Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 3 (2025)

A Comprehensive Review of Secure Threat Detection Models and Emerging Paradigms for IoT Networks

Harmeet Singh[*1], Sikander Singh Cheema[2]
Department of Computer Science, Punjabi University Patiala[*1]*
Department of Computer Science and Engineering, Punjabi University Patiala[2]

Abstract: - The rapid proliferation of the Internet of Things (IoT) has introduced a vast and complex attack surface, intensified by the resource-constrained nature of devices and a lack of universal security standards. This review provides a comprehensive analysis of secure threat detection models and emerging paradigms designed to address these challenges. The article first establishes a systematic taxonomy of cybersecurity threats across the IoT's architectural layers such as Perception, Network, and Application. It then delves into a critical examination of advanced intrusion detection systems (IDS), with a focus on models leveraging machine learning (ML), deep learning (DL), and hybrid architectures. The performance of these models is evaluated against key metrics and benchmark datasets. The review further explores cutting-edge concepts such as federated learning for privacy-preserving detection, adversarial machine learning, and post-quantum cryptography. This synthesis offers a strategic overview of the current landscape, identifying research gaps and outlining a path toward building resilient, adaptable, and trustworthy IoT ecosystems for the future.

Keywords*: Internet of Things (IoT), Threat Detection, Machine Learning, Deep Learning, Cybersecurity, Federated Learning.*

1. Introduction

Emerging paradigms in IoT threat detection are rapidly evolving, with advanced deep learning and ensemble techniques delivering high detection accuracy while maintaining efficiency for deployment in resource-constrained IoT networks [1,52]. A recent systematic review underscores the significance of data-driven learning models such as federated learning, reinforcement algorithms, and hybrid classifiers in adapting to diverse threat vectors at different IoT stack layers [2,53]. Another study presents a lightweight and energy-efficient deep learning-based IDS architecture, striking a careful balance between model complexity and deployment feasibility on edge devices [4,54]. Moreover, a comprehensive survey of access control models across the IoT ecosystem highlights the convergence of AI, blockchain, and traditional methods for robust, scalable security solutions [3,55]. These integrated approaches collectively enhance network resilience by enabling adaptive, transparent, and context-aware threat mitigation strategies for IoT environments [5,56].

1.1 The Proliferation and Significance of Internet of Things (IoT) Technologies

The Internet of Things (IoT) signifies a transformative technological movement, wherein everyday physical objects are imbued with sensors, software, and networking capabilities, enabling them to collect, exchange, and act upon data.1 This widespread connectivity is creating an intelligent environment that is fundamentally altering living standards and operational paradigms across numerous industries [1]. From facilitating remote patient monitoring in healthcare to optimizing energy usage in smart cities and automating processes in manufacturing, IoT has become an integral and foundational component of the modern digital landscape [2]. The trajectory of this technological proliferation is staggering; industry projections indicate that the number of globally connected IoT devices will reach approximately 30.9 billion by 2025, a testament to the rapid pace at which individuals and industries are adopting these advancements [2]. This exponential growth underscores the immense societal and

economic value of IoT, but it simultaneously highlights the critical need to secure these expanding networks against a dynamic and evolving threat landscape.

1.2 Inherent Security Challenges in the IoT Ecosystem

Despite its potential, the swift expansion of the IoT has inadvertently created a vast and complex attack surface. A core challenge lies in the fundamental design of many IoT devices, which are often constrained by limited processing power, memory, and battery capacity [2]. These resource limitations frequently prevent the implementation of conventional, robust security measures, leaving devices vulnerable to compromise [1]. Furthermore, the IoT ecosystem is characterized by a significant degree of heterogeneity, with a multitude of devices from different manufacturers using diverse communication standards and protocols. This lack of standardization and interoperability complicates the development of uniform security solutions, thereby exposing the entire network to a wide range of sophisticated cyber threats.1 Cybersecurity incidents, such as the infamous Mirai botnet attack, which leveraged unsecured IoT systems to launch massive distributed denial-of-service (DDoS) attacks, serve as a stark reminder of the potential hazards posed by these systemic insecurities [2]. Consequently, fortifying the security protocols of these devices is not merely a technical concern but a strategic imperative to protect network integrity and user privacy.

1.3 Scope and Structure of the Review

This comprehensive review article is designed to provide an exhaustive and insightful analysis of the current state of secure threat detection models and emerging paradigms for IoT networks. The report is structured to first lay the groundwork by defining the fundamental architectural layers of IoT and identifying the specific vulnerabilities inherent to each. It then proceeds to present a systematic taxonomy of cybersecurity threats that target these layers. A major portion of the review is dedicated to an in-depth exploration of advanced intrusion detection systems (IDS), with a particular focus on models leveraging machine learning (ML) and deep learning (DL) techniques to overcome the limitations of traditional security methods. The report also includes a critical section on the performance evaluation of these models, discussing key benchmark datasets and the metrics used to assess their effectiveness. Finally, the review addresses cutting-edge topics such as adversarial machine learning, post-quantum cryptography, and the role of regulatory frameworks, offering a forward-looking perspective on the future of a resilient and secure IoT ecosystem. The primary objective is to translate highly technical research findings into a strategic and accessible overview for a diverse professional audience, including corporate leaders, technical experts, and policymakers.

2. Foundational Concepts and Architectural Layers of IoT

2.1 Defining the IoT Architectural Model

To fully comprehend the security vulnerabilities and threat detection mechanisms within the IoT ecosystem, it is essential to first understand its foundational architectural structure. The architecture of an IoT system can be represented by a layered model, which provides a logical framework for analyzing the flow of data and identifying potential points of failure [3]. While a simplified three-layer architecture (Perception, Network, Application) is a commonly cited model in research, more granular five- or even seven-layer models exist to provide a more detailed view of the complex interactions between heterogeneous devices and systems [5]. The three-layer model, however, serves as an effective and broadly accepted paradigm for discussing security challenges, as it neatly categorizes vulnerabilities based on their location within the system, from the physical device itself to the software that processes its data.

2.2 The Perception Layer: Devices, Sensors, and Physical Vulnerabilities

The Perception Layer, alternatively referred to as the device, sensor, or object layer, constitutes the physical bedrock of the IoT [5]. This layer is composed of a vast collection of interconnected physical objects, embedded sensors, and actuators that are responsible for directly sensing, collecting, and interacting with data from the environment [5] Examples of devices at this layer include RFID tags, GPS modules, and various types of sensors that measure everything from blood pressure to climate conditions. The core function of the perception layer is to gather raw data and securely transmit it to the upper layers of the architecture [5].

However, this layer is also the most susceptible to a wide array of attacks, both physical and digital. The resource-constrained nature of these devices which often possessing minimal processing power and memory makes them a primary target, as they lack the capacity to implement complex security measures [2]. Attackers can exploit these limitations through physical tampering, for example, by directly interacting with a device to extract sensitive information such as encryption keys or routing tables [5]. Another significant threat is the 'Slumber Denial Attack,' where an adversary prevents a battery-operated device from entering its power-saving sleep mode by providing a constant stream of false feedback. This leads to rapid battery drainage and eventual power failure, effectively launching a denial-of-service attack at a physical level [5]. Other vulnerabilities include malicious code injection, where a rogue node is inserted into a communication channel to take control, and replay attacks, where valid data transmissions are intercepted and resent to deceive the recipient into performing an unintended action [5]. The inherent trade-off between device functionality, cost, and security in this layer is a significant contributor to widespread vulnerabilities, as manufacturers have often prioritized low-cost production over robust security features. This creates a foundational fragility that can be exploited for large-scale attacks.

2.3 The Network Layer: Communication Protocols and Interconnectivity Risks

The Network Layer, also known as the routing or transmission layer, serves as the critical communication link between the perception layer and the application layer [5]. This layer is responsible for processing, routing, and transmitting information across various network technologies, including wireless networks and the internet [6]. It plays a crucial role in managing the vast volume of data generated by IoT devices and is a primary target for attacks aimed at disrupting communication or compromising data integrity [8]. The heterogeneity of communication standards and protocols at this layer, such as MQTT and CoAP, often results in a lack of standardized, built-in security controls, leaving it open to exploitation [9].

A major category of threats at this level are DDoS attacks, which aim to make a network service unavailable by overwhelming it with a flood of malicious traffic from multiple sources.8 In the IoT context, these are often orchestrated by botnets networks of compromised devices acting as 'zombies' under the control of an attacker [10]. The Mirai botnet is a prime example of this type of attack, which leveraged insecure IoT devices to launch some of the largest DDoS attacks on record [2]. Other critical threats include Man-in-the-Middle (MITM) attacks, which compromise the confidentiality and integrity of data by intercepting communications, and Sybil attacks, where a single malicious node impersonates multiple legitimate nodes to corrupt network operations [5]. Routing attacks, which involve manipulating network routing tables to redirect or destroy data, also pose a significant risk to the network's reliability and function [5].

2.4 The Application Layer: Services, Firmware, and Software-Specific Threats

The Application Layer is the top layer of the IoT architecture, responsible for processing the data received from the network and presenting it to end-users through applications and services [5]. This layer encompasses a wide range of functions, including data storage, service management, and the execution of user-facing applications in domains like healthcare and smart homes [1].

Vulnerabilities at this layer are often tied to software and firmware, and they are frequently exploited to gain unauthorized access, steal data, or manipulate devices. Common security flaws include weak authentication, such as the use of default or easily guessed passwords, and insecure firmware that lacks the ability to be updated or patched [11]. The use of insecure APIs that lack proper encryption and validation also provides an easy entry point for attackers to access private data or take control of a device [11]. Another pervasive and dangerous issue is the failure to implement timely and secure firmware updates, which leaves devices permanently exposed to vulnerabilities discovered after their release [11]. This highlights a critical deficiency in the IoT ecosystem's approach to lifecycle management, where devices with unfixable flaws are allowed to remain in the network. This systemic issue is a major factor behind large-scale security incidents, as a single unpatched device can serve as a gateway for an attacker to compromise a larger network. This was a key element in the proliferation of the Mirai botnet, which targeted devices with weak credentials and unpatched vulnerabilities to build its army of infected devices [10]. The security of this layer is not just about the applications themselves, but about the entire process of how a device is developed, managed, and supported throughout its operational life [12].

3. A Taxonomy of Cybersecurity Threats in IoT Environments

The interconnected and multi-layered nature of the IoT ecosystem provides a fertile ground for a diverse range of cyber threats. A systematic classification of these threats is essential for developing targeted and effective defense mechanisms. This taxonomy outlines attacks based on the architectural layer they primarily target, offering a clear framework for understanding the threat landscape.

3.1 Attacks Targeting the Perception Layer

Threats at the perception layer often involve a combination of physical and digital manipulation, directly compromising the integrity of devices and their data collection processes. A primary concern is physical tampering, where an attacker physically accesses a device to steal or alter sensitive information, such as cryptographic keys [5]. Another insidious attack is the

Slumber Denial Attack, which targets the energy efficiency of a device by preventing it from entering a low-power state. By supplying fake feedback, an attacker forces the device to remain active, causing its battery to drain prematurely and leading to a denial of service [5].

Digital attacks at this layer also include malicious code injection, in which a rogue node is inserted into the network to take over a communication channel, and replay attacks, which involve capturing a legitimate data transmission and replaying it later to trick a device into performing an unauthorized action [5].

Node jamming is another form of attack that perturbs a device's communication channel with a transmitter, resulting in a denial of service [5]. These attacks underscore the vulnerability of the most foundational components of the IoT, where limited resources and physical accessibility are significant weaknesses.

3.2 Attacks Targeting the Network Layer

The network layer, with its role in data transmission and routing, is a prime target for attacks that seek to disrupt services, compromise data, and commandeer device control. A major class of attacks is Distributed Denial of Service (DDoS), where a service is flooded with traffic from a multitude of sources, rendering it unavailable to legitimate users [8, 10]. In the IoT context, these attacks are frequently executed using botnets a network of compromised devices, often IoT devices with weak security, that are remotely controlled by an attacker, or ‘bot herder’ [10]. The Mirai botnet serves as the most prominent example of this threat, having harnessed a vast number of unsecured IoT devices to launch devastating volumetric DDoS attacks [10].

Other significant network-level threats include Man-in-the-Middle (MITM) attacks, which involve an attacker secretly intercepting and possibly altering the communication between two devices, thereby compromising data confidentiality and integrity [5].

Sybil attacks are another concern, where a single malicious node impersonates multiple legitimate nodes to gain disproportionate influence within the network, affecting the availability and trust of the system [5]. Finally, routing attacks can lead to network destruction by changing routing data, affecting the confidentiality, availability, and authentication of the entire system [5]. These attacks highlight the critical need for robust security measures that can defend against threats that compromise the very fabric of IoT communication.

3.3 Attacks Targeting the Application Layer and Protocols

Attacks at the application layer focus on exploiting vulnerabilities within software, services, and the protocols that facilitate data exchange. The default insecurity of many lightweight IoT protocols, such as MQTT and CoAP, makes this layer particularly susceptible [9]. These protocols often lack strong, built-in security controls like encryption, authentication, and authorization, creating an environment ripe for exploitation when improperly configured [9]. Threats include data leakage and unauthorized access, where attackers can eavesdrop on sensitive data streams or gain control of devices due to a lack of identity verification [9].

Malicious payload injection is a significant risk, as attackers can send malicious requests to overwrite resource values or manipulate device logic [9]. A compromised MQTT broker, for instance, can be used to intercept, modify, or drop messages and even impersonate legitimate clients, effectively giving an attacker full control over

device communication [9]. These vulnerabilities are often compounded by insecure software development practices and a failure to address well-known security flaws [11]. The existence of these software- and protocol-based weaknesses demonstrates that even with a physically secure device and network, the application layer can still be the point of failure.

3.4 Case Study: The Mirai Botnet and its Legacy in IoT Attacks

The Mirai botnet stands as a seminal case study in IoT security, perfectly illustrating the catastrophic consequences of the security deficiencies inherent in the ecosystem. Mirai was a piece of malware designed to relentlessly scan the internet for unsecured IoT devices, specifically targeting those with weak or default credentials [10]. Once it identified a vulnerable device, it would attempt to log in using a list of common factory-set passwords and, upon successful access, would infect the device and recruit it into a large botnet [10]. This network of compromised devices, or 'zombie army,' was then used to launch massive volumetric DDoS attacks that consumed immense amounts of bandwidth and resources, effectively taking targeted services offline [10]. The attack against Dyn DNS in 2016, for example, was one of the largest DDoS attacks on record at the time, demonstrating the unprecedented power of a distributed network of unsecured IoT devices [10].

The strategic and economic implications of the Mirai incident are profound. The primary targets of Mirai were low-cost, consumer-grade devices like wireless routers and IP cameras, which often come with hardcoded default passwords and a lack of timely security updates [13,14]. The public release of Mirai's source code further exacerbated the problem, leading to the proliferation of numerous variants that continue to pose a threat [10]. This case study highlights a critical market failure: the collective security of the internet is only as strong as its weakest and most numerous components. It demonstrates that as long as manufacturers are incentivized to produce low-cost devices with minimal security features, the entire digital ecosystem remains at risk. This realization has spurred a demand for proactive regulatory intervention and industry-wide standards to ensure that security is an integrated, non-negotiable part of the design process for all IoT devices [15].

Table 1: Taxonomy of IoT Threats by Architectural Layer

Architectural Layer	Attack Type	Description/Impact	Referenecs
Perception	Physical Tampering	An attacker physically modifies the device or its components to gain access to sensitive information.	[5]
	Slumber Denial Attack	An intruder supplies false feedback to a device, preventing it from entering sleep mode and draining its battery.	[5]
	Malicious Code Injection	A malicious node is inserted between a sender and receiver to take over the communication channel.	[5]
	Replay Attack	An attacker intercepts a valid data transmission and re-transmits it to deceive a device.	[5]
Network	Distributed Denial of Service (DDoS)	A service is overwhelmed with a flood of traffic from a botnet of compromised devices, making it unavailable.	[8]

	Man-in-the-Middle (MITM)	An attacker secretly intercepts communication between two parties, Compromising dataconfidentiality and integrity.	[5]
	Sybil Attack	An injected node claims to be an original node or impersonates multiple nodes, affecting system availability.	[5]
	Routing Attack	An attacker alters a network's routing tables, leading to network destruction and service disruption.	[5]
Application	Weak Authentication	Use of default, weak, or easily guessed passwords, making devices susceptible tounauthorized access.	[11]
	Insecure Firmware/Unpatched Updates	Manufacturers fail to provide timely security updates, leaving devices permanently vulnerable to known exploits.	[11]
	Data Leakage/ Unauthorized Access	Improperly configured protocols or APIs allow attackers to eavesdrop on sensitive data.	[9]
	Malicious Payload Injection	Attackers send malicious requests to overwrite resource values or inject code into an application.	[8]

4. Intrusion Detection Systems (IDS) for IoT Networks

4.1 Limitations of Traditional IDS in Resource-Constrained Environments

Traditional intrusion detection systems, historically designed for enterprise-level IT networks, are often ill-suited for the unique and challenging environment of the IoT. A fundamental limitation is their high computational and memory footprint, which makes them impractical for deployment on resource-constrained IoT devices with limited processing power and battery life [17]. Furthermore, conventional IDS models typically rely on pre-defined rule sets or a database of known attack signatures [7]. This reactive approach struggles to keep pace with the sheer volume, diversity, and novelty of attacks in the dynamic IoT ecosystem. A system based on known signatures, for instance, is inherently incapable of detecting a ‘zero-day’ attack, which exploits a previously unknown vulnerability [2]. These deficiencies have necessitated the development of adaptive and lightweight detection mechanisms tailored to the unique constraints of IoT.

4.2 Classification of IDS by Detection Method

Intrusion detection systems can be broadly categorized based on their core methodology for identifying threats. The two primary approaches are signature-based and anomaly-based detection.

Signature-Based Detection

This method is the most traditional form of intrusion detection. It operates by maintaining a database of known attack patterns, or signatures, and then actively scanning network traffic for any matches [7]. When a packet or a sequence of packets matches a signature in the database, the system flags it as a malicious activity [7]. The main advantage of this approach is its high accuracy in detecting previously identified attacks [19,20]. However, its core weakness is its reliance on a pre-existing knowledge base; it is fundamentally incapable of detecting new or evolving threats for which no signature has yet been created [7]. This makes it a reactive defense mechanism that struggles against the fast-paced, constantly changing threat landscape of the IoT.

Anomaly-Based Detection

Developed to overcome the limitations of signature-based systems, anomaly-based detection is a more proactive approach. Instead of looking for malicious patterns, this method first establishes a baseline of 'normal' network or device behaviour [7]. It then monitors for any significant deviations from this established baseline, flagging any anomalous behavior as a potential threat [7]. Machine learning algorithms are particularly effective in this domain, as they can build sophisticated models of normal activity and adapt to new data over time [2]. The principal strength of anomaly-based detection is its ability to identify novel, previously unknown attacks, including zero-day exploits [19]. A key challenge, however, is the potential for a high rate of false positives, where legitimate but unusual activity is mistakenly flagged as malicious [18].

4.3 Classification of IDS by Deployment Location

The physical or logical placement of an IDS is another critical factor in its design and effectiveness. IDS can be deployed either at the network level or on individual hosts.

Network Intrusion Detection Systems (NIDS)

NIDS are strategically placed at key points within the network, such as gateways, routers, or switches, to monitor the flow of all network traffic [19]. These systems analyze data packets in real time or offline to detect suspicious activity and identify threats that could affect the entire network [19]. NIDS offers a broad view of the network's health and can be effective for detecting attacks like DDoS, which often manifest at the network level [8].

Host-Based Intrusion Detection Systems (HIDS)

In contrast to NIDS, HIDS are deployed directly on individual devices or hosts within the network [19]. They function by monitoring internal processes, file system changes, and system logs to detect signs of compromise [19]. HIDS provides a more granular level of protection by identifying threats that may have already bypassed network-level defenses. However, implementing HIDS on resource-constrained IoT devices is particularly challenging due to their limited processing power and memory [1]. This has made NIDS a more common approach for securing IoT networks, where devices often lack the capacity to run a dedicated security agent.

5. Leveraging Machine Learning and Deep Learning for Threat Detection

5.1 Overview of Machine Learning Approaches

The limitations of traditional, signature-based intrusion detection systems have catalyzed a major shift toward machine learning (ML) as a more adaptive and scalable solution for IoT security [2]. ML-based models possess the unique capability to learn from large volumes of network data, identify complex patterns, and make intelligent predictions about the presence of threats without relying on a static database of known signatures [2].

ML techniques for intrusion detection can be categorized into two primary approaches:

- **Supervised Learning:** These models are trained on labeled datasets, where network traffic is pre-categorized as either 'normal' or 'malicious' [2]. The goal of a supervised model is to learn the distinguishing features between these classes so that it can accurately classify new, unseen data [22]. Prominent examples in this category include Random Forest, a powerful ensemble technique that builds multiple decision trees to improve accuracy, and Support Vector Machines (SVM), which finds an optimal hyperplane to separate different classes of data [21].

- **Unsupervised Learning:** This approach is particularly valuable for detecting novel or zero-day attacks, as itdoes not require pre-labeled data [2]. Unsupervised models analyze unlabeled network traffic and identify patterns that deviate from the norm, flagging these anomalies as potential threats [21]. Autoencoders are a common type of unsupervised model used for this purpose, as they are trained to reconstruct normal data and are typically unable to accurately reconstruct anomalous data, thus highlighting the deviation [21].

5.2 Deep Learning Architectures for IoT IDS

Deep learning (DL), a specialized branch of machine learning, has emerged as a powerful tool for IoT intrusion detection due to its ability to automatically extract high-level features from raw data and handle complex, unstructured traffic patterns [21]. Several DL architectures have shown promising results.

[1]. Convolutional Neural Networks (CNNs): Originally designed for image recognition, CNNs have been adapted to analyze network traffic by treating it as a grid of data [27]. They are highly effective at extracting spatial features and identifying subtle patterns within data flows, which can be indicative of a cyber-attack [22]. Studies on the CICIoT2023 dataset have shown that CNNs can achieve a good balance between detection performance and computational efficiency, making them suitable for deployment on edge devices [27].

[2]. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTMs): RNNs are architectures specifically designed for processing sequential or time-series data, making them ideal for analyzing the temporal nature of network traffic [22]. LSTMs, a type of RNN, are particularly effective because they can remember long-term dependencies in data, which is crucial for identifying complex, multi-stage attacks that unfold over time [22].

[3]. Hybrid DL Models: A growing body of research is focused on combining different deep learning architectures to create more robust and effective models. A hybrid CNN-LSTM model, for example, can leverage a CNN's ability to extract spatial features from network packets and an LSTM's capability to capture the temporal relationships between those packets, leading to a more comprehensive analysis of attack patterns [22].

5.3 Hybrid and Ensemble Learning Models for Enhanced Performance

To further improve the accuracy and robustness of threat detection, researchers have increasingly turned to hybrid and ensemble learning models [28]. These models combine multiple machine learning or deep learning algorithms to create a more powerful and resilient classifier [22, 23]. The rationale behind this approach is that by leveraging the complementary strengths of different algorithms, the system can achieve superior performance compared to any single model acting alone.

A hybrid ensemble model might, for instance, combine tree-based classifiers like Random Forest and XGBoost with other algorithms like K-Nearest Neighbors (KNN) and AdaBoost in a voting-based classifier.30 A study using the IoT- 23 dataset demonstrated that such a hybrid model outperformed standalone approaches across multiple metrics, including accuracy, precision, and F1-score [30, 31]. Similarly, a stacked ensemble model might use algorithms like Gaussian Naive Bayes, Support Vector Machines, and Multi-Layer Perceptron's as base classifiers, with a meta-classifier like Logistic Regression making the final decision based on their outputs [21]. These hybrid and ensemble approaches have been shown to enhance detection accuracy, scalability, and adaptability, making them particularly well-suited for addressing the multifaceted nature of IoT security threats [21].

5.4 Federated Learning for Privacy-Preserving and Decentralized Detection

Federated learning (FL) is an innovative machine learning paradigm that addresses one of the most critical challenges in IoT: data privacy and resource constraints [2]. In traditional ML, all data from different devices is sent to a centralized server for training, which poses significant privacy risks and places a heavy burden on network resources [33]. FL offers a decentralized solution. Instead of transmitting raw data, an FL framework trains a global model by distributing it to participating IoT devices [2]. Each device then trains a local version of the model using its own private data and subsequently sends only the updated model parameters (not the data itself) back to a central server [27]. The server aggregates these updates to create a new, improved global model, which is then redistributed to the devices for the next round of training [32,33]. This process is repeated until the model reaches an optimal level of performance. This approach offers numerous benefits: it preserves data privacy

by keeping sensitive information local to the device, reduces network latency and communication overhead, and mitigates the risk of a single point of failure by eliminating the need for a centralized data repository [2]. FL represents a paradigm shift toward a more secure, efficient, and privacy- conscious approach to machine learning in the IoT, aligning with the architectural constraints and operational requirements of modern, distributed networks.

6. Performance Evaluation and Benchmark Datasets

6.1 Essential Metrics for Model Assessment

The true effectiveness of a threat detection model is validated through rigorous performance evaluation using a standardized set of metrics. While Accuracy, which measures the ratio of correctly predicted instances to the total number of instances, is a common starting point, it can be misleading in datasets where there is a significant class imbalance (i.e., a small number of attack instances compared to normal traffic) [26]. Therefore, a more nuanced set of metrics is essential for a comprehensive evaluation.

i. Accuracy:
Accuracy represents the number of correctly classified data instances over the total number of data instances.

$$\frac{True\_Positive + True\_Negative}{True\_Positive + True\_Negative + False\_Positive + False\_Negative} \quad [31]$$

ii. Precision:
A classification model's capability to determine only the most pertinent information points. Precision is defined mathematically as shown below in equation 5.

$$\frac{True\_Positive}{True\_Positive + False\_Positive} \quad [34]$$

iii. Recall:
An algorithm's capability to identify every applicable class within a data collection. We define recall statistically as shown below in equation 6.

$$\frac{True\_Positive}{True\_Positive + False\_Negative} \quad [34]$$

iv. F1 Score:
As illustrated below, the F1 score is determined as the harmonic average of the recall and precision scores. It goes from 0 to 100%, with an elevated F1 score indicating a higher quality classifier.

$$2 * \frac{Recall * Precision}{Recall + Precision} \quad [34]$$

False Positive Rate (FPR): This metric measures the rate of false alarms, or the proportion of benign instances that were incorrectly classified as malicious. A low FPR is critical for real-world deployments to prevent alert fatigue and wasted resources [26].

A comprehensive assessment also often involves a confusion matrix, which visually represents the performance of a model across all classes, allowing for a detailed analysis of per-class performance and the nature of misclassifications [27].

6.2 Key Benchmark Datasets for IoT Security Research

The development and comparison of IDS models rely heavily on publicly available benchmark datasets that accurately represent real-world IoT traffic.

- **UNSW-NB15:** This dataset is a widely used benchmark for network intrusion detection research. It contains a comprehensive range of attack types, including DoS, reconnaissance, and exploits, making it more representative of modern security challenges than older datasets like KDDCUP99 [26].
- **BoT-IoT:** Created specifically to simulate IoT botnet attacks, this dataset is indispensable for developing and testing models designed to detect DDoS attacks. It contains a massive number of instances, with over 38 million records specifically for DDoS attacks, providing a realistic environment for training [35,36].
- **CICIoT2023:** As a more recent and extensive dataset, CICIoT2023 offers a vast collection of both benign and malicious traffic, including a wide variety of attack categories [27]. Its large scale (over 46 million

records) necessitates advanced data preprocessing techniques like stratified random sampling to manage computational overhead while ensuring a balanced class representation for robust model training [27].

6.3 A Comparative Analysis of Model Performance on Standard Datasets

A review of the literature reveals that the choice of an optimal model depends heavily on the specific dataset and the desired trade-offs between performance metrics and computational cost. Studies have shown that no single model is universally superior. For example, research on the UNSW-NB15 dataset has indicated that a Random Forest model can achieve a high F1-score of 97.80% and an accuracy of 98.63% [26]. A different study using deep learning models on the same dataset found that a GRU model achieved the highest accuracy, with 92.71% for binary classification and 78.62% for multiclass classification [29].

When analyzing the CICIoT2023 dataset, a deep learning-based study demonstrated that a CNN model achieved the best trade-off between detection performance and computational efficiency, reaching approximately 98% accuracy with low latency and a compact model size suitable for deployment on resource-constrained devices [27]. This contrasts with a more complex CNN-BiLSTM architecture, which achieved a slightly higher accuracy (~99%) at a significantly greater computational cost, highlighting the crucial trade-off between performance and efficiency in real-world IoT deployments [27]. The data in Table 2 provides a snapshot of these comparative results.

Table 2: Comparative Performance of ML/DL Models for IoT IDS

Model/Architecture	Dataset Used	Key Metrics (Accuracy, F1-Score, FPR)	Key Findings	References
Random Forest	UNSW-NB15	Accuracy: 98.63%, F1-Score: 97.80%, FPR: 1.36%	Consistently high accuracy with low false alarms, making it a strong choice for improving IDS security.	[26]
GRU (Deep Learning)	UNSW-NB15	Binary Accuracy: 92.71%, Multiclass Accuracy: 78.62%	Achieved the highest accuracy among other deep learning models for both binary and multiclass classification.	[29]
CNN (Deep Learning)	CICIoT2023	Accuracy: ~98%	Achieved the best trade-off between detection performance and computational efficiency for edge deployment.	[27]
CNN-BiLSTM (Hybrid)	CICIoT2023	Accuracy: ~99%	Yielded slightly higher accuracy than CNN but at a significantly greater computational cost.	[27]
Hybrid Ensemble Model	IoT-23	All metrics were high, outperforming standalone models.	Showed superior performance across all metrics for both binary and multi-class classification.	[30]

Federated Ensemble Learning (FEI)	IoT-23_Combined	Accuracy: 87.94%, F1-Score: 88.44%	Surpassed the AMLI model, demonstrating superior performance across all metrics.	[37]
OSNN (Optimized SNN)	UNSW-NB15	Accuracy: 96.80%	Showed strong performance, which can be attributed to careful hyperparameter optimization.	[20]

7. Emerging Challenges and Future Research Directions

7.1 Adversarial Machine Learning and Countermeasures in IoT Security

The maturation of machine learning-based threat detection has introduced a new and formidable challenge: adversarial machine learning (AML). In an AML attack, adversaries intentionally craft malicious inputs, known as 'adversarial examples,' to deceive an ML model into making an incorrect prediction [38]. These attacks exploit the inherent vulnerabilities of deep neural networks, where a subtle, often imperceptible, perturbation to an input can cause the model to misclassify it [39]. In the context of IoT security, this could mean an attacker injecting a minimal perturbation into a network packet to make a malicious data flow appear benign, thereby bypassing an IDS and gaining unauthorized access to a network [40].

The threat posed by AML is particularly critical for IoT because of the difficulty in implementing robust defenses on resource-constrained devices. Many of the most effective countermeasures, such as adversarial training, are computationally intensive and require significant resources for model retraining, which may not be feasible in a typical IoT environment [40] This represents a new front in cybersecurity, where attackers are no longer just exploiting software flaws but are actively manipulating the very intelligence systems designed to protect networks. The development of lightweight and efficient defense mechanisms, such as feature engineering that respects protocol-specific constraints, is an active area of research aimed at building resilient systems against these sophisticated attacks [41].

7.2 The Role of Explainable AI (XAI) in Cybersecurity Applications

As AI and ML models become more complex and integral to cybersecurity, the need for transparency has become paramount. This has driven the emergence of Explainable AI (XAI), a field focused on making the decision-making processes of AI models transparent and understandable to humans [42]. Traditional AI models are often perceived as 'black boxes' that produce results without offering any insight into how those conclusions were reached [42]. In security- critical domains, this lack of transparency is a major obstacle to trust and effective incident response.

XAI addresses this by acting as a 'cognitive translator,' providing clear explanations for why a model flagged a particular activity as a threat [43]. For security professionals, this is invaluable, as it enables them to understand the root cause of an alert, validate the model's behavior, and make more informed decisions during an attack [43]. XAI can also aid in vulnerability and risk assessment by clarifying the rationale behind prioritizing certain security measures, which helps organizations allocate resources more effectively. Furthermore, it plays a crucial role in ensuring that AI-driven security measures comply with regulatory standards like GDPR and HIPAA, which require transparent and accountable data protection decisions [43]. Ultimately, the integration of XAI with IoT security is essential for fostering greater collaboration between human analysts and AI systems, leading to more robust, trustworthy, and adaptable defense strategies.

7.3 Post-Quantum Cryptography for a Future-Proofed IoT

The advent of large-scale, fault-tolerant quantum computers poses a significant, long-term threat to the security of the IoT. These future machines will have the power to break many of the public-key cryptographic algorithms

that are the foundation of modern digital security, including those used for encrypting and authenticating IoT communications [44]. This is a particularly pressing issue for IoT devices, which have long lifecycles and may be vulnerable to 'harvest now, decrypt later' attacks, where encrypted data is collected today in anticipation of future quantum decryption capabilities [45].

To address this impending threat, the field of Post-Quantum Cryptography (PQC) is dedicated to developing new cryptographic algorithms that are secure against both classical and quantum computers [44]. Research efforts are primarily focused on a few key approaches:

- **Lattice-based cryptography:** This approach leverages the mathematical difficulty of solving problems in high-dimensional lattices. It is considered a promising candidate due to its efficiency and the fact that some schemes, like NTRU, have been studied for many years without being broken [44].
- **Multivariate cryptography:** This method is based on the complexity of solving systems of multivariate polynomial equations. While some encryption schemes have failed, signature schemes based on this approach could provide a basis for quantum-secure digital signatures [44].
- **Hash-based cryptography:** These schemes use cryptographic hash functions to generate signatures. While they have a limitation on the number of signatures that can be generated, they are highly resistant to quantum attacks and have been studied since the 1970s [44].

The development of lightweight and efficient PQC solutions is a crucial area of research to ensure that the IoT remains secure in the post-quantum era, particularly given the resource constraints of many devices [2].

7.4 Integration of Blockchain for Decentralized Trust and Data Integrity

Blockchain technology, with its defining characteristics of decentralization, immutability, and tamper-proof data storage, is a powerful paradigm for addressing some of the most critical challenges in IoT security [33]. The centralized nature of many current IoT architectures presents a single point of failure that an attacker can exploit to compromise an entire network. Blockchain's distributed ledger technology eliminates this risk by distributing information across multiple nodes, making it highly resilient to data breaches and cyberattacks [33].

A particularly promising area of research involves the integration of blockchain with federated learning. In this combined framework, the decentralized and tamper-proof nature of the blockchain can be used to manage the integrity of the model updates that are shared in federated learning [33]. It can also provide a transparent and auditable record of all operations, ensuring that the model parameters have not been corrupted or tampered with [33]. Furthermore, blockchain can be used to create a built-in incentive mechanism, rewarding devices with digital tokens for their participation in the training process, thereby encouraging more active and resource-intensive contributions to the network [33]. While this hybrid approach offers significant benefits for security, privacy, and resilience, researchers continue to face challenges related to the computational overhead of blockchain and its scalability with the massive number of IoT devices [46].

8. IoT Security Standards and Regulatory Frameworks

8.1 Overview of Major Standards

The establishment of clear and authoritative security standards is a foundational step in mitigating the security risks of the IoT ecosystem. These standards provide a common set of best practices and technical controls that guide manufacturers, developers, and integrators in building and deploying secure devices. Key players in this space include:

- **ISO/IEC:** The International Organization for Standardization and the International Electrotechnical Commission have collaborated on standards like ISO/IEC 27400:2022, which is widely regarded as a comprehensive standard for IoT security. It covers a broad range of aspects, from authentication and communication to device updates and physical security [15]
- **NIST:** The U.S. National Institute of Standards and Technology has developed a suite of publications, such as NISTIRs 8259A and 8259B, to provide foundational cybersecurity guidance for IoT device manufacturers and customers [47]

- **ETSI:** The European Telecommunications Standards Institute has published ETSI EN 303 645, a standard focused on consumer-level IoT devices.[15]

These standards are vital for ensuring a minimum level of security across a fragmented and heterogeneous market, where a lack of security could have ripple effects across the entire digital infrastructure [16].

8.2 Differentiating Standards from Legally Binding Regulations

A critical distinction must be made between security standards and legal regulations. A standard provides a set of voluntary best practices and technical controls that organizations can choose to adopt [15]. While compliance with a standard is often beneficial for marketability and customer trust, it is not legally mandated. In contrast, a regulation is a legally enforced requirement that an organization must compulsorily meet [15]. For instance, a high-level regulation like HIPAA in the healthcare industry may mandate the protection of sensitive data, but it is a standard like NIST or ISO that provides the detailed technical guidance on how to achieve that protection securely [15]. The U.S. IoT Cybersecurity Improvement Act of 2020 is an example of legislation that has started to move the industry toward legally-enforced security requirements, prohibiting federal agencies from procuring IoT devices that do not comply with NIST standards [16,49]. This demonstrates a growing trend toward using regulatory pressure to compel security improvements in the IoT sector.

8.3 The NIST IoT Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has developed a comprehensive and multi-faceted framework to guide the secure design and deployment of IoT devices. The framework is notable for its holistic approach, addressing both technical and non-technical aspects of security.

- **NISTIR 8259A:** The Technical Baseline: This publication defines an 'IoT device cybersecurity capability core baseline,' which is a set of essential technical features that a device should possess to support common cybersecurity controls [48,51]. These capabilities include a unique device identity for authentication and tracking, the ability to securely configure device software, and mechanisms to protect data both in transit and at rest [48,52].
- **NISTIR 8259B:** The Non-Technical Baseline: This publication complements the technical baseline by defining a 'non-technical supporting capability core baseline' [47]. This is a crucial aspect of the framework that recognizes that a secure device is only part of the solution.

This report recommends that manufacturers provide a set of non-technical supporting capabilities, including:

- **Documentation:** Clear and comprehensive information for customers on how to securely use andconfigure the device.
- **Information and Query Reception:** A formal process for receiving and responding to customer feedback, questions, and reports of vulnerabilities.
- **Information Dissemination:** A channel for proactively notifying customers of new vulnerabilities and available security updates.
- **Education and Awareness:** Providing educational content to help users understand and manage the security risks of their devices [47].

The dual focus of the NIST framework on both technical and non-technical capabilities is a testament to the reality that security failures are often a result of human factors, not just technical flaws [16,52]. The widespread use of default passwords, for example, is not a technical vulnerability of the device itself but a failure in user education and awareness, a major weakness exploited by the Mirai botnet [10,53]. By addressing these non-technical issues, the NIST framework provides a blueprint for a more resilient and trustworthy IoT ecosystem that considers the entire lifecycleand the human element in security.

Table 3: Key IoT Security Standards and their Focus

Standard/Body	Focus Areas	Relevance	Reference
NIST	Secure device identification, configuration, data protection, and non-technical support (documentation, updates, user education).	U.S. Federal Government, critical infrastructure, and manufacturers.	[15]
ISO/IEC 27400:2022	Comprehensive security for all aspects of a device's lifecycle, including authentication, communication, updates, and physical security.	Global industry standard, widely used across various sectors.	[15]
ETSI EN 303 645	Baseline security for consumer-grade IoT devices, promoting security by design.	European Union, focused on consumer products.	[15]
OWASP IoT Top 10	A list of the most critical web application security risks in the IoT, for developers and security professionals.	General guidance for developers and practitioners globally.	[15]

9. Conclusion

This comprehensive review has provided an in-depth analysis of the evolving security landscape for IoT networks, synthesizing a wide body of research to offer a detailed and strategic perspective. The report has underscored the foundational challenges inherent to the IoT ecosystem, primarily stemming from the resource-constrained and highly heterogeneous nature of the devices, which traditional security measures are ill-equipped to handle. A central finding is the paradigm shift in threat detection from antiquated, signature-based systems to dynamic, AI-driven anomaly- based models. A key trend identified in recent literature is the development and adoption of sophisticated hybrid and ensemble learning models, which combine the complementary strengths of various algorithms to achieve superior detection accuracy, adaptability, and robustness against a diverse range of attacks. These advanced models, particularly when integrated with frameworks like federated learning, offer a promising path toward decentralized, privacy-preserving, and scalable security solutions.

The review has further highlighted that security vulnerabilities are not confined to a single layer of the IoT architecture but permeate the entire ecosystem, from physical devices and network protocols to software and firmware. The case study of the Mirai botnet served as a potent illustration of how systemic flaws, such as weak default passwords and a lack of timely updates, can be exploited to launch large-scale, catastrophic attacks. This points to a broader reality: the security of the IoT is inextricably linked to both technological and non-technical factors, necessitating a holistic and layered defense strategy. Based on the evidence and analysis presented, fortifying IoT security requires a multi-pronged, defense-in-depth approach that addresses vulnerabilities at every architectural layer. The following recommendations provide a strategic blueprint for building a resilient IoT ecosystem:

Prioritize Security by Design: Manufacturers must embed security as a core, non-negotiable feature from the initial design phase of a device. This includes implementing secure firmware updates, strong authentication, and robust data protection measures, as outlined in the NISTIR 8259A framework. The days of sacrificing security for cost or simplicity must end.

Embrace Intelligent, Distributed Threat Detection: The deployment of intelligent threat detection systems is no longer optional. Networks should leverage AI-driven, anomaly-based models to detect novel threats. Furthermore, adopting distributed and privacy-preserving approaches like federated learning is essential to manage the scale and heterogeneity of IoT networks while simultaneously protecting sensitive data.

Address the Human and Lifecycle Factors: A truly resilient security posture extends beyond technology. It requires a commitment to non-technical support, as highlighted in the NISTIR 8259B framework. This includes providing clear documentation, implementing a mechanism for user feedback and vulnerability reporting, and establishing a program for user education and security awareness. The entire device lifecycle, from manufacturing to end-of-life, must be governed by a proactive and continuous security management strategy.

The future of IoT security will be shaped by the ongoing convergence of several cutting-edge technological and strategic fields. The battle against adversarial machine learning attacks will drive the development of more robust, transparent, and resilient AI models, fueled by advancements in Explainable AI. Simultaneously, the imminent threat of quantum computing will accelerate the transition to lightweight and efficient post-quantum cryptographic algorithms. The integration of decentralized trust mechanisms, such as blockchain, with federated learning will continue to offer novel solutions for data integrity and privacy at scale. Ultimately, the successful creation of a trustworthy and resilient digital ecosystem for the next generation of IoT devices will depend on the proactive and thoughtful integration of these advanced technologies, guided by authoritative standards and legally binding regulations. The challenge is immense, but the strategic direction is now clearer than ever.

References

[1] M. Bezawada and V. K. P., 'Comparative study on techniques used for anomaly detection in IoT data,' Int. J. Comput. Eng. Res. Trends, vol. 10, no. 4, pp. 177–181, 2023.

[2] R. Alghamdi and M. Bellaiche, 'A cascaded federated deep learning-based framework for detecting wormhole attacks in IoT networks,' Comput. Secur., vol. 125, art. no. 103014, 2023.

[3] R. A. Devi and A. R. Arunachalam, 'Enhancement of IoT device security using an improved elliptic curve cryptography algorithm and malware detection utilizing deep LSTM,' High-Confidence Comput., art. no. 100117, 2023.

[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, 'Demystifying IoT security: Survey, vulnerability analysis, and empirical evaluation at internet scale,' IEEE Commun. Surv. Tuts., vol. 21, no. 3, pp. 2702–2733, 2019.

[5] J. Wang et al., 'IoT-DeepSense: Behavioral security detection of IoT devices based on firmware virtualization and deep learning,' Secur. Commun. Netw., vol. 2022, Art. ID 1443978, 2022.

[6] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, 'Malicious insider attack detection in IoTs using data analytics,' IEEE Access, vol. 8, pp. 11743–11753, 2019.

[7] S. K. Choi, C. H. Yang, and J. Kwak, 'Novel machine learning algorithms for detecting and preventing attacks on IoT devices,' in Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), 2018, pp. 1–7.

[8] F. O. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, 'Internet of Things security: A survey,' J. Netw. Comput. Appl., vol. 88, pp. 10–28, 2017.

[9] S. N. Kouicem, A. Bouabdallah, and H. Lakhlef, 'Internet of things security: A top-down survey,' Comput. Netw., vol. 141, pp. 199–221, 2018.

[10] J. S. Kumar and D. R. Patel, 'A survey on internet of things: Security and privacy issues,' Int. J. Comput. Eng., vol. 16, no. 5, pp. 11–17, 2014.

[11] P. Varga, S. Plosz, G. Soos, and C. Hegedus, 'Security threats and issues in automation IoT,' in Proc. 12th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), 2017, pp. 1–7.

[12] A. Thakkar and R. Lohiya, 'A review on machine learning and deep learning perspectives of anomaly detection in IoT,' Arch. Comput. Methods Eng., vol. 29, no. 4, pp. 1–28, 2022.

[13] A. Verma and V. Ranga, 'Utilizing ML classification algorithms for building IDS in order to secure IoT against DoS attacks,' in Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), 2020, pp. 1–7.

[14] V. Choudhary, S. Tanwar, and T. Choudhury, 'A hybrid deep learning model for intrusion detection system in the Internet of Things environment,' in Proc. 4th Int. Conf. Data Manage., Anal. Innov. (ICDMAI), 2023, pp. 1–6.

[15] S. S. Alsaleh, M. E. B. Menai, and S. Al-Ahmadi, 'Federated learning-based model to lightweight IDSs for heterogeneous IoT networks: State-of-the-art, challenges, and future directions,' IEEE Access, vol. 12, pp. 1–15, 2024.

[16] A. Gendreau and M. Moorman, 'Survey of intrusion detection systems towards an IoT-based IDS,' in Proc. FiCloud, 2016, pp. 240–245.

[17] U. Alam and W. Almobaideen, 'A comprehensive analysis of the machine learning algorithms in IoT IDS systems,' in Proc. Int. Conf. Comput. Sci. Inf. Technol. (CSIT), 2023, pp. 1–6.

[18] M. Idrissi, M. Azizi, and F. El Bousty, 'BotIDS: A deep learning-based botnet intrusion detection system for IoT,' J. Commun. Netw., vol. 23, no. 2, pp. 91–101, 2021.

[19] A. Abdulla, M. A. Abououf, and M. Alshamrani, 'A systematic review on IoT security threats, mitigation strategies and future directions,' Int. J. Res. Rev., vol. 8, no. 7, pp. 1–10, 2021.

[20] M. Elhoseny, A. Kannan, and H. N. Nguyen, 'A deep learning-based anomaly detection system for IoT networks,' J. Cybersecur. Privacy, vol. 2, no. 1, pp. 1–12, 2022.

[21] Y. N. Kunang, A. Abduvaliyev, T. Baker, and J. Liu, 'A hybrid deep learning-based intrusion detection system for IoT platforms,' J. Netw. Comput. Appl., vol. 183, pp. 1–15, 2021.

[22] L. Wei, H. Zhang, J. Zhou, and Y. Wang, 'Adaptive learning rate adjustment mechanism for deep learning-based IDS models,' IEEE Trans. Ind. Informat., vol. 18, no. 5, pp. 1–10, 2022.

[23] K. Kaliyaperumal and H. Arrama, 'CNN-FDSA: A hybrid deep learning framework for botnet attack detection in IoT networks,' J. Eng. Appl. Sci., vol. 18, no. 2, pp. 1–15, 2023.

[24] Q. Xuan, L. Yang, and Z. Yang, 'A hybrid DBN-RNN framework for detecting advanced persistent threats,' Comput. Secur., vol. 138, pp. 1–10, 2024.

[25] S. Javed, M. Usman, and R. Akhtar, 'Machine learning for IoT security: A comprehensive review,' Appl. Sci., vol. 13, no. 4, pp. 1–15, 2023.

[26] M. Banaamah and S. Ahmad, 'Implementation of deep learning techniques for intrusion detection using CNN, LSTM and GRU,' in Proc. 5th Int. Conf. Comput. Inf. Sci. (ICCIS), 2022, pp. 1–7.

[27] S. Bouazza, A. Abdelli, and M. Benslimane, 'A survey of intrusion detection systems towards an IoT-based IDS,' J. Eng. Sci. Technol., vol. 17, no. 5, pp. 1–15, 2022.

[28] X. Jing, Q. Yan, and W. Lou, 'Lightweight and efficient intrusion detection system for resource-constrained IoT devices,' High-Confidence Comput., vol. 2, no. 2, pp. 1–10, 2022.

[29] S. Almasoud and A. M. Bahaa-Eldin, 'A hybrid deep learning model for intrusion detection system in the Internet of Things environment,' in Proc. 4th Int. Conf. Data Manage., Anal. Innov. (ICDMAI), 2023, pp. 1–6.

[30] W. Sun, Z. Cai, Y. Li, and X. Fang, 'A survey on security aspects of IoT,' J. Netw. Comput. Appl., vol. 111, pp. 1–10, 2018.

[31] A. Gendreau and M. Moorman, 'Complex event-processing IDS for Internet of Things,' in Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., 2016, pp. 1–7.

[32] M. Solanki, K. Patel, and R. Kumar, 'A lightweight decision tree-based intrusion detection framework for IoT environments,' Comput. Secur., vol. 121, pp. 1–15, 2022.

[33] S. Murali and A. Jamalipour, 'A taxonomy of machine learning-based intrusion detection systems for the Internet of Things: A survey,' IEEE Internet Things J., vol. 9, no. 12, pp. 9444–9466, 2022.

[34] L. Cai, Y. Liu, J. Xu, and M. Jin, 'A comprehensive study of adversarial attacks against machine learning models for IoT intrusion detection,' IEEE Trans. Ind. Informat., vol. 19, no. 5, pp. 1–10, 2023.

[35] R. Reyes-Acosta, C. Dominguez-Baez, R. Mendoza-Gonzalez, and M. Vargas-Martin, 'A hybrid deep learning model for intrusion detection in IoT networks,' Comput. Secur., vol. 130, pp. 1–10, 2023.

[36] W. Almobaideen, S. Al-Mobaideen, and K. AlAzab, 'A lightweight decision tree-based intrusion detection framework for IoT,' IEEE Internet Things J., vol. 10, no. 1, pp. 1–10, 2023.

[37] L. Liu, X. Zhang, and H. Wang, 'An intrusion detection method for IoT based on objective prejudgment and frequency self-adjustment,' EURASIP J. Wirel. Commun. Netw., vol. 2018, art. no. 113, 2018.

[38] K. V. V. N. L. S. Kiran, A. Rao, and R. Singh, 'Machine learning classifiers for identifying attacks in IT networks,' in Proc. 5th Int. Conf. Comput., Commun. Autom. (ICCCA), 2020, pp. 1–6.

[39] S. B. Hussain, M. Ali, and F. Ahmad, 'A hybrid approach for cyber threat detection in IoT networks using federated deep learning,' Sensors, vol. 23, no. 1, pp. 1–15, 2023.

[40] C. V. Nguyen, T. T. Tran, and P. H. Le, 'A hybrid ensemble learning-based intrusion detection system for IoT,' Sensors, vol. 23, no. 2, pp. 1–15, 2023.

[41] C. V. Nguyen, T. T. Tran, and P. H. Le, 'FLARE: A feature-based lightweight aggregation for robust evaluation of IoT intrusion detection,' Sensors, vol. 23, no. 3, pp. 1–15, 2023.

[42] S. Suwais, H. Alqahtani, and M. Alghamdi, 'A hybrid model for intrusion detection in IoT networks using federated learning and blockchain,' IEEE Access, vol. 12, pp. 1–10, 2024.

[43] *S. Reynaud and A. Roxin, 'Review of eXplainable Artificial Intelligence for cybersecurity systems,' Discover Artificial Intelligence*, vol. 5, art. no. 78, 2025.

[44] M. Abomhara and G. M. Køien, 'Security and privacy in the Internet of Things: Current status and open issues,' J. Cyber Secur. Mobility, vol. 4, no. 1, pp. 1–20, 2015.

[45] S. Mann and R. Singh, 'A state-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions,' IEEE Access, vol. 9, pp. 1–15, 2021.

[46] X. Chen, Z. Chen, and Y. Ma, 'A survey on IoT interface positioning and localization,' IEEE Access, vol. 6, pp. 1–10, 2018.

[47] M. Abomhara and G. M. Køien, 'An overview of security threats in the Internet of Things,' Int. J. Wireless Mobile Netw., vol. 7, no. 1, pp. 1–15, 2015.

[48] P. M. and D. S. D. K., 'ICN scheme and proxy re-encryption for privacy data sharing on the blockchain,' Int. J. Comput. Eng. Res. Trends, vol. 10, no. 4, pp. 172–176, 2023.

[49] S. Peter, R. K. Gupta, and V. Yadav, 'Comparative analysis of DDoS attack detection techniques in IoT networks,' J. Netw. Comput. Appl., vol. 102, pp. 1–12, 2018.

[50] S. Mehmood, M. Imran, and T. Talib, 'A review on machine learning-based intrusion detection systems for IoT,' IEEE Access, vol. 9, pp. 1–15, 2021.

[51] A. Gendreau and M. Moorman, 'Complex event-processing IDS in IoT: Design approach,' in Proc. IEEE Conf. Dependable Syst. Netw. (DSN), 2016, pp. 1–7.

[52] V. Pai, 'Systematic approach for malware detection in IoT devices,' Journal of Cloud Computing, vol. 2025, art. no. 00939, 2025. doi: 10.1007/s44196-025-00939-9

[53] H. Zhang, 'Development of an intelligent intrusion detection system for IoT using ensemble deep learning,' Springer Nature Computer Science, vol. 2025, art. no. 00177, 2025. doi: 10.1007/s43926-025-00177-7

[54] H. G. A. Umar, 'Energy-efficient deep learning-based intrusion detection for IoT networks,' Journal of Cloud Computing, vol. 2025, art. no. 00762, 2025. doi: 10.1186/s13677-025-00762-9

[55] M. S. Ahsan and A.-S. K. Pathan, 'A comprehensive survey on access control models in IoT: State-of-the-art,' IoT, vol. 6, no. 1, art. no. 9, 2025. doi: 10.3390/iot6010009

[56] O. A. Alimi, 'Data-driven learning models for Internet of Things security,' Technologies, vol. 13, no. 5, art. no. 176, 2025. doi: 10.3390/technologies13050176