Security Challenges in IoT Networks: A Systematic Review of Layered Threats and a Comparative Evaluation of Intrusion-Detection Techniques

Ankur Sharma
Bourns, Inc. / IT & Security
Western Governors University, Millcreek, USA

ABSTRACT

The rise of the Internet of Things (IoT) has already altered contemporary digital ecosystems by enabling the seamless interconnection of heterogeneous devices. Nonetheless, this growth has posed serious security challenges, including a scarcity of resources, device heterogeneity, and exposure to a large attack surface. This work explores the security threats that pose a critical issue for IoT networks, as well as modern detection techniques and prevention methods. To categorize IoT-specific threats, a systematic review of the available literature is conducted, covering network-level, device-level, and application-level threats. The paper also assesses detection techniques, including signature-based, anomaly-based, and machine-learning-based approaches, and their usefulness and limitations in dynamic IoT settings. Moreover, different preventive schemes, such as cryptography, authentication mechanisms, and privacy-preserving communication models, are discussed with respect to their flexibility and scalability. The results indicate that although higher-performing detection models improve threat-detection accuracy, issues of computational cost and real-time responsiveness persist. To ground this synthesis in measured behavior, a controlled benchmarking experiment is additionally conducted, comparing signature-based, anomaly-based, and machine-learning-based detectors on the NSL-KDD intrusion-detection dataset; the experiment quantifies the precision-recall trade-off between these paradigms and reveals that rare attack classes remain largely undetected despite high aggregate accuracy. The paper concludes with a statement on the necessity of lightweight, adaptive, and scalable security frameworks to address evolving IoT threats and ensure robust network protection.

General Terms

Security, Computer Networks, Internet of Things, Machine Learning, Intrusion Detection.

Keywords

Internet of Things (IoT), IoT Security, Cybersecurity, IoT Threats, Intrusion Detection Systems (IDS), Anomaly Detection, Secure Communication.

1. INTRODUCTION

The Internet of Things (IoT) has quickly become an essential part of the digital infrastructure of the modern age and enables convenient connectivity among physical elements, sensors, and systems across different application areas. From smart homes and the health industry to industrial control settings and smart farming, IoT technologies have greatly contributed to automation, operational efficiency, and timely decision-making. Such unprecedented expansion has led to a tremendous proliferation of interrelated devices that drive the creation and flow of large amounts of data. However, in tandem with those developments, IoT network growth has created a plethora of security risks that disrupt traditional cybersecurity paradigms [3], [7].

Contrary to traditional computing settings, IoT networks are inherently heterogeneous, comprising devices with varying computational abilities, communication protocols, and operational availability. Numerous IoT devices are resource-constrained, with limited processing power, memory, and energy, which limits the implementation of intensive security measures. Consequently, these devices have low levels of protection and can become targets of cyber adversaries. Moreover, IoT systems present a large attack surface because they are designed to be deployed in large numbers and are decentralized, allowing threat actors to find multiple points of entry into the network [15], [16].

IoT network vulnerabilities span multiple layers, including device-level, network-level, and application-level vulnerabilities. Denial-of-service attacks, such as distributed denial-of-service (DDoS), man-in-the-middle, and routing attacks, may interfere with communication and affect service availability at the network level. The manipulation of firmware, physical abuse of the system, and illegal access pose additional risks at the device level, further complicating the issue of system insecurity. In addition, application-level attacks, such as data leakage and malware injection, compromise data confidentiality and integrity. These threats are multidimensional and underscore the difficulty of securing IoT environments and the need to explore solutions that are comprehensive and dynamic [10], [17].

To tackle these issues, substantial research has produced effective detection systems to identify malicious activities in IoT networks. Conventional intrusion detection systems (IDSs), such as signature- and rule-based defenses, have been widely used but are mostly constrained in dynamic, changing threat environments. This has led to a gradual shift toward anomaly-based detection and intelligent methods that leverage machine learning and deep learning models. Through these methods, previously unknown threats are identified by studying patterns and deviations in network behavior, which enhances detection accuracy and flexibility [2], [9], [14].

In addition to detection, prevention strategies are key to reducing IoT security risks. The basic elements of IoT security architectures are cryptographic techniques, secure authentication methods, and access control frameworks. In recent years, new technologies such as blockchain, artificial intelligence, and software-defined networking (SDN) have been incorporated into IoT security architectures to enhance trust, scalability, and resilience. Examples include blockchain-based approaches, which offer decentralized data integrity and security, and AI-driven systems, which can provide real-time adaptive responses to threats [1], [8], [21]. Nevertheless, limited resources, including computational overhead, latency, interoperability, and

standardization challenges, have remained a barrier to the popularization of these solutions, especially in resource-constrained contexts [5], [13].

Furthermore, IoT integration with new network platforms, such as 5G and future 6G systems, adds new complexities to maintaining communication pathways and connecting massive numbers of devices. This intersection of technologies requires advanced, scalable, and intelligent security solutions that can respond to existing and emerging threats [6], [11]. Simultaneously, innovative strategies that arise to defend against or detect emerging attack methods, such as AI-driven cyberattacks and botnets, persistently test existing defense methodologies, making it necessary to continue innovating in the field of IoT security research [18], [22].

A systematic treatment of security issues, detection, and threat prevention is urgently required due to the changing and dynamic nature of IoT ecosystems. Although research on specific areas of IoT security has been conducted, there is still a lack of coherent perspectives that provide an overview of threats, detection methods, and mitigation strategies within a single framework. The present research aims to fill this gap through a descriptive synthesis of the available literature, categorization of key threats in IoT security, critique of modern detection techniques, and analysis of effective prevention policies. In this manner, this paper should help establish scalable, adaptive, and lightweight security solutions that will effectively protect the next generation of IoT networks.

2. METHODS

This research employs the systematic literature review (SLR) as a methodological tool to address security issues in IoT networks, with a specific emphasis on security threats, their detection systems, and prevention techniques. The SLR methodology is well suited for synthesizing the existing knowledge base, identifying research gaps, and developing a well-organized understanding of the intricate and dynamic field of IoT security.

2.1 Research Design

To gather, assess, and compile appropriate academic literature in the domain of IoT cybersecurity, a qualitative, review-based research design was used. A structured review protocol was followed in this study to provide transparency, reproducibility, and methodological rigor. The major focus is the categorization and critical analysis of established methods of IoT security. To complement this qualitative synthesis, a controlled benchmarking experiment is also conducted (Section 4) to empirically validate the comparative detection trade-offs identified in the reviewed literature.

2.2 Data Sources and Search Strategy

Peer-reviewed academic journals, conference publications, and reliable scientific sources on cybersecurity and IoT were identified as relevant to the research topic. The selection criteria were based on quality and on recent research on IoT threats, intrusion detection systems, machine-learning-driven security models, and prevention models. Priority was given to publications listed in established databases and indexed journals to ensure credibility and relevance.

A keyword-based search strategy was used, with terms such as IoT security, cyber threats in IoT, intrusion detection in IoT, machine learning for IoT security, and prevention of attacks on IoT. This approach enabled the identification of studies that directly address the main research elements, namely threats, detection, and prevention.

2.3 Inclusion and Exclusion Criteria

To guarantee the relevance and quality of the chosen studies, specific inclusion and exclusion criteria were used.

Inclusion Criteria:

- Research involving IoT security issues, threats, or threat detection and prevention.
- Conference papers and peer-reviewed journal articles.
- Articles from recent years that reflect current developments.
- Studies that involve machine learning, artificial intelligence, or advanced security systems.

Exclusion Criteria:

- Articles unrelated to IoT security.
- Sources that have not been peer reviewed or are of low quality.
- Articles that are insufficiently detailed in terms of methodology or technical description.
- Overlapping or redundant studies.

This screening process minimized the inclusion of low-impact and irrelevant studies in the analysis.

2.4 Data Extraction and Categorization

The selected studies were analyzed systematically to elicit important information about the threats associated with IoT security, methods of detection, and prevention. Extracted data included:

- Forms of security threats (e.g., network-level, device-level, application-level).
- Detection strategies (e.g., anomaly-based, signature-based, machine-learning-based).
- Prevention schemes (e.g., cryptography, authentication procedures, blockchain systems).
- Performance considerations (e.g., scalability, computational overhead, adaptability).

The extracted data were subsequently coded into thematic categories to enable a structured analysis and comparison across studies.

2.5 Analytical Framework

The thematic analysis method was used to reveal trends, consistencies, and inconsistencies across the sampled studies. Three main dimensions were considered in the analysis:

- Threat Classification: detection and classification of typical IoT security threats.
- Detection Mechanisms: assessment of methods of detecting malicious activities.
- Prevention Strategies: evaluation of measures that can be taken to prevent or discourage attacks.

Further, a comparative lens was applied to assess the strengths and weaknesses of various methods, especially when considering resource limitations and the scalability challenges of the IoT environment.

2.6 Validity and Reliability Considerations

To increase the reliability and validity of the study, various precautions were taken. Peer-reviewed sources help ensure the credibility of the information, and systematic selection criteria help minimize bias in the selection of studies. In addition, the processes of categorization and analysis were carried out uniformly across all the chosen studies to ensure analytical rigor.

Despite these measures, some limitations remain, such as possible publication bias and the exclusion of non-English or unpublished studies. Nevertheless, the comprehensive and systematic stance taken in the present study mitigates these shortcomings and provides a strong foundation for the analysis of IoT security issues.

3. RESULTS

This section presents a synthesis of the reviewed literature on security issues in IoT networks, focusing on three interrelated aspects: the threat landscape, detection schemes, and prevention measures. A common trend in the selected works is that IoT security is influenced not only by the frequency and variety of attacks, but also by the structural peculiarities of IoT ecosystems, such as the heterogeneity of devices, limited resources, decentralized deployment, and reliance on constant connectivity. The literature therefore suggests the inability to defend IoT security with a single protection tool; instead, there is a need to promote layered, adaptive, and context-aware methods that integrate threat identification, real-time detection, and preemptive prevention.

3.1 Classification of IoT Security Threats

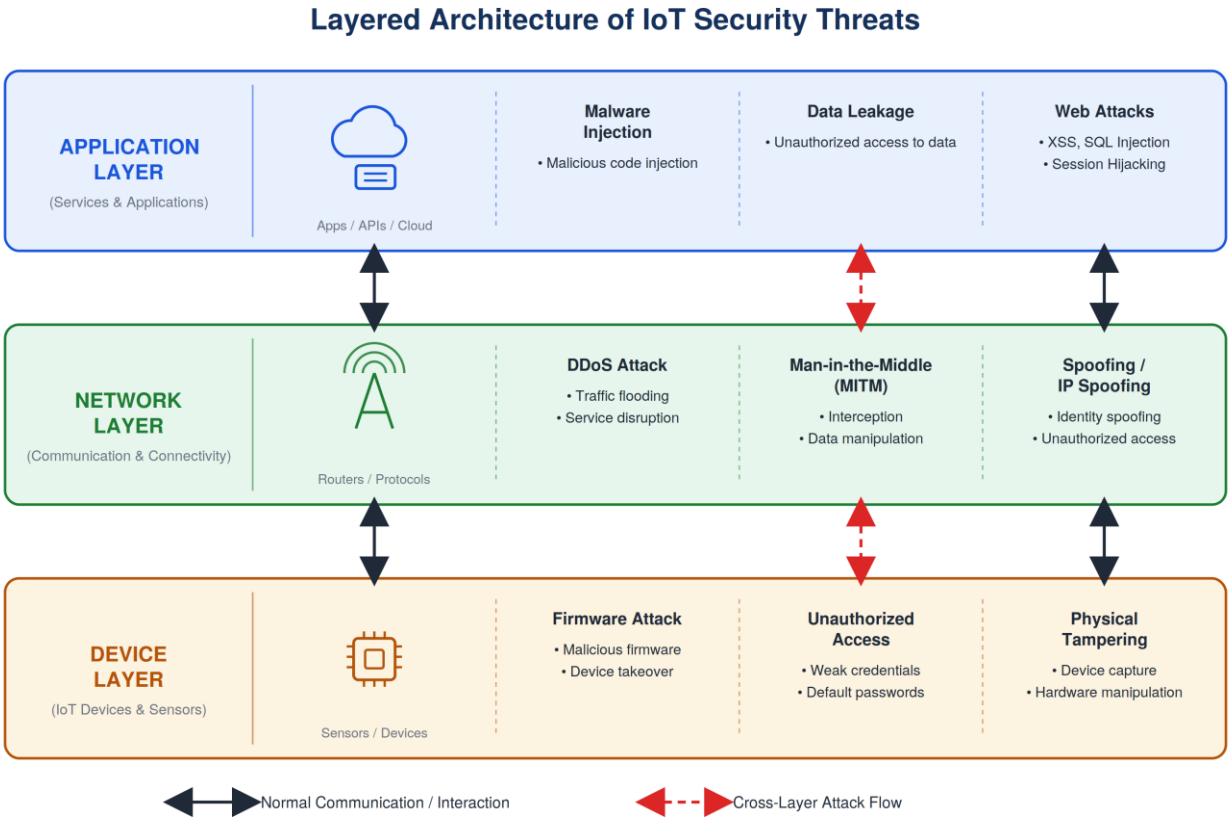

Figure 1: Layered Architecture of IoT Security Threats

Throughout the literature studied, it is evident that IoT threats exist at various architectural levels and exploit weaknesses in both technical and operational capabilities. To distinguish the different threats described in the literature, they can be categorized as network-level, device-level, application-level, and systemic or cross-layer threats, as illustrated in Figure 1.

Distributed denial-of-service (DDoS) attacks are among the most visible network-level attacks in IoT settings. These attacks exploit the connectivity and large number of IoT devices to saturate network resources, degrade service quality, and interfere with endpoint communication. Known to uniquely disrupt the functionality of smart-home and software-defined IoT contexts, DDoS attacks can target central controllers and distributed edge devices, disrupting service continuity and network accessibility [10]. Past research on the behavior of IoT botnets also reveals that unsecured IoT nodes can be detected and coordinated into a massive attack infrastructure, which is why IoT devices are not only targets of attacks but also contributors to wider cyber campaigns [17]. This result is important because it shows that IoT imposes a twofold security cost: devices need protection against compromise and against being turned into a weapon by compromise.

In the literature, spoofing, man-in-the-middle (MITM), replay, and routing attacks are also cited as persistent threats at the network layer. These attacks compromise the authenticity and integrity of communicated data by listening to communications, impersonating legitimate nodes, or altering routing information. Such attacks are particularly hard to thwart in resource-constrained settings, where lightweight protocols are often prioritized over strong encryption and authentication [3]. The analyzed literature suggests that such threats are not merely technical idiosyncrasies but structural outcomes of IoT design decisions that prioritize low power consumption, cost-effectiveness, and interoperability over robust built-in security measures [7].

Findings at the device level show that endpoint security is one of the most critical vulnerabilities in IoT networks. Many IoT devices are configured with default credentials, lack firmware protection, receive infrequent patches, and have weak access controls. All these vulnerabilities provide fertile ground for

compromising the system, interfering with firmware, installing malware, and capturing equipment. The literature indicates that insecure devices can serve as a starting point for attacks that subsequently spread to the wider network and increase operational and safety risks in sector-specific environments, such as smart agriculture and electric power information systems [15], [16]. The importance of this observation is that the risk in IoT is cumulative: a compromised device can cause a cascade of failures that affect communication, control, and data reliability.

Physical tampering is another distinctive IoT threat identified in the reviewed studies. Unlike traditional enterprise computing systems, which typically operate within physically secured facilities, many IoT devices are deployed in open, remote, or unattended environments and are therefore vulnerable to direct physical manipulation. A device capture can provide the attacker with access to credentials, allow the attacker to decompile firmware, or inject malicious code. This is an especially critical vulnerability in industrial or infrastructure deployments that are physically accessible, due to the potential for immediate cyber-physical effects [16]. The findings indicate that IoT security should be treated as both a cybersecurity and a physical-security challenge.

At the application layer, malware injection, data leakage, session hijacking, and code exploitation, as well as web-based threats such as cross-site scripting (XSS), are among the significant threats. As IoT ecosystems grow increasingly dependent on dashboards, mobile apps, APIs, and cloud-integrated services, the attack surface extends beyond the device and network layers to application logic and user-engagement points. For example, research on XSS attack detection in IoT over 5G networks indicates that application-layer vulnerabilities remain relevant even in highly industrialized communication environments [11]. This implies that application insecurity is not eliminated by enhanced connectivity infrastructure. Similarly, broader surveys of IoT security issues reveal that breaches of confidentiality and privacy are frequently driven by poorly implemented data-transfer procedures at the software and application layers, rather than by communication failures [3].

Besides these layer-specific threats, the literature also identifies cross-layer or systemic threats that arise from the combination of several weaknesses. These include botnet coordination, multi-vector attacks, the use of AI to evade detection, and the exploitation of interoperability vulnerabilities among heterogeneous devices and protocols. The studies reviewed indicate that the complexity of the IoT increases the difficulty of addressing compounded threats in environments where devices from various vendors run on uneven security models [6], [18]. Overall, the findings reveal that the IoT threat landscape cannot be considered fixed or independent; it is dynamic, multi-layered, and increasingly adaptive. The classification of IoT security threats across different layers is summarized in Table 1.

Table 1. Classification of Security Threats in IoT Networks

Threat Category	Type of Attack	Description	Impact
Network-Level	DDoS	Overloads network resources with traffic	Service disruption
Network-Level	MITM	Intercepts communication between devices	Data compromise
Device-Level	Firmware Attack	Malicious modification of device software	Device takeover
Device-Level	Unauthorized Access	Exploitation of weak credentials	System intrusion
Application-Level	Malware Injection	Malicious code insertion	Data corruption
Application-Level	Data Leakage	Unauthorized data exposure	Privacy breach

3.2 Detection Techniques for IoT Networks

The literature depicts a clear shift in IoT threat detection from simple, rule-based approaches toward intelligent and hybrid detection systems. This shift reflects the growing ineffectiveness of traditional detection models against rapidly evolving and frequently obfuscated attack behaviors.

Signature-based intrusion detection systems are still used to detect threats that are recognizable from known patterns. Their main strength is precision: properly defined attack signatures can be detected conveniently and with low computational complexity. Nevertheless, the analyzed research consistently points to the same weakness: signature-based systems do not work well against zero-day attacks, polymorphic malware, or evolving attack variants that are not represented in databases [14]. In IoT networks, where new devices, communication patterns, and vulnerabilities keep arising, this constraint greatly diminishes the efficacy of purely signature-based models in the long run.

Consequently, there has been significant interest in anomaly-based detection. These strategies establish a baseline of normal behavior for the system or network and then identify anomalies that may indicate a malicious attack. The key benefit of anomaly detection is its ability to detect previously unknown attacks, which is necessary given the heterogeneity and constant change of the IoT ecosystem. Studies that aim to provide explainable intrusion detection for IoT have highlighted the significance of such models in dynamic cyber-defense contexts, especially when they must guarantee transparency and interpretability to support operational trust [9]. The synergy of genetic algorithms and ensemble methods has also been explored to strengthen anomaly-based traffic detection in IoT communications [12]. The findings, however, also reveal that anomaly-based systems suffer from false positives, particularly in environments where legitimate behavior varies widely across devices and scenarios. This demonstrates a central trade-off in IoT detection: the more sensitive a mechanism is to new threats, the less specific and efficient its operation tends to be.

In an attempt to address the limitations of traditional IDS models, machine learning (ML) and deep learning (DL) based detection systems are becoming increasingly popular in the literature. These methods derive patterns from traffic information, device activities, and multi-feature data to identify sophisticated or

subtle attack patterns. Several of the reviewed articles demonstrate the strong performance of learning-based models in detecting intrusions in IoT contexts. Lin et al. [2] introduce a cloud-computing and multi-feature-extraction extreme learning machine model, which enhances intrusion-detection capability by using richer feature representations. Qureshi et al. [4] also demonstrate that hybrid deep-learning mechanisms have the potential to reinforce cyber-threat detection in secure networks. According to Alzahrani [13], combining an extreme learning machine with a long short-term memory network is effective for detecting suspicious activities in higher-order IoT systems. Reinforcement-learning-based optimization has likewise been applied to internet-wide port scanning to improve IoT security and network resilience [20]. Taken together, these results suggest that intelligent detection models are gradually becoming the core focus of IoT cybersecurity research due to their superior adaptability, classification potential, and ability to handle complex traffic patterns.

Another finding is the increasing interest in hybrid and multi-stage detection architectures. Rather than relying on a single detection logic, these systems combine anomaly detection, signature matching, ensemble learning, cooperative monitoring, image-based authentication, or explainable-AI elements to enhance performance. For example, MP-GUARD proposes a multi-pronged model for scalable SD-IoT systems that leverages ensemble learning and cooperative monitoring to enhance both detection and mitigation [23]. PictureGuard incorporates image-based authentication and a two-stage AI-driven intrusion-detection model to improve security in SDN-IoT [5]. These findings indicate that the future of IoT detection may lie not so much in the choice of an optimal algorithm as in the formulation of combined architectures that balance precision, adaptability, scalability, and trust.

3.3 Prevention and Mitigation Measures

The reviewed literature demonstrates that detection alone is insufficient and must be complemented by effective prevention and mitigation approaches. In this regard, the literature outlines key prevention strategies, including cryptographic protection, authentication and access control, blockchain-based trust models, software-defined security management, and adaptive defenses.

In IoT systems, cryptographic mechanisms remain fundamental to ensuring the confidentiality, integrity, and authenticity of communication. The findings, however, consistently point in a similar direction: traditional cryptographic solutions tend to be difficult to implement effectively on low-power, low-memory devices. This has prompted growing interest in lightweight encryption and communication-aware security models that maintain protection without exceeding device capabilities [3]. The essence of this finding is that the efficacy of IoT security cannot be separated from its practical viability; theoretically powerful mechanisms can break down in operation when they cannot be sustained by constrained devices.

Authentication and access control are also important preventive measures. The literature highlights the need for lightweight, robust, and scalable authentication protocols that can both prevent unauthorized access and reduce computational load. Enhanced authentication in smart and distributed environments is often associated with greater trust establishment and reduced exposure to impersonation and unauthorized interference [15]. The evidence reviewed suggests that weakly implemented identity management remains one of the primary contributors to several higher-level IoT attacks.

A second prominent outcome is the development of blockchain-driven prevention systems. These strategies aim to enhance trust, immutability, transparency, and decentralized control in IoT ecosystems. Blockchain has been proposed as a tool to enhance both detection and prevention within smart-city security by ensuring that transaction records are secure and not subject to centralized decision-making [8], [25]. Related studies also note the expected synergy among machine learning, AI, and blockchain in supporting adaptive IoT defense architectures [21]. On the one hand, the literature anticipates promising opportunities; on the other hand, blockchain-based solutions can introduce latency, storage, and scalability issues, especially in large-scale, real-time IoT deployments.

Finally, the findings point to an increasing shift toward adaptive and software-defined prevention models in 5G-, SDN-, and future 6G-based settings. These models provide centralized visibility, elastic policy enforcement, and rapid defensive reconfiguration in response to emerging threats [6]. Clustering-based adaptive security combined with regression learning has also been proposed to strengthen protection in IoT wireless sensor networks [24]. Overall, the literature indicates that the most useful prevention measures are lightweight, adaptive, layered, and interoperable when applied in a heterogeneous IoT environment. A comparative evaluation of detection and prevention techniques is presented in Table 2.

Table 2. Comparative Analysis of IoT Detection and Prevention Techniques

Technique	Category	Advantages	Limitations
Signature-Based IDS	Detection	High accuracy for known threats	Cannot detect new attacks
Anomaly Detection	Detection	Detects unknown threats	High false positives
Machine Learning Models	Detection	High adaptability and accuracy	Computational overhead
Cryptography	Prevention	Ensures data confidentiality	Resource intensive
Authentication Mechanisms	Prevention	Prevents unauthorized access	Scalability challenges
Blockchain-Based Security	Prevention	Decentralized and tamper-proof	Latency and complexity

4. EXPERIMENTAL EVALUATION

To complement the qualitative synthesis presented above and to empirically examine the detection trade-offs identified in the reviewed literature, a controlled benchmarking experiment was conducted. The objective was not to propose a new detector but to quantify, under identical conditions, how the three families of

detection approaches discussed in this review — signature/rule-based, anomaly-based, and machine-learning/deep-learning-based — behave on a common intrusion-detection benchmark. This provides concrete, reproducible evidence for the comparative observations made throughout the paper.

4.1 Experimental Setup

The experiments were performed on the NSL-KDD dataset, a refined and widely adopted benchmark for evaluating network intrusion-detection systems that addresses the redundancy and bias problems of the earlier KDD Cup 1999 data [26]. Although NSL-KDD is a general network-intrusion benchmark rather than an IoT-native capture, it remains one of the most common reference datasets in the IoT intrusion-detection literature and is well suited for comparing detection paradigms under a standard protocol. The dataset provides an official training partition (KDDTrain+) and a separate, more challenging testing partition (KDDTest+) that deliberately contains attack variants not present in the training data, enabling a realistic assessment of how detectors generalize to previously unseen threats. The composition of both partitions is summarized in Table 3.

Table 3. Composition of the NSL-KDD Dataset (Records per Class)

Subset	Total	Normal	Attack	DoS	Probe	R2L	U2R
Training (KDDTrain+)	125,973	67,343	58,630	45,927	11,656	995	52
Testing (KDDTest+)	22,544	9,711	12,833	7,460	2,421	2,885	67

Each record is described by 41 features spanning basic connection attributes, content features, and traffic-based statistics. The three categorical features (protocol type, service, and flag) were one-hot encoded, and all numerical features were standardized; the encoders and scalers were fitted exclusively on the training partition and then applied to the test partition to prevent information leakage. After encoding, each record was represented by a 122-dimensional feature vector. The detection task was framed as binary classification, distinguishing normal traffic from attack traffic, while the original fine-grained attack labels were retained and grouped into the four canonical categories (DoS, Probe, R2L, and U2R) for category-level analysis.

Four detectors were selected so that each represents one of the detection families examined in the review. A Decision Tree, which learns explicit and interpretable decision rules, was used as a proxy for signature/rule-based detection. An Isolation Forest, trained exclusively on normal traffic and flagging deviations as anomalies, represented anomaly-based detection. A Random Forest represented ensemble machine-learning detection, and a multilayer-perceptron neural network represented deep-learning-based detection. The supervised models were trained on the full training partition, whereas the anomaly detector was trained only on the benign subset, consistent with how anomaly-based systems are deployed in practice. All models were implemented with the scikit-learn library using fixed random seeds for reproducibility [27].

Performance was assessed on the held-out KDDTest+ partition using accuracy, precision, recall, F1-score, and the false-positive rate, since the review repeatedly highlights false alarms as a central operational concern. The area under the receiver-operating-characteristic curve (AUC) was additionally computed as a threshold-independent measure of discriminative ability. To expose behavior that aggregate metrics can conceal, the per-category detection rate was also measured for each of the four attack classes.

4.2 Experimental Results

Table 4 reports the performance of all four detectors on the test partition, and Figure 2 visualizes the same results. Several consistent patterns emerge. Every method achieved high precision, between 92.6% and 96.7%, but markedly lower recall, between 60.7% and 70.4%, indicating that although flagged alerts were overwhelmingly correct, a substantial fraction of attacks evaded detection. This gap is a direct consequence of the deliberately hard KDDTest+ partition, whose novel attack variants are not represented during training, and it concretely demonstrates the generalization challenge that the reviewed literature associates with IoT threat detection.

Table 4. Detection Performance on the NSL-KDD Test Set

Detection Method	Category	Accuracy	Precision	Recall	F1-Score	FPR	AUC
Decision Tree	Signature-based	79.2%	96.6%	65.7%	78.2%	3.1%	0.813
Isolation Forest	Anomaly-based	80.0%	92.6%	70.4%	80.0%	7.4%	0.937
Random Forest	ML (ensemble)	76.5%	96.7%	60.7%	74.6%	2.8%	0.960
Neural Network	Deep learning	80.9%	96.1%	69.2%	80.4%	3.7%	0.909

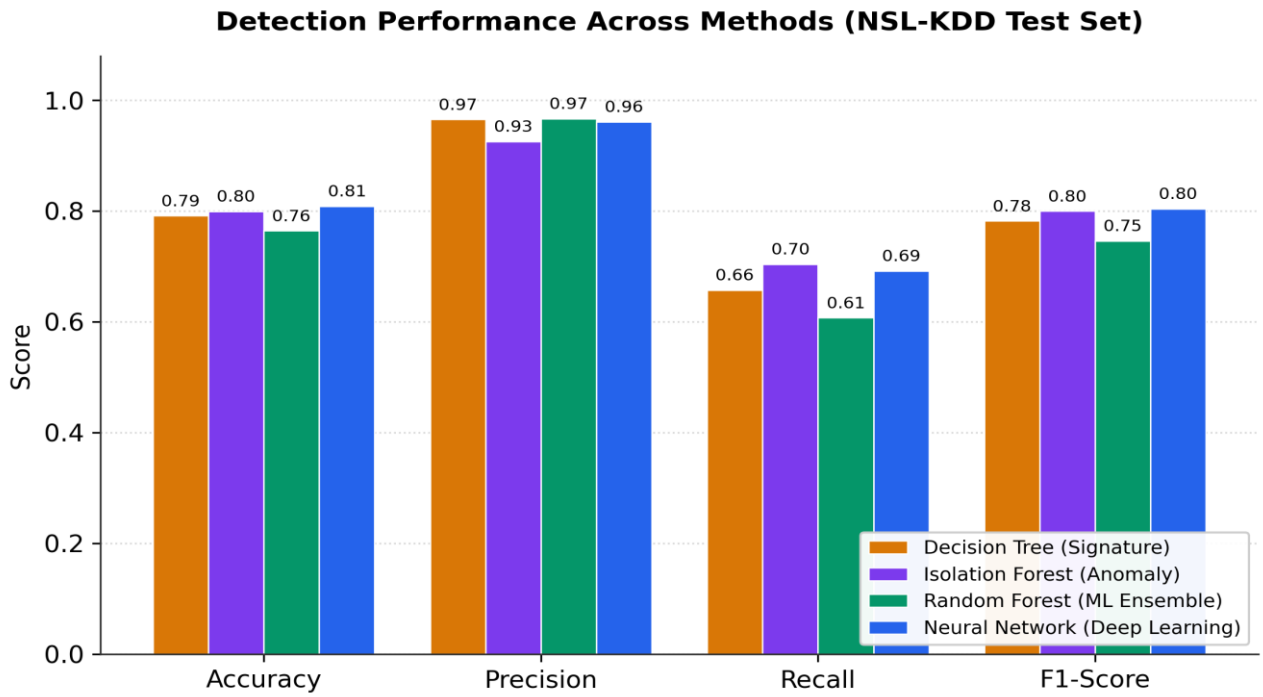

Figure 2: Detection Performance of the Evaluated Methods on the NSL-KDD Test Set

The deep-learning neural network attained the highest operating-point accuracy (80.9%) and F1-score (80.4%), while the Random Forest achieved the strongest threshold-independent discrimination, with an AUC of 0.960 (Figure 4). The anomaly-based Isolation Forest, despite being trained without any attack examples, produced the highest recall (70.4%), detecting more attacks — including unseen ones — than any supervised model, but it did so at the cost of the highest false-positive rate (7.4%) and the lowest precision (92.6%). The signature-proxy Decision Tree recorded the lowest AUC (0.813), reflecting limited ability to rank previously unseen attacks. These outcomes empirically reproduce the core trade-off emphasized throughout this review: signature-based detection is precise on known patterns but brittle against novel attacks, whereas anomaly-based detection generalizes better to unknown threats at the expense of more false alarms.

4.3 Analysis of Results

Aggregate metrics, however, mask a more serious limitation that becomes evident only at the category level. Figure 3 shows the detection rate of the Random Forest for each attack class. High-volume, high-frequency attacks were detected reliably — 78.7% for DoS and 73.0% for Probe — because such attacks generate distinctive, repetitive traffic patterns and are abundantly represented in the training data. In sharp contrast, remote-to-local (R2L) and user-to-root (U2R) attacks were almost entirely missed, with detection rates of only 5.3% and 10.4%, respectively.

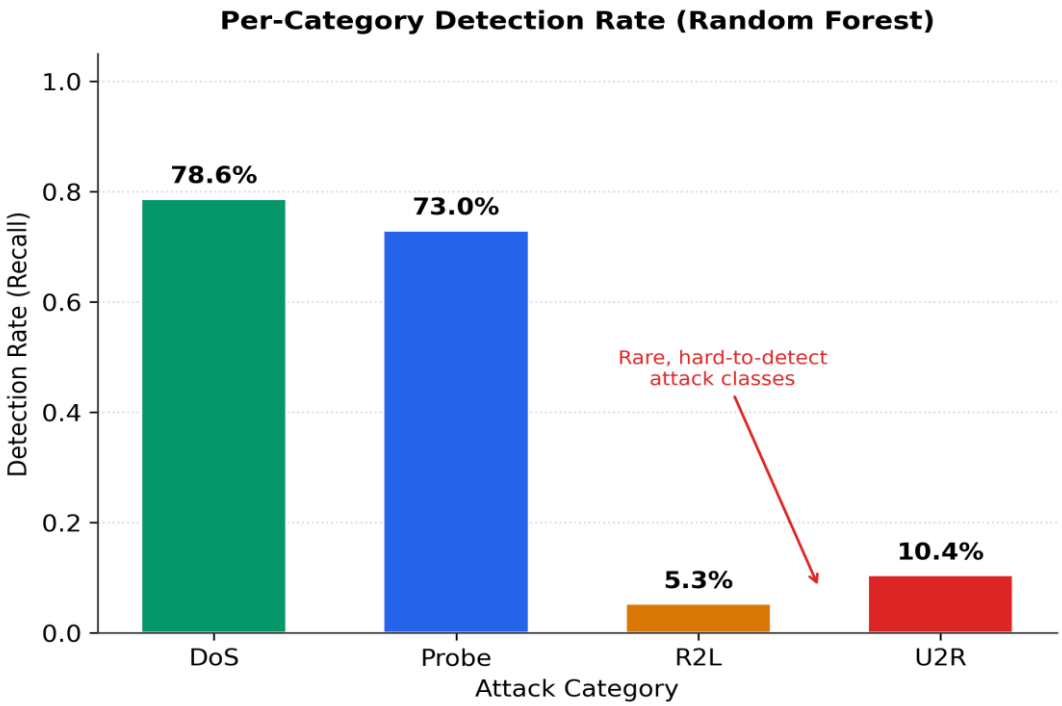

Figure 3: Per-Category Attack Detection Rate of the Random Forest Classifier

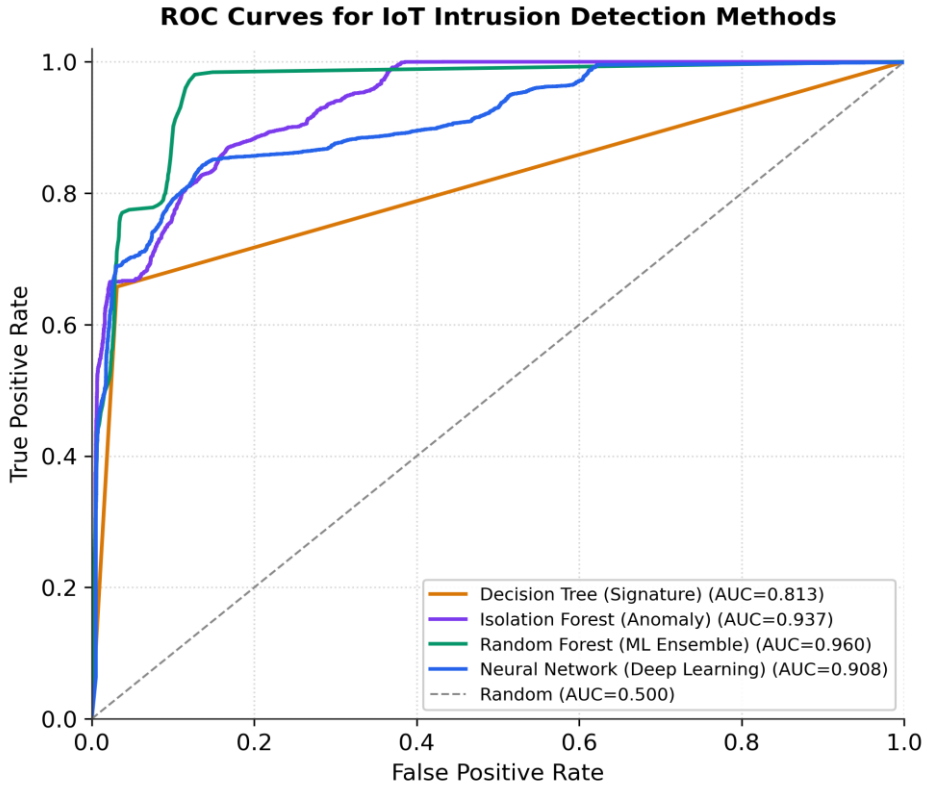

Figure 4: ROC Curves and AUC Values for the Evaluated Detection Methods

This disparity is explained by two compounding factors that the reviewed literature repeatedly identifies. First, R2L and U2R attacks are severely underrepresented: the training partition contains only 995 R2L and 52 U2R records, against more than 45,000 DoS records, leaving the models with insufficient examples to learn their characteristics. Second, these attacks are behaviorally subtle — they often manifest as a small number of connections that closely resemble legitimate activity — so they produce weak statistical signals. The practical implication is significant: a detector reporting roughly 80% overall accuracy may nonetheless fail to detect the very privilege-escalation and unauthorized-access attacks that are among the most damaging in IoT deployments. This finding reinforces the review's argument that IoT intrusion-detection systems must be evaluated

with per-class, imbalance-aware metrics rather than aggregate accuracy alone, and that rare but high-impact attack classes call for targeted countermeasures such as cost-sensitive learning, data resampling, or hybrid anomaly-supervised pipelines.

The receiver-operating-characteristic curves in Figure 4 confirm that the ensemble and anomaly-based detectors maintain strong separability between normal and attack traffic across a range of decision thresholds, whereas the signature proxy degrades more quickly. The confusion matrices in Figure 5 make the error structure explicit: for every model the dominant error type is the false negative — attack traffic classified as normal — rather than the false positive. In an IoT security context, where undetected intrusions can propagate across resource-constrained devices, this asymmetry argues for detection pipelines and operating thresholds that are tuned to minimize missed attacks, even at the price of additional manual triage.

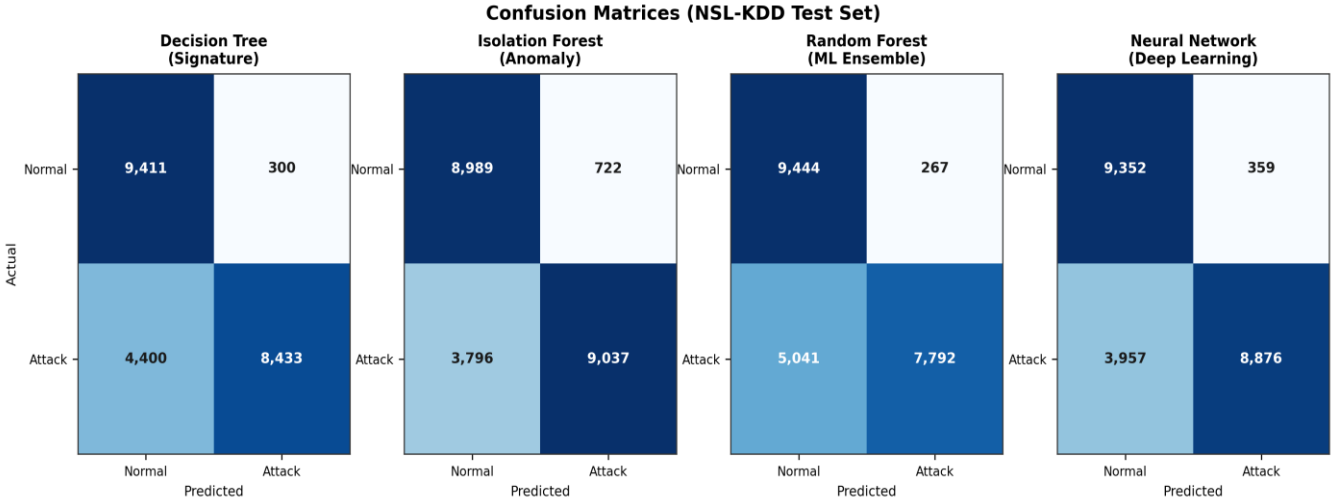

Figure 5: Confusion Matrices for the Evaluated Detection Methods on the NSL-KDD Test Set

Several limitations of this evaluation should be acknowledged. NSL-KDD captures general network-intrusion behavior rather than IoT-native traffic; although it is widely used as an intrusion-detection benchmark, datasets collected directly from IoT devices — such as N-BaIoT, Bot-IoT, and TON_IoT — more faithfully represent device-level attack patterns, and validating these findings on such datasets is an important direction for future work. In addition, the detectors were evaluated with default hyperparameters and decision thresholds; systematic tuning would likely shift the precision-recall balance and is left to subsequent study. Finally, the task was framed as binary detection, and extending the analysis to fine-grained multiclass classification would yield further insight. Nonetheless, because all detectors were compared under identical conditions, the relative patterns reported here provide reliable, reproducible empirical support for the comparative conclusions drawn from the literature.

5. DISCUSSION

The results in this paper highlight the dynamic and complex nature of security issues in IoT networks. Integrating recent literature, this section critically analyzes the implications of the identified threats, the suitability of existing detection and prevention technologies, and the gaps in the field that impede the development of robust IoT security models. Where relevant, the discussion also draws on the empirical benchmarking results of Section 4 to ground these observations in measured detection behavior.

One of the main observations from the results is that IoT security issues are inherently structural rather than incidental. Unlike traditional information systems, IoT environments are typically decentralized, heterogeneous, and resource constrained. These attributes severely limit the use of traditional cybersecurity models. The proliferation of low-power devices with limited built-in security features creates systemic vulnerabilities that cannot be fully addressed by isolated technical solutions [3], [7]. The implication of this structural constraint is that IoT security should be treated as a matter of overall system design rather than a set of isolated defensive mechanisms.

The classification of threats by network, device, and application layers further indicates that attacks on IoT are becoming multi-layered and coordinated. For example, network disruptions such as DDoS attacks can be launched through device-level vulnerabilities, and data exfiltration and unauthorized control can be achieved through application-level vulnerabilities. Such complexity indicates that IoT security violations are not isolated events but rather propagate across layers, amplifying their impact [10], [17]. A successful defense strategy therefore requires a holistic, multi-layered perspective that encompasses defenses at each level of the IoT architecture.

As far as detection mechanisms are concerned, there is a significant paradigm shift in cybersecurity, moving from legacy signature-based models toward intelligent, learning-based ones. Signature-based methods are inherently reactive and resource-light but limited to known threats. Conversely, by analyzing anomalies and applying machine-learning techniques, previously unseen attacks can be identified by detecting deviations in how systems operate. The literature indicates that such intelligent methods can yield significant improvements in detection and greater flexibility in the ever-changing IoT context [2], [9]. Yet this progress introduces new challenges, especially regarding computational cost, model training, and the need for high-quality datasets. These constraints can affect the real-world implementation of sophisticated detectors in resource-constrained IoT settings [13].

Another vital insight concerns the trade-off between detection accuracy and operational efficiency. Although deep-learning and ensemble models achieve better detection performance, they require significant processing power and energy, which may not be available on edge devices. This creates a conflict between security robustness and system efficiency, motivating demand

for lightweight, optimized detection algorithms tailored to IoT use. Hybrid models, which combine various detection methods to balance accuracy and resource consumption, offer a promising solution. However, their practical implementation is still constrained by issues such as system complexity, integration difficulty, and the absence of standards [5], [23].

Regarding prevention, the results suggest that conventional techniques such as cryptography and authentication remain critical but are insufficient when applied individually. Although encryption guarantees the confidentiality and integrity of data, it is not always effective due to computational limitations and key-management issues in distributed IoT systems. Similarly, authentication protocols are important for access control but may be exposed when they are not designed to scale across heterogeneous devices. Emerging strategies such as blockchain-based models and software-defined networking are increasingly capable of providing decentralized trust management and dynamic security enforcement [8], [21]. Nevertheless, these technologies also introduce new issues, such as latency and scalability problems, that must be carefully addressed.

The integration of IoT with advanced communication technologies such as 5G and future 6G networks adds further complexity to the security environment. These technologies can achieve high-speed, low-latency communication; however, their performance creates additional attack surfaces and vulnerabilities related to virtualization, network slicing, and edge computing. The reviewed works indicate that next-generation IoT systems require adaptive and context-aware security frameworks that can operate across a wide range of highly dynamic environments [6], [11]. This underscores the increasing value of intelligent, autonomous security systems capable of responding to threats in real time. The synergy of AI and quantum computing has also been examined as a future direction for strengthening IoT security and privacy [19].

Despite the substantial advances in IoT security, several serious gaps remain. First, there is a lack of standardized security models applicable across heterogeneous IoT ecosystems. Second, many existing solutions are tested in controlled settings and may not be effective in large-scale, variable, and unpredictable real-world conditions. Third, interoperability among devices from different manufacturers remains an obstacle to establishing a unified security policy. Moreover, the rapid evolution of attack strategies driven by AI-driven cyberattacks and similar threats demands continuous adaptation of defense systems [18].

In practical terms, the findings of this study have significant implications for researchers, system designers, and policymakers. Security-by-design requirements in IoT development are clearly needed to ensure that security factors are incorporated at the early stages of system architecture rather than added at the final stages. Moreover, collaboration among academia, industry, and regulatory bodies is necessary to develop standards, exchange threat intelligence, and create scalable security solutions. Policymakers should also contribute to the effective enforcement of security regulations and the promotion of best practices to secure critical IoT infrastructure.

Future studies should focus on developing lightweight, scalable, and energy-efficient security systems that perform well in resource-constrained environments. The combination of artificial intelligence, blockchain, and edge computing offers promising opportunities to make IoT more secure, but these methods require optimization for real-world use. In addition, greater emphasis on explainable and transparent security models would enhance the trust and usability of IoT-based systems.

Overall, this discussion demonstrates that IoT security is a complex and dynamic problem that must be addressed in a multidisciplinary manner. Although detection and prevention measures have improved, implementing strong, scalable security in IoT networks remains an open research problem. Overcoming this difficulty will require further innovation, collaboration, and a transition toward adaptive, intelligent, and system-level security frameworks. An integrated framework combining detection and prevention mechanisms is illustrated in Figure 6.

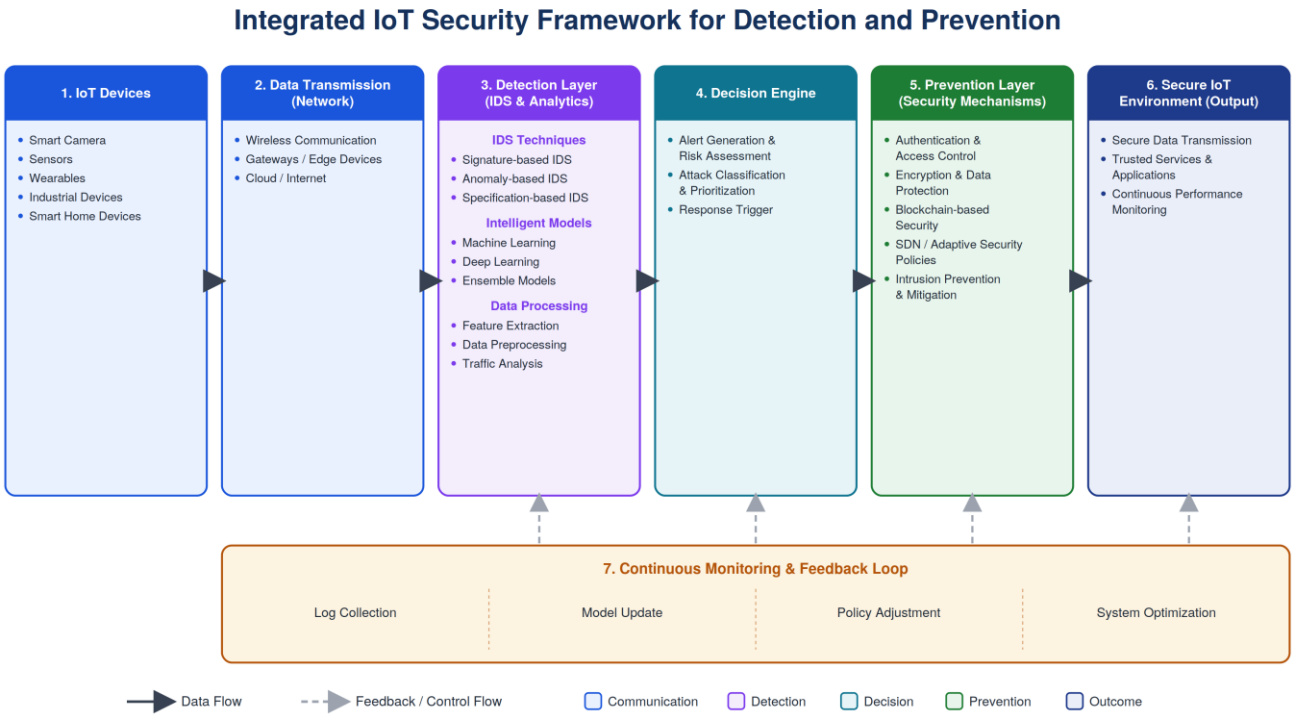

Figure 6: Integrated IoT Security Framework for Detection and Prevention

6. CONCLUSION

The rapid growth of the Internet of Things (IoT) ecosystem has brought unprecedented opportunities for connectivity, automation, and data-driven innovation across various domains. Nevertheless, this development has come with critical security issues arising from the attributes of the IoT setting, such as device heterogeneity, resource scarcity, and the enormous exposure of networks. This paper provides a detailed discussion of IoT security by critically reviewing major threats, detection and prevention measures, and strategies to address them in the literature.

The results indicate that IoT security vulnerabilities are multi-layered and interconnected, spanning network, device, and application levels. Threats such as distributed denial-of-service, unauthorized access, malware injection, and data leakage are compounded by persistent structural vulnerabilities in IoT architectures. In response, detection methods have transitioned from traditional signature-based systems to more sophisticated anomaly-based and machine-learning-driven methods that offer greater flexibility and accuracy. Likewise, the scope of prevention has expanded to include cryptography-based solutions, authentication systems, blockchain-based architectures, and software-defined protection models.

Despite these innovations, several challenges persist. Most available solutions are limited by scalability, computational overhead, interoperability, and real-time responsiveness, especially in resource-constrained environments. These limitations underscore the importance of more dynamic and efficient security architectures that can address the multifaceted nature of IoT networks.

This research contributes to the current literature by offering an organized overview of the security challenges of the IoT and outlining the outstanding gaps in current strategies. It also highlights the need for multi-layered, integrated, and intelligent security solutions that balance robustness and efficiency. Further studies are needed to develop lightweight, scalable, and context-aware security systems and to encourage standardization and cooperation among stakeholders. Ultimately, improving IoT security is crucial to enhancing the reliability, resilience, and trustworthiness of next-generation digital systems.

7. REFERENCES

[1] Mishra, A. 2025. AI-Powered Cybersecurity Framework for Secure Data Transmission in IoT Network. International Journal of Advances in Engineering and Management, 7(3), 5–13.

[2] Lin, H., Xue, Q., Feng, J., and Bai, D. 2023. Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. Digital Communications and Networks, 9(1), 111–124.

[3] Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., and Hong, W. C. 2021. Internet of Things: Evolution, concerns and security challenges. Sensors, 21(5), 1–35.

[4] Qureshi, S., He, J., Tunio, S., Zhu, N., Akhtar, F., Ullah, F., and Wajahat, A. 2021. A Hybrid DL-Based Detection Mechanism for Cyber Threats in Secure Networks. IEEE Access, 9, 73938–73947.

[5] Hatamleh, H., Alnaser, A. M. A., Saloum, S. S., Sharadqeh, A., and Alkasassbeh, J. S. 2025. PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and AI-Powered Two-Stage Intrusion Detection. Technologies, 13(2).

[6] Kalodanis, K., Papapavlou, C., and Feretzakis, G. 2025. Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. Future Internet, 17(7).

[7] Sen, R. K., and Dash, A. 2023. Unveiling the Shadows: Exploring the Security Challenges of the Internet of Things (IoT). International Journal of Scientific Research in Engineering and Management, 7(7).

[8] Albugmi, A. 2025. Hybrid smart IoT detection and prevention framework for smart cities using blockchain technology. International Journal of Advanced and Applied Sciences, 12(4), 107–115.

[9] Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., and Tari, Z. 2023. Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions. IEEE Communications Surveys and Tutorials, 25(3), 1775–1807.

[10] Karmous, N., Aoueileyine, M. O. E., Abdelkader, M., Romdhani, L., and Youssef, N. 2024. Software-Defined-Networking-Based One-versus-Rest Strategy for Detecting and Mitigating Distributed Denial-of-Service Attacks in Smart Home IoT Devices. Sensors, 24(15).

[11] AlJamal, M., Alquran, R., Alsarhan, A., Aljaidi, M., Alhmmad, M., Al-Jamal, W. Q., and Albalawi, N. 2024. A Robust Machine Learning Model for Detecting XSS Attacks on IoT over 5G Networks. Future Internet, 16(12).

[12] Seyedi, B., and Postolache, O. 2025. Securing IoT Communications via Anomaly Traffic Detection: Synergy of Genetic Algorithm and Ensemble Method. Sensors, 25(13).

[13] Alzahrani, M. E. 2024. Elevating Smart Industry Security: An Advanced IoT-Integrated Framework for Detecting Suspicious Activities using ELM and LSTM Networks. International Journal of Advanced Computer Science and Applications, 15(2), 652–660.

[14] Dinkar, A. K., and Choudhary, A. K. 2024. Exploring Intrusion Detection Systems (IDS) in IoT Environments. Seminars in Medical Writing and Education, 3.

[15] Adewusi, A. O., Chiekezie, N. R., and Eyo-Udo, N. L. 2022. Securing smart agriculture: Cybersecurity challenges and solutions in IoT-driven farms. World Journal of Advanced Research and Reviews, 15(3), 480–489.

[16] Orkena, M., Abdumauvlenovna, B. D., Tursynkanovna, Z. A., Mekebayev, N., Serikov, T., Zhazira, S., and Aizat, K. 2025. Cybersecurity Framework for IoT-Integrated Electric Power Information Systems. International Journal of Industrial Engineering and Management, 16(2), 124–137.

[17] Miller, B., and Zhang, X. 2020. A Multi-Layer Approach to Detecting and Preventing IoT-Based Botnet Attacks. Issues in Information Systems, 21(3), 168–178.

[18] Roopesh, M., Nishat, N., Arif, I., and Bajwa, A. E. 2024. A Comprehensive Review of Machine Learning and Deep Learning Applications in Cybersecurity: An Interdisciplinary Approach. Academic Journal on Science, Technology, Engineering & Mathematics Education, 4(4), 37–53.

[19] Alzahrani, A. I. A. 2025. Exploring AI and quantum computing synergies in holographic counterpart frameworks for IoT security and privacy. Journal of Supercomputing, 81(11).

[20] Komatnani Govindan, S., Vijayaraghavan, H., Kishore Anthuvan Sahayaraj, K., and Mary Joy Kinol, A. 2024. Optimizing Internet-Wide Port Scanning for IoT Security and Network Resilience: A Reinforcement Learning-Based Approach in WLANs with IEEE 802.11ah. Fiber and Integrated Optics, 43(1), 14–42.

[21] Bin Zainuddin, A. A., Sairin, H., Mazlan, I. A., Muslim, N. N. A., and Wan Sabarudin, W. A. S. 2024. Enhancing IoT Security: A Synergy of Machine Learning, Artificial Intelligence, and Blockchain. Data Science Insights, 2(1).

[22] Bakhsh, S. T., Alghamdi, S., Alsemmeari, R. A., and Hassan, S. R. 2019. An adaptive intrusion detection and prevention system for Internet of Things. International Journal of Distributed Sensor Networks, 15(11).

[23] El-Sayed, A., Said, W., Tolba, A., Alginahi, Y., and Toony, A. A. 2024. MP-GUARD: A novel multi-pronged intrusion detection and mitigation framework for scalable SD-IoT networks using cooperative monitoring, ensemble learning, and new P4-extracted feature set. Computers and Electrical Engineering, 118.

[24] Chaurasia, N., and Kumar, P. 2025. CREN-RLC: Clustering-Based Adaptive Security with Regression Learning for IoT-WSNs. IEEE Sensors Journal, 25(24), 44984–44993.

[25] Vasigala, P., and Pinniboina, P. K. 2025. Security Challenges in Connected Device Networks: A Blockchain-Based Approach. International Journal of Advanced Research in Science, Communication and Technology, 366–373.

[26] Tavallaee, M., Bagheri, E., Lu, W., and Ghorbani, A. A. 2009. A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 1–6.

[27] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., and Duchesnay, E. 2011. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 12, 2825–2830.