sure. (laughs) #00:23:07-6#

I: It will-, #00:23:09-1#

R: So, that will be done but you know, but yeah. #00:23:12-1#

I: This falls then also under the category of manuals, slow manual processes. So, for example, if you bring up a configuration, they said it-, said that in configuration, however, you realise that there's an error and it needs again to be redone, this is still the process. So, this is more or less the maintain or the adjustment process. So, do you see-

, #00:23:38-1#

R: No, then let me switch to medium in the matrix. We have to switch to medium. #00:23:43-2#

I: Mhm. See the whole until it's all rightly configured. #00:23:47-1#

R: Yeah. #00:23:47-4#

I: Yes. Please. #00:23:48-2#

R: Yeah, but it's too rare and the possibility, it's unlikely, between unlikely and rare in my vision. And therefore, it can be much more critical because the run time will be longer. So, it can be critical but unlikely but it can be happening. #00:24:05-7#

I: Mhm. So, we are at medium, right? #00:24:07-5#

R: Yeah, medium. #00:24:08-5#

I: Mhm. And last but not least in case of a dispute that some of the parties will deny a configuration. #00:24:15-8#

R: That's high. Let's take this very high. Let me watch through the matrix-, #00:24:24-8#

I: Ja. #00:24:24-9#

R: - and-, #00:24:25-4#

I: Take your time. #00:24:26-4#

R: - get my, (laughs) get my - that's very high, between, because I think they are in the, in the country out of Europe. So, we have to agree where our or where our judges will have set up. And that can be a discussion that takes a long time. And if this happened, it's a, would be a mess. I mean, 400-ish people have said that Google will be a good customer. So, (laughs) I would like to go with possible and catastrophe, my God. #00:25:33-0#

I: Catastrophe. #00:25:34-4#

R: Yeah. I would like to go with very high. #00:25:35-5#

I: Ja, exactly. So, that's fine. All right. And now, the farmers, so, the case C. #00:25:45-0#

R: Mhm. Well-, #00:25:50-0#

I: So, now the question is that this big company implements something which will then-, #00:25:54-6#

R: Can we go to down on the (laughs) that's the case up here. So, I just have to // I just have to watch out where, what the provider was doing just-, #00:26:12-7#

I: Ja. Sure, sure, sure. Take your time. #00:26:15-2#

R: What the provider wants, so, where the-, what did the provider C already (unclear) #00:26:24-0# okay, yeah, yeah, okay. Yeah, okay. No, no, no. I would like to go with-, it can be possible but don't interrupt my money. So, I would have to go low. #00:26:39-4#

I: Mhm. #00:26:40-7#

R: In this case. The risk and the implementation of the compliance-driven risk. So, they just want to have product but a lot of people in this case from a customer point of view, provider can implement in this case like, you know, pretty fast. And I don't think that that will be a mess. (laughs) So, they deliver a product. So, it's going fast. So, I would like to go also low. #00:27:22-8#

I: Mhm. #00:27:23-5#

R: - in here. So, it can be possible, but it will be (raw?) #00:27:28-3# but the money is maximum in the money now case. So, they don't spend that much time on it. There will be no much delay at least, I think. The risk of implementation (unclear) #00:27:44-8# they will lose (laughs) sorry. (laughs) it's minimised, so. It's high. It's high. #00:28:02-3#

I: All right. I think we have the first round so to say. So, this was more or less the risks from the current architecture, cloud architecture we know, and which we all are aware of. Now, I would like to propose you the architecture I developed during my PhD. And then we do exactly the same. So, we do again the risk assessment here. All right? I explain you the architecture based on a concrete implementation case as it is an architecture and explaining an architecture without a use case is quite (laughs) quite generic. That's why here we do have a use case. The use case of an intrusion detection system. Okay? #00:28:56-6#

R: Yeah, mhm. #00:28:57-9#

I: During that archi/-, or with that architecture, first and foremost, we do have three participants. We do have a cloud application consumer. This is a person who uses the cloud application. We do have a cloud application provider. This is the person who provides the cloud application and we do have the cloud application itself, as an independent, you can see it as a technical user. Okay? #00:29:27-8#

R: Okay. #00:29:28-4#

I: So, those are the three participants of that architecture. Now, what they are doing at the beginning of the architecture and this is shown here also as step one is they use a Diffie-Hellman protocol, which is a protocol for creating symmetric shared key. So, what they are doing is, they are using the blockchain for sharing symmetric, or for creating a shared symmetric key. Everyone starts his public Diffie-Hellman value on the blockchain and uses that public Diffie-Hellman value and does create a shared symmetric key. So, every one of those three participants at the end has access to the shared symmetric key. #00:30:10-5#

R: Okay. #00:30:13-4#

I: I will always stop after an explanation step to see-, #00:30:17-3#

R: (laughs) Okay. I got you. (laughs) #00:30:18-6#

I: - whether I lost you or not. Okay. #00:30:22-8#

R: Yeah. #00:30:23-0#

I: But that's, that's amazing. #00:30:24-1#

R: No loss man. (laughs) #00:30:26-0#

I: This is the first thing. So, the first thing is now all three participants have access to the same symmetric shared key. In the next step, the person who would like to configure the cloud application, let's assume the cloud application consumer would like to configure the cloud application, uses a configuration, a configuration you can think of as a text document, as a text file, as a JSON file, as an XML file or whatever, whatever structure you can think of but at the end, you can bring it back to text format. Okay? #00:30:59-0#

R: Mhm. #00:30:59-8#

I: Now, the cloud consumer writes down his configuration based on a text file for example, and encrypts that text file with a shared symmetric key. Hmm? #00:31:13-6#

R: Mhm. #00:31:14-6#

I: Okay. Next step, and this is again, this step here. He or she, so, the person who would like to configure the cloud application starts that encrypted configuration on the blockchain. In the next step, the cloud application, so, now a case to intrusion detection system, uses an extended backend script, the so-called management script. This, you can think of as a python script-, #00:31:44-1#

R: Mhm. #00:31:44-5#

I: - which runs in the background. That script monitors the blockchain for changes. So, that script monitors whether something changed on the blockchain. As the cloud application consumer start configuration on the blockchain, this cloud management script will realise that and will download the configure-, the encrypted configuration from the blockchain. Having access to the symmetric key, it is able to encrypt, to decrypt the configuration and is able to get the plain text of the encrypted start configuration. #00:32:21-8#

R: Mhm. #00:32:23-3#

I: Ja. A question or still clear? #00:32:27-8#

R: No, no, no, no. #00:32:29-1#

I: All fine? #00:32:31-1#

R: I got you fine, yes. #00:32:32-0#

I: Okay. Okay. In the next step, as this cloud management script now has access to the encrypted, so, to the decrypted, sorry. To the decrypted configuration, so, to the plain text to be more precise, it uses that configuration and overrides the existing application configuration. So, you can think of in Snort, the configuration is nothing than a text document. And if you just replace that text document, you have implemented a new configuration. Huh?

Beside overwriting the configuration of the application, the cloud management script also monitors the log files of the cloud application. In that, or using that, it is possible or able to see whether the configuration was implemented successfully or not. Now, we assume the configuration was implemented successfully. So, it's overwritten, restarted and in the log files we see it's fine, it's working. Now, the idea is as soon as the cloud management scripted text, okay, everything worked fine, it triggers, it starts, it initiates a backup from the virtual machine on which the cloud application is running. So, the whole virtual machine on which a cloud management script is running and the application, so, the intrusion detection in ours, in our case gets backup. Okay? #00:34:08-0#

R: Mhm. #00:34:08-6#

I: That backup is then used and the hash value out of that backup is created. #00:34:15-4#

R: Mhm. #00:34:17-8#

I: That hash value is then written back to the cloud application, to the blockchain-, #00:34:24-1#

R: Mhm. #00:34:25-1#

I: - as proof of implementation. Now, the idea is in case of for example a dispute and someone says, this was not what we implemented or agreed on, // on the configuration you take the backup, which you could maybe agree on downloading, you take the hash value and say, "Hey, this is the hash value you confirmed on the blockchain. Please show me the backup corresponding to that backup and now we can investigate that. And having that said, this is more or less (laughs) the architecture I wanted to present you. So, the configuration is more or less done by encrypting a text file or-, #00:35:02-9#

R: I have one question before I forget. (laughs) #00:35:04-4#

I: Ja, sure. Sure, sure, sure, fire up. #00:35:06-7#

R: Why? Why don't you do a backup before updating the plain text message to the server? #00:35:14-1#

I: I mean, you do have already a backup. I mean, and initially you could do a backup, so, you could set up the system, you could make a backup. And then follow up in the // (unclear) #00:35:29-8#

R: I mean, your process, you already described the process-, #00:35:32-7#

I: Ja. #00:35:33-3#

R: - which one we run. So, in case of a backup. #00:35:36-1#

I: Ja. #00:35:36-8#

R: So, if I did my backup and the change on the config doesn't happen that often I think-, #00:35:43-6#

I: Ja. #00:35:44-1#

R: So, in case I have a backup of a configuration that's more than one year old, maybe I did a backup or did an update or something like this, and these guys haven't done your job. (laughs) So, in my point of view, I think if you implement a backup before updating the configuration, you have a clear backup what was, yeah, per hour or two hours old. So, after that, you're doing all this, you can having a, yeah, two hours of backup and with the same structure and the same backend structure also. So, maybe just a (unclear) #00:36:37-8# proven (laughs), proving the concept. (laughs) #00:36:42-9#

I: Ja, sure, sure. I mean, the thing is (laughter) at the end, you need or the thing is to prove the implementation of a configuration. It's not necessarily the point in time and depending on which you agree on. I mean, there might be, and every second the change which tremendously change everything. So-, #00:37:08-9#

R: Yeah. #00:37:09-3#

I: - doing a backup one minute before, or two minutes before or ten hours before wouldn't change the overall concept of it. I agree. #00:37:17-1#

R: No, no, no. No. #00:37:18-4#

I: That it would be more likely or easier to investigate at the end-, #00:37:25-8#

R: Mhm. #00:37:26-1#

I: But at the end, in both cases, the implementation of the configuration gets hashed. #00:37:32-2#

R: Yeah, yeah, yeah, sure. #00:37:33-8#

I: And this is the point here. #00:37:35-1#

R: Yeah. #00:37:35-7#

I: Though from a practical perspective, I really agree with what you said. #00:37:40-1#

R: Yeah. Nice. (laughs) #00:37:43-6#

I: Ja. #00:37:44-4#

R: Our bias (laughs). #00:37:45-5#

I: You just have to use it. (laughs) #00:37:48-7#

R: Yeah. #00:37:49-0#

I: All right. So, coming back to the risk management and to the use cases we just discussed, and now, we are assuming that we are using the architecture I proposed to you here to configure the cloud applications. I would like again to do the risk assessment with the three cases you already investigated, we already discussed. So, provider A, provider B, provider C. We assume-, #00:38:21-3#

R: Mhm. #00:38:21-5#

I: - you know provider A, provider B and provider C are implementing the proposed approach. And we would like to do now the risk assessment here. A quick disclaimer, there is, as always in life nearly nothing you can assume, except that the blockchain here in that case is secure. So-, #00:38:45-5#

R: Mhm. #00:38:45-7#

I: - please do not assume that any 50 plus attack or something like that take place. Please abstract from the blockchain security in that case. #00:38:54-5#

R: Mhm. #00:38:55-4#

I: Beside that, you can even not assume and this is also in cryptography or wherever that the provider 100 percent correctly implemented it. So, that might also be a risk (laughter) (which remains?) #00:39:08-8#. And having that said, I think that hopefully answered your question if there was one. #00:39:17-7#

R: I can run through this point at least. But I would like to quick thing about. So, assuming technology on architecture like I have seen in your case right now, it's much more trustful I think, it was a presentation start with this. So, first of all, I think that-, I think that breaks up some trust feeling in my mind so (laughs) I just say okay, using this, that kind of architecture. So, not nice and I do understand this as a customer. That's also a point. But I think that will be minimise some risk in some cases. So first, we're running through case A, correct? #00:40:14-8#

I: Mhm. #00:40:15-2#

R: Case A? #00:40:15-6#

I: Ja, yes please. #00:40:16-8#

R: In this case, this will go risk (unclear) #00:40:27-5# improving the (unclear) #00:40:28-8# so, we need to think about what the-, it doesn't change on the technical side, it only change on technical side. But I will have to go down on low on this because I think if the provider can implement technology (unclear) #00:40:58-2# team, I too get them that he knows what he is doing and yeah. (unclear) #00:41:12-4# Yeah, that depends more on my point of view on the, on my company A, company. #00:41:25-3#

I: It's company A. #00:41:27-9#

R: Yeah, with company A. #00:41:29-1#

I: Ja, it's company A. #00:41:29-3#

R: So, that's on my company A. So, I think I'm surprised or so in the matrix, I would like to think that it's still possible if this happened. It's, that's still medium. Sorry. #00:41:53-2#

I: Mhm. #00:41:53-6#

R: Still medium. #00:41:55-0#

I: Fine, that's fine. You can rate whatever. It's your interview (laughter) so you can rate however you want. (laughs) And the risk of denying the implementation of configuration in case of dispute. #00:42:08-5#

R: It's still expensive. I would like to go into, go down to unlikely and critical. So, I would like to put medium point, point. Company B. #00:42:31-7#

I: Yup. #00:42:32-2#

R: I don't trust this (unclear) #00:42:36-9#. I stay with high in this case. No. #00:42:46-7#

I: The process? #00:42:50-0#

R: And in this case, I would like to go up. #00:42:54-2#

I: Mhm. #00:42:55-0#

R: Why? (laughs) If a company who I'm not trusting presenting a complex structure architecture, I am not that peaceful that they can implement it in a good, yeah, in a good, good configuration. And also, I probably have to hesitate with some delays and all this. And with-, so, I would like to go up with high at least. #00:43:37-8#

I: Okay. #00:43:38-9#

R: Because I think the structure is too complex for a provider that came from India and have 400 Google ratings. Sorry for that. (laughs) #00:43:57-3#

I: So, can you rate here on the risk matrix that? #00:44:02-7#

R: Yeah. It's like I said before, I go with the answer before possible, and minor, and then I would like to go with likely because I think it's much more possible. And still the money is minor also, go, went up to high. #00:44:29-0#

I: All right. Then let's do that. And here, in the case of dispute. #00:44:37-7#

R: Yeah, still very high. #00:44:42-2#

I: Mhm. All right. And last but not least. #00:44:49-8#

R: Yeah. It's still low. #00:44:53-4#

I: Mhm. #00:44:54-2#

R: Because the provider we are searching is set up and just a little. Next one-, #00:45:04-9#

I: Yes. #00:45:05-6#

R: - also, low. And in the last point, I would like to go down on medium because I think the possibility is lower, the catastrophic is still there (laughs) but it depends on the matrix to medium. #00:45:27-6#

I: Cool. So, you're fine with that? #00:45:38-6#

R: Yeah. #00:45:40-1#

I: Amazing. #00:45:42-2#

R: When you say that (laughs) #00:45:47-3#

I: So, let me just check. Okay. There was some stuff-, ja, I forgot of course one question. Question nine was forgotten. So, now I repeat it. And this is actually after I presented you the architecture but I think (laughter) you already answered that question also during the presentation. So, the question is again quantitative, and I would like to ask you or provide you with the statement, I've understood the approach. #00:46:24-1#

R: Yeah, that (laughs) I did. #00:46:27-0#

I: So, strongly agree, agree, neutral, disagree, strongly disagree? #00:46:30-7#

R: Sorry. Agree. #00:46:32-5#

I: Okay. Perfect. We did the evaluation and now that you have seen the approach and you have also with risk management made some risk management with it, I do have the question, do you think the use of the blockchain makes sense at this approach and yes, why or no, why not? How could you maybe replace it? #00:46:56-6#

R: First of all, it's the first time, I've seen this case. So, I haven't seen this before. Second, I do think that that will make sense because it improves the security of the architecture and the way of communication, the communication ways at least. So, I can do this on different way of communication in case of I communicate with B and 2. So, all this makes sense for me. #00:47:28-1#

I: Okay. And now, also, that we are slowly coming to the end of the interview, I would again emphasise three topics which we maybe quickly can also discuss. If we are recalling the presented approach here, do you think the presented approach improves the transparency of cloud application configurations? Do you think that approach makes cloud configurations more transparent? #00:47:59-4#

R: No. (laughs) I don't think so. #00:48:03-9#

I: Mhm. #00:48:04-7#

R: So, it increase the complexity. And every time you increase complexity, much more people don't understand the structure. #00:48:13-0#

I: Mhm. Okay. #00:48:14-3#

R: So-, #00:48:14-3#

I: Ja, that's fine. Anything to add or? #00:48:19-1#

R: No. #00:48:19-6#

I: I don't want-, I don't want to interrupt you. Do you think the presented approach can help to configure cloud applications in an automated way? #00:48:27-7#

R: I do think so. Because all these processes that would mean I only explain the architecture sounds for me like an automating process. That's why I thought about the backup doing before in. #00:48:44-7#

I: Ja. Okay. And what do you think about the presented approach, whether it can help to investigate security incidents more easily? Do you think it can help to investigate security incidents more easily? #00:49:00-6#

R: It depends on the investigation team. But yes, I think we're doing a lot of documentation in this architecture at least in the blockchain where all processes have been documentated. So, yes, I do think the investigation can be much faster. #00:49:32-1#

I: Mhm. Okay. And the last but not least, do you think that the presented approach can help to identify responsible parties in a legally secure way? So, in case of a dispute, help to identify a responsible person? #00:49:52-1#

R: Sure, because documentated. And so, yes, it can be improved this. #00:49:58-5#

I: Mhm. All right. Those were my final questions, but before we finish the interview, now, it's actually the time on which you are free to also propose your ideas. You're free to also bring in here, your thoughts on whether that approach has some improve, need for improvements, some weaknesses or maybe you also see some upcoming risks which you would like to mention at the end. So, more or less summarised, now it is that the stage is yours and you can comment and bring up some other thoughts on that approach. #00:50:40-1#

R: Yeah. First of all, I think that's a good study. And I already did my thought on the backup. And I think it's not bad because I, first, enter this, the question with do this architecture (is no longer?) #00:51:06-9# complexity. So, I don't, I answered with no and I don't think that's bad. I think that's even good because we need some human understanding to build a complex architecture, what cannot be easily hacked. And for that, we have to improve our processes and many ways probably also more automative. But I think in this case, we implement things like the blockchain where we're documentating a lot of things in a way that can't be changed without a log. That's the best way for investigation, and sounds good. #00:51:58-4#

I: Amazing. So, if you have nothing to add, we are in the closing phase of the interview. And during the closing phase, I would like to ask you to recap all your questions you provided here or your answers you provided here. I provided the questions. And (laughter) I would like to ask you to rate your experience and the quality of your statements based on school marks. So, based on school marks in European or in German school, would you say the statements you provided, you're an expert in that area and the statements you provided were very good, good, satisfactory, sufficient, poor, or insufficient, which would be a six and a very good would be a one. A good would be a two, a three would be a satisfactory, a four would be a sufficient, a five would be a poor, and a six would be insufficient. #00:52:52-4#

R: Yeah. So, my own answers I have to rate, right? #00:52:58-8#

I: Mhm. Ja, exactly. #00:52:59-9#

R: Okay. #00:53:00-2#

I: So, now that you've seen everything and what do you think the statements, how would you rate them? #00:53:05-4#

R: I'd say two. #00:53:07-9#

I: Mhm. Okay. Then thanks a lot for your openness for the participation and your time. As mentioned, as an outlook here, what happen will next is that it will be transcript. It will be anonymised and it will be used for the evaluation of my PhD. Thank you very much and I will stop the recording. #00:53:33-0#

R: Thank you, bye. #00:53:34-5#

(End of interview)