



Review

AI-Enabled IoT Intrusion Detection: Unified Conceptual Framework and Research Roadmap

Antonio Villafranca ¹, Kyaw Min Thant ¹, Igor Tasic ² and Maria-Dolores Cano ^{1,*}¹ Department of Information and Communication Technologies, Universidad Politécnica de Cartagena, 30202 Cartagena, Spain² Faculty of Economics and Business, UCAM Universidad Católica San Antonio de Murcia, 30107 Murcia, Spain

* Correspondence: mdolores.cano@upct.es

Abstract

The Internet of Things (IoT) revolutionizes connectivity, enabling innovative applications across healthcare, industry, and smart cities but also introducing significant cybersecurity challenges due to its expanded attack surface. Intrusion Detection Systems (IDSs) play a pivotal role in addressing these challenges, offering tailored solutions to detect and mitigate threats in dynamic and resource-constrained IoT environments. Through a rigorous analysis, this study classifies IDS research based on methodologies, performance metrics, and application domains, providing a comprehensive synthesis of the field. Key findings reveal a paradigm shift towards integrating artificial intelligence (AI) and hybrid approaches, surpassing the limitations of traditional, static methods. These advancements highlight the potential for IDSs to enhance scalability, adaptability, and detection accuracy. However, unresolved challenges, such as resource efficiency and real-world applicability, underline the need for further research. By contextualizing these findings within the broader landscape of IoT security, this work emphasizes the critical importance of developing IDS solutions that ensure the reliability, privacy, and security of interconnected systems, contributing to the sustainable evolution of IoT ecosystems.

Keywords: Internet of Things; intrusion detection systems; IoT security; Industry 4.0; XAI; blockchain; cybersecurity



Academic Editor: Lorenzo Carnevale

Received: 27 August 2025

Revised: 18 September 2025

Accepted: 30 September 2025

Published: 6 October 2025

Citation: Villafranca, A.; Thant, K.M.; Tasic, I.; Cano, M.-D. AI-Enabled IoT Intrusion Detection: Unified Conceptual Framework and Research Roadmap. *Mach. Learn. Knowl. Extr.* **2025**, *7*, 115. <https://doi.org/10.3390/make7040115>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things (IoT) represents one of the most significant technological transformations in recent decades, enabling the interconnection of billions of devices that collect, process, and share information in real time. This ecosystem, spanning from industrial sensors to smart-home devices, has revolutionized sectors such as healthcare, industry, and smart cities by improving efficiency, optimizing processes, and opening new opportunities for innovation. According to IHS Markit, the number of IoT devices is expected to reach 125 billion by 2030 [1]. However, this massive connectivity also significantly expands the attack surface, exposing critical vulnerabilities and making cybersecurity a key priority to ensure the reliability and continuity of connected systems.

In this context, the IDSs play a crucial role in safeguarding the integrity and confidentiality of data while ensuring the continuous operation of systems. IDSs are tools designed to detect, monitor, and respond to malicious activities within networks and devices, which is especially critical in distributed and dynamic environments like IoT.

As illustrated in Figure 1, the main functionalities of an IDS include analyzing vulnerabilities, system configurations, and attack patterns; monitoring network traffic and file activity in real time; evaluating system integrity through behavioral analysis and detecting unauthorized changes; tracking and logging security incidents; generating reports, including audit trails and compliance monitoring; and responding proactively through alerts and risk mitigation. These capabilities allow IDSs not only to detect threats but also to contain and mitigate them in real time, ensuring the protection of highly interconnected systems. Modern IDS solutions increasingly integrate AI techniques, such as anomaly detection with deep learning (DL) models and federated learning (FL) approaches, to adapt to evolving threats in dynamic IoT environments [2,3].

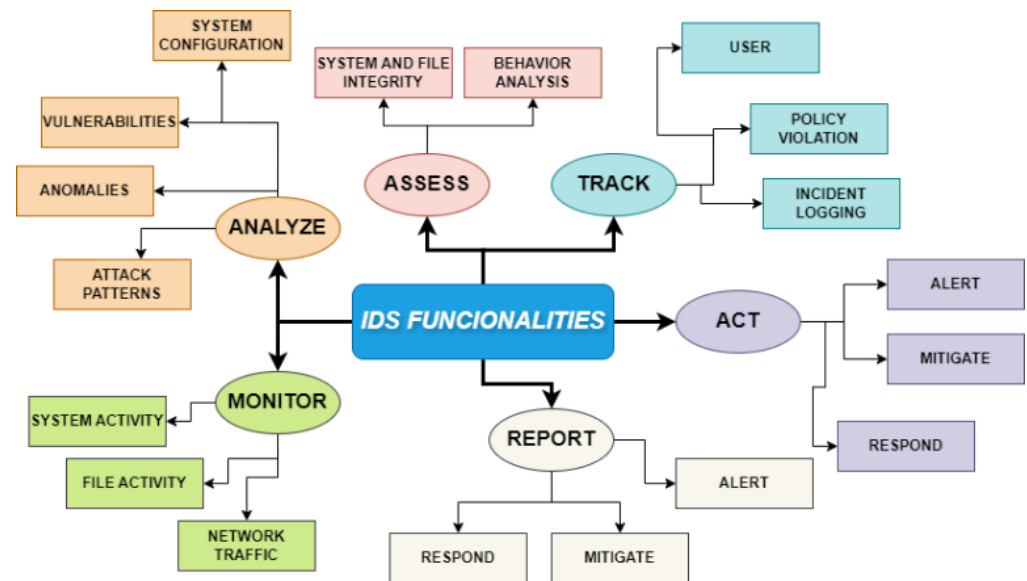


Figure 1. IDS Functionalities. Main functions of an IDS, including analysis, monitoring, reporting, assessment, tracking, and response to security incidents.

IoT environments pose specific challenges for IDSs due to the resource-constrained devices, including limited processing power, storage, and energy consumption, as well as their distributed and heterogeneous architectures. The implementation of IDSs in IoT demands solutions that not only detect threats but also adapt to the limitations of devices while offering scalability and efficiency in dynamic settings. Emerging strategies such as Edge AI [4,5] and FL [6] have shown potential in addressing these challenges by decentralizing detection and minimizing resource usage while preserving data privacy.

As shown in Figure 2, the IoT security market is projected to reach \$20,771 million by 2025, with a compound annual growth rate (CAGR) of 40%, according to IoT-Analytics. This growth underscores the urgent need for robust security solutions capable of protecting an ever-expanding ecosystem.

Despite advancements in IDS design for IoT, significant gaps remain in the scientific literature. Most studies focus on isolated aspects, such as anomaly detection techniques or challenges in device integration, without providing a comprehensive and systematic perspective that addresses both the strengths and limitations of current proposals. Furthermore, many existing works emphasize static models, overlooking novel approaches such as blockchain-based IDSs [7,8], Explainable AI (XAI) [9,10], and generative models for data synthesis to enhance the detection of advanced threats. This lack of exhaustive analysis limits the ability of researchers and practitioners to identify key trends, emerging challenges, and opportunities to develop more scalable and adaptable solutions.

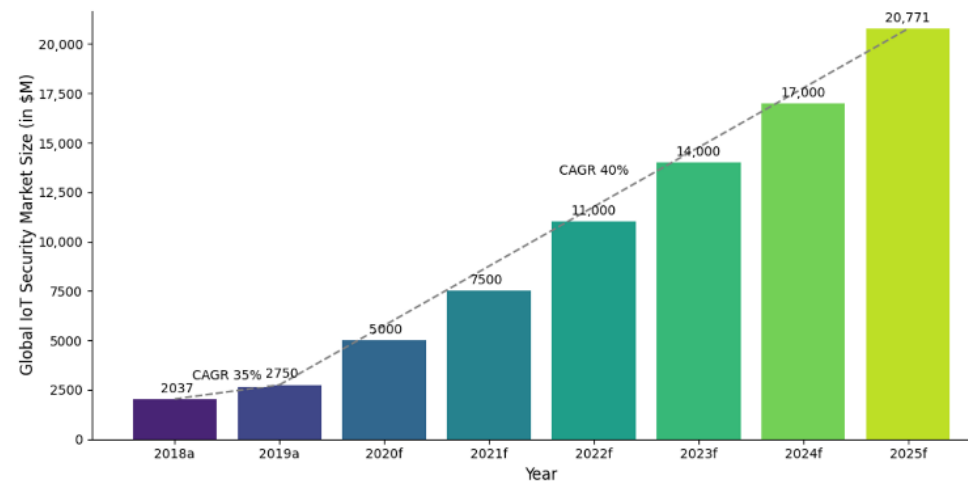


Figure 2. Global IoT Security Market Size (in \$M). Projected growth of the global IoT security market from 2018 to 2025, highlighting significant increases in market size and CAGR.

This article addresses this gap by conducting a literature review (LR) exclusively focused on IDSs designed for IoT. To provide a structured analysis, this study is guided by six key research questions:

- RQ1. What types of IDS are proposed in the related literature for IoT?
- RQ2. Do they include an evaluation of the proposal? If so, is it conducted through simulation, experimentation, or neither? Are datasets used? Which ones?
- RQ3. What aspects of the proposals are usually optimized?
- RQ4. Is AI used? What are the main approaches?
- RQ5. Are the proposals related to the industry? How?
- RQ6. What aspects are identified as open challenges/opportunities for improvement/future work in these proposals?

In recent years, IDSs specifically designed for IoT have started incorporating advanced technologies to overcome traditional limitations. Research has demonstrated the effectiveness of AI techniques, such as machine learning (ML) and DL [11–15], in enhancing intrusion detection accuracy and reducing false positives (FPs). For example, deep neural networks (DNNs) [16] and algorithms like Random Forest have been successfully implemented to identify anomalous patterns in network traffic, achieving significant improvements in threat detection.

Additionally, recent trends, including the use of Generative Adversarial Networks (GANs) for data synthesis and XAI improving decision transparency, remain underexplored in the context of IoT IDS. For example, Y. Saheed et al. [17] have presented an innovative approach for zero-day botnet detection in the Internet of Vehicles. Saheed and Misra [18] introduce CPS-IoT-PPDNN, an explainable, privacy-preserving deep neural network for anomaly detection in CPS-enabled IoT environments. The model employs a single-layer LSTM autoencoder to compress network traffic data into a low-dimensional latent space, applies adaptive differential privacy to protect sensitive inputs, and uses Deep SHAP to generate both local and global explanations of its decisions. When tested on the Edge-IIoTset and X-IIoTID datasets, CPS-IoT-PPDNN achieves perfect precision, recall, and F1 scores in binary detection and exceeds 99.9% accuracy in multi-class scenarios, all while maintaining fast training times and real-time operational capability.

Hybrid approaches and mathematical optimization methods have been explored to improve IDS efficiency in industrial and commercial scenarios. However, these solutions need to be further tailored to the unique characteristics of IoT devices, such as their limited computational resources and distributed nature.

The rest of this paper is structured as follows. Section II outlines the LR methodology, including article selection, classification, and analysis; Section III details the key findings, covering both overall techniques and challenges as well as an evaluation per research question; and Section IV summarizes the contributions and suggests future directions for IDS development in IoT environments.

The main contributions of this work include the following:

- A detailed classification and analysis of the types of IDSs applied in IoT, evaluating their methodologies, architectures, and operational approaches.
- A critical evaluation of the performance metrics and datasets employed in recent research, highlighting key trends and inherent limitations.
- Identification of opportunities and open challenges such as scalability and energy efficiency in resource-constrained environments, and provision of guidance for future research directions.
- An exploration of advanced AI paradigms, e.g., FL, edge-based detection, and blockchain-assisted architectures, emphasizing their applicability in modern IDS solutions for IoT security.

Beyond synthesizing existing research, the review provides value to different audiences. For researchers, the proposed taxonomy and mapping of methods to datasets highlight open research gaps and avenues for innovation. For practitioners, the comparative analysis and dataset-selection guidance serve as a practical reference to design and deploy IDSs adapted to real-world IoT environments. For policymakers and standardization bodies, the identification of interoperability issues, lack of benchmarking, and energy-awareness gaps provides an evidence base to inform regulatory frameworks and the development of global evaluation standards.

2. LR Method

The LR has been applied to obtain a comprehensive and detailed view of IDSs in the IoT domain to identify its current state. The LR methodology used in this research is divided into the sections described below.

2.1. Collection, Inclusion and Exclusion of Articles

The articles selected for this study on IDSs applied to IoT were filtered using standardized inclusion and exclusion criteria to ensure consistency and comparability across reviewed works. To maximize relevance, the search was structured using a predefined set of terms: “Intrusion Detection Systems” OR “IDS” AND “IoT”, “Malware Detection in IoT”, “Intrusion Prevention Systems (IPS) for IoT”, and “Anomaly Detection in IoT”. These terms were applied to IEEE Xplore [19] and Science Direct [20], two of the most reputable databases in the fields of engineering, technology, and cybersecurity.

These databases were chosen based on their comprehensive coverage of peer-reviewed literature and their frequent updates, which ensure access to the most current studies. Preliminary scoping searches further confirmed that most relevant articles on IDSs and IoT were available in these sources, thus justifying our focused approach.

Search terms had to appear in article titles, abstracts, or keywords to keep the review focused, and standardized inclusion/exclusion criteria (detailed in Table 1) were applied to filter out irrelevant studies. Every paper was then double-blind screened by two reviewers, any disagreements were settled by a third, senior reviewer, and a secondary technical check ensured consistency and minimized subjective bias. Although IDS methods span many domains, this work concentrates exclusively on IoT-specific solutions, given the unique demands of IoT environments (limited processing power, decentralized architectures, and resource-constrained devices) that call for tailored detection techniques.

Table 1. Inclusion and exclusion criteria for the reviewed articles with their explanation.

I/E	Criteria	Explanation
Exclusion	Duplicate articles	Articles that appear repeatedly in one or more databases.
	No full text	The full content of the article cannot be accessed, thus limiting the ability to evaluate it.
	Misclassification	The article is misclassified, i.e., belonging to a conference Instead of a journal.
	Article in another language	English is a universal language, so if the article is not in English, it will be excluded.
	Incorrect relation	Articles that do not include an IDS solution proposal for the IoT field or cannot be applied in this field due to incompatibilities will be excluded.
	Implicit relation	The article mentions IoT tangentially or in non-central sections, without an explicit focus on the topic.
Inclusion	Summary or review	The article presents a detailed analysis related to IDSs in IoT.
	Proposal evaluation	The article carries out an evaluation of the proposal either through simulation or real implementation.
	Future research opportunity	Articles that allow for an open framework for future improvements will be studied.

2.2. Data Collection

To enhance the accuracy, relevance, and objectivity of the literature review, a secondary filtering process was applied to the selected articles. This additional step aimed to identify the most technically significant and innovative contributions related to intrusion detection in IoT environments, ensuring that only articles with substantial scientific value were retained for further analysis. The criteria for this second filter include the following:

- IoT-specific focus: inclusion only of articles addressing IDS solutions tailored to IoT constraints.
- IDS classification: categorization by detection type (signature-based, anomaly-based, hybrid).
- AI integration: analysis of AI methodologies (e.g., DL, FL).
- Algorithm evaluation: identification of intrusion-detection algorithms and models for comparative analysis.
- Industrial applicability: assessment of relevance to real-world scenarios (industrial, smart infrastructure).
- Validation approach: review of experimental setup (real-world deployment, simulation, datasets).
- Emerging technologies: attention to blockchain-based IDS, XAI, and Edge AI for enhanced security and transparency.

This filtering phase prioritized articles that aligned closely with the research objectives while systematically excluding publications that failed to meet the selection criteria. By focusing on technical relevance and methodological rigor, this approach enabled a clearer identification of current research trends, technological gaps, and areas requiring further development.

2.3. Data Analysis

The collected data were processed using a hybrid qualitative and quantitative research methodology. For the qualitative analysis, each article was examined and coded based

on a comprehensive set of predefined attributes, including: the type of IDS proposed; its intended application in IoT environments; the technology employed (e.g., ML, DL); the identification of opportunities for future research; whether the solution incorporates blockchain; if it is theoretical or empirical; its industrial applicability; focus on network security; the presence of case studies; implementation details (real-world vs. simulated); the datasets used; and the inclusion of emerging technologies.

These criteria provided a structured framework that allowed us to extract and group key qualitative themes across the literature. Quantitative methods were subsequently applied to the coded data to statistically validate trends and generate graphical representations of the findings, thereby ensuring a clear and reproducible representation of the literature landscape.

The categorized data were structured in alignment with our six research questions. Articles addressing RQ1 were classified by IDS type, which facilitated a comparative review of detection strategies. For RQ2, studies were grouped by evaluation methods and datasets used to ensure diversity and reproducibility. RQ3 focused on optimization techniques, including resource consumption reduction, improved detection accuracy, and reduced response time, which are critical factors for resource-limited IoT environments.

For RQ4, articles were assessed based on their use of AI techniques (particularly DNN, FL, and XAI) to understand their impact on detection performance and false positive reduction. RQ5 analyzed the real-world applicability of IDSs across various sectors such as industrial automation, smart cities, healthcare, defense, financial services, energy infrastructures, and AgriTech, emphasizing aspects like threat mitigation, data privacy, and resource efficiency. Finally, RQ6 identified existing gaps, limitations, and future research directions, noting the potential of Blockchain-based IDS, Edge AI, and Generative Models in enhancing detection accuracy, scalability, and overall security in IoT environments.

2.4. Other Reviews

In the current literature, many reviews of IoT IDSs provide broad overviews yet lack standardized evaluation frameworks, which hinders direct comparisons. Table 2 outlines various aspects evaluated by different authors. For example, while Mohiuddin et al. [21] discuss computational complexity and false positives, and Mohanta et al. [22] focus on interoperability, others like Choudhary et al. [23] highlight emerging techniques without supplying measurable performance metrics. Many studies concentrate on a single technology (e.g., ML or DL) or on specific solutions like FL or blockchain, leaving out newer approaches such as XAI, generative GANs, or Edge AI.

Our proposal overcomes these limitations by offering a clear, standardized evaluation of IoT IDS. We introduce a conceptual framework of IDS-for-IoT analysis dimensions (see Figure 3) that organizes detection Type, Evaluation Method, Optimization Goals, AI Techniques, Industrial Applicability, and Open Challenges across the surveyed works. We also provide concise guidelines for selecting datasets based on diversity, balance, and real-world relevance, while addressing issues like synthetic bias. Moreover, we outline optimization strategies to enhance detection accuracy, computational efficiency, and system adaptability. Finally, we map IDS applications across sectors such as smart cities, industrial IoT, healthcare, and agriculture, demonstrating tangible improvements in false positive reduction and threat detection.

Table 2. Thematic scope of existing IDS-in-IoT surveys. Each column indicates whether a given review covers that topic.

Ref	Year	Contribution	Techniques Evaluated	Deployment Strategies	Validation Strategies	Datasets Evaluated	Emerging Technologies Evaluated	Challenges Addressed
[21]	2016	Categorizes network anomaly detection techniques into classification, statistical, information theory, and clustering methods, and discusses dataset challenges.	Yes	No	Yes	Yes	No	Highlights issues such as dataset limitations, data noise, and evolving network behaviors.
[22]	2020	Survey of security challenges in IoT and ML, AI and blockchain based solutions	Yes	No	No	No	Yes	Confidentiality, integrity, availability and issues by protocol layers
[23]	2019	Identification of necessary infrastructure for IDSs in IoT, emerging techniques to solve security problems.	Yes	Yes	No	No	No	Resource constraints (computation, energy), heterogeneity of devices
[24]	2017	Review of contemporary IoT IDS techniques, attack classification and future challenges.	Yes	Yes	Yes	Yes	Yes	ML, DL
[25]	2021	Critical review of IDS techniques in IoT, deployment and validation strategies, attacks, public datasets and challenges.	Yes	Yes	Yes	Yes	Yes	Advanced detection, communication security
[26]	2018	Survey of IDSs for smart IoT environments, covering methods, features and mechanisms, as well as vulnerabilities and use cases.	Yes	Yes	No	No	Yes	Power and computational constraints, device heterogeneity, need for lightweight and robust solutions for IoT.
[27]	2024	A survey reviewing Blockchain and federated learning-based IDSs for edge-enabled industrial IoT networks, emphasizing privacy and security improvements and offering future research recommendations.	Yes	Yes	Yes	No	Yes	Highlights privacy, security, and computational challenges
[28]	2023	Develops a taxonomy of IoT attacks by domains, threat types, execution methods, software surfaces, protocols, device properties, adversary location, and damage level, while reviewing detection mechanisms and outlining open challenges.	Yes	No	No	Yes	No	Highlights vulnerabilities due to device heterogeneity, lack of standard security measures, and evolving attack dynamics
[29]	2024	A survey reviewing energy-based attack detection in IoT devices by examining how power consumption analysis can reveal anomalies and malicious activities.	Yes	Yes	No	No	No	Highlights issues such as noise filtering in power signals, subtle variations in energy consumption, and the lack of standard evaluation methods
[30]	2025	Review DL-based IDSs for IoT botnet detection.	Yes	No	Yes	Yes	Yes	Botnet detection, ensemble methods, adversarial vulnerability
[31]	2025	Modern IDS techniques in IoT that reviews methods, datasets, metrics, and outlines future research directions.	Yes	No	Yes	Yes	No	Highlights computational complexity, high false positives, data imbalance
[32]	2025	AI-based malware detection in IoT networks within smart cities, reviewing approaches such as SVMs, decision trees, and deep neural networks, and discussing detection accuracy and energy consumption challenges.	Yes	No	No	No	No	Addresses issues including detection accuracy, energy consumption costs, and the complexity of securing heterogeneous IoT networks.
This	2025	Technical evaluation of IoT, datasets, evaluation of proposals, optimized aspects, techniques used, application fields and future opportunities.	Yes	Yes	Yes	Yes	Yes	AI, datasets, used techniques and new directions

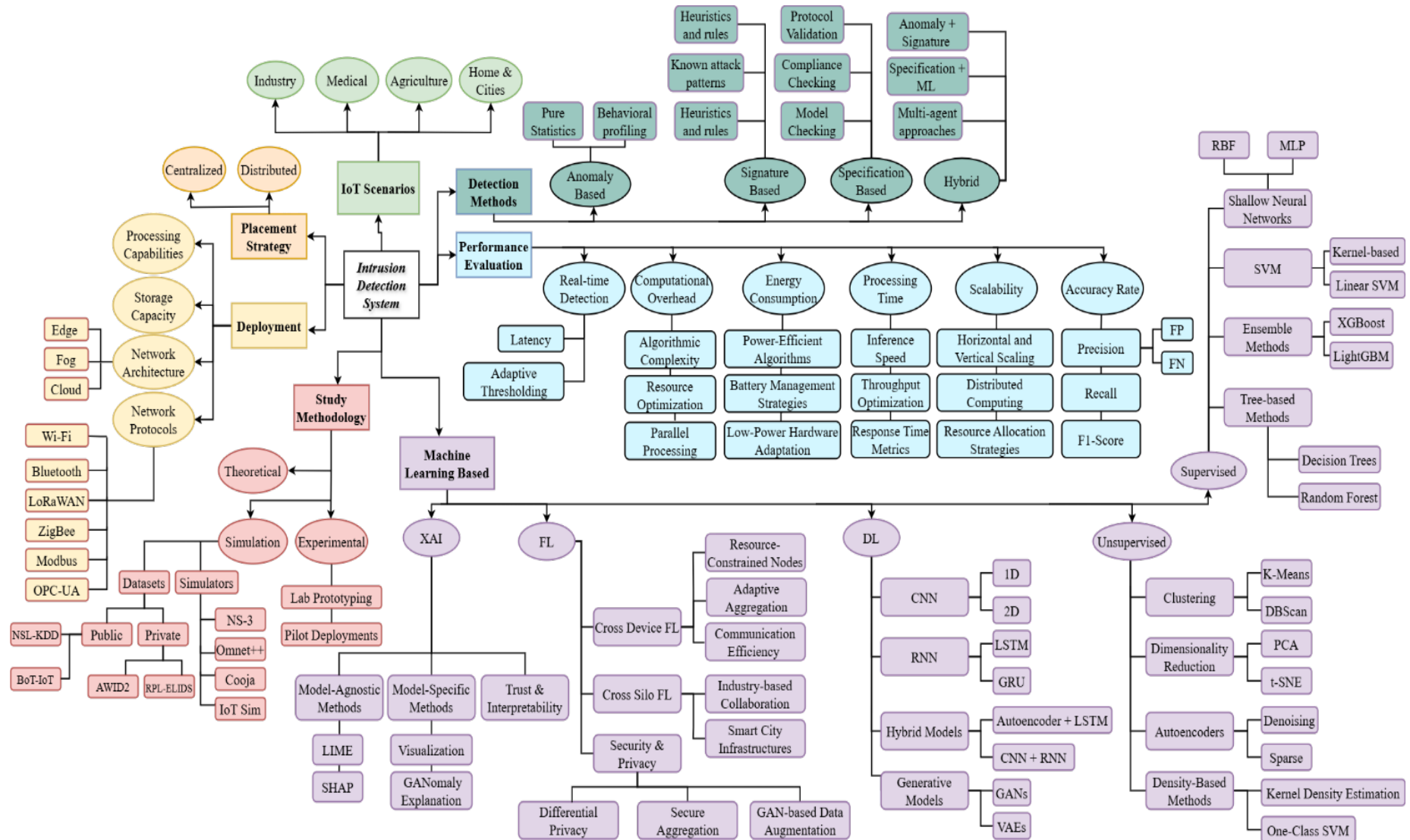


Figure 3. Conceptual framework of IDS-for-IoT analysis dimensions. This diagram outlines the six key aspects (detection Type, Evaluation Method, Optimization Goals, AI Techniques, Industrial Applicability, and Open Challenges) that structure our survey.

3. LR Findings

This section presents the findings obtained through the LR process described earlier. Figure 4 highlights the increasing scientific interest in IDSs for IoT environments since 2018. Despite a brief stagnation in 2020–2021 due to global disruptions like the SARS-CoV-2 pandemic, the research field experienced a strong resurgence from 2022 onwards, driven by the massive proliferation of IoT devices and advancements in AI-based detection strategies. In Figure 5, we can see the flowchart illustrating the procedure followed for the study of the articles.

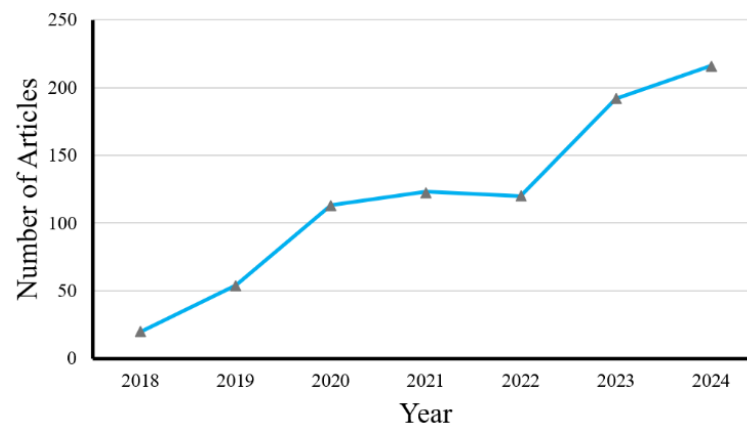


Figure 4. Annual number of articles retrieved by keyword search on IDSs in IoT (IEEE Xplore and ScienceDirect) from 2018 to 2024 (pre-screening).

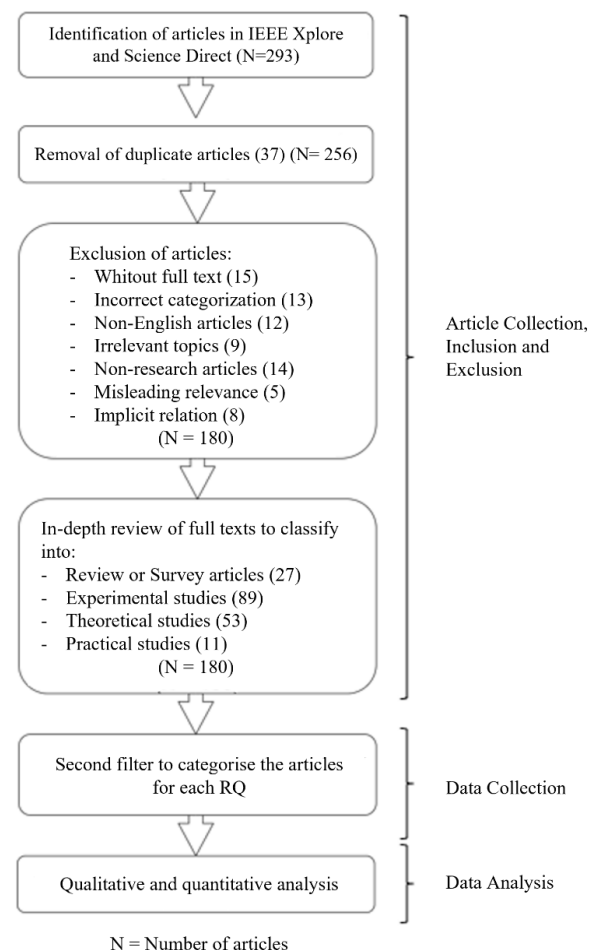


Figure 5. PRISMA flow diagram.

These findings emphasize the growing importance of IoT security and the scientific community's continuous effort to address emerging threats in complex technological ecosystems. The following sections provide a detailed analysis of the identified trends, methodologies, and technologies shaping modern IDSs for IoT.

3.1. IDS Types

To answer RQ1, it is crucial to understand the different approaches of IDSs present in the literature. IDSs can be broadly categorized into five main types. Network-based IDSs (NIDSs) monitor network traffic in real time, analyzing data to identify malicious behavior across the network. These systems provide a comprehensive view of network activity, making them particularly effective in highly dynamic and distributed IoT environments. Recent developments in Edge AI IDSs extend this concept by performing traffic analysis closer to the data source, reducing latency and enhancing privacy protection in IoT environments [33].

Host-based IDSs (HIDSs), on the other hand, are installed directly on devices, where they monitor their activity and detect unauthorized changes. While valuable for safeguarding critical devices, HIDSs are less commonly used because their scope is limited to the individual device, making them less effective for broader threat detection [34].

Anomaly-based IDSs (AIDSs) operate by creating profiles of normal behavior and generating alerts when significant deviations occur. This approach is especially beneficial for identifying new and unknown threats, which is crucial in IoT settings characterized by continuously evolving attack vectors. However, their implementation can be complex and is often accompanied by challenges such as higher rates of FP.

Behavior-based IDSs (BIDSs) analyze patterns of behavior to detect anomalies, but their configuration and maintenance can be challenging due to the inherent noise in behavioral data. Recent proposals, such as the one by J. Tang et al. [35], aim to mitigate this issue by incorporating social context into behavior modeling. Their system uses behavior comparison and correlation across IoT nodes to improve detection accuracy while minimizing irrelevant behavioral fluctuations.

Lastly, Signature-based IDSs (FIDSs) rely on comparing network traffic to a database of known attack signatures. While efficient against previously documented threats, FIDSs are less effective at addressing emerging or unknown attacks, limiting their applicability in rapidly changing environments. Blockchain-based IDSs enhance signature-based detection by ensuring tamper-proof logging of security events and alerts. By using a distributed ledger, these IDSs prevent log manipulation and improve trust in data integrity, making them suitable for critical infrastructures and collaborative IoT systems [36].

A review of the literature indicates that all IDS types are being used in IoT security, though their application varies by context. Figure 6 shows that NIDSs are the most prevalent due to their effectiveness in real-time network monitoring in distributed environments. In contrast, while AIDSs can adapt to new attack vectors, they often suffer from high false positive rates, and HIDS, though less frequent, are crucial for protecting critical devices. FIDSs and BIDSs are less common due to limitations in detecting emerging threats and managing noisy behavioral data. This diversity underscores the need to tailor IDS solutions to the specific challenges of IoT. Hybrid approaches, grouped as "others" in the literature, merge several detection techniques to address specific IoT challenges. By integrating multiple methodologies, these solutions achieve higher accuracy and lower false positive rates than traditional IDS types.

The architecture of IDSs, whether centralized or decentralized, also plays a critical role in their application. Centralized IDSs consolidate data analysis at a single point, offering a unified global security view and facilitating advanced monitoring through comprehensive

data aggregation. However, they require significant computational resources and may suffer scalability issues, e.g., larger networks can lead to bottlenecks, increased latency, and reduced responsiveness. Additionally, a centralized design creates a single point of failure that may compromise overall security. In contrast, decentralized IDSs distribute detection tasks across multiple nodes, enabling parallel processing that reduces the latency of transmitting data to a central server and improves real-time responsiveness. This approach also enhances privacy by localizing processing on edge devices. Nevertheless, the inherent coordination among heterogeneous nodes increases system complexity, requiring robust protocols to maintain data coherence and effective synchronization.

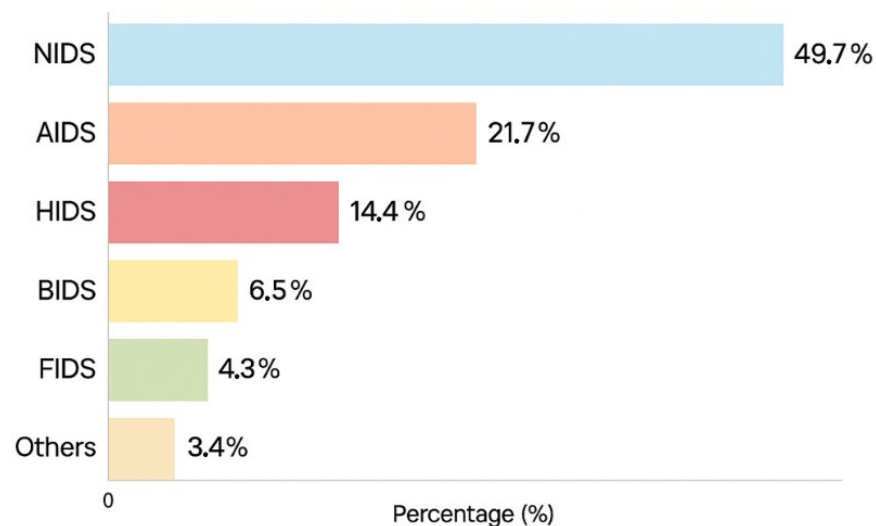


Figure 6. Graph illustrating the distribution of IDS types used in the literature, highlighting the prevalence of NIDSs, AIDSs, HIDSs, BIDSs, FIDSs, and others.

Edge IDSs exemplify decentralized approaches by performing security analysis near the data source, further minimizing latency and preserving user privacy, which is critical in time-sensitive environments like healthcare IoT and industrial control systems. Additional trade-offs include energy efficiency and maintenance: while centralized systems benefit from high-performance servers, they incur higher energy costs and simpler maintenance that poses risks due to single-point failures. Decentralized models, although offering improved fault tolerance and scalability, demand complex integration and interoperability solutions.

In summary, centralized IDSs provide comprehensive data visibility and simplified management but may struggle in large-scale, dynamic IoT environments due to latency and resource bottlenecks. Conversely, decentralized architectures offer better scalability and responsiveness with enhanced privacy, although they introduce challenges in system complexity, coordination, and energy management.

Table 3 provides a comparative analysis of the main IDS types used in IoT environments, detailing their detection approaches, advantages, limitations, and practical use cases. It reveals that no single IDS type is optimal for all contexts, as the choice depends on the threat model and specific constraints. For instance, NIDSs are highly effective for detecting broad, real-time threats such as DDoS attacks in smart cities, but may overlook device-level issues like firmware tampering in medical devices, which HIDSs better address.

Similarly, AIDSs can identify zero-day attacks by spotting deviations from normal behavior; however, they tend to produce high false positive rates. FIDS, while dependable for known threats, struggle with zero-day attacks due to their reliance on fixed signatures. Additionally, Blockchain IDSs ensure tamper-proof logging, which is ideal for critical financial systems, whereas Edge IDSs reduce latency by analyzing data near the source,

proving advantageous for real-time detection in industrial IoT. Hybrid IDSs combine multiple methods to effectively address both known and emerging threats, enhancing overall accuracy and efficiency.

Table 3. Detailed Comparison of IDS Types Based on Detection Approach.

Type of IDS	Detection Approach	Advantages	Disadvantages	Use Case Examples
NIDS	Monitors network traffic patterns.	Scalable, monitors entire network, effective in distributed systems.	Limited visibility on device-level activity.	Smart cities, Healthcare.
HIDS	Monitors activity on a single device.	Device-specific security, effective for high-value devices.	Cannot detect network-wide threats, limited scalability.	Critical medical devices.
AIDS	Detects deviations from normal behavior.	Detects zero-day attacks, adaptive to new threats.	High FP rate, complex to train and maintain.	Industrial control systems.
BIDS	Detects anomalies in behavior patterns.	Flexible for dynamic environments, good for behavior profiling.	Noisy data requires continuous tuning, prone to behavior drift.	Smart homes, Autonomous vehicles.
FIDS	Matches traffic with known attack patterns.	Highly accurate for known threats, fast detection.	Fails against zero-day attacks and novel threats.	Enterprise networks, Web servers.
Edge IDS	Local analysis near data source.	Reduces latency, improves privacy, less bandwidth usage.	Limited by local resources, it requires synchronization with global IDS.	Healthcare IoT, Industrial IoT.
Blockchain IDS	Distributed ledger for event logging.	Tamper-proof event logging ensures data integrity.	High computational cost, complex integration with resource-constrained devices.	Financial institutions, Defense.

3.2. Types of Proposal Evaluation

In the reviewed articles, approximately 70% include some form of evaluation, which is crucial for assessing IDS performance, yet the absence of standardized metrics often hinders direct comparisons across studies. The majority of the articles employ two main evaluation methods: simulation or practical experimentation, as depicted in Figure 7.

Simulations are particularly popular for evaluating IDS performance, as they allow the creation of controlled environments that replicate real IoT conditions. Specialized tools such as NS-3 [37] or IoT Simulator [38] are frequently used in these studies.

For example, M. Amiri-Zarandi et al. [39] presented an IDS based on FL called the Social Intrusion Detection System (SIDS). The SIDS addresses the limitations of traditional centralized methods, which collect all data on a central server and therefore increase computational load and privacy risks, by training models locally on IoT devices and then aggregating them on a central server. Their study demonstrated that the SIDS improves detection accuracy, optimizes resource usage, and preserves privacy compared to centralized and individual approaches.

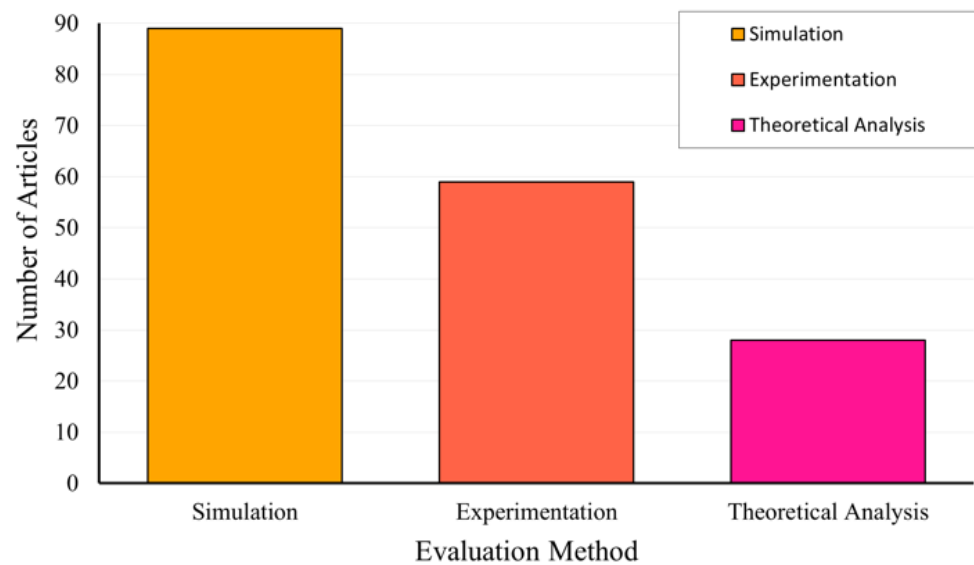


Figure 7. Different methods of evaluation used for IDS proposals in the reviewed articles, highlighting the prevalence of simulation, experimentation, and theoretical analysis.

Recent work by Kipongo et al. [40] and Sharadqh et al. [41] employs NS-3.26 to validate IDSs in IoT settings. Kipongo et al. simulate an AI-based IDSs in edge-assisted SDWSNs, achieving over 90% detection accuracy and packet-delivery ratios while balancing energy and latency. Sharadqh et al. assess HybridChain-IDS, a blockchain-anchored, bi-level framework, reporting high precision, recall, and F1 scores without degrading throughput or latency. These studies underscore NS-3's utility for capturing IoT complexity and heterogeneity.

Other articles opt for practical experiments conducted in real or controlled environments, which, although more costly, provide robust validation by capturing the inherent complexities of IoT. A. Verma et al. [42] carried out an experimental evaluation of seven supervised ML-based IDS classifiers (tuning them on CIDDS-001, UNSW-NB15 and NSL-KDD datasets) and then deployed each model on a Raspberry Pi 3 Model B+ to measure average response times and determine the best trade-off between detection performance and real-time latency. These tests demonstrated the system's effectiveness in real-time intrusion detection while addressing the complexity and variability of IoT environments. Similarly, M. Osman et al. [43] propose ELG-IDS, a hybrid intrusion detection system for RPL-based IoT networks that combines genetic-algorithm feature selection with a stacking ensemble of classifiers. In experiments on RPL attack datasets, ELG-IDS achieves up to 99.66% detection accuracy, demonstrating the effectiveness of GA-driven feature reduction and ensemble learning. Shalabi et al. [44], in their systematic literature review of blockchain-based IDS/IPS for IoT networks, highlight how distributed ledgers can ensure tamper-proof logging of security events and bolster trust in collaborative IoT environments, though they themselves do not implement new experiments.

Building on this, S. Li et al. [45] introduce HDA-IDS, which fuses signature-based and anomaly-based detection using a CL-GAN model. When evaluated on benchmark datasets such as NSL-KDD and CICIDS2018, HDA-IDS shows around a 5% improvement in detection accuracy and significant reductions in both training and testing times, underscoring the value of controlled experiments for validating IDS performance in heterogeneous IoT scenarios. These findings emphasize that a combination of simulations and real-world experiments is essential to comprehensively assess IDS scalability, accuracy, and practical applicability in IoT.

It is also essential to highlight the importance of using datasets in the evaluation of proposals. A dataset is an organized collection of data used to train and evaluate intrusion detection models. However, many publicly available datasets for IDS evaluation lack diversity, often failing to cover the full spectrum of IoT threats, such as low-rate DoS attacks or adversarial examples. This limitation can result in models performing well under controlled conditions but may fail in real-world scenarios. Using diverse datasets improves detection accuracy, model robustness, and generalization capacity, as shown in Figure 8.

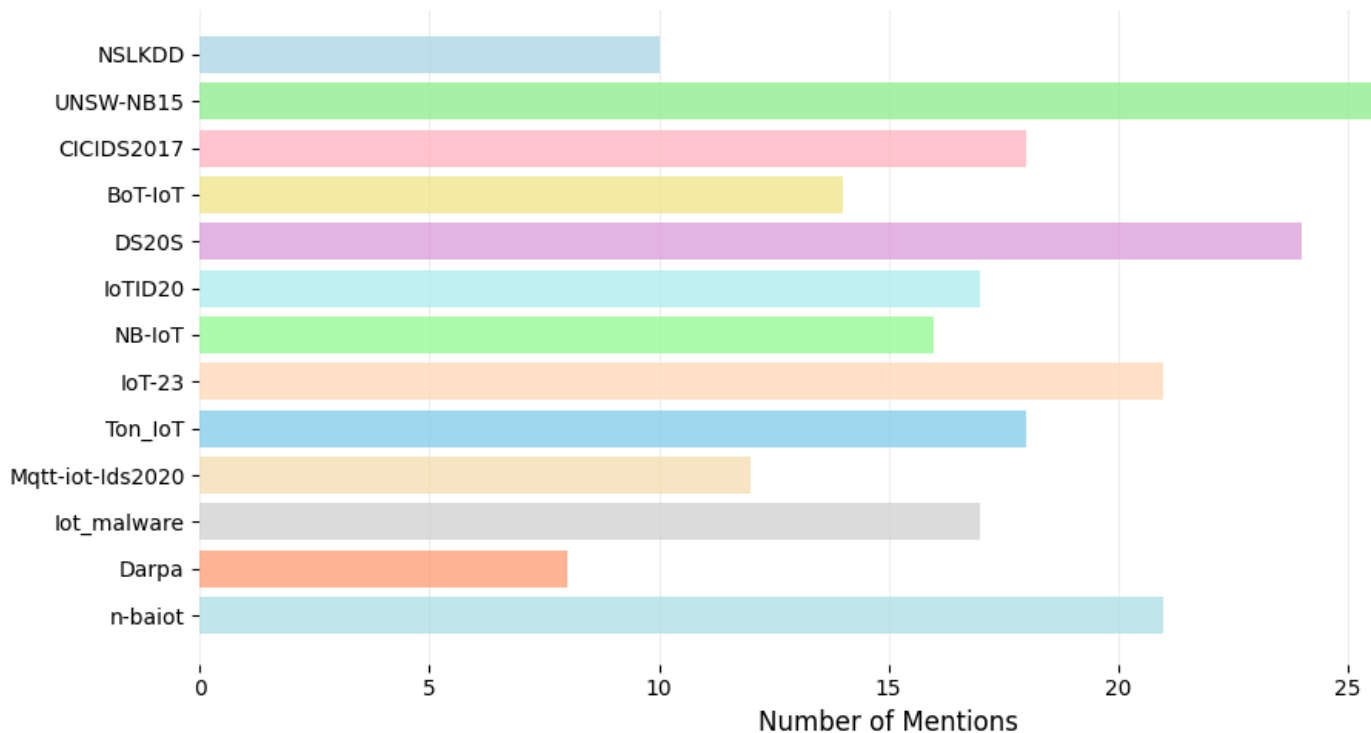


Figure 8. Frequency of usage of various datasets in the reviewed IDS articles, highlighting the prevalence of specific datasets used for evaluating IDS performance.

A common limitation is the reliance on synthetically generated data, which simplifies dataset creation but often fails to capture the dynamic nature of IoT traffic. For example, datasets like UNSW-NB15 and NSL-KDD rely heavily on simulated attacks, lacking more sophisticated threats such as polymorphic malware or encrypted traffic often found in real environments. This results in models that can detect straightforward threats but struggle with more complex patterns like zero-day attacks, which exploit previously unknown vulnerabilities.

Dataset imbalance is another frequent issue. Many datasets are dominated by either attack traffic or benign data, which can skew the model's learning process. For example, NSL-KDD contains a disproportionately high number of attack samples, leading models to over-prioritize attack detection while overlooking subtle variations in normal traffic. Conversely, datasets with few attack samples may cause models to miss rare threats such as low-rate DoS attacks. Although techniques like Synthetic Minority Over-sampling Technique (SMOTE) can help balance the data, they may introduce synthetic patterns that do not fully represent actual traffic behavior, potentially distorting detection metrics.

Lastly, the lack of realism in many datasets is a major concern. Real IoT networks often include multiple device types, variable traffic loads, encrypted communications, and sporadic interactions (factors that synthetic datasets struggle to replicate). For example, although datasets such as BoT-IoT and N-BaIoT are specifically designed for IoT environments, they are generated under controlled conditions and frequently lack the variability

of genuine network traffic. Figure 9 illustrates a side-by-side performance benchmark of five representative IDS models on the CICIDS 2017 dataset, comparing Precision, Recall, and F1-score for each approach [46].

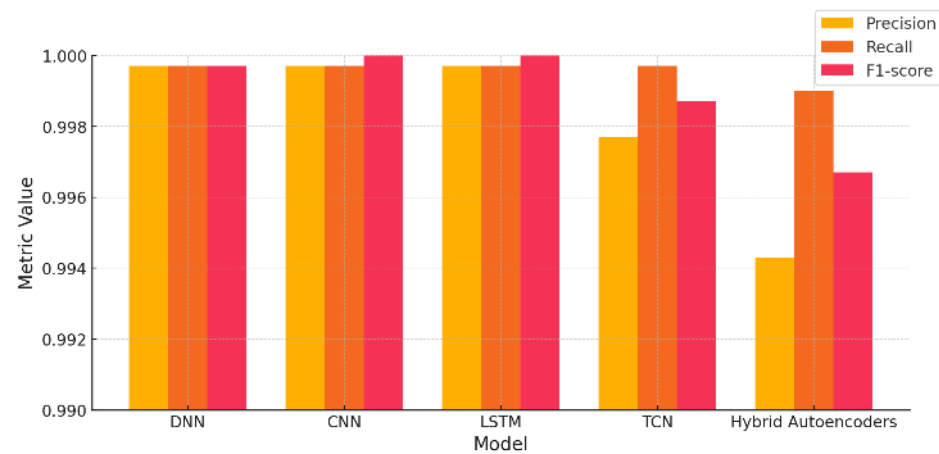


Figure 9. Performance Benchmark of Representative IDS Models on CICIDS 2017 (Precision, Recall, F1-score) [46].

Several studies have attempted to address these limitations by combining datasets to improve coverage. F. Nie et al. [47] introduce M2VT-IDS, a multi-task, multi-view learning framework that represents IoT traffic via three perspectives—spatio-temporal series, header-field patterns, and payload semantics—and processes these through a shared network followed by task-specific attention modules. Evaluated on the BoT-IoT, MQTT-IoT-IDS2020, and IoT-Network-Intrusion datasets, achieves over 99.8% accuracy in anomaly detection and similarly high precision, recall, and F1 for attack identification and device identification, all while avoiding redundant feature engineering. Similarly, S. Racherla et al. [48] evaluated Deep-IDS using the CIC-IDS2017 dataset, reaching a detection rate of 96.8%. While these results are promising, the datasets primarily focus on a limited set of threats, such as DDoS attacks, and fail to capture the full range of IoT-specific vulnerabilities.

Several studies have compared IDS performance against established benchmarks. For instance, R. Ahmad et al. [46] evaluated the effectiveness of hybrid classifiers using datasets such as BoT-IoT, N-BaIoT, CICIDS2017, and UNSW-NB15. However, these datasets often exhibit repetitive attack patterns, typically limited to basic scans and floods, which tends to overlook more complex, multi-stage attacks or encrypted payloads.

To select the most suitable dataset for IDS evaluation, it is essential to prioritize those that encompass a diverse range of attack types, device behaviors, and traffic patterns to prevent overfitting to a limited threat landscape. Datasets should reflect realistic network conditions, including encrypted traffic, dynamic variations in load, and sporadic device activity, as commonly observed in IoT environments. Additionally, the balance between benign and malicious traffic must be carefully considered, as datasets skewed towards a majority class can distort model evaluation. Finally, the dataset size should be sufficient to capture network complexity without overwhelming computational resources, particularly in resource-constrained IoT devices, ensuring a comprehensive and reliable assessment of IDS performance.

Table 4 summarizes datasets used in IDS evaluations, revealing disparities in data diversity, feature count, and balance. Historical datasets like NSL-KDD and UNSW-NB15 are synthetic and imbalanced, limiting their suitability for modern IoT scenarios. BoT-IoT and NB-IoT better represent IoT environments but lack coverage of complex attack vectors, such as multi-stage attacks or encrypted traffic. Varying feature counts and imbalance

ratios highlight the challenge of standardizing IDS evaluations, underscoring the need for more diverse, realistic, and representative datasets for consistent performance comparisons.

Table 4. Detailed summary of the datasets used in IDS evaluations, including their year of creation, dataset links, number of instances, features, whether the dataset collection was performed in an IoT environment, and the type of dataset (balanced or imbalanced). “#” denotes “number of”.

Dataset	Year	Reference	Instances	# Features	IoT Dataset	Type of Dataset
NSLKDD	2009	[49]	148,519	41	No	Imbalanced
UNSW-NB15	2015	[50]	2,540,044	49	No	Imbalanced
CICIDS2017	2017	[51]	2,830,743	83	No	Imbalanced
BoT-IoT	2019	[52]	73,370,443	29	Yes	Imbalanced
DS2OS	2018	[53]	409,972	13	Yes	Imbalanced
IoTID20	2020	[54]	625,783	83	Yes	Imbalanced
NB-IoT	2020	[55]	10,722	55	Yes	Balanced
IoT-23	2020	[56]	175,000	60	Yes	Balanced
Ton_iot	2019	[57]	180,000	70	Yes	Balanced
Mqtt-iot-Ids2020	2020	[58]	185,000	75	Yes	Balanced
Iot_malware	2018	[59]	160,000	85	Yes	Balanced
Darpa	1998	[60]	20,000	100	No	Balanced
n-baiot	2018	[61]	225,000	37	Yes	Balanced

While our review highlights these significant limitations, we recognize the need to bridge the gap between controlled experimental evaluations and the dynamic conditions of real-world networks. To address this, future studies should incorporate datasets collected directly from operational IoT networks to capture the authentic diversity of traffic, including encrypted communications and the heterogeneous behaviors of various devices, and pursue collaborations with industry partners to conduct pilot deployments and field experiments. These initiatives would enable IDSs to be tested under realistic conditions of network load, device variability, and genuine attack scenarios.

Integrating hybrid evaluation frameworks that combine synthetic and real-world datasets bolsters model robustness by ensuring performance metrics such as detection accuracy and false-positive rates and accurately capturing both controlled test conditions and dynamic operational environments. Collectively, these methods establish a more comprehensive assessment paradigm that drives IDS research toward practical, scalable solutions capable of meeting the stringent demands of real-world IoT deployments.

3.3. Optimized Aspects

To address the third research question, it is important to examine the aspects that are commonly optimized in IDS proposals for IoT environments, as shown in Figure 10. These include challenges such as resource constraints, data privacy, adaptability to dynamic threats, and scalability. Recent approaches highlight the importance of multi-objective optimization to balance competing priorities, such as detection accuracy and energy efficiency, especially in resource-constrained IoT devices [62,63].

In IoT environments, security is paramount due to the vast number of interconnected devices handling sensitive data. Recent advancements include analyzing network traffic and device behavior through DL and signature-based IDS. For instance, F. Sadikin et al. [64] proposed a hybrid IDS for ZigBee networks, wireless technology designed for low-power, short-range applications. Their approach combined rule-based detection and anomaly detection through ML, addressing both known attacks like DoS and emerg-

ing threats such as device hijacking, where attackers take control of devices, rendering legitimate users powerless.

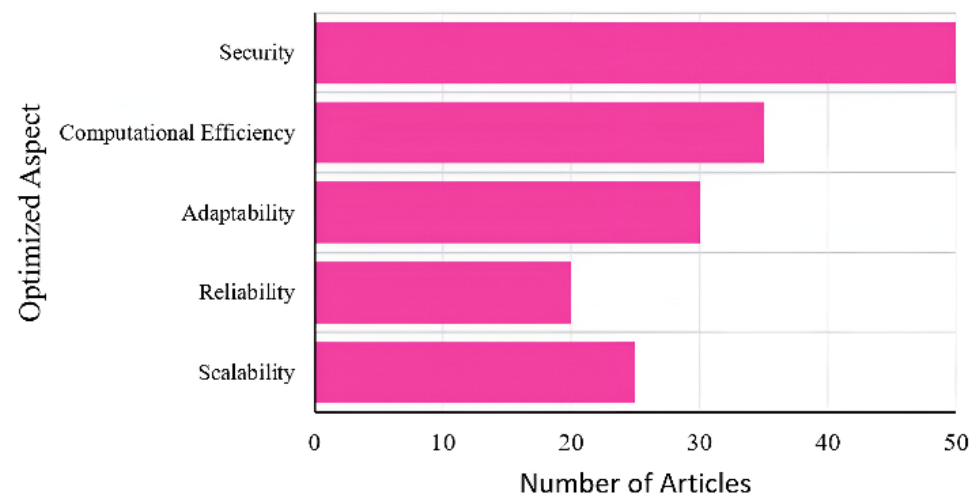


Figure 10. Articles that focus on optimizing different aspects of IDSs for IoT, such as scalability, reliability, adaptability, computational efficiency, and security.

Additionally, Tasmanian Devil Optimization, a bio-inspired metaheuristic, has been combined with a deep autoencoder for intrusion detection in UAV networks, achieving up to 99.36% accuracy and high precision in comparative experiments [65]. Similarly, hybrid optimization schemes that integrate multi-objective algorithms for feature selection and hyperparameter tuning have proven essential for balancing detection performance and false-positive rates.

Similarly, A. Abusitta et al. [66] leveraged anomaly detection using denoising autoencoders, a DL method capable of robustly representing data in noisy environments. Their solution achieved 94.6% accuracy in intrusion detection, highlighting the efficiency of autoencoders in identifying anomalous patterns in network traffic. Furthermore, IoT-PRIDS [67] introduces a packet-representation-based IDS that builds lightweight profiles solely from benign traffic—eschewing labeled attack data altogether—and demonstrates strong detection performance with minimal false alarms in practical IoT scenarios.

Computational efficiency is a critical factor in IoT systems due to the resource constraints of devices, such as limited processing power and energy availability. Researchers have focused on optimizing IDSs for high detection accuracy with minimal resource consumption. For instance, S. Bakhsh et al. [68] evaluate three deep learning models—Feed-Forward Neural Network (FFNN), Long Short-Term Memory (LSTM), and Random Neural Network (RandNN)—on the CIC-IoT22 dataset, achieving detection accuracies of 99.93%, 99.85% and 96.42%, respectively, which highlights their potential suitability for deployment in resource-constrained IoT environments.

Edge AI involves deploying artificial intelligence algorithms directly on IoT devices or edge servers, enabling localized data processing and analysis without relying heavily on cloud resources. This decentralized approach reduces latency, enhances privacy, and minimizes bandwidth usage, making it particularly suitable for resource-constrained IoT environments. When integrated with IDS, Edge AI allows real-time anomaly detection by processing traffic and behavioral data at the network’s edge, ensuring quicker responses to threats while preserving sensitive information locally.

Nguyen et al. [69] introduce TS-IDS, a GNN-based framework that fuses node- and edge-level features for intrusion detection. On the NF-ToN-IoT benchmark, TS-IDS improves weighted F1 by 183.49% over an EGraphSAGE baseline—and achieves additional

F1 gains of 6.18% on NF-BoT-IoT and 0.73% on NF-UNSW-NB15-v2—while reaching an AUC of 0.9992. Moreover, its $O(N)$ computational complexity ensures scalable deployment in large-scale IoT networks.

Similarly, Javanmardi et al. [70] introduced the M-RL model, a mobility-aware IDS for IoT-Fog networks, which combined Rate Limiting (RL) and Received Signal Strength (RSS) analysis to optimize resource usage. This lightweight solution achieved over 99% detection accuracy in dynamic environments while mitigating spoofing attacks. Additionally, hybrid Deep Autoencoder models have demonstrated high performance in anomaly detection by reducing dimensionality and enabling both binary and multiclass classifications, as evidenced by experiments with the BoT-IoT dataset. Together, these innovations highlight the potential of Edge AI to deliver scalable, precise, and resource-efficient IDS solutions in diverse IoT contexts.

Similarly, Y. Saheed et al. [71] addresses threat detection in the industrial IoT environment using a model that combines a genetic algorithm for feature selection with an attention mechanism and an adaptation of the Adam optimizer in LSTM networks. This lightweight solution allows reducing computational complexity and optimizing detection on resource-constrained devices, achieving exceptionally high performance metrics on real datasets (SWaT and WADI). The integration of SHAP in the model also reinforces the transparency of the process, facilitating the interpretation of the results by experts.

By incorporating Edge AI, IDS solutions can adapt dynamically to network variations, handle large-scale IoT deployments, and ensure reliable detection with minimal computational overhead. These innovations underscore the growing relevance of Edge AI in building robust, efficient, and scalable IDSs for modern IoT ecosystems.

FL is a decentralized ML approach where devices collaboratively train a global model without sharing raw data. Instead, only model updates are exchanged, ensuring data privacy and reducing bandwidth usage. This makes FL particularly suitable for IoT environments, where devices are resource-constrained and often handle sensitive information. In IDS, FL enables localized detection by training models on-device, capturing unique network behaviors while aggregating insights to improve global model robustness [72,73].

Building on this, V. Rey et al. [74] applied FL to IDSs by using the N-BaIoT dataset. Their approach reduced communication overhead by transmitting model updates instead of raw data. Additionally, techniques like trimmed mean aggregation excluded outliers, and s-resampling minimized model heterogeneity, enhancing system integrity and resilience against adversarial attacks.

Mansi H. Bhavasar et al. [6] present FL-IDS, a federated learning-based intrusion detection framework deployed on Raspberry Pi and Jetson Xavier edge devices that reaches up to 99% accuracy and reduces model loss to 0.009 compared to a centralized baseline, all while never sharing raw data. Tabassum et al. [2] enhance this paradigm with EDGAN-IDS, integrating a GAN at each client to generate synthetic samples that correct class imbalance and accelerate convergence—achieving over 97% accuracy across multiple IoT datasets. Finally, Ma et al. [75] propose ADCL, a similarity-based collaborative learning scheme that selectively combines models trained on related networks, boosting F-score by up to 80% in adaptability and 42% in learning integrity without exchanging user data.

Adaptability is vital in IoT due to the dynamic nature of networks and evolving threats. Advanced ML techniques have been explored to improve IDS adaptability. G. Thamilarasu et al. [76] developed an IDS for the Internet of Medical Things (IoMT) using ML algorithms and regression techniques. This hierarchical system employed mobile agents for distributed attack detection, demonstrating high adaptability and low resource consumption in hospital networks. J. Jeon et al. [77] propose Mal3S, a static IoT malware-detection framework that first extracts five types of features from each binary—raw bytes, opcode sequences,

API-call patterns, DLL imports and embedded strings—then encodes each feature set as a grayscale image and feeds these into a multi-SPP-net CNN for classification. Evaluated on a diverse IoT-malware corpus, Mal3S substantially outperforms conventional static detectors and demonstrates strong ability to identify novel malware families.

Emerging methodologies, such as Variational Autoencoders (VAEs) and XAI, are further enhancing adaptability in IDS. VAEs, a type of generative model, address data imbalance by generating realistic synthetic samples of rare or unseen attack patterns. For example, Li et al. [78] propose VAE-WGAN, a hybrid generative framework that combines a variational autoencoder with a Wasserstein GAN to synthesize labeled attack samples and rebalance the training set. When used to augment data for an LSTM+MSCNN classifier, it achieves 83.45% accuracy and an F1-score of 83.69% on NSL-KDD, and surpasses 98.9% in both metrics on AWID. XAI complements this by making decision processes interpretable and transparent, i.e., analysts can see why certain patterns are flagged and adjust detection strategies accordingly. Han et al. [79] introduce XA-GANomaly, an adaptive semi-supervised GAN-based IDS that incrementally retrains on incoming data batches and integrates SHAP, reconstruction-error visualization, and t-SNE to interpret and refine detection decisions dynamically.

Reliability is another critical parameter for ensuring accurate detection in IoT environments. Several studies have utilized advanced architectures to improve IDS reliability while minimizing FP. For example, S. Soliman et al. [80] implemented models based on LSTM, Bidirectional LSTM (Bi-LSTM), and Gated Recurrent Units (GRU), achieving near 100% accuracy and a classification error below 0.01%. S. Khan et al. [81] propose SB-BRSTM, a novel CNN block that combines dilated split-transform-merge operations with squeezed-boosted channels, and demonstrate its effectiveness by comparing it against standard architectures (SqueezeNet, ShuffleNet, DenseNet-201, etc.) on the IoT_Malware dataset—achieving a top accuracy of 97.18%. Santosh K. Smmarwar et al. [82] combined DWT-based feature extraction, GAN-driven data augmentation and CNN classification to achieve near-perfect accuracy, demonstrating strong resilience in smart-agriculture IoT scenarios. Similarly, S. Racherla et al. [48] proposed Deep-IDS, an LSTM-based edge system validated on the CIC-IDS2017 dataset, which attains 97.67% detection accuracy with a low false-alarm rate. This system demonstrated high reliability in identifying threats while minimizing FP, ensuring consistent performance in diverse IoT environments.

VAEs and XAI play crucial roles in improving IDS reliability by addressing key challenges in detecting accuracy and interpretability. VAEs enhance robustness by generating diverse synthetic attack data, as demonstrated by Li et al. [78], whose VAE-WGAN framework that synthesizes attack samples to rebalance training data, yielding 83.45% accuracy and an 83.69% F1-score on NSL-KDD, and over 98.9% in both metrics on AWID. Meanwhile, Han et al. [79] showed how SHAP, reconstruction-error visualization, and t-SNE can be integrated into XA-GANomaly to explain and refine its outputs, yielding an 8% improvement in F1-score and an 11.51% increase in accuracy on UNSW-NB15 while maintaining stable detection performance.

Scalability is essential in IoT, given the large number of devices and data volumes. M. Osman et al. [43] proposed an ensemble learning approach combined with feature selection via genetic algorithms, achieving 97.9% accuracy in detecting attacks in Routing Protocol for Low-Power and Lossy Networks (RPL). This method reduces computational complexity and memory footprint by selecting a compact subset of predictive features, which enhances scalability in resource-constrained RPL deployments. M. Amiri-Zarandi et al. [39] demonstrated that FL can effectively address scalability challenges in IDSs by distributing model training across devices, reducing central server dependency. This approach not only lowers

communication overhead but also enhances privacy by ensuring sensitive data remains on local nodes.

Blockchain technology offers a decentralized, immutable framework that strengthens IDS functionality by securely logging intrusion events and ensuring the integrity of threat intelligence. In this context, blockchain creates a distributed ledger where each detected event, such as anomalous traffic patterns or security alerts, is recorded with timestamps and cryptographic validation (e.g., via secure hash functions like SHA-256), which prevents any alteration or deletion of logs. In addition, smart contracts are programmed with predefined conditions that automatically trigger responses (like alerting administrators or isolating compromised nodes) when specific attack patterns are detected. The blockchain's consensus mechanism, such as Proof-of-Authority or similar lightweight protocols, ensures that the validation process is distributed across multiple nodes, thereby eliminating single points of failure, fostering trust in collaborative environments, and enabling scalable intrusion detection, especially in critical scenarios like industrial IoT or smart city infrastructures.

Furthermore, Saveetha et al. [83] introduce a deep-learning-based IDS and outline how integrating blockchain could anchor detection logs immutably (reinforcing tamper resistance) without yet implementing the full ledger. Y. Sunil Raj et al. [84] present a real-time adaptive IoT IDS that combines federated learning with blockchain to immutably record and verify model updates, strengthening the integrity of the collaborative training process. B. Hafid et al. [85] explore IDS deployment on resource-constrained edge devices, suggesting that blockchain can secure detection logs and enable safe information sharing among nodes, thus mitigating vulnerabilities inherent to centralized architectures.

Y. Loari et al. [86] further enhance the IDS landscape by developing a collaborative system that combines anomaly-based and signature-based methods, using blockchain to securely store and distribute critical threat data through smart contracts. S. Alharbi et al. [87] build on this idea with a framework that shares a blacklist of malicious IP addresses across multiple IDS nodes via blockchain, reducing data redundancy and boosting scalability. Finally, while Liu et al. [88] develop an AI-, IoT-, and blockchain-based framework for food authenticity and traceability in smart agriculture, they do not propose an IDS. Nevertheless, their discussion of immutable logging and transparent record-keeping illustrates how similar ledger mechanisms could be leveraged to secure IDS detection logs and bolster resilience across IoT networks.

Blockchain-based IDS solutions are on the rise. For example, consider a smart factory where an IDS continuously monitors network traffic from critical IoT sensors and controllers. When the system detects a sudden surge of failed login attempts from a previously unrecognized IP address (potentially indicating a brute force attack), the IDS computes a secure hash of the event details (timestamp, source IP, and anomaly type) using SHA-256, and appends this hashed data to the blockchain ledger, making it tamper-proof. Simultaneously, a smart contract pre-programmed with thresholds for suspicious activity automatically alerts network administrators, isolates the affected device by updating firewall rules, and disseminates the intrusion alert to other nodes via a lightweight consensus protocol like Proof-of-Authority, thus curtailing any lateral movement by the attacker.

Despite these strengths, current limitations include scalability challenges in high-volume networks, latency introduced by consensus protocols, and integration difficulties with resource-constrained IoT devices.

R. Alghamdi et al. [89] propose a cascaded federated deep learning framework that pushes CNN and LSTM training to individual IoT nodes (preserving privacy) while a lightweight trust-based pre-filter minimizes latency and computational overhead, thus demonstrating true scalability and efficiency for real-time IDS deployment in resource-constrained IoT networks.

3.4. Main AI Approaches

This section focuses exclusively on AI-based intrusion-detection techniques for IoT, presenting supervised, tree-based, deep-learning, federated-learning, and generative approaches in a self-contained block to improve clarity and avoid cross-sectional repetition.

AI has gained popularity in the field of cybersecurity due to its ability to dynamically adapt to new threats, improve detection accuracy, and reduce FP. AI-based IDSs continuously learn from data to identify anomalous patterns, allowing them to detect unknown threats more effectively. However, they face significant challenges.

Figure 11 presents a classification of the most commonly used AI techniques in IDS. This classification is divided into five main categories: Supervised ML, tree-based methods, DL, FL and GANs. Each section highlights the specific algorithms and methods most commonly used in the literature. The following sections will highlight specific studies that have used these techniques to enhance intrusion detection, demonstrating how they have been implemented in various environments and the results obtained.



Figure 11. Sunburst diagram illustrating the five main AI approaches most used in IoT-IDS research. The inner ring shows the high-level categories (ML, Tree-Based, DL, FL, GANs); the middle ring details key algorithms; and the outer ring annotates each approach's principal strengths and challenges.

AI in IDSs has grown, improving threat detection by analyzing anomalous network traffic patterns, boosting accuracy, and reducing false positives as data grows. However, AI solutions need large datasets and high computational resources, limiting IoT applicability, and are vulnerable to adversarial attacks, requiring robust designs. Tra-

ditional non-AI models, simpler and effective for known threats, remain valuable in resource-constrained settings.

Several studies highlight the application of advanced techniques in IDS. R. Ahmad et al. [46] present a comprehensive benchmark showing that pure convolutional networks train in roughly 10–20 min—significantly faster than hybrid autoencoder + BRNN or autoencoder + LSTM models, which may require several hours—while still exceeding 98% accuracy on datasets such as CICIDS2017 and NSL-KDD. Similarly, A. Kumar et al. [90] introduce EDIMA, a two-stage edge-AI IDS that first uses a lightweight ML detector to flag scanning sessions and then applies an autocorrelation-based test to pinpoint infected devices; in two 15-min replay scenarios with real IoT malware traces, it achieves a 100% detection rate with zero missed detections and very low false positives.

Distributed IDS solutions leveraging FL have emerged as a promising approach to address the scalability, data privacy, and resource constraints in IoT. M. H. Bhavsar et al. [6] developed FL-IDS, which trains logistic regression and CNN models locally on Raspberry Pi and Jetson Xavier devices—never sharing raw traffic—and aggregates only model updates on a central server. Deployed on transportation IoT systems, it attains 94% accuracy on NSL-KDD and 99% on the Car-Hacking dataset. Their method employs an iterative federated training process where a central server initializes a global model, distributes it to edge devices for local training, and then aggregates the model updates to refine the global model continuously. A simplified pseudocode outlining this process is shown in Algorithm 1.

Algorithm 1 lays out our federated training workflow in plain steps. First, the server creates an initial IDS model with random weights. In each training round, it picks a group of edge devices based on their availability. Each device that has collected enough local data trains the received model for a few epochs using its own dataset and then computes the difference between its updated model and the one it received. It sends that “delta” plus its dataset size back to the server; devices without enough data simply sit out that round. The server then fuses all incoming updates by taking a weighted average (so larger datasets have more influence) to produce the next global model. Periodically, the server tests the new model on a separate validation set, and if performance has plateaued, it stops early. This loop ensures data privacy (raw data never leaves the devices), handles devices of varying capacity, and converges efficiently to a robust IDS model for heterogeneous IoT scenarios.

In addition to the main training loop, Algorithm 1 depends on three helper functions. `SelectDevices` ($n, K, \text{availability}_{\text{scores}}$) returns a subset S_t of K devices (out of the total n) chosen based on their availability scores. `LocalUpdate` ($G_{t-1}, D_i, \eta, \alpha$) carries out FedProx-regularized local training of the global model G_{t-1} on device i 's dataset D_i using learning rate η and proximal term α , and returns the updated weights $L_{i,t}$. Finally, `Evaluate` (G_t, D_{test}) computes and returns the loss of the newly aggregated global model G_t on the held-out test set D_{test} .

R. Kumar et al. [91] propose a fog-based IDS that runs Random Forest (RF) and XGBoost (XGB) locally on BoT-IoT nodes. In binary detection RF achieves 99.81% accuracy (F1 99.90%) and XGB 99.999% (F1 99.999%); in multi-class tests RF maintains ~99.99% accuracy (F1 99.997%) while XGB's accuracy is similar but F1 drops to 87.9%. As fog nodes scale from 1 to 20, per-node training time falls from 340 s to 155 s for RF (~55% reduction) and from 1480 s to 920 s for XGB (~38% reduction), demonstrating improved scalability and efficiency. S. Khanday et al. [92] propose a SMOTE-balanced, feature-selected DDoS detector for constrained IoT devices, reaching over 98% accuracy with near-zero false positives on BOT-IoT and TON-IoT while keeping model complexity minimal.

Algorithm 1: Federated IDS Training Process

Inputs: Total rounds (T), Number of devices (n), Local dataset for each device $I(D_i)$, Minimum devices per round (K), Learning rate (η), Convergence threshold (τ), FedProx parameter (α), Minimum samples per device ($m_{\min}$), Evaluation frequency ($eval_{freq}$), Global test set (D_{test}), Availability scores for all devices ($availability_{scores}$)

Output: Final global model G_T

```

1. Initialize global model  $G_0$  with random weights and  $last_{loss} \leftarrow \infty$ .
2. for each round  $t = 1$  to  $T$ :
3.    $S_t \leftarrow \text{SelectDevices}(n, K, availability_{scores})$ 
4.   for each device  $i \in S_t$  in parallel do
5.     if  $|D_i| \geq m_{\min}$  then
6.        $L_i^t \leftarrow \text{LocalUpdate}(G_{t-1}, D_i, \eta, \alpha)$ 
7.        $\Delta w_i^t \leftarrow L_i^t - G_{t-1}$ 
8.        $\text{Send}(\Delta w_i^t, |D_i|)$ 
9.     else
10.       $\Delta w_i^t \leftarrow 0, |D_i| \leftarrow 0$ 
11.    end if
12.  end for
13.   $total\_samples \leftarrow \sum_{i \in S_t} |D_i|$ 
14.   $G_t \leftarrow G_{t-1} + \sum_{i \in S_t} (|D_i| / total\_samples) \times \Delta w_i^t$ 
15.  if  $t \bmod eval_{freq} = 0$  then
16.     $loss_t \leftarrow \text{Evaluate}(G_t, D_{test})$ 
17.    if  $|loss_t - last_{loss}| < \tau$  then
18.      return  $G_t$ 
19.    end if
20.     $last_{loss} \leftarrow loss_t$ 
21.  end if
22. end for
23. return  $G_T$ 

```

Expanding on these approaches, B. Gupta et al. [93] proposed a distributed optimization system for IoT attack detection using FL combined with the Siberian Tiger Optimization (STO) algorithm. In their framework, the server first optimizes the CNN model's hyperparameters using STO, balancing exploration and exploitation to minimize a global loss function, and then distributes these optimized parameters to clients for local training. Finally, the server aggregates the local updates to refine the global model iteratively. Moreover, F. Hendaoui et al. [94] introduced FLADEN, a comprehensive FL framework for anomaly detection that constructs a diverse, real-world threat intelligence dataset, updates the federated learning library for efficient resource allocation, and achieves detection accuracies exceeding 99.9% while preserving data privacy.

The choice of algorithms in IDSs depends on the specific environment and constraints. Neural networks excel in handling large data volumes and detecting complex patterns, while Random Forest is robust in noisy data scenarios. Support Vector Machines (SVM) is particularly effective for binary classifications and high-dimensionality problems, and genetic algorithms optimize feature selection, improving detection efficiency. Hybrid systems often combine these methods with traditional techniques, such as signature-based approaches, or advanced methods like DWT for multiresolution analysis, as demonstrated in earlier studies.

Traditional AI techniques in IDSs primarily depend on supervised learning models, which require extensive labeled datasets and often fail to generalize to new threats. As highlighted in Section III.B, many IDS datasets suffer from imbalances and lack diversity. To overcome these challenges, Generative AI methods such as VAEs and GANs have been developed to generate synthetic data that simulates a wider range of attack scenarios and compensates for dataset imbalances.

The synthetic data generation algorithm using GAN for IoT IDSs employs an adversarial training paradigm in which two neural networks compete to improve the realism of generated samples. First, both a generator (G) and a discriminator (D) are initialized with random weights. During each training iteration, the discriminator is updated multiple times on batches of real IoT traffic and generator-produced samples, while enforcing a gradient-penalty term (WGAN-GP) to stabilize learning. Next, the generator is trained to “fool” the discriminator by producing ever more realistic data. Periodically, we assess quality using Fréchet Inception Distance (FID) to measure visual similarity and a coverage metric to ensure all attack classes are represented. Training stops once pre-specified quality thresholds or the maximum iteration count are met, yielding a generator capable of producing high-quality synthetic data that enhances the diversity and balance of IDS training sets. To further clarify this process, the following pseudocode (Algorithm 2) outlines the general WGAN-GP training procedure for generating synthetic IoT intrusion data.

Recent advances in IoT security demonstrate the application of Large Language Model architectures to radio frequency fingerprinting (RFFI) for device identification and authentication. Gao et al. [95] developed a BERT-LightRFFI framework that uses knowledge distillation to transfer RFF feature extraction capabilities from a pre-trained BERT model to lightweight networks suitable for 6G edge devices, achieving 97.52% accuracy in LoRa networks under multipath fading and Doppler shift conditions. Similarly, Zheng et al. [96] proposed a dynamic knowledge distillation approach using a modified GPT-2 architecture (RFF-LLM) with proximal policy optimization for UAV individual identification, achieving 98.38% accuracy with only 0.15 million parameters in complex outdoor environments. These works demonstrate how Transformer-based architectures can be effectively adapted for wireless security applications through specialized training on I/Q signal data rather than natural language. In parallel, diffusion models have emerged as a new generative paradigm for synthesizing highly realistic data distributions, offering potential for IDS training and augmentation beyond the capabilities of GANs and VAEs.

In addition to the core training loop, Algorithm 2 relies on several helper functions. `SampleBatch(D, m)` draws a minibatch of m real samples from dataset D uniformly at random. `Sample( $p(z)$ , m)` returns m independent noise vectors drawn from the distribution $p(z)$. `Uniform(0,1,m)` generates a vector of m scalars sampled uniformly in $[0,1]$ for interpolating between real and fake data. `CalculateFID( $x_{eval}$ ,  $D_{real}$ )` computes the Fréchet Inception Distance between the generated sample set x_{eval} and the real dataset D_{real} , providing a measure of distributional similarity. Finally, `CalculateCoverage( $x_{eval}$ ,  $D_{real}$ )` evaluates what fraction of the attack classes present in D_{real} also appear at least once in x_{eval} , ensuring diverse class coverage.

For instance, Rahman et al. [97] developed the SYN-GAN framework, which generated synthetic datasets for training IDS models, achieving 90% accuracy on the UNSW-NB15 dataset and 100% on the BoT-IoT dataset. This approach not only addresses issues like false data and outliers but also enriches the training data, thereby enhancing the robustness of IDSs against previously unseen threats.

Algorithm 2: WGAN-GP Synthetic Data Generation for IDS

Inputs: Iterations N , Minibatch size m , Real dataset D_{real} , Noise distribution $p(z)$, Learning rates η_G, η_D , Discriminator steps k , Gradient penalty λ , Frequency of quality evaluation $\text{eval}_{\text{freq}}$, Number of samples for quality evaluation $\text{eval}_{\text{size}}$, FID threshold for early stopping $\text{threshold}_{\text{FID}}$, Coverage threshold for early stopping $\text{threshold}_{\text{coverage}}$, Size of final synthetic dataset $\text{target}_{\text{size}}$

Output: Trained generator network G^* and final synthetic dataset D_{syn}

1. Initialize generator G with random weights
2. Initialize discriminator D with random weights
3. **for** $t = 1$ **to** N **do**
4. **for** $j = 1$ **to** k **do**
5. $x_{\text{real}} \leftarrow \text{SampleBatch}(D_{\text{real}}, m)$
6. $z \leftarrow \text{Sample}(p(z), m)$
7. $x_{\text{fake}} \leftarrow G(z)$
8. $\varepsilon \leftarrow \text{Uniform}(0,1,m)$
9. $\hat{x} \leftarrow \varepsilon \times x_{\text{real}} + (1 - \varepsilon) \times x_{\text{fake}}$
10. $L_D \leftarrow \text{Mean}(D(x_{\text{fake}})) - \text{Mean}(D(x_{\text{real}})) + \lambda \times \text{Mean}(\|\nabla_{[\hat{x}]} D(\hat{x})\|_2 - 1)^2)$
11. $D \leftarrow D - \eta_D \times \nabla_D L_D$
12. **end for**
13. $z' \leftarrow \text{Sample}(p(z), m)$
14. $L_G \leftarrow -\text{Mean}(D(G(z')))$
15. $G \leftarrow G - \eta_G \times \nabla_G L_G$
16. **if** $t \bmod \text{eval}_{\text{freq}} = 0$ **then**
17. $z_{\text{eval}} \leftarrow \text{Sample}(p(z), \text{eval}_{\text{size}})$
18. $x_{\text{eval}} \leftarrow G(z_{\text{eval}})$
19. $\text{FID}_t \leftarrow \text{CalculateFID}(x_{\text{eval}}, D_{\text{real}})$
20. $\text{coverage}_t \leftarrow \text{CalculateCoverage}(x_{\text{eval}}, D_{\text{real}})$
21. **if** $\text{FID}_t < \text{threshold}_{\text{FID}}$ and $\text{coverage}_t > \text{threshold}_{\text{coverage}}$ **then**
22. **break**
23. **end if**
24. **end if**
25. **end for**
26. $z_{\text{final}} \leftarrow \text{Sample}(p(z), \text{target}_{\text{size}})$
27. $D_{\text{syn}} \leftarrow G(z_{\text{final}})$
28. **return** G, D_{syn}

Recent studies have further advanced this line of work by proposing deep generative architectures tailored to IoT environments. C. Qian et al. [98] propose RGAAnomaly, a reconstruction-based GAN that combines an autoencoder and a variational autoencoder within a dual-transformer architecture, specifically designed for multivariate time series anomaly detection in IoT systems. Their model effectively extracts and fuses temporal and metric features, outperforming prior approaches such as MAD-GAN and OmniAnomaly across four benchmark datasets.

Similarly, D. Hamouda et al. [99] introduce FedGenID, a federated IDS architecture based on conditional GANs (cGANs) that performs data augmentation across distributed industrial IoT nodes. Their system enhances detection accuracy, particularly under non-IID data distributions and zero-day attacks, surpassing traditional federated methods by 10% in high-privacy scenarios. In a complementary domain, Y. Jin et al. [100] present HSGAN-IoT, a semi-supervised GAN framework for hierarchical IoT device classification. Although not

an IDS per se, its ability to identify unseen devices based on traffic patterns contributes to the early detection of anomalous or spoofed behaviors in networked environments.

While these models show promising results, they share several limitations. First, the use of deep generative models often entails a significant computational cost, making real-time deployment in constrained IoT devices challenging. Second, most approaches require careful alignment between synthetic and real data distributions to avoid overfitting or detection bias. Finally, the stability of GAN training remains a concern, particularly in unsupervised or federated settings where data heterogeneity is high.

Moreover, incorporating XAI techniques not only clarifies the decision-making process of AI-based IDSs in IoT but also enhances system reliability by providing interpretable insights into which features drive the model's predictions. For instance, Han and Chang [79] introduced the XA-GANomaly model, which fuses adaptive semi-supervised learning with SHAP-based explanations to improve anomaly detection in dynamic network environments. Similarly, Li et al. [78] demonstrated that a hybrid VAE-WGAN model could generate synthetic samples tailored to rare attack types, significantly boosting detection performance on imbalanced datasets.

In addition, Arafah et al. [101] improved feature representation by combining a denoising autoencoder with a Wasserstein GAN to generate realistic synthetic attacks across datasets like NSL-KDD and CIC-IDS2017, while Sharma et al. [10] highlighted the integration of XAI techniques such as SHAP and Local Interpretable Model-Agnostic Explanations (LIME) to provide interpretable results in IDS models, fostering trust and reliability in AI-driven cybersecurity systems.

Building on these approaches, recent studies have further advanced the application of XAI in IDSs for IoT. S.B. Hulayyil et al. [102] presented an explainable AI-based intrusion detection framework explicitly designed for IoT systems. Their framework integrates ML classifiers with XAI techniques to offer real-time, interpretable explanations for detected vulnerabilities (e.g., those related to Ripple20), thereby enabling security analysts to understand and fine-tune model behavior more effectively.

While SHAP-based explanations (see Sections III-B, III-C, and III-D) significantly improve transparency, they impose non-trivial computational overhead that may limit real-time applicability on resource-constrained IoT devices, highlighting a key challenge for practical deployments.

Complementarily, A. Gummadi et al. [103] conducted a systematic evaluation of white-box XAI methods, such as Integrated Gradients (IG), Layer-wise Relevance Propagation (LRP), and Deep-SHAP, using comprehensive metrics (descriptive accuracy, sparsity, stability, efficiency, robustness, and completeness). Their results underscore the importance of these metrics to quantify the quality of explanations in IoT anomaly detection contexts.

By grounding these advanced techniques in the specific deficiencies identified in current IDS datasets, namely, imbalance, limited representation of rare threats, and inadequate simulation of real-world traffic, Generative AI and XAI not only improve detection accuracy and reduce false positives but also offer practical solutions to these concrete data-related challenges. This revised approach reinforces the applicability of these technologies in addressing the critical gaps detailed in Section III.B.

3.5. IDS Application Fields

At this point, the main fields of IDS implementation identified in the evaluated articles include Industry 4.0, medical and healthcare services, smart cities and homes, and agriculture, as illustrated in Figure 12. These sectors are pivotal to economic growth, public health, and food security, making the protection of their infrastructure and data from cyber threats imperative. The deployment of IDSs in these fields ensures not only operational

continuity but also compliance with regulatory standards, protection of sensitive data, and resilience against evolving threats.

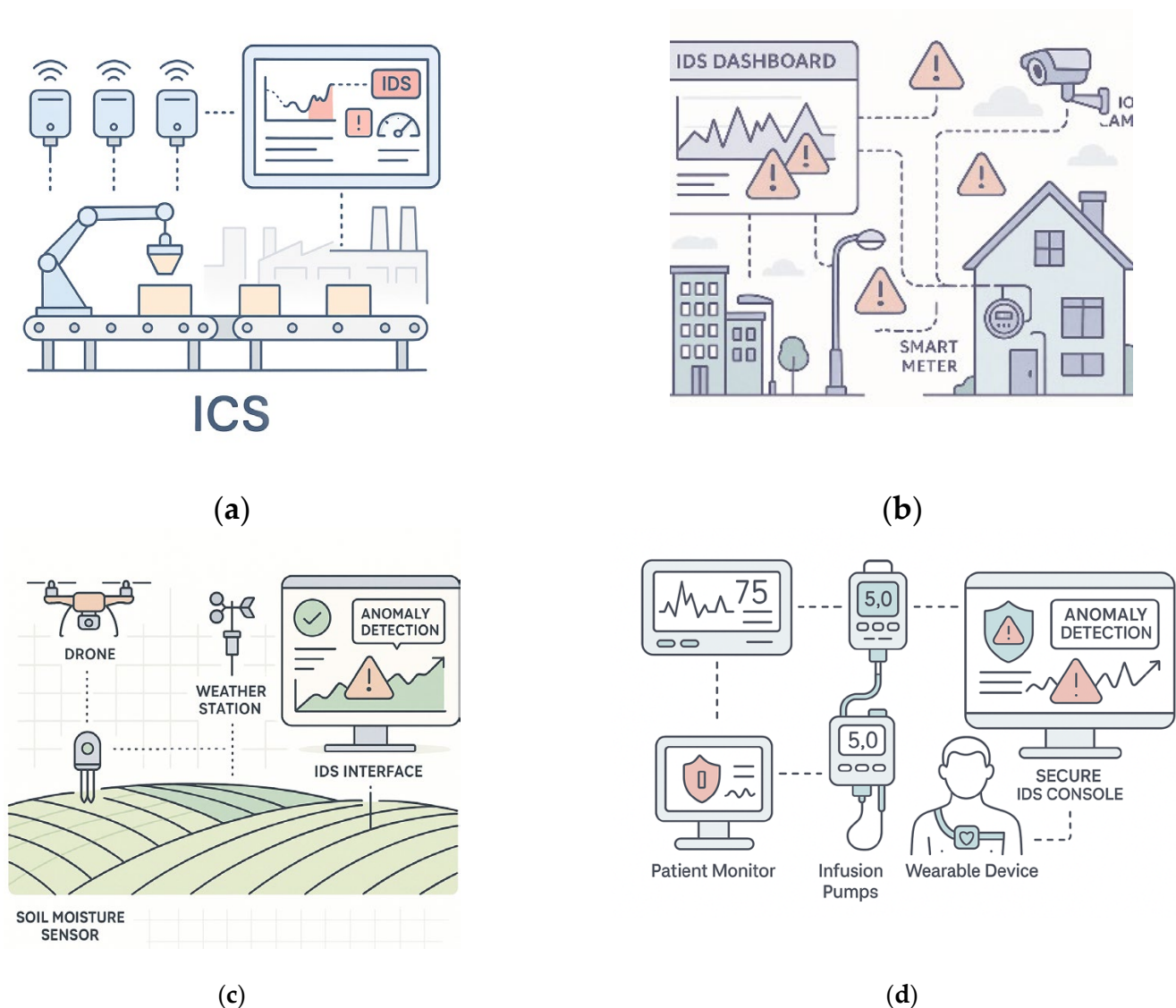


Figure 12. IDS application fields in IoT across four key domains: (a) Industry and Manufacturing, (b) Smart Homes and Cities, (c) Smart Agriculture, (d) Medical Systems and Healthcare.

In industrial manufacturing environments, IDSs play a crucial role in protecting Industrial Control Systems (ICS), which form the backbone of power grids, water treatment facilities, and production lines. Past cyberattacks targeting industrial systems, such as the notorious Stuxnet malware, have demonstrated the potentially catastrophic consequences of compromised industrial infrastructure. The implementation of IDSs in these environments ensures operational continuity, reduces downtime caused by cyberattacks, and minimizes the economic impact of disruptions.

Several researchers have made significant contributions to IDS solutions for industrial applications. Y. Saheed et al. [104] proposes a dimensionality reduction mechanism using an autoencoder that integrates DCNN and LSTM for network data analysis in ICS. This methodology allows for implementing an IDS that does not require detailed prior information about the system topology, facilitating its deployment in critical infrastructures and demonstrating high accuracy and robustness results against attacks in real environments.

X. Yu et al. [4] introduced the Edge Computing-based anomaly detection algorithm (ECADA), which efficiently detects anomalies from both single-source and multi-source

time series in industrial environments, enhancing detection accuracy while simultaneously reducing the computational load on cloud data centers. This improvement not only strengthens detection capabilities but also promotes industrial sustainability through more efficient resource utilization.

Alireza Zohourian et al. [67] with IoTPRIDS, a lightweight, packet-representation-based intrusion detection framework designed for general IoT deployments. IoT-PRIDS trains exclusively on benign network traffic, without resorting to complex machine-learning models, and operates in a host-based configuration, delivering near-real-time detection of complex attack patterns with minimal false alarms. Its low computational footprint and reliable performance make it especially well-suited for resource-constrained or safety-critical environments, including industrial control systems. K. Ramana et al. [105] presented an intelligent IDS for IoT-assisted wireless sensor networks, employing a whale optimization algorithm for hyperparameter optimization that substantially improved detection accuracy while reducing false positives in industrial environments.

Further advancing the field, Mirdula S. et al. [106] present a deep learning-based anomaly detection framework for IoT-integrated smart buildings, leveraging Manufacturer Usage Description (MUD) profiles to dynamically monitor device behavior and detect network-level anomalies. Validated on real smart-building traffic, it achieves high detection accuracy (>99%) with a lightweight design suitable for heterogeneous IoT deployments. Fengyuan Nie et al. [47] contributed with their innovative M2VT-IDS architecture, which adapts seamlessly to dynamic and distributed industrial networks, significantly enhancing anomaly detection capabilities and operational efficiency.

K. Shalabi et al. [44] conducted a systematic review of blockchain-based IDSs/IPSSs for IoT networks, covering work published between 2017 and 2022 in industrial and healthcare settings. Their analysis highlights how blockchain strengthens data integrity, decentralization and scalability of threat response, and points out open challenges in resource-constrained deployments.

In the healthcare sector, the integration of IDSs is vital for safeguarding the confidentiality and security of sensitive medical data while ensuring the integrity of connected medical devices [76]. H. Alamro et al. [107] developed the BHS-ALOHDL system, which leverages blockchain technology to enhance data security and facilitate intrusion detection in healthcare environments. In evaluations on ToN-IoT and CICIDS-2017 datasets, it achieved up to 99.31% detection accuracy (with comparably high precision, recall, F1-score and AUC) while maintaining lower execution and transaction-mining times than competing PoW-based approaches. By preventing unauthorized access and safeguarding patient information, these IDS solutions ensure the reliability and trustworthiness of medical services.

For smart homes and cities, IDS technologies protect critical infrastructure and user privacy from an ever-growing range of cyber threats. For example, E. Anthi et al. [108] designed a three-layer supervised IDS for smart home IoT devices, achieving F-measure scores of 96.2%, 90.0% and 98.0% on profiling, anomaly detection and attack classification tasks. Sarwar et al. [109] presented an anomaly-detection framework for smart homes using classifiers such as Random Forest, Decision Tree and AdaBoost, reporting perfect precision, recall and F1 on the UNSW-BoT-IoT benchmark.

In the agricultural sector, IDS technologies are optimizing productivity and securing systems against cyber threats that could disrupt food supply chains. S. K. Smmarwar et al. [82] propose a novel three-phase Deep Malware Detection framework—DMD-DWT-GAN—specifically designed for IoT-based smart agriculture systems. First, extracted features such as opcodes, bytecode, call logs, executable files and strings are converted into binary form and then concatenated into 8-bit sequences that are mapped directly to pixel intensities,

producing grayscale “visualizations” of each malware sample (which are subsequently normalized, colorized and resized to 32×32 pixels to standardize input). Next, a Discrete Wavelet Transform decomposes each image into Approximation (Ac) and Detail (Dc) coefficients, which are fused with a GAN—the generator processes Dc while the discriminator processes Ac—to enhance discriminative malware patterns. Finally, a lightweight Convolutional Neural Network classifies the malware family in real time. Evaluated on both the IoT-malware and Maling benchmark datasets, this IDS achieves 99.99% accuracy, precision, recall and F1 score—outperforming existing state-of-the-art—while maintaining a low prediction time of 9 s.

Despite major technological strides, industrial intrusion detection systems (IIDS) still face critical hurdles: the lack of unified standards limits interoperability and complicates integration, while many solutions demand heavy computational power and energy, making them ill-suited for constrained environments. As networks and data volumes expand, scalability becomes more difficult to maintain, and high false-positive rates can overwhelm operators, whereas false negatives may leave dangerous threats undetected, jeopardizing production, patient safety, or infrastructure. Overcoming these issues will require the creation of lightweight, adaptive, and highly accurate IDS solutions tailored to each sector’s needs, fully compatible with existing systems and optimized for efficient resource use.

Deployment Case Studies

To illustrate practical applications of IDS in IoT, we summarize three real-world pilot implementations across industrial, healthcare, and smart-home domains. Table 5 presents each deployment’s context, the core IDS technology used, key performance metrics, and the main lessons learned.

Table 5. Deployment Case Studies: Real-world IDS Pilots across Industry, Healthcare, and Smart-Home Domains.

Domain	Deployment Context	IDS Technology	Key Metrics	Lessons Learned	Ref.
Industry	Smart machinery plant—telemetry sensors, IoT cameras, and control devices for industrial equipment	SVM, CNN (thermal and visual images), HMM-based time-series detector, VAE	Detection rate increased by 11% (system-wide), 13% (telemetry sensors); FP rate decreased by 9% (system-wide), 3% (telemetry sensors)	Real-time data processing reduces response time to 1.8 s and enhances safety; continuous model retraining needed to adapt to evolving plant conditions	[110]
Healthcare	Cloud-based hospital network monitoring of medical IoT devices (wearables, infusion pumps, ECG)	Neural network IDSs with spectral analysis (kurtosis, crest)	Accuracy 95.72%; Specificity 95.29%	Cloud deployment supports real-time monitoring of medical IoT devices; data privacy and real-time processing require efficient system design	[111]
Smart city	IoT-enabled urban network in a smart city pilot, integrating smart traffic and energy management systems	Distributed machine learning-based IDSs using Random Forest and fog-edge analytics	Detection accuracy: 97.8%; False Positive Rate: 2.1%; Processing latency: 0.3 s per packet in fog nodes	Distributed IDS reduces latency compared to centralized systems; fog-edge coordination enhances scalability but requires robust node synchronization	[112]

In this smart manufacturing plant, the choice of algorithms reflected both the diversity of data sources and operational requirements. CNNs analyzed thermal and visual imagery to detect subtle mechanical anomalies, while HMMs modeled temporal dynamics in sensor readings. VAEs compressed high-dimensional signals, with SVMs providing robust classification on the reduced feature space. This multi-algorithm strategy shows that industrial

environments require complementary techniques for different data modalities, and that sustained performance relies on continuous retraining as plant conditions evolve.

In the cloud-based healthcare case, the IDS design had to balance classification accuracy with stringent data security requirements in a medical IoT context. Neural networks were employed to model the nonlinear patterns in ECG signals and device traffic, offering the flexibility needed for both arrhythmia detection and intrusion identification. Their performance was enhanced through a Hybrid Tempest optimization process, which integrated multiple search strategies to fine-tune network parameters and avoid local minima, a key factor when working with heterogeneous hospital data. Complementary feature extraction techniques were introduced to ensure efficiency: statistical descriptors captured variability across patients, while spectral features reduced computational load during real-time monitoring. This layered strategy reflects the dual challenge of healthcare IoT—delivering precise diagnostics while protecting sensitive information—and demonstrates that robust anomaly detection in medical environments depends on careful algorithmic integration rather than reliance on a single model.

In the smart city case, the IDS was designed to manage the massive flow of data generated by connected infrastructures such as traffic systems, energy grids, and home devices. Rather than relying solely on centralized monitoring, detection was pushed to fog and edge nodes so that anomalies could be identified close to their source, reducing response latency and network overhead. Random Forest models provided fast, reliable classification of diverse traffic patterns, while edge analytics ensured scalability across heterogeneous devices. This deployment illustrates how IDSs in smart environments act as a distributed nervous system—filtering malicious activity in real time, preserving service continuity, and protecting both public infrastructure and private households from evolving cyber threats.

Taken together, these pilots illustrate how different IDSs approaches align with context-specific needs. In industrial plants with strict uptime requirements, hybrid combinations of VAEs, HMMs, and CNNs, supported by edge AI, prove effective for handling diverse signals and ensuring real-time response, while explainable AI methods are needed to foster operator trust. In healthcare, neural IDSs optimized with metaheuristics and, prospectively, federated learning frameworks provide accuracy while respecting privacy constraints. In municipal or smart-home networks, rules-based IDS engines like Suricata remain valuable when augmented with anomaly detection for broader coverage. Looking forward, large language model architectures applied to radio-frequency fingerprinting represent a promising option for wireless IoT and UAV identification, while generative models such as GANs, VAEs, and diffusion models can create realistic attack scenarios to support training where data scarcity persists.

Beyond these documented deployments, several emerging application scenarios demonstrate the expanding scope of IoT-IDS implementations: in healthcare, hospitals could adopt federated IDSs so that multiple institutions collaboratively train models without sharing raw patient data, while blockchain ensures integrity of alerts. In industrial contexts, edge-based IDSs can be placed close to PLCs to deliver sub-100 ms responses that prevent cascading failures, with cloud coordination for long-term adaptation. In agriculture, lightweight IDSs tailored to sensor networks could intercept denial-of-service attempts that risk disrupting irrigation or food supply chains. In smart cities, hybrid blockchain-ML IDSs may secure video surveillance and transport systems, providing tamper-evident alerts and ensuring scalable policy enforcement across distributed fog nodes.

3.6. Open Research Questions

The development of sophisticated and adaptive ML and DL algorithms is crucial for addressing rapidly evolving cyber threats in IoT environments. IDSs must move beyond static models by incorporating continuous learning frameworks, such as reinforcement and online learning, and emerging approaches like meta-learning and few-shot learning, which enable adaptation to novel threats with minimal labeled data. For example, a smart-home IDSs must adapt rapidly when new IoT appliances are introduced, while an industrial IoT deployment may require online learning to handle unforeseen attacks without interrupting operations.

Efficient management of large data volumes remains a critical challenge. Distributed and edge computing techniques can enhance real-time processing by bringing data analysis closer to source devices, thus reducing latency and network overhead. Deploying edge AI models and combining DL methods with dimensionality reduction (e.g., PCA or autoencoders) can help optimize resource usage in environments with limited computational power. In vehicle IoT networks, for instance, low-latency IDS decisions are required to prevent cascading failures in connected cars, highlighting the importance of lightweight edge-based detection.

Standardization is vital in overcoming current IDS limitations. The lack of consistent, validated datasets and diverse IDS implementations hampers comparability and replicability. Establishing global repositories and universal communication protocols would improve interoperability across diverse IoT devices and facilitate the development of robust evaluation frameworks. A concrete example is the disparity between public datasets (e.g., CICIDS, UNSW-NB15) and the traffic observed in real smart city deployments, where encrypted protocols and heterogeneous devices are predominant—underscoring the urgency of standardized benchmarks.

The integration of blockchain technology offers a decentralized, immutable framework for securing IDS operations. By ensuring tamper-proof logging through distributed ledgers and automating response mechanisms via smart contracts, blockchain enhances data integrity and resiliency, particularly in critical sectors like industrial automation and healthcare. In parallel, FL, especially when combined with transfer learning (TL) [113] and optimized for resource-constrained devices, provides promising avenues for decentralized training and improved scalability. Techniques such as adaptive compression and edge computing further support these decentralized models. For example, in healthcare IoT, FL could enable hospitals to collaboratively train IDS models without exposing sensitive patient data, while blockchain ensures integrity and auditability of alerts across institutions.

The urgency and complexity of these challenges vary significantly across deployment contexts, directly informing our temporal roadmap. Short-term priorities (2024–2026) focus on enhancing detection accuracy in constrained environments—for instance, agricultural IoT networks require sub-50 ms anomaly detection with less than 1% false positive rates to prevent irrigation system disruptions, while smart manufacturing demands 99.99% uptime during adaptive learning phases. Medium-term objectives (2027–2029) center on scalable interoperability, where standardized APIs must accommodate the projected 75 billion IoT devices by 2030. Long-term goals (2030–2035) emphasize autonomous security ecosystems capable of self-evolution, exemplified by smart city infrastructures that can autonomously detect, classify, and mitigate novel attack vectors without human intervention while maintaining citizen privacy through zero-knowledge proof mechanisms.

AI is essential for IDS transparency, using methods like SHAP or LIME to deliver real time, feature level explanations that help administrators validate decisions and fine tune configurations. Equally critical are extensive real world trials—in smart cities, industrial networks, etc.—to expose deployment challenges beyond the lab and foster industry–academia

collaboration for robust, reliable systems. For instance, deploying IDS pilots in municipal IoT infrastructures could reveal practical challenges such as bandwidth constraints in surveillance cameras or interoperability issues in heterogeneous sensor gateways. Finally, achieving scalability requires hybrid signature and anomaly based detection, augmented by generative models (VAEs, GANs) to synthesize diverse attack scenarios. Looking ahead, the integration of Generative AI and large language models (LLMs) promises to make IoT security more adaptive and intelligent: LLMs can parse unstructured device logs and network traffic to flag novel threats, optimize lightweight encryption and authentication protocols for constrained sensors, automatically generate and verify smart contracts in blockchain-backed IDS frameworks, and enable intuitive, natural language access control interfaces—laying the groundwork for a secure, self-evolving IDS ecosystem [114]. Data balancing techniques such as SMOTE or denoising autoencoders remain vital to handle class imbalance and missing values without degrading performance.

Future developments will hinge on seamlessly integrating AI with traditional methods, leveraging techniques like transfer learning and automated hyperparameter optimization to reduce reliance on large training datasets and enable deployment in resource-constrained IoT environments, while employing AI-driven hyperparameter tuning and architecture search to achieve real-time adaptability with minimal computational overhead. Equally important will be interdisciplinary collaboration among cybersecurity experts, software engineers, and data scientists to create holistic IDS solutions capable of evolving alongside new threats; their long-term success will depend on this synergy.

Figure 13 illustrates our research roadmap across three time horizons, linking each open question to targeted implementation, optimization, and scale-up activities. These time horizons were determined through a comprehensive analysis of the papers reviewed in this survey, systematically evaluating the current maturity level, reported limitations, and implementation challenges of each technique. Short-term horizons (2024–2026) encompass technologies with demonstrated proof-of-concept implementations but requiring optimization for IoT constraints, such as federated learning approaches that show promise but face communication overhead challenges. Medium-term horizons (2027–2029) include techniques showing theoretical feasibility with limited practical validation, like blockchain-based IDS frameworks that require scalability improvements. Long-term horizons (2030–2035) represent emerging paradigms with significant research gaps, such as quantum-resistant protocols and fully autonomous security ecosystems. This timeline reflects the consistent patterns observed across reviewed literature regarding development cycles from research prototype to practical deployment in resource-constrained IoT environments.

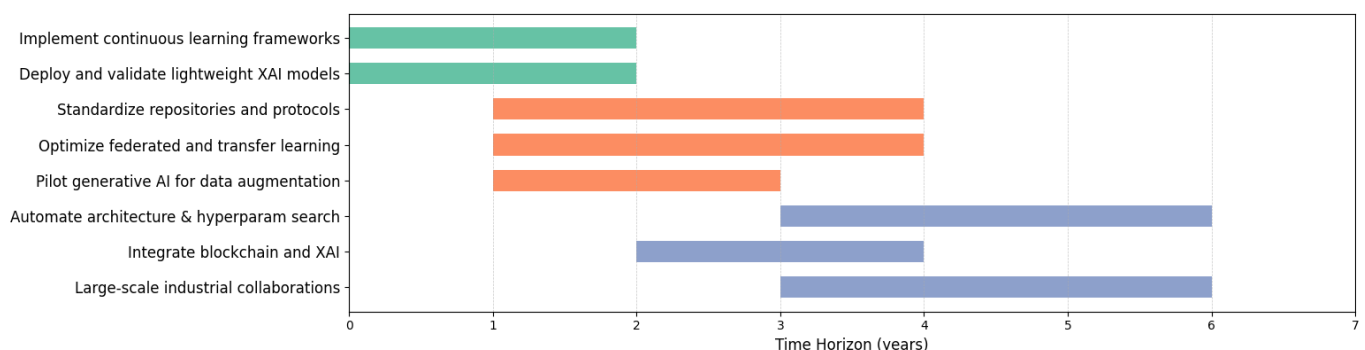


Figure 13. Research Roadmap: Three Time Horizons for IDS Research Questions.

Another promising but still underexplored direction is intrusion detection at the physical layer of wireless IoT systems. Since most IoT devices communicate over broadcast wireless channels (e.g., Wi-Fi, ZigBee, LoRa, NB-IoT, Bluetooth), they are inherently vul-

nerable to spoofing, jamming, and signal injection attacks. IDS solutions at this layer can exploit radio-frequency (RF) features such as signal strength, phase, and device-specific fingerprints to detect anomalies and impersonation attempts. However, research in this area remains limited compared to network- and application-layer IDS. Expanding future work to incorporate physical-layer intrusion detection would strengthen IoT security holistically by addressing threats that arise before higher-layer protocols can provide protection.

4. Conclusions

This review shows that advanced techniques such as XAI, FL, Edge AI, and Generative AI are transforming IDS for IoT. These methods enable adaptive, scalable systems that improve detection accuracy and reduce false positives while addressing data privacy and responsiveness challenges. In particular, GANs and VAEs enhance IDS training by generating synthetic data, whereas FL and Edge AI support decentralized processing to overcome resource constraints and latency issues. XAI further boosts trust by clarifying AI-driven decisions.

Key findings reveal a transition from static to dynamic IDS models that leverage continuous learning and decentralized processing, and they underscore the growing adoption of hybrid approaches, including blockchain-enhanced solutions for tamper-proof logging, and the importance of using realistic, diverse datasets with standardized evaluation methods. However, issues such as interoperability, energy efficiency, and the lack of standardized benchmarking remain.

To address these gaps, future research should prioritize pilot deployments in operational IoT networks, develop lightweight adaptive algorithms for resource-constrained devices, and enhance model transparency via explainable AI. In addition, establishing collaborative frameworks and global repositories for standardized datasets and evaluation protocols is essential. These steps will ensure robust, scalable, and transparent protection against emerging threats.

This review also consolidates a fragmented body of work into a unified conceptual framework across six dimensions (detection types, evaluation methods, optimization goals, AI techniques, industrial applicability, and open challenges). By pairing this framework with practical dataset-selection guidance and a cross-walk between methods and application domains, the study provides both researchers and practitioners with a concrete reference. For practitioners, it clarifies key trade-offs—latency, privacy, and resource budgets—and offers a checklist to guide architectural and evaluation choices. For researchers and standardization bodies, it motivates a common reporting schema (dataset properties, class balance, attack coverage, energy/memory/latency, and FP/FN rates) to foster comparability and reproducibility at scale. In this way, the study contributes not only a synthesis of past work but also a roadmap to accelerate the development of reliable, transparent, and future-ready IDSs for IoT.

By aligning scientific insights with practical and regulatory needs, the study aims to accelerate the transition from academic prototypes to standardized, deployable, and trustworthy IDS solutions for IoT.

Author Contributions: Conceptualization, A.V., K.M.T., I.T. and M.-D.C.; methodology, A.V., I.T. and M.-D.C.; validation, A.V., I.T. and M.-D.C.; investigation, A.V., I.T. and M.-D.C.; resources, A.V., K.M.T., I.T. and M.-D.C.; data curation, A.V.; writing—original draft preparation, A.V.; writing—review and editing, I.T. and M.-D.C.; visualization, A.V.; supervision, I.T. and M.-D.C.; project administration, M.-D.C.; funding acquisition, M.-D.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the project R&D&I Lab in cybersecurity, privacy, and secure communications (TRUST Lab), financed by European Union NextGeneration-EU, the Recovery Plan, Transformation and Resilience, through INCIBE.

Data Availability Statement: This article is a review and did not generate new data. All datasets referenced and analyzed are publicly available through the original publications cited in the References section.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. IHS Markit. Available online: <https://euristiq.com/future-of-iot/> (accessed on 3 October 2025).
2. Tabassum, A.; Erbad, A.; Lebda, W.; Mohamed, A.; Guizani, M. FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning. *Comput. Commun.* **2022**, *192*, 299–310. [CrossRef]
3. Friha, O.; Ferrag, M.A.; Benbouzid, M.; Berghout, T.; Kantarci, B.; Choo, K.-K.R. 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. *Comput. Secur.* **2023**, *127*, 103097. [CrossRef]
4. Yu, X.; Yang, X.; Tan, Q.; Shan, C.; Lv, Z. An edge computing based anomaly detection method in IoT industrial sustainability. *Appl. Soft Comput.* **2022**, *128*, 109486. [CrossRef]
5. Eskandari, M.; Janjua, Z.H.; Vecchio, M.; Antonelli, F. Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices. *IEEE Internet Things J.* **2020**, *7*, 6882–6897. [CrossRef]
6. Bhavsar, M.H.; Bekele, Y.B.; Roy, K.; Kelly, J.C.; Limbrick, D. FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT. *IEEE Access* **2024**, *12*, 52215–52226. [CrossRef]
7. Sarhan, M.; Lo, W.W.; Layeghy, S.; Portmann, M. HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. *Comput. Electr. Eng.* **2022**, *103*, 108379. [CrossRef]
8. Li, W.; Stidsen, C.; Adam, T. A blockchain-assisted security management framework for collaborative intrusion detection in smart cities. *Comput. Electr. Eng.* **2023**, *111*, 108884. [CrossRef]
9. Hooshmand, M.K.; Huchaiah, M.D.; Alzighaibi, A.R.; Hashim, H.; Atlam, E.-S.; Gad, I. Robust network anomaly detection using ensemble learning approach and explainable artificial intelligence (XAI). *Alex. Eng. J.* **2024**, *94*, 120–130. [CrossRef]
10. Sharma, B.; Sharma, L.; Lal, C.; Roy, S. Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach. *Expert Syst. Appl.* **2024**, *238*, 121751. [CrossRef]
11. Le, T.-T.; Wardhani, R.W.; Putranto, D.S.C.; Jo, U.; Kim, H. Toward Enhanced Attack Detection and Explanation in Intrusion Detection System-Based IoT Environment Data. *IEEE Access* **2023**, *11*, 131661–131676. [CrossRef]
12. Olanrewaju-George, B.; Pranggono, B. Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. *Cyber Secur. Appl.* **2025**, *3*, 100068. [CrossRef]
13. Tufan, E.; Tezcan, C.; Acarturk, C. Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network. *IEEE Access* **2021**, *9*, 50078–50092. [CrossRef]
14. Abdel-Basset, M.; Hawash, H.; Sallam, K.M.; Elgendi, I.; Munasinghe, K.; Jamalipour, A. Efficient and Lightweight Convolutional Networks for IoT Malware Detection: A Federated Learning Approach. *IEEE Internet Things J.* **2023**, *10*, 7164–7173. [CrossRef]
15. Pohar, M.; Blas, M.; Turk, S. A secure edge computing model using machine learning and IDS to detect and isolate intruders. *Adv. Methodol. Stat.* **2004**, *1*, 143–161. [CrossRef]
16. Alkhonaini, M.A.; Alohal, M.A.; Aljebreen, M.; Eltahir, M.M.; Alanazi, M.H.; Yafaz, A.; Alsini, R.; Khadidos, A.O. Sandpiper optimization with hybrid deep learning model for blockchain-assisted intrusion detection in iot environment. *Alex. Eng. J.* **2025**, *112*, 49–62. [CrossRef]
17. Saheed, Y.K.; Chukwuere, J.E. XAIEnsembleTL-IoV: A new eXplainable Artificial Intelligence ensemble transfer learning for zero-day botnet attack detection in the Internet of Vehicles. *Results Eng.* **2024**, *24*, 103171. [CrossRef]
18. Saheed, Y.K.; Misra, S. CPS-IoT-PPDNN: A new explainable privacy preserving DNN for resilient anomaly detection in Cyber-Physical Systems-enabled IoT networks. *Chaos Solitons Fractals* **2025**, *191*, 115939. [CrossRef]
19. IEEE Xplore. Available online: <https://ieeexplore.ieee.org/> (accessed on 3 October 2025).
20. Science Direct. Available online: <https://www.sciencedirect.com/> (accessed on 3 October 2025).
21. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
22. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
23. Choudhary, S.; Kesswani, N. A survey: Intrusion detection techniques for internet of things. *Int. J. Inf. Secur. Priv.* **2019**, *13*, 86–105. [CrossRef]

24. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [\[CrossRef\]](#)
25. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 18. [\[CrossRef\]](#)
26. Elrawy, M.F.; Awad, A.I.; Hamed, H.F.A. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 21. [\[CrossRef\]](#)
27. Ali, S.; Li, Q.; Yousafzai, A. Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Netw.* **2024**, *152*, 103320. [\[CrossRef\]](#)
28. Sasi, T.; Lashkari, A.H.; Lu, R.; Xiong, P.; Iqbal, S. A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *J. Inf. Intell.* **2023**, *2*, 455–513. [\[CrossRef\]](#)
29. Merlino, V.; Allegra, D. Energy-based approach for attack detection in IoT devices: A survey. *Internet Things* **2024**, *27*, 101306. [\[CrossRef\]](#)
30. Al-Shurbaji, T.; Anbar, M.; Manickam, S.; Hasbullah, I.H.; Alfriehate, N.; Alabsi, B.A.; Alzighaibi, A.R.; Hashim, H. Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review. *IEEE Access* **2025**, *13*, 11792–11822. [\[CrossRef\]](#)
31. Rahman, M.; Al Shakil, S.; Mustakim, M.R. A survey on intrusion detection system in IoT networks. *Cyber Secur. Appl.* **2025**, *3*, 100082. [\[CrossRef\]](#)
32. Alhamdi, M.J.; Lopez-Guede, J.M.; AlQaryouti, J.; Rahebi, J.; Zulueta, E.; Fernandez-Gamiz, U. AI-based malware detection in IoT networks within smart cities: A survey. *Comput. Commun.* **2025**, *233*, 108055. [\[CrossRef\]](#)
33. Almorabea, O.M.; Khanzada, T.J.S.; Aslam, M.A.; Hendi, F.A.; Almorabea, A.M. IoT Network-Based Intrusion Detection Framework: A Solution to Process Ping Floods Originating from Embedded Devices. *IEEE Access* **2023**, *11*, 119118–119145. [\[CrossRef\]](#)
34. Satilmis, H.; Akleylek, S.; Tok, Z.Y. A Systematic Literature Review on Host-Based Intrusion Detection Systems. *IEEE Access* **2024**, *12*, 27237–27266. [\[CrossRef\]](#)
35. Tang, J.; Qin, T.; Kong, D.; Zhou, Z.; Li, X.; Wu, Y.; Gu, J. Anomaly Detection in Social-Aware IoT Networks. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 3162–3176. [\[CrossRef\]](#)
36. Einy, S.; Oz, C.; Navaei, Y.D. The Anomaly- And Signature-Based IDS for Network Security Using Hybrid Inference Systems. *Math. Probl. Eng.* **2021**, *2021*, 6639714. [\[CrossRef\]](#)
37. NS-3 Simulator. Available online: <https://www.nsnam.org/> (accessed on 3 December 2024).
38. IoT Simulator. Available online: <https://aws.amazon.com/es/solutions/implementations/iot-device-simulator/> (accessed on 3 October 2025).
39. MAMiri-Zarandi, M.; Dara, R.A.; Lin, X. SIDS: A federated learning approach for intrusion detection in IoT using Social Internet of Things. *Comput. Netw.* **2023**, *236*, 110005. [\[CrossRef\]](#)
40. Kipongo, J.; Swart, T.G.; Esenogho, E. Artificial Intelligence-Based Intrusion Detection and Prevention in Edge-Assisted SDWSN With Modified Honeycomb Structure. *IEEE Access* **2023**, *12*, 3140–3175. [\[CrossRef\]](#)
41. Sharadqh, A.A.M.; Hatamleh, H.A.M.; Alnaser, A.M.A.; Saloum, S.S.; Alawneh, T.A. Hybrid Chain: Blockchain Enabled Framework for Bi-Level Intrusion Detection and Graph-Based Mitigation for Security Provisioning in Edge Assisted IoT Environment. *IEEE Access* **2023**, *11*, 27433–27449. [\[CrossRef\]](#)
42. Verma, A.; Ranga, V. Machine Learning based Intrusion Detection Systems for IoT Applications. *Wirel. Pers. Commun.* **2020**, *111*, 2287–2310. [\[CrossRef\]](#)
43. Osman, M.; He, J.; Zhu, N.; Mokbal, F.M.M. An ensemble learning framework for the detection of RPL attacks in IoT networks based on the genetic feature selection approach. *Ad Hoc Netw.* **2024**, *152*, 103331. [\[CrossRef\]](#)
44. Shalabi, K.; Abu Al-Haija, Q.; Al-Fayoumi, M. A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A systematic review. *Procedia Comput. Sci.* **2024**, *236*, 410–419. [\[CrossRef\]](#)
45. Li, S.; Cao, Y.; Liu, S.; Lai, Y.; Zhu, Y.; Ahmad, N. HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN. *Expert Syst. Appl.* **2024**, *238*, 122198. [\[CrossRef\]](#)
46. Ahmad, R.; Alsmadi, I.; Alhamdani, W.; Tawalbeh, L. A comprehensive deep learning benchmark for IoT IDS. *Comput. Secur.* **2022**, *114*, 102588. [\[CrossRef\]](#)
47. Nie, F.; Liu, W.; Liu, G.; Gao, B. M2VT-IDS: A multi-task multi-view learning architecture for designing IoT intrusion detection system. *Internet Things* **2024**, *25*, 101102. [\[CrossRef\]](#)
48. Racherla, S.; Sripathi, P.; Faruqui, N.; Kabir, A.; Shah, S.A. Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning. *IEEE Access* **2024**, *12*, 63584–63597. [\[CrossRef\]](#)
49. NSL-KDD. Available online: <https://www.kaggle.com/datasets/hassan06/nsldata> (accessed on 3 October 2025).
50. UNSW-NB15 Dataset. Available online: <https://research.unsw.edu.au/projects/unswnb15-dataset> (accessed on 3 October 2025).
51. CICIDS2017 Dataset. Available online: <https://www.unb.ca/cic/datasets/ids-2017.html> (accessed on 3 October 2025).

52. BoT-IoT Dataset. Available online: <https://research.unsw.edu.au/projects/bot-iot-dataset> (accessed on 3 October 2025).
53. DS2OS Dataset. Available online: <https://www.kaggle.com/datasets/libamariyam/ds2os-dataset> (accessed on 3 October 2025).
54. IoTID20. Available online: <https://www.kaggle.com/datasets/rohulaminlabid/iotid20-dataset> (accessed on 3 October 2025).
55. NB-IoT Dataset. Available online: <https://ieee-dataport.org/keywords/nb-iot> (accessed on 3 October 2025).
56. IoT-23 Dataset. Available online: <https://www.stratosphereips.org/datasets-iot23> (accessed on 3 October 2025).
57. Ton_IoT Dataset. Available online: <https://research.unsw.edu.au/projects/toniot-datasets> (accessed on 3 October 2025).
58. MQTT-IoT 2020. Available online: <https://ieee-dataport.org/open-access/mqtt-iot-ids2020-mqtt-internet-things-intrusion-detection-dataset> (accessed on 3 October 2025).
59. IoT_malware Dataset. Available online: <https://www.kaggle.com/datasets/anaselmasry/iot-malware> (accessed on 3 October 2025).
60. Darpa Dataset. Available online: <https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset> (accessed on 3 October 2025).
61. N-BaIoT. Available online: <https://archive.ics.uci.edu/dataset/442/detection+of+iot+botnet+attacks+n+baiot> (accessed on 3 October 2025).
62. Bhale, P.; Chowdhury, D.R.; Biswas, S.; Nandi, S. OPTIMIST: Lightweight and Transparent IDS with Optimum Placement Strategy to Mitigate Mixed-Rate DDoS Attacks in IoT Networks. *IEEE Internet Things J.* **2023**, *10*, 8357–8370. [CrossRef]
63. Sharma, S.; Kumar, V.; Dutta, K. Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review. *Internet Things Cyber Phys. Syst.* **2024**, *4*, 258–267. [CrossRef]
64. Sadikin, F.; van Deursen, T.; Kumar, S. A ZigBee Intrusion Detection System for IoT using Secure and Efficient Data Collection. *Internet Things* **2020**, *12*, 100306. [CrossRef]
65. Negm, N.; Alamro, H.; Allafi, R.; Khalid, M.; Nouri, A.M.; Marzouk, R.; Othman, A.Y.; Ahmed, N.A. Tasmanian devil optimization with deep autoencoder for intrusion detection in IoT assisted unmanned aerial vehicle networks. *Ain Shams Eng. J.* **2024**, *15*, 102943. [CrossRef]
66. Abusitta, A.; de Carvalho, G.H.; Wahab, O.A.; Halabi, T.; Fung, B.C.; Al Mamoori, S. Deep learning-enabled anomaly detection for IoT systems. *Internet Things* **2023**, *21*, 100656. [CrossRef]
67. Zohourian, A.; Dadkhah, S.; Molyneaux, H.; Neto, E.C.P.; Ghorbani, A.A. IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks. *Comput. Secur.* **2024**, *146*, 104034. [CrossRef]
68. Bakhsh, S.A.; Khan, M.A.; Ahmed, F.; Alshehri, M.S.; Ali, H.; Ahmad, J. Enhancing IoT network security through deep learning-powered Intrusion Detection System. *Internet Things* **2023**, *24*, 100936. [CrossRef]
69. Nguyen, H.; Kashef, R. TS-IDS: Traffic-aware self-supervised learning for IoT Network Intrusion Detection. *Knowl.-Based Syst.* **2023**, *279*, 110966. [CrossRef]
70. Javanmardi, S.; Ghahramani, M.; Shojafar, M.; Alazab, M.; Caruso, A.M. M-RL: A mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks. *Comput. Secur.* **2024**, *140*, 103778. [CrossRef]
71. Saheed, Y.K.; Omole, A.I.; Sabit, M.O. GA-mADAM-IIoT: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data. *Sens. Int.* **2025**, *6*, 100297. [CrossRef]
72. Zhang, H.; Ye, J.; Huang, W.; Liu, X.; Gu, J. Survey of federated learning in intrusion detection. *J. Parallel Distrib. Comput.* **2025**, *195*, 104976. [CrossRef]
73. Quyen, N.H.; Duy, P.T.; Nguyen, N.T.; Khoa, N.H.; Pham, V.-H. FedKD-IDS: A robust intrusion detection system using knowledge distillation-based semi-supervised federated learning and anti-poisoning attack mechanism. *Inf. Fusion* **2025**, *117*, 102807. [CrossRef]
74. Rey, V.; Sánchez, P.M.S.; Celdrán, A.H.; Bovet, G. Federated learning for malware detection in IoT devices. *Comput. Netw.* **2022**, *204*, 108693. [CrossRef]
75. Ma, Z.; Liu, L.; Meng, W.; Luo, X.; Wang, L.; Li, W. ADCL: Toward an Adaptive Network Intrusion Detection System Using Collaborative Learning in IoT Networks. *IEEE Internet Things J.* **2023**, *10*, 12521–12536. [CrossRef]
76. Thamilarasu, G.; Odesile, A.; Hoang, A. An intrusion detection system for internet of medical things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
77. Jeon, J.; Jeong, B.; Baek, S.; Jeong, Y.-S. Static Multi Feature-Based Malware Detection Using Multi SPP-net in Smart IoT Environments. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 2487–2500. [CrossRef]
78. Li, Z.; Huang, C.; Qiu, W. An intrusion detection method combining variational auto-encoder and generative adversarial networks. *Comput. Netw.* **2024**, *253*, 110724. [CrossRef]
79. Han, Y.; Chang, H. XA-GANomaly: An Explainable Adaptive Semi-Supervised Learning Method for Intrusion Detection Using GANomaly. *Comput. Mater. Contin.* **2023**, *76*, 221–237. [CrossRef]
80. Soliman, S.; Oudah, W.; Aljuhani, A. Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alex. Eng. J.* **2023**, *81*, 371–383. [CrossRef]

81. Khan, S.H.; Alahmadi, T.J.; Ullah, W.; Iqbal, J.; Rahim, A.; Alkahtani, H.K.; Alghamdi, W.; Almagrabi, A.O. A new deep boosted CNN and ensemble learning based IoT malware detection. *Comput. Secur.* **2023**, *133*, 103385. [\[CrossRef\]](#)
82. Smmarwar, S.K.; Gupta, G.P.; Kumar, S. Deep malware detection framework for IoT-based smart agriculture. *Comput. Electr. Eng.* **2022**, *104*, 108410. [\[CrossRef\]](#)
83. Saveetha, D.; Maragatham, G. Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning. *Pattern Recognit. Lett.* **2022**, *153*, 24–28. [\[CrossRef\]](#)
84. Sunil, R.Y.; Parimala, E.H.; Bosco, V.S.J.P.; Samuel Raj, A.; Kumar, P.J.R.V.; Kolluru, V. Real-Time Adaptive Intrusion Detection System [RTPIDS] for Internet of Things Using Federated Learning and Blockchain. In Proceedings of the 2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI), Tirunelveli, India, 18–20 November 2024; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2024; pp. 298–305. [\[CrossRef\]](#)
85. Hafid, B.; Ezzouhairi, A.; Haddouch, K. Strengthening Security in the Internet of Things (IoT): Integrated Approach of Intrusion Detection Systems (IDS) and Edge Computing. In Proceedings of the 2024 3rd International Conference on Embedded Systems and Artificial Intelligence (ESAI), Fez, Morocco, 19–20 December 2024; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2024. [\[CrossRef\]](#)
86. Loari, Y.Y.S.; Bassole, D.; Sawadogo, L.M.; Koala, G.; Sié, O. IoT Devices Security Improvement Based on Collaborative Intrusion Detection System and Blockchain Technology. In Proceedings of the 2024 International Conference on Computer and Applications (ICCA), Cairo, Egypt, 17–19 December 2024; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2024. [\[CrossRef\]](#)
87. Alharbi, S.; Alghazzawi, D.; Hakeem, A.; Mohaisen, L.; Cheng, L.; Attiah, A. A Blockchain-Based Collaborative Intrusion Detection Systems Framework. *IEEE Internet Things J.* **2024**, *11*, 25481–25493. [\[CrossRef\]](#)
88. Liu, Z.; Yu, X.; Liu, N.; Liu, C.; Jiang, A.; Chen, L. Integrating AI with detection methods, IoT, and blockchain to achieve food authenticity and traceability from farm-to-table. *Trends Food Sci. Technol.* **2025**, *158*, 104925. [\[CrossRef\]](#)
89. Alghamdi, R.; Bellaiche, M. A cascaded federated deep learning based framework for detecting wormhole attacks in IoT networks. *Comput. Secur.* **2023**, *125*, 103014. [\[CrossRef\]](#)
90. Kumar, A.; Shridhar, M.; Swaminathan, S.; Lim, T.J. Machine learning-based early detection of IoT botnets using network-edge traffic. *Comput. Secur.* **2022**, *117*, 102693. [\[CrossRef\]](#)
91. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Garg, S.; Hassan, M.M. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *J. Parallel Distrib. Comput.* **2022**, *164*, 55–68. [\[CrossRef\]](#)
92. Khanday, S.A.; Fatima, H.; Rakesh, N. Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks. *Expert Syst. Appl.* **2023**, *215*, 119330. [\[CrossRef\]](#)
93. Gupta, B.B.; Gaurav, A.; Alhalabi, W.; Arya, V.; Alharbi, E.; Chui, K.T. Distributed optimization for IoT attack detection using federated learning and Siberian Tiger optimizer. *ICT Express* **2025**, *11*, 542–546. [\[CrossRef\]](#)
94. Hendaoui, F.; Meddeb, R.; Trabelsi, L.; Ferchichi, A.; Ahmed, R. FLADEN: Federated Learning for Anomaly DETection in IoT Networks. *Comput. Secur.* **2025**, *155*, 104446. [\[CrossRef\]](#)
95. Gao, N.; Liu, Y.; Zhang, Q.; Li, X.; Jin, S. Let RFF do the talking: Large language model enabled lightweight RFFI for 6G edge intelligence. *Sci. China Inf. Sci.* **2025**, *68*, 170308. [\[CrossRef\]](#)
96. Zheng, H.; Gao, N.; Cai, D.; Jin, S.; Matthaiou, M. UAV Individual Identification via Distilled RF Fingerprints-Based LLM in ISAC Networks. *arXiv* **2025**, arXiv:2508.12597. [\[CrossRef\]](#)
97. Rahman, S.; Pal, S.; Mittal, S.; Chawla, T.; Karmakar, C. SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. *Internet Things* **2024**, *26*, 101212. [\[CrossRef\]](#)
98. Qian, C.; Tang, W.; Wang, Y. RGAAnomaly: Data reconstruction-based generative adversarial networks for multivariate time series anomaly detection in the Internet of Things. *Futur. Gener. Comput. Syst.* **2025**, *167*, 107751. [\[CrossRef\]](#)
99. Hamouda, D.; Ferrag, M.A.; Benhamida, N.; Seridi, H.; Ghanem, M.C. Revolutionizing intrusion detection in industrial IoT with distributed learning and deep generative techniques. *Internet Things* **2024**, *26*, 101149. [\[CrossRef\]](#)
100. Jin, Y.; Zhou, J.; Gao, Y. HSGAN-IoT: A hierarchical semi-supervised generative adversarial networks for IoT device classification. *Comput. Netw.* **2024**, *243*, 110299. [\[CrossRef\]](#)
101. Arafah, M.; Phillips, I.; Adnane, A.; Hadi, W.; Alauthman, M.; Al-Banna, A.-K. Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks. *Appl. Soft Comput.* **2025**, *168*, 112455. [\[CrossRef\]](#)
102. Bin Hulayyil, S.; Li, S.; Saxena, N. Explainable AI-based intrusion detection in IoT systems. *Internet Things* **2025**, *31*, 101589. [\[CrossRef\]](#)
103. Gummadi, A.N.; Arreche, O.; Abdallah, M. A systematic evaluation of white-box explainable AI methods for anomaly detection in IoT systems. *Internet Things* **2025**, *30*, 101505. [\[CrossRef\]](#)
104. Saheed, Y.K.; Misra, S.; Chockalingam, S. Autoencoder via DCNN and LSTM Models for Intrusion Detection in Industrial Control Systems of Critical Infrastructures. In Proceedings of the 2023 IEEE/ACM 4th International Workshop on Engineering and Cybersecurity of Critical Systems, EnCyCriS 2023, Melbourne, Australia, 15 May 2023; pp. 9–16. [\[CrossRef\]](#)

105. Ramana, K.; Revathi, A.; Gayathri, A.; Jhaveri, R.H.; Narayana, C.L.; Kumar, B.N. WOGRU-IDS—An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks. *Comput. Commun.* **2022**, *196*, 195–206. [[CrossRef](#)]
106. Mirdula, S.; Roopa, M. MUD enabled deep learning framework for anomaly detection in IoT integrated smart building. *E-Prime—Adv. Electr. Eng. Electron. Energy* **2023**, *5*, 100186. [[CrossRef](#)]
107. Alamro, H.; Marzouk, R.; Alruwais, N.; Negm, N.; Aljameel, S.S.; Khalid, M.; Hamza, M.A.; Alsaied, M.I. Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning. *IEEE Access* **2023**, *11*, 82199–82207. [[CrossRef](#)]
108. Anthi, E.; Williams, L.; Slowinska, M.; Theodorakopoulos, G.; Burnap, P. A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 9042–9053. [[CrossRef](#)]
109. Sarwar, N.; Bajwa, I.S.; Hussain, M.Z.; Ibrahim, M.; Saleem, K. IoT Network Anomaly Detection in Smart Homes Using Machine Learning. *IEEE Access* **2023**, *11*, 119462–119480. [[CrossRef](#)]
110. Jaramillo-Alcazar, A.; Govea, J.; Villegas-Ch, W. Anomaly Detection in a Smart Industrial Machinery Plant Using IoT and Machine Learning. *Sensors* **2023**, *23*, 8286. [[CrossRef](#)]
111. Patel, S.K. Improving intrusion detection in cloud-based healthcare using neural network. *Biomed. Signal Process. Control* **2023**, *83*, 104680. [[CrossRef](#)]
112. Rahman, A.; Asyhari, A.T.; Leong, L.; Satrya, G.; Tao, M.H.; Zolkipli, M. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustain. Cities Soc.* **2020**, *61*, 102324. [[CrossRef](#)]
113. Okey, O.D.; Melgarejo, D.C.; Saadi, M.; Rosa, R.L.; Kleinschmidt, J.H.; Rodriguez, D.Z. Transfer Learning Approach to IDS on Cloud IoT. *IEEE Access* **2023**, *11*, 1023–1038. [[CrossRef](#)]
114. Alwahedi, F.; Aldhaheri, A.; Ferrag, M.A.; Battah, A.; Tihanyi, N. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 167–185. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.