

Cyber Attacks in the Internet of Things (IoT) and Intelligent Defense Mechanisms

Esraa Mohssin Ward^{1,*}, Seyed Amin Hosseini Seno²

¹Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, Razavi Khorasan, IRAN.

²Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, Razavi Khorasan, IRAN.

*Corresponding Author: Esraa Mohssin Ward

DOI: <https://doi.org/10.31185/wjcms.532>

Received 09 June 2026; Accepted 22 August 2026; Available online 30 September 2026

ABSTRACT: The Internet of Things (IoT) has connected billions of physical objects to the internet, enabling smarter homes, manufacturing, critical infrastructure, transportation, and healthcare. However, IoT ecosystems are increasingly vulnerable to cyberattacks due to the growing number of resource-limited devices, weak authentication techniques, and insufficient security deployments. Common threats include ransomware targeting smart firmware and home systems, Man-in-the-Middle (MITM) attacks intercepting device-to-device communication, and Distributed Denial of Service (DDoS) attacks exploiting compromised IoT devices as botnets. Because of their decentralized nature and limited computational resources, traditional security solutions such as firewalls and signature-based intrusion detection systems (IDSs) are not sufficient for IoT environments. Although many studies have addressed IoT security, a key gap remains in systematically reviewing and comparing recent intelligent and adaptive defense mechanisms for highly distributed and resource-constrained IoT systems. This study fills this gap by reviewing major IoT cyberattacks and analyzing intelligent defense strategies based on machine learning (ML), deep learning (DL), blockchain, and federated learning. ML and DL models are widely used for anomaly detection, traffic classification, and automated threat response, while blockchain enables secure authentication and decentralized trust management. Federated learning and lightweight encryption further support secure computation in constrained devices without significant performance loss. However, challenges remain in ensuring user privacy, achieving real-time detection, and balancing energy consumption with security requirements. The findings of this review show that proactive, cooperative, and self-healing security mechanisms are more effective than traditional reactive approaches. The study also provides recommendations for developing scalable, energy-efficient, and privacy-preserving IoT security frameworks for future research.

Keywords: Cybersecurity, Internet of Things (IoT), IoT Attacks, Intelligent Defense Mechanisms, Machine Learning Security.



1. INTRODUCTION

In recent years, several sectors such as smart cities, manufacturing, and healthcare have been influenced by the increasing use of smart devices, often referred to as the Internet of Things (IoT). With over a billion IoT connections expected, IoT growth has become broadly important. Given the critical role of IoT in such sectors, protecting it against financial loss, system failures, and security breaches is essential. However, this rapid expansion has introduced significant cybersecurity challenges, which remain unresolved in existing IoT security solutions [1].

The IoT architecture comprises the application layer, the terminal perception layer, and the network layer. Due to their resource constraints, heterogeneity, and large-scale deployment, IoT systems are highly vulnerable to a wide range of security threats. Ensuring secure operation in such environments remains a complex and open research problem. In addition, IoT introduces challenges in data processing, trust management, standardization, privacy preservation, interoperability, storage, and device authentication, all of which must be addressed to achieve a reliable and secure IoT ecosystem [2].

Although many traditional security mechanisms have been proposed, they are not fully effective in IoT environments due to their limited adaptability to resource-constrained and distributed architectures. Therefore, general security strategies that consider the specific requirements of IoT contexts are necessary. Existing security frameworks for information and wireless networks must be redesigned to handle lossy communication, global connectivity, and device limitations in IoT systems. Conventional approaches such as application security, network security, authentication, encryption, and access control often fail to provide sufficient protection in this context [3].

Despite the large number of existing survey studies on IoT security, most of them focus either on specific attack types or isolated defense mechanisms. There is still a lack of a comprehensive and up-to-date review that systematically integrates recent intelligent defense approaches, particularly those based on machine learning (ML), deep learning (DL), and blockchain technologies. This gap motivates the need for a more structured analysis of modern IoT security strategies.

To address this gap, this study aims to review major cyberattacks targeting IoT systems and to analyze intelligent defense mechanisms designed to mitigate them. The novelty of this work lies in its focused comparison of recent AI-driven and blockchain-based security solutions and in providing a structured synthesis of their strengths and limitations.

The rest of this study is structured as follows: the background and typical IoT attacks are reviewed in Section 2; intelligent defense techniques are covered in Section 3; the literature is compared in Section 4; and findings, recommendations, and conclusions are presented in Sections 5 and 6.

2. BACKGROUND

An advanced network of linked devices with the ability to gather, share, and act upon data is known as the Internet of Things (IoT). This network includes a wide range of gadgets, from commonplace home appliances such as wearable fitness trackers, smart thermostats, and refrigerators to sophisticated industrial machinery such as robotic arms, sensors, and automated manufacturing systems. Basically, IoT develops functionality, automation, and efficiency by integrating digital intelligence into physical things and letting them connect with centralized systems and with each other. The IoT has expanded as a result of several technological enhancements. Smart gadgets that can observe and handle agents in real life have been made feasible by the availability of fairly priced sensors and actuators. Seamless device connectivity has been enabled by the broad usage of wireless communication technologies such as cellular networks, Wi-Fi, high-speed internet, and Bluetooth. To control and analyze the broad amounts of data produced by IoT devices, edge computing and cloud computing are necessary, and they facilitate well-informed decision-making [5].

2.1 ARCHITECTURE OF THE IOT

The architecture of IoT has been explained in various ways. The processing, perception, application, and transmission layers are the four general elements of IoT architecture [4].

(1) The perception layer is in charge of fully perceiving external information, collecting different kinds of data from sensor nodes, and obtaining transmission and aggregation of data through radio frequency readers, sensor networks, and other devices and networks [4].

(2) The information collected by the perception layer is consistently and securely transferred to the transport and information-processing layer. Mobile communication networks, the internet, and satellite networks are examples of the network infrastructure that enables the transport layer functions [4].

(3) Information transferred by the transmission layer can be computed and processed by the processing layer. Significant technologies such as intelligent computing, parallel computing, data mining, and cloud computing are studied here [4].

(4) After intelligent processing, the data is used by the application layer. It creates the appropriate business plan and operates the appropriate application system in accordance with user requirements [4].

2.2 TYPES OF CYBER ATTACKS IN IOT

Attacks are acts carried out to damage a system or interfere with regular operations by taking advantage of weaknesses using a variety of methods and resources. Attackers carry out attacks to accomplish objectives for compensation or personal fulfillment. Attack cost is the measurement of an attacker's effort, defined in terms of resources, motivation, and level of experience. Attack actors are those who pose a risk to the online environment; they might be thieves, hackers, or even governments. Attacks themselves can take many forms, such as close-in attacks, insider exploitation, passive attacks like monitoring unprotected network communications to decrypt weakly encrypted traffic and obtain authentication information, and active network attacks. The following are typical forms of cyberattacks [6]:

(a) Physical attacks: hardware components are tampered with in these attacks. Since the Internet of Things is dispersed and unsupervised, the majority of its gadgets usually function outdoors, which makes them extremely vulnerable to physical assaults.

(b) Reconnaissance attacks: unauthorized identification and mapping of systems, services, or vulnerabilities. Network port scanning, packet sniffing, traffic analysis, and submitting inquiries regarding IP address details are a few instances of reconnaissance attacks.

(c) Denial-of-service (DoS): In the Internet of Things, DoS attacks include tactics like jamming, in which disruptive signals prevent valid communication, in an effort to interfere with service availability. To lessen these attacks on Industry 4.0 technologies, several strategies are employed. For instance, jamming is detected by the Packet Delivery Ratio (PDR)

and signal strength monitoring. Attacks using spoofing and Sybil take advantage of flaws in wireless communication; defenses include auxiliary fields for identity verification and channel-based detection. Content-chaining protects packet integrity by preventing replay attacks caused by fragmentation. Splitting buffer space makes it more difficult for attackers to target device resources in buffer reservation attacks. To defend against replay attacks, CoAP security makes use of 6LBR message filtering and TLS-DTLS tunneling. To preserve routing integrity, sinkhole attacks that reroute network traffic are countered by parent fail-over techniques and rank verification. Adjusting communication timing and managing trust are two ways to combat wormhole assaults that manipulate message relays [7]. The DoS assaults and related defenses are depicted in Fig. 1.

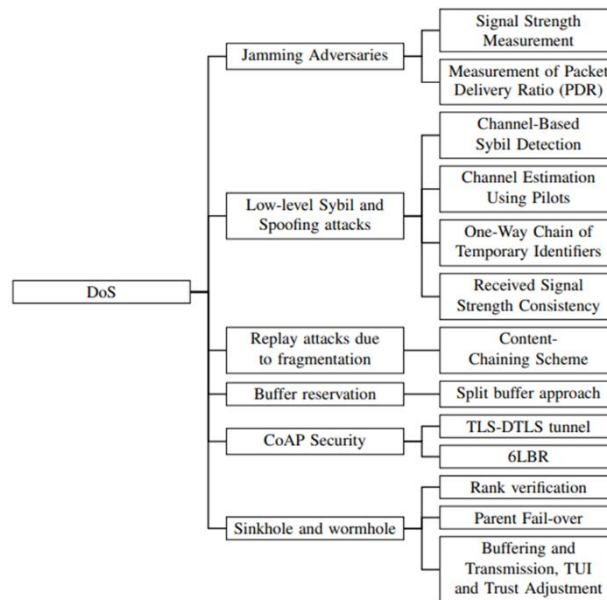


Fig 1. DoS assaults and suggested defenses [7]

(d) Access attacks: these occur when unauthorized users obtain access to equipment or networks that they are not allowed to use. Access attacks come in two varieties. The first is physical access, in which the attacker obtains physical access to a device. The second method involves gaining remote access to devices that are connected to IP.

(e) Privacy attacks: because so much data is readily accessible through remote access methods, protecting privacy in the Internet of Things has grown more difficult. The most frequent threats to user privacy include data mining, which allows attackers to find information in databases that they would not expect; cyber espionage, the use of harmful software and intrusion techniques to spy on or obtain private information about people, businesses, or governments; eavesdropping, the practice of listening in on a conversation between two parties; tracking, in which a device's unique identifier (UID) is used to track a user's movements; and password-based attacks, in which attackers try to replicate a legitimate user's password.

(f) Destructive attacks: large-scale disruption and destruction of property and life. Retaliation assaults and acts of terrorism are two instances of destructive attacks.

(g) Attacks on Supervisory Control and Data Acquisition (SCADA): the SCADA system is susceptible to numerous cyberattacks, just like any other TCP/IP system. The system could be attacked by denial-of-service attacks to bring it to a halt, or by taking over the system with viruses or Trojan horses. For example, a virus called Stuxnet was used in an attack on an Iranian nuclear facility in Natanz.

3. INTELLIGENT DEFENSE MECHANISMS

Machine learning algorithms for classification have advanced to the point that they are now among the most often utilized detection methods for malware in DDoS attacks. The recently suggested detection methods listed below can be applied to a successful DDoS defense.

The following subsections present representative intelligent defense mechanisms selected from the literature to illustrate how machine learning and deep learning techniques are practically applied for IoT cyberattack detection. These approaches were chosen because they represent different deployment scenarios, including cloud-assisted malware detection, gateway-based traffic monitoring, and deep learning-based network anomaly detection.

3.1 IMAGE TRAINING TO DETECT IOT MALWARE BOTNETS

A lightweight method for identifying DDoS malware is suggested, particularly for malware developing in the IoT context [8]. Various malware behaviors are identified and analyzed using image processing. First, one-channel grayscale images translated from malware binary files are extracted. A lightweight convolutional neural network is then used to differentiate between various IoT malware families. Because it attempts to eliminate other malware to obtain sufficient

computational resources for itself, IoT malware behaves somewhat differently from conventional malware. Convolutional neural networks (CNNs) are used for lightweight classification because, unlike SVM and K-nearest neighbors, they do not require hand-crafted features. Malware filters are deployed on cloud servers to get around the resource and memory limitations of IoT. Cloud servers also offer superior defense against DDoS-induced node failures and facilitate regular malware database updates. The remote cloud-based system therefore features a two-tier detection architecture that first identifies suspicious binaries locally before sending them to a remote cloud server for in-depth analysis. A binary image of malware is reformatted as an 8-bit sequence and transformed into a one-channel grayscale image with pixel values ranging from 0 to 255 before classification. Because it processes quickly and only needs an 8-bit vector to transform the binaries into images for the CNN, this technique is far superior to typical signature matching. Owing to its deep-learning-based automatic feature extraction and superior test efficiency, the CNN emerges as an effective classifier.

CNN-based malware classification is particularly effective because it automatically learns discriminative features from malware images without requiring manual feature engineering. In the original study, the proposed lightweight CNN achieved high malware classification performance while maintaining low computational overhead, making it suitable for cloud-assisted IoT security environments. Typical evaluation metrics for such models include classification accuracy, precision, recall, F1-score, and false positive rate, which together provide a comprehensive assessment of detection capability.

3.2 AN IOT MIDDLEBOX WITH MACHINE-LEARNING-BASED DETECTION

To monitor the traffic between consumer IoT devices and the internet, a machine learning solution for DDoS defense integrates a smart-home LAN with a gateway router (middlebox) [9]. With the aid of several machine learning algorithms, including neural networks, it uses IoT-specific network characteristics, such as the restricted number of endpoints and the regular time interval between packets, to perform feature selection and achieve higher accuracy in detecting DDoS in IoT network traffic. The anomaly detection process has several stages: traffic capture, packet grouping by device and time, feature extraction, and binary classification. The capture procedure records the source IP address, source port, destination IP address, destination port, packet size, and timestamp of every IP packet sent by an IoT device in a smart-home application. The three most prevalent DDoS attack types, a TCP SYN flood, a UDP flood, and an HTTP GET flood, are all replicated. Packets are grouped by source IP and separated into non-overlapping time windows. Feature extraction produces both stateless features, lightweight features derived from flow-independent characteristics such as packet size and inter-packet interval, and stateful features, which capture aggregated flow information such as bandwidth and IP address cardinality and novelty over brief time periods. Binary classification is then performed using K-nearest neighbors, random forests, support vector machines, and deep neural networks. Decision tree algorithms and K-nearest neighbors were determined to be the most accurate.

The effectiveness of ML-based middleboxes is commonly evaluated using accuracy, detection rate (true positive rate), false positive rate, and processing latency. These metrics are particularly important in IoT environments because excessive false alarms or delayed detection may negatively affect the availability of smart-home services. A practical example is the deployment of ML-enabled gateway routers that monitor smart cameras, smart TVs, and voice assistants, where abnormal traffic generated by DDoS attacks can be detected before reaching external networks.

3.3 NETWORK-BASED ANOMALY DETECTION IN IOT USING DEEP LEARNING

Deep learning models are used to identify anomalies in the IoT network [10]. The dense and complex architecture of deep learning models, which use numerous layers to train, test, and predict, makes them among the most accurate classification methods, so this approach can be viewed as a more comprehensive form of machine-learning-based defense. Deep autoencoders are employed independently for each type of IoT device in the network. The advantage of autoencoders is their ability to encode and compress data optimally, which suits the restrictions of IoT. Autoencoders condense the gathered normal IoT communication snapshots; when the autoencoder cannot restore a recorded snapshot to its basic shape, suspicion in the traffic is identified. Compared with other ML algorithms, the offered strategy produces fewer false positives.

Deep autoencoder-based anomaly detection is especially suitable for IoT environments because it learns the normal communication behavior of individual devices without requiring labeled attack data. Performance is generally assessed using accuracy, detection rate, precision, recall, F1-score, and false positive rate. This approach is particularly useful in industrial IoT and smart healthcare systems, where early detection of abnormal communication can significantly reduce the impact of cyberattacks while maintaining normal network operations.

4. LITERATURE REVIEW

The rapid spread of IoT devices across various sectors such as transportation, smart homes, and healthcare has brought about a novel era of pervasive connectivity. As a result, IoT infrastructures are now vulnerable to a broad range of threats such as DDoS assaults, Man-in-the-Middle intrusions, malware infections, and botnet exploitation, as this enormous proliferation has expanded the cyberattack surface. Investigators have offered a broad range of security measures to guarantee secure and dependable IoT functions, ranging from ML- and DL-driven IDSs to access control and conventional encryption. In addition to grouping prevalent cyberthreats that target different IoT ecosystem layers,

this section presents a general overview of IoT architecture and critically evaluates the pros and cons of present protection tactics.

Rather than only describing existing studies, this review critically compares recent IoT security solutions in terms of their detection capability, computational efficiency, scalability, and practical deployment. Particular attention is given to identifying common limitations across existing approaches, including high computational complexity, limited real-time applicability, insufficient support for resource-constrained IoT devices, and the lack of unified evaluation benchmarks.

Alkhudaydi et al. apply ML and DL approaches to accurately extract significant components from a real-network IoT traffic dataset, then evaluate how well 10 distinct ML strategies detect malware, including four DL architectures (RNN, LSTM, GRU), ensemble classifiers (LGBM, Extra Trees, AdaBoost), and single classifiers (SVM, KNN) [11].

Using a DL model, Saharkhizan et al. present a way to detect cyberattacks in IoT methods. The model combines LSTM units into a joint detector, which is integrated using a decision tree (DT) to produce a single output [12].

Alattas and Mardani offer a structural model for trade producers such as transportation that conveys a stochastic dimension of launching restrictions using a novel adaptive deep learning (ADL) method. The structure incorporates an arbitrary conflict component and depends on five protection steps that scale the IDS and forensic system [13].

Maghrabi et al. focus on the Golden Jackal Optimizer in the IIoT network with the DL-driven Cyber Threat Detection and Classification (GJODL-CADC) technique. The system uses a GJO-based feature selection approach, followed by a multiple auto-encoder-driven deep belief network (AE-DBN). The pelican optimization algorithm (POA) improves efficiency [14].

Farhin et al. apply software-defined networks (SDNs) to enhance attack identification for IoT. SDNs analyze the traffic stream, block source nodes and outside traffic, and spot anomalies. Side-network attacks, bad-code attacks, Man-in-the-Middle attacks, and DDoS can all be identified using a fuzzy neural network (FNN)-based method [15].

Bhattacharjee et al. develop a CNN-based IDS for network security. For grouping network intrusions, the model classifies whole-system packet traffic as either malicious or benign. Four experimental DL methods were used: logistic regression, CNN, RF, DNN, and AdaBoost [16].

Vijayalakshmi and Karthika provide a combined DL method, DCCNN-SMO, that integrates the Spider Monkey Optimizer (SMO) with a Hybrid Dual-Channel CNN (DCCNN) [17].

Tawfik et al. devise a middleware-based strategy that incorporates ML methods to provide automated defense against cyberattacks on SDN-controlled IoT systems [18].

Presekal et al. define a multiple DL model that integrates a deep convolutional network with Graph Convolutional Long Short-Term Memory (GC-LSTM) [19].

Nanjappan et al. propose DeepLG SecNet, which integrates Crossover Chaos Game Optimization (CCGO) with DL strategies such as a gated Secure Network (SecNet) and LSTM [20].

Sarker et al. study the IoT paradigm with a focus on smart adjustments that employ IoT, discuss security problems of ML solutions, and investigate DL and ML methods that could improve IoT security, exploring feasible future approaches [21].

Ahmed and Askar propose a complete examination of security rules in the IoT context, focusing on cybersecurity and the combination of AI models to solve security risks, stressing the significance of DL methods [22].

Mohanta et al. discuss security concerns such as accessibility, confidentiality, and integrity across many layers, providing an overview of IoT and its uses and a complete analysis of blockchain, ML, and AI methods for security [23].

Idrissi et al. present a recent IoT security study examination focused on analyzing IDSs, particularly DL-based ones, and propose a classification system that links security risks to the related Cisco IoT reference model components [24].

Babu and Veena carry out a broad study analysis presenting the features and issues of applying DL and ML to IoT security [25].

Aversano et al. provide a complete overview of the IoT security area with a systematic review focused on application areas, security issues, datasets, and DL architecture implementation, classifying DL strategies [26].

Ahanger et al. present a study summary grouping research by IoT vulnerabilities, attacker types, and risks and consequences, exploring enterprise authentication technologies, weak points, and workable fixes, and discussing real-life techniques for handling broad harmful IoT devices [27].

Wu et al. analyze IoT security solutions, examining four main security issues relevant to DoS assaults, device authentication, and defenses against DDoS attacks, and investigate the use of AI methods such as ML and DL, with a focus on IDS and malware detection [28].

Thakkar and Lohiya group several IDS installation and analysis methods in IoT architecture, cover various intrusion types, and examine DL and ML strategies for IoT network threat detection, concluding that new IoT detection methods remain insufficient against various assaults [29].

Farooq et al. examine the basic security issues and open challenges in IoT infrastructure, analyze developed ML-driven strategies, and suggest the development of lightweight ML-driven security solutions and a layered strategy [30].

Al-Garadi et al. present a complete analysis of ML and DL strategies for strengthening security protocols in IoT systems and safeguarding the application, perception, and network layers, investigating known and unknown risks, feasible attack levels, and the advantages and disadvantages of each approach [31].

Yue et al. examine DL applications in the IoT security and privacy context from the standpoint of system architecture and methods, and present a novel method that uses a functional layer to enable meaningful device modeling for accurate device identification [32].

Ahmad and Alsmadi perform a Systematic Literature Review of big data, machine learning, cybersecurity, and the Internet of Things, discussing ML algorithms used to improve IoT security, the vulnerability of large-scale IoT attacks, and methods used to identify and mitigate such attacks [33].

Mrabet et al. present an improved IoT architecture with five layers, introduce a new classification of security concerns and attacks, and highlight open research topics such as standardized encryption, the potential of ML, and the use of blockchain technology [34].

Da Costa et al. investigate recent enhancements in IDS and smart methods applied in IoT to safeguard data, with a focus on ML applications [35].

Hassija et al. analyze security issues and threat sources for IoT applications, considering launched and novel technologies such as ML, fog and edge computing, and blockchain, and discussing problems at the application, measurement, gateway, middleware, and network layers [36].

Zeadally and Tsikerdekis examine ML strategies for network- and host-level security developments in IoT [37].

Geetha and Thilagam study the research body on ML and DL strategies for cybersecurity threats, presenting a categorization of algorithms and examining their use for recognizing different attack types [38].

Khan et al. explain the intricacies and issues of computer networks and IoT regarding dependability, secrecy, security, and privacy, and evaluate IDSs using metrics such as false alarm rate, accuracy, detection rate, recall, and F1 score [39].

Salih et al. analyze a cyberattack dataset and emphasize the significance of applying DL and ML methods in cybersecurity [40].

Ravikumar et al. present a broad IoT analysis investigating security concerns at each IoT tier and the advantages and disadvantages of using DL techniques for IoT security [41].

Erfan et al. propose a blockchain-based IIoT security framework that integrates decentralized federated learning and CNN for detecting Sybil attacks, achieving an average detection accuracy of 91.13% and recall of 91.37% [42].

Alauthman et al. introduce an HHO-optimized deep Q-network (DQN) for adaptive Web of Things security. Evaluation on the CIC-IoT-2023 and Bot-IoT datasets demonstrates faster convergence and higher accuracy than several conventional reinforcement learning approaches [43].

Ramya et al. propose a hypergraph-based authentication scheme integrated with a pre-authentication IDS to protect IoT systems against DoS and DDoS attacks. The proposed approach achieves 98.7% detection accuracy with a 1.1% false-positive rate and low computational overhead [44].

Abi Sen et al. develop a hybrid IoT security framework combining blockchain, deep learning, and fog-based aggregation for adaptive cyberattack detection. Experiments on the IoT-23 dataset achieve an average accuracy above 89% and a PR-AUC of approximately 90% [45].

Sankaran et al. propose a Quantum Federated Learning framework for privacy-preserving intrusion detection in Industrial IoT environments. The approach aims to improve detection accuracy, convergence, response time, and energy efficiency while reducing the computational burden on IIoT devices [46].

Table 1. Comparative analysis of IoT security and cyberattack detection methods

Study	Technique / Model Used	Accuracy	Scalability	Strengths	Limitations
Alkhudaydi et al. [11]	Multiple ML & DL classifiers (KNN, SVM, Extra Trees, LSTM, GRU)	High	Moderate (multiple models increase computational cost)	Comprehensive comparison of models on a real BoT-IoT dataset	High computation due to many models; no focus on lightweight solutions
Saharkhizan et al. [12]	Hybrid LSTM + decision tree	High	Moderate (not validated for large-scale real-time IoT)	Improved detection accuracy via ensemble fusion	Lacks real-time validation; no evaluation on diverse IoT devices
Alattas & Mardani [13]	Adaptive deep learning (ADL)	High	Low (complex architecture for resource-constrained devices)	Dynamic thresholding improves intrusion response	Architecture complexity unsuitable for low-power IoT nodes
Maghrabi et al. [14]	Optimizer-based DL (AE-DBN + GJO + POA)	High	Low (meta-heuristic optimization increases latency)	Enhanced feature selection and classification	Heavy meta-heuristic algorithms; high latency
Farhin et al. [15]	Fuzzy neural network (FNN)	Moderate	Moderate (SDN improves management but scalability remains limited)	Capable of detecting multiple attack types	Limited scalability in large SDN-based IoT networks

Bhattacharjee et al. [16]	CNN-based IDS	High	Moderate (CNN suitable for packet classification but computationally intensive)	High detection accuracy for packet classification	CNNs may struggle with temporal dependencies in traffic
Vijayalakshmi & Karthika [17]	Hybrid CNN + optimizer (DCCNN-SMO)	High	Low (optimization-based training overhead)	Improved convergence and robustness	Requires high training overhead
Tawfik et al. [18]	Middleware-based ML defense	High	Moderate-High (middleware facilitates deployment)	Integrable at network level for automated protection	Limited visibility into device-level attacks
Presekal et al. [19]	Graph-based DL (GC-LSTM + CNN)	High	Low (graph computation increases complexity)	Captures spatial-temporal traffic relations	Graph modeling adds complexity
Nanjappan et al. [20]	LSTM + Secure Network (SecNet) + CCGO	High	Moderate (hybrid architecture without lightweight evaluation)	Strong hybrid architecture with optimization	No assessment on lightweight deployment
Sarker et al. [21]	Survey on ML/DL in IoT security	Not evaluated (Survey)	Not evaluated	Broad insights into current approaches	Lacks implementation or benchmarking
Ahmed & Askar [22]	Review on AI in IoT security	Not evaluated (Review)	Not evaluated	Highlights AI advantages in intrusion defense	No comparison across threat models
Mohanta et al. [23]	Review of ML, AI & blockchain	Not evaluated (Survey)	Not evaluated	Multidimensional perspective across layers	More conceptual, less technical evaluation
Idrissi et al. [24]	Review of DL-based IDS	Not evaluated (SLR)	Not evaluated	Classifies threats using the Cisco IoT model	No unified benchmark across studies
Babu & Veena [25]	Review on ML/DL challenges	Not evaluated (Survey)	Not evaluated	Identifies key obstacles in deployment	No proposed mitigation strategies
Aversano et al. [26]	Systematic review on DL for IoT security	Not evaluated (Systematic Review)	Not evaluated	Well-organized taxonomy of DL architectures	No analysis of hardware requirements
Ahanger et al. [27]	Vulnerability & attack classification	Not evaluated (Survey)	Not evaluated	Includes real-time mitigation strategies	Focused more on threat analysis than defense
Wu et al. [28]	Survey on AI-enhanced IoT security	Not evaluated (Survey)	Not evaluated	Covers DoS, authentication, and DDoS defense	Limited technical benchmarking
Thakkar & Lohiya [29]	Review of IDS for IoT	Not evaluated (Review)	Not evaluated	Groups IDS methods and intrusion types	Insufficient coverage of new detection methods
Farooq et al. [30]	Review of ML-driven IoT security	Not evaluated (Review)	Not evaluated	Highlights lightweight, layered strategies	Limited empirical evaluation
Al-Garadi et al. [31]	Survey of ML/DL for IoT security	Not evaluated (Survey)	Not evaluated	Covers all main IoT layers	Largely conceptual
Yue et al. [32]	Survey on DL for IoT security	Not evaluated (Survey)	Not evaluated	Novel functional-layer device modeling	Limited real-world deployment
Ahmad & Alsmadi [33]	Systematic literature review	Not evaluated (SLR)	Not evaluated	Links big data, ML, and IoT security	No experimental benchmarking
Mrabet et al. [34]	Five-layer IoT architecture review	Not evaluated (Survey)	Not evaluated	New classification of attacks and layers	Conceptual; limited validation
Da Costa et al. [35]	Survey on ML-based IDS	Not evaluated (Survey)	Not evaluated	Focus on smart IDS methods	Limited dataset diversity
Hassija et al. [36]	Survey on IoT security threats	Not evaluated (Survey)	Not evaluated	Covers blockchain, fog/edge, ML	Broad, less technical depth
Zeadally & Tsikerdekis [37]	ML for IoT security	Not evaluated (Survey)	Not evaluated	Network- and host-level techniques	Limited algorithmic detail

Geetha & Thilagam [38]	Review on ML/DL attack detection	Not evaluated (Review)	Not evaluated	Clear taxonomy of algorithms	No performance benchmarks
Khan et al. [39]	Review of intrusion detection models	Not evaluated (Review)	Not evaluated	Evaluated with performance metrics	No discussion on resource usage
Salih et al. [40]	Dataset-based ML/DL security study	Not evaluated (Survey)	Not evaluated	Highlights importance of ML/DL	Limited dataset diversity
Ravikumar et al. [41]	Review on IoT security & DL	Not evaluated (Review)	Not evaluated	Covers attack risks at each IoT level	Limited real-world validation
Erfan et al. [42]	Decentralized FL + CNN + Blockchain	Moderate	High	Privacy-preserving Sybil detection	Communication overhead
Alauthman et al. [43]	HHO-optimized DQN	High	High	Faster convergence; adaptive detection	Model complexity
Ramya et al. [44]	Hypergraph Authentication + IDS	High	High	High accuracy; low overhead	Implementation complexity
Abi Sen et al. [45]	Blockchain + DL + Fog	Moderate	High	Adaptive detection; data integrity	Computational overhead
Sankaran et al. [46]	Blockchain + DL + Fog	Not explicitly reported in the provided study description	Promising	Privacy preservation; efficient learning	Privacy preservation; efficient learning

According to the comparative assessment, recent IoT security research has gradually moved away from conventional rule-based techniques toward intelligent detection mechanisms driven by machine learning and deep learning. Hybrid architectures, such as CNNs with meta-heuristic optimizers or LSTM with decision trees, generally achieve higher detection accuracy and better adaptability to evolving attack patterns. However, these improvements are often accompanied by increased computational complexity and higher training costs, which makes them unsuitable for lightweight or resource-limited IoT devices. Survey-based research provides useful taxonomies and identifies new research gaps but generally lacks experimental benchmarking, deployment considerations, and quantitative comparisons across different security solutions. Although AI-based IDSs offer many benefits for protecting IoT infrastructures, lightweight, scalable, and real-life security frameworks that balance accuracy and efficiency are still needed. Furthermore, few studies comprehensively integrate AI-driven detection, blockchain-based trust management, and privacy-preserving techniques within a unified security framework. These limitations highlight important research gaps and motivate the development of more adaptive and practically deployable IoT defense mechanisms.

5. RESULTS AND COMPARATIVE ANALYSIS

This section shows the comprehensive analysis outcomes performed on the reviewed papers based on cyber-attacks and smart defense algorithms in IoT areas. Against conventional experimental papers, this review paper's outcome is achieved via present research works' systematic comparison and classification given AI methods, attack kinds, security apps, and recognized issues. The reviewed papers are analyzed to show current paper trends, different AI-driven strategies' efficiency, and the restrictions that hinder the practical smart IoT security solutions deployment. Also, comparative tables and graphical representations are presented for bolding the AI-based cybersecurity algorithms' evolution also recognize potential future research directions.

Table 2. Comparative Analysis of AI Techniques Used in IoT Cybersecurity Research

AI Technique	Representative References	Primary Security Task	Typical Performance	Key Challenges
Deep Learning	[11], [13], [16], [18], [42], [44], [45], [46]	Attack Prediction, Intrusion Detection	High	High computational cost, large training data requirement
Recurrent Neural Networks (LSTM/GRU/DRNN)	[12], [20]	Network Traffic Analysis, Intrusion Detection	High	Long training time, vanishing gradient for long sequences
Hybrid Deep Learning	[17], [19]	Cyberattack Detection, Cyber-Physical System Security	Very High	High model complexity, computational overhead

AI Technique	Representative References	Primary Security Task	Typical Performance	Key Challenges
SDN-based Security	[15], [18]	Network Monitoring and Intrusion Detection	High	Scalability and deployment complexity
Optimization-based Deep Learning	[14], [17], [43]	Intrusion Detection and Model Optimization	High	Parameter tuning, computational overhead
Fuzzy Neural Network	[15]	Intrusion Detection	Moderate–High	Parameter tuning, computational overhead

Table 2 briefs the main AI method developed in the reviewed research articles for IoT cybersecurity. DL is the most broadly adopted strategy due to its robust ability to learn complicated attack models and obtain high diagnosis accuracy. Recurrent neural networks, such as DRNN, LSTM, and GRU, are basically used for network traffic analysis because of their capability to capture temporal dependencies. In addition, hybrid DL models and optimization-related strategies generally present greater diagnosis performance by integrating complementary learning approaches; however, they impose higher computational costs and implementation complexity. SDN-related security frameworks develop network monitoring and centralized attack mitigation, while fuzzy neural networks efficiently control uncertain network manner however might suffer from restricted generalization and scalability. Generally, the comparative analysis shows that obtaining high diagnosis accuracy while keeping computational efficiency is one of the main issues in smart IoT cybersecurity systems.

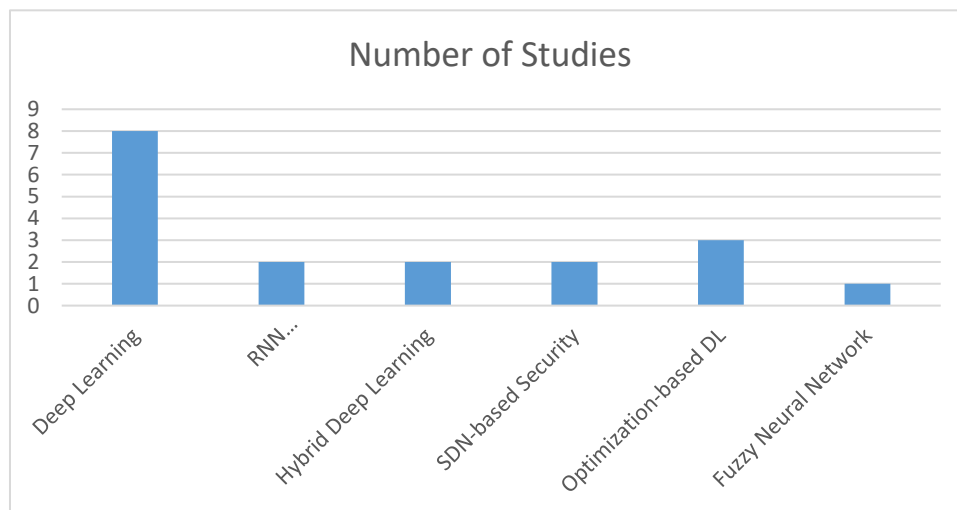


Fig 2. Distribution of Artificial Intelligence Techniques Used in IoT Cybersecurity Research

Figure 2 shows the distribution of AI methods adopted in the reviewed study papers. DL-driven strategies show the dominant group because of their capability to automatically extract complicated features from IoT network traffic. Recurrent neural networks, such as DRNN, LSTM, and GRU, are frequently developed to model temporal dependencies in sequential network data. In addition, hybrid and optimization-related DL frameworks have gained increasing attention because they improve diagnosis performance by integrating several approaches of learning. However, such strategies normally incur additional computational complexity, which is an important issue for resource-limited IoT areas.

Table 3. Distribution of Cyberattack Categories Investigated in IoT Security Research

Cyberattack Category	Representative References	Primary Target Environment	Main Detection Approaches	Key Challenges
Intrusion Detection	[12], [15], [20], [24], [29], [39], [42], [46]	IoT Networks	Deep Learning, LSTM/GRU, Hybrid Models	Unknown and evolving attack patterns
DDoS Attacks	[11], [21], [39], [44]	IoT Communication Networks	Deep Learning-based Detection	High-volume traffic and real-time detection
Industrial IoT Attacks	[13], [14], [19], [41], [45]	IIoT and Cyber-Physical Systems	Hybrid DL, Optimization-based Models	Resource constraints and scalability

Cyberattack Category	Representative References	Primary Target Environment	Main Detection Approaches	Key Challenges
Smart Home Attacks	[18], [23], [36]	Smart Home IoT Systems	SDN and AI-based Security	Heterogeneous devices and privacy issues
Malware/Botnet Attacks	[21], [30], [33], [39]	IoT Devices and Networks	ML/DL Classification Models	Limited labeled datasets
General IoT Security Threats	[22], [27], [31], [34], [43]	Multi-domain IoT Applications	AI, ML, and DL Frameworks	Comprehensive protection of diverse IoT layers

Table 3 briefs the main groups of cyberattacks explored in the reviewed papers. Intrusion detection shows the most broadly studied research direction due to the increasing IoT network traffic complexity as well as the ongoing presence of sophisticated attacks. Some papers have concentrated on industrial IoT areas because of their crucial role in cyber-physical systems and manufacturing apps. Although attacks targeting malware propagation and botnet activities remain challenging due to IoT devices' heterogeneity and resource restrictions. The analysis shows that AI-driven strategies have developed attack diagnosis abilities, improving adaptive and scalable solutions, but threats remain an open study concern.

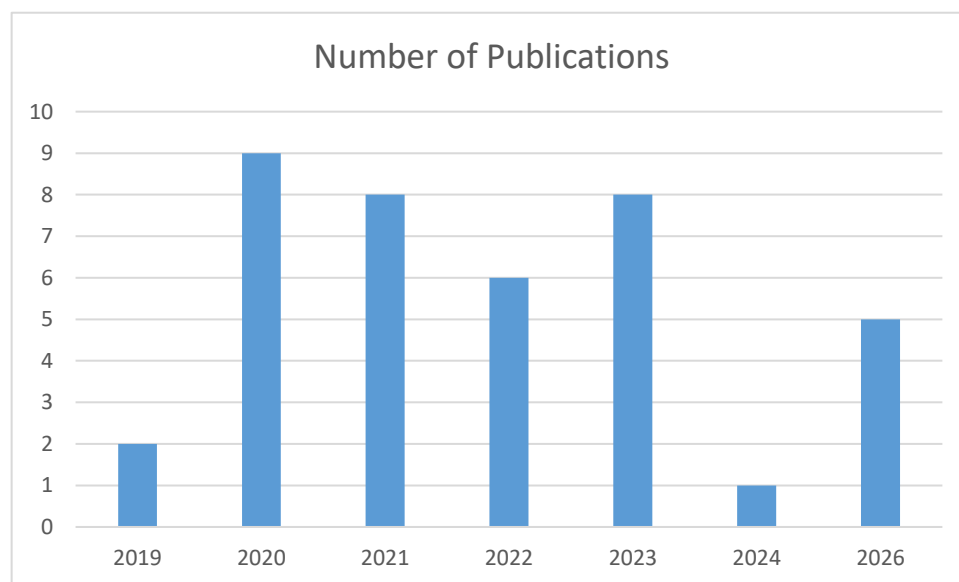


Fig 3. Publication Trend of Reviewed Studies (2019–2026)

Figure 3 shows the research paper's publication trend associated with IoT cybersecurity and smart defense algorithms between 2019 and 2026. The analysis shows an important development in study activity after 2019, with the highest publications' number seen in 2021. This growth reflects the developing IoT technologies' adoption as well as the increasing issues considering cybersecurity vulnerabilities in interconnected areas. However, the publications' number slightly reduced after 2021; research interest remained robust, especially in DL-driven intrusion detection, multiple AI models, and smart defense frameworks. The seen trend shows the ongoing significance of developing adaptive and scalable security solutions for future IoT ecosystems.

Table 4. Dataset Characteristics Used in IoT Cybersecurity Research

Dataset	Domain	Data Type	Attack Categories	Usage in Literature	Key Limitations
NSL-KDD	Network IDS	Network traffic records	DoS, Probe, R2L, U2R	Benchmark evaluation of ML/DL-based IDS models	Outdated traffic patterns and limited IoT representation
UNSW-NB15	Network Security	Flow-based network data	Fuzzers, Exploits, DoS, Worms, Reconnaissance	Evaluation of machine learning and deep learning approaches	Limited IoT-specific device characteristics
CICIDS2017	Network IDS	Packet and flow-based traffic	DDoS, Botnet, Malware, Brute Force, Web attacks	Deep learning validation and intrusion classification	Partially generated traffic and limited IoT scenarios

Dataset	Domain	Data Type	Attack Categories	Usage in Literature	Key Limitations
IoT-23	IoT Networks	Network flows from IoT devices	Malware, Botnet, C&C communication	IoT-specific security analysis	Limited diversity of IoT devices and attacks
Bot-IoT	IoT/IIoT Security	Network traffic traces	Botnet, DDoS, DoS, Reconnaissance	Attack detection and anomaly detection evaluation	Highly synthetic traffic distribution

Table 4 briefs the most broadly adopted sets of data in IoT cybersecurity studies. Traditional sets of data like NSL-KDD and UNSW-NB15 are well-known for benchmarking ML models; although their real-world IoT features' restricted representation decreases their suitability for the IoT areas. More recent sets of data, such as IoT-23 and Bot-IoT, present more realistic IoT traffic models and attack manners; however, challenges like synthetic traffic generation, restricted attack diversity, and class imbalance remain unresolved. So, suitable dataset selection is yet a crucial issue to develop reliable and generalizable AI-driven IoT intrusion detection systems.

Table 5. Performance Comparison of AI-Based IoT Cybersecurity Models

Ref.	Proposed Model	Dataset	Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
[11]	ML/DL models (LSTM, GRU, RNN, XGBoost, CatBoost + SMOTE)	BoT-IoT	Malware/IoT attacks	98.52	98.06	96.54	97.27
[12]	Ensemble Deep RNN (LSTM + Decision Tree)	Modbus network traffic	IoT cyber attacks	99.62	99.42	98.88	99.14
[13]	Adaptive Deep Learning Prediction	Bot-IoT	Industrial IoT attacks	100	N/R	N/R	N/R
[14]	Golden Jackal Optimization + Deep Learning	UNSWNB15 and UCI SECOM datasets	IIoT cyber attacks	98.40	98.41	98.40	98.40
[15]	SDN + Fuzzy Neural Network	NSL-KDD	IoT attack detection	83.00	N/R	N/R	N/R
[16]	Deep Learning IDS Model	NSL-KDD	IoT intrusion detection	97.00	92.00	16.00	81.00
[17]	DCCNN + Spider Monkey Optimization	The dataset was gathered via Google Code Jam (GCJ)	Cybersecurity threats	98.12	98.01	97.90	97.65
[18]	SDN + Deep Learning Middleware	IoTID20	Smart home attacks	98.30	N/R	N/R	85.9
[19]	Hybrid Deep Learning Attack Graph	simulated OT network traffic dataset	Cyber-physical attacks	96.45	N/R	N/R	65.03
[20]	DeepLG SecNet (LSTM + GRU)	NSL-KDD	IoT intrusion detection	98.92	97.81	98.25	98.68
[42]	Decentralized FL + CNN + Blockchain	Public IIoT dataset	Sybil Attack	93.46	93.51	93.46	93.46
[43]	HHO-optimized DQN	CIC-IoT-2023, Bot-IoT	IoT/WoT Cyberattacks	97.81	97.23	97.56	97.39
[44]	Hypergraph Authentication + Pre-authentication IDS	IoT/Edge environment	DoS/DDoS	98.70	98.20	97.80	98.00
[45]	Blockchain + Deep Learning + Dual-chain + Fog	IoT-23	IoT Cyberattacks	90.09	88.88	88.00	88.40

Table 5 shows the present AI-driven IoT cybersecurity strategies' comparative assessment in terms of Recall, F1-score, Accuracy, and Precision. As seen before, most DL-driven strategies obtain high diagnosis performance, showing the smart models' efficiency in recognizing complicated models of cyberattacks in areas of IoT. The ensemble deep

recurrent neural network offered in [12] obtained the highest overall performance with an accuracy of 99.62% and an F1-score of 99.14%, showing the recurrent architectures' ability to efficiently take temporal network traffic features. Likely, the adaptive DL framework in [13] achieved 100% accuracy for industrial IoT attack diagnosis, illustrating the adaptive models' ability for specialized IoT areas.

Optimization-related DL strategies like Golden Jackal Optimization integrated with DL [14] and DCCNN with Spider Monkey Optimization [17] showed competitive performance with accuracy values above 98%. Such outcomes suggest that optimization mechanisms could develop feature selection and model convergence. In addition, hybrid architectures combining LSTM and GRU networks, like DeepLG SecNet [20], obtained balanced performance over F1-score, accuracy, recall, and precision, validating the efficiency of integrating hybrid DL approaches for intrusion detection.

However, SDN-driven strategies [15], [18] present benefits in network management and centralized security control; their performance heavily depends on the developed diagnosis model and dataset features. For instance, the SDN-driven fuzzy neural network in [15] obtained lower accuracy in comparison to other DL techniques. Also, several papers like [16] and [19] reported lower recall and F1-score values, showing issues in diagnosing whole attack groups, especially in imbalanced and complicated IoT traffic scenarios.

Generally, Table 5 shows that DL and multiple AI-driven techniques perform better than conventional strategies in IoT attack diagnosis. However, the high computational complexity, reliance on large-scale labeled sets of data, and restricted generalization over heterogeneous IoT areas are important issues for real-life development.

6. FINDINGS AND RECOMMENDATIONS

The rapid and often haphazard development of IoT devices across different locations presents several complicated difficulties for IoT cybersecurity. In addition to being technical, these concerns cover operational, regulatory, and economic domains, each with unique complications that must be resolved to protect the IoT ecosystem.

The comparative analysis presented in Table 1 indicates that recent IoT security research has increasingly shifted toward AI-driven defense mechanisms. Among the reviewed implementation studies, deep learning and hybrid models generally achieved higher detection performance than conventional machine learning methods, although they often required greater computational resources. Likewise, survey studies consistently identified scalability, computational overhead, privacy preservation, and real-time deployment as the most important open challenges for intelligent IoT security systems.

The heterogeneity of IoT devices, which vary greatly in security needs, hardware abilities, and communication protocols, is one of the most important concerns, and it is particularly significant across application fields [47]. Real-life protection methods are essential for industrial IoT systems to protect crucial operational data and prevent downtime in predictive maintenance. Advanced privacy methods are important for wearable devices used in healthcare and fitness to safeguard sensitive personal data while upholding user consent. Autonomous vehicles require ultra-low-latency communication systems to guarantee secure navigation and resilience against assaults on sensor data and control systems. These examples underscore the importance of field-specific security tactics that consider the distinct operational and legal circumstances of each IoT application [48].

Legacy devices that were not designed with security in mind and are often difficult or impossible to update form another main obstacle. Such devices pose considerable security threats and make up a sizable fraction of the present IoT ecosystem. The coexistence of secure, novel devices with vulnerable, older ones creates a weakest-link concern. Enhancing gateway solutions that serve as a security bridge between legacy devices and the broader network, or retrofitting security features onto present devices, are two creative ways to address this complexity.

These observations are consistent with the reviewed studies, which repeatedly report that high detection performance alone is insufficient if security solutions cannot be efficiently deployed on resource-constrained IoT devices. Therefore, computational efficiency and scalability should be considered alongside detection accuracy when evaluating future defense mechanisms.

Interoperability across IoT devices and systems is another important concern, particularly where tools from several vendors must function together. Important vulnerabilities can arise in the absence of standardized security frameworks and communication protocols, as attackers can exploit gaps between systems. Future research should focus on robust interoperability standards with security as a basic element, comprising not only technical demands but also agreements on accountability and governance between parties.

IoT privacy considerations extend beyond data protection; they include the need to give users control over their data and transparency over its use [49]. The challenge is balancing the importance of datasets, which are often significant for IoT functionality, against the need to protect user privacy. This becomes complex in situations involving broad data collection and analysis, when anonymization may not be enough to prevent re-identification. Although privacy-preserving techniques such as federated learning and secure multi-party computation are interesting research directions, their integration into IoT systems remains hard because of resource restrictions and the need for real-life processing.

Another main security concern is the dynamic and frequently unpredictable nature of IoT environments. Unlike traditional IT systems, IoT networks are decentralized and broadly dispersed, with devices entering and departing the

network regularly. This fluidity makes it hard to detect and react to threats in real time and to maintain consistent security standards. Novel approaches that efficiently control the scale and dynamic nature of IoT networks should be developed, since traditional security monitoring technologies are often not enough. By dispersing trust and reducing single points of failure, methods such as decentralized identity management and distributed ledger technology (DLT) can improve the security and resilience of IoT networks.

The IoT security area is predicted to become even more complicated as a result of present technologies such as edge computing and 5G. These technologies present important performance gains, but they also worsen preexisting weaknesses and open new attack avenues. The move to edge computing, for instance, lowers latency by processing data nearer to its generation point, but it simultaneously expands the attack surface by spreading processing across a large number of potentially insecure edge devices. AI-based security analytics that operate in real time and adapt to shifting threats are among the novel techniques required to safeguard such edge environments.

From a deployment perspective, intelligent security models should satisfy multiple practical requirements, including low inference latency, minimal memory consumption, reduced communication overhead, and compatibility with edge computing platforms [50]. Achieving an appropriate balance between detection performance and resource utilization remains one of the principal challenges for real-world IoT security deployment.

A lot of regions lack sufficient legal frameworks to control the specific complexities of IoT devices, showing that the regulatory area around IoT security is still in its infancy. The lack of clear standards and norms causes a patchwork of security techniques that varies greatly among businesses and regions. Establishing regulatory standards that provide a common foundation for IoT security while allowing for regional settings requires significant international cooperation, including frameworks for data privacy, security, and the ethical use of IoT technology.

Overall, the reviewed implementation studies demonstrate that hybrid deep learning approaches generally outperform conventional machine learning techniques in terms of detection capability, whereas lightweight ML models remain more suitable for resource-limited IoT environments because of their lower computational cost [50]. This trade-off between security performance and deployment efficiency should be considered when selecting defense mechanisms for different IoT applications.

Economics is another significant concern affecting IoT security. Many businesses, particularly in industries with narrow profit margins such as small-scale manufacturing and agriculture, may find the cost of putting advanced security measures in place unaffordable [51]. This financial obstacle often causes security to become less of a priority, leaving weak systems open to abuse. In short, the concerns with IoT cybersecurity are numerous and varied, signifying the need for a multidisciplinary approach that considers legal, operational, and financial factors in addition to technical fixes [52]. Future work must look into creative business models that encourage investment in IoT security and into affordable security solutions that do not sacrifice protection. The focus must be on adaptable, secure, cost-effective, and scalable solutions that can keep up with the rapid development of IoT technology. Combined and robust security measures will be more essential as IoT expands, and ongoing cooperation among government, business, and academia will be essential to guarantee the security and dependability of the IoT ecosystem.

7. CONCLUSION

Connectivity and automation have been greatly developed by the rapid spread of IoT devices across various industries such as industrial systems, healthcare, and smart cities. However, this growth leaves IoT devices vulnerable to various active cyberthreats such as DDoS attacks, Man-in-the-Middle attacks, malware, physical tampering, and botnets. The particular difficulties of IoT environments, such as device heterogeneity, changing network conditions, and resource limitations, are frequently not adequately addressed by conventional security measures such as authentication, encryption, and network-level safeguards.

This review systematically examined recent cyberattacks targeting IoT environments and critically analyzed intelligent defense mechanisms based on machine learning, deep learning, blockchain, and related AI-driven technologies. The main contribution of this paper is the integration and comparative assessment of recent intelligent security approaches, highlighting their strengths, limitations, and applicability to resource-constrained IoT environments.

This paper focuses on the critical need for smart defenses that can adapt to complex and changing threats, such as ML-based IDSs, blockchain-enabled security solutions, and anomaly detection. By applying such cutting-edge methods, IoT systems can attain enhanced resilience, improved threat detection, and better overall security. The findings indicate that intelligent and hybrid security mechanisms generally provide more adaptive and effective protection than traditional rule-based approaches, although challenges related to computational overhead, scalability, and real-world deployment remain.

Future work must focus on building scalable and resource-efficient security frameworks, incorporating real-life threat monitoring, and examining hybrid systems that combine several intelligent protection approaches. Future research should also emphasize lightweight AI models for resource-constrained IoT devices, privacy-preserving techniques such as federated learning, standardized benchmarking across security solutions, and real-world validation in industrial and smart-city environments. Robust IoT security is critical to protect trust and dependability in the increasingly connected digital ecosystem and to safeguard data and privacy.

Funding

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

- [1] N. U. Prince, M. A. Al Mamun, A. O. Olajide, O. U. Khan, A. B. Akeem, and A. I. Sani, "IEEE standards and deep learning techniques for securing Internet of Things (IoT) devices against cyber attacks," *J. Comput. Anal. Appl.*, vol. 33, no. 7, 2024.
- [2] L. Zolfagharipour, M. H. Kadhimi, and T. H. Mandeel, "Enhance the security of access to IoT-based equipment in fog," in *2023 Al-Sadiq Int. Conf. Commun. Inf. Technol. (AICCIT)*, Jul. 2023, pp. 142–146.
- [3] H. A. S. Ali, "Machine learning for Internet of Things (IoT) security: A comprehensive survey," *Int. J. Comput. Netw. Appl.*, vol. 11, no. 5, pp. 617–659, 2024.
- [4] P. Sun, S. Shen, Y. Wan, Z. Wu, Z. Fang, and X. Z. Gao, "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 34567–34591, 2024.
- [5] A. Adewuyi et al., "The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems," *Convergence*, vol. 20, p. 21, 2024.
- [6] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobility*, vol. 4, no. 1, pp. 65–88, 2015.
- [7] J. Cecilio and A. Souto, "Security issues in industrial Internet-of-Things: Threats, attacks and solutions," in *2024 IEEE Int. Workshop Metrol. Ind. 4.0 & IoT*, 2024, pp. 458–463.
- [8] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition," in *2018 IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, 2018, pp. 664–669.
- [9] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *2018 IEEE Secur. Privacy Workshops (SPW)*, 2018, pp. 29–35.
- [10] H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K. K. R. Choo, "A deep recurrent neural network based approach for Internet of Things malware threat hunting," *Future Gener. Comput. Syst.*, vol. 85, pp. 88–96, 2018.
- [11] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, "A deep learning methodology for predicting cybersecurity attacks on the Internet of Things," *Information*, vol. 14, no. 10, p. 550, 2023.
- [12] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8852–8859, 2020.
- [13] K. A. Alattas and A. Mardani, "A novel extended Internet of Things (IoT) cybersecurity protection based on adaptive deep learning prediction for industrial manufacturing applications," *Environ. Dev. Sustain.*, vol. 24, no. 7, pp. 9464–9480, 2022.
- [14] L. A. Maghrabi, I. R. Alzahrani, D. Alsalman, Z. M. AlKubaisy, D. Hamed, and M. Ragab, "Golden jackal optimization with a deep learning-based cybersecurity solution in industrial Internet of Things systems," *Electronics*, vol. 12, no. 19, p. 4091, 2023.
- [15] F. Farhin, I. Sultana, N. Islam, M. S. Kaiser, M. S. Rahman, and M. Mahmud, "Attack detection in Internet of Things using software-defined network and fuzzy neural network," in *2020 Joint 9th ICIEV and 4th ICIVPR*, 2020, pp. 1–6.
- [16] A. Bhattacharjee, "Cyber security intrusion detection deep learning model for Internet of Things (IoT)," Ph.D. dissertation, Nat. College of Ireland, Dublin, 2022.
- [17] P. Vijayalakshmi and D. Karthika, "Hybrid dual-channel convolution neural network (DCCNN) with spider monkey optimization (SMO) for cyber security threats detection in Internet of Things," *Meas. Sens.*, vol. 27, p. 100783, 2023.
- [18] M. Tawfik, N. M. Al-Zidi, B. Alsellami, A. M. Al-Hejri, and S. Nimbhore, "Internet of Things-based middleware against cyber-attacks on smart homes using software-defined networking and deep learning," in *2021 2nd Int. Conf. Comput. Methods Sci. & Technol. (ICCMST)*, 2021, pp. 7–13.
- [19] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, 2023.

- [20] M. Nanjappan, K. Pradeep, G. Natesan, A. Samydarai, and G. Premalatha, "DeepLG SecNet: Utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments," *Cluster Comput.*, vol. 27, no. 4, pp. 5459–5471, 2024.
- [21] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 296–312, 2023.
- [22] K. D. Ahmed and S. Askar, "Deep learning models for cyber security in IoT networks: A review," *Int. J. Sci. Bus.*, vol. 5, no. 3, pp. 61–70, 2021.
- [23] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, p. 100227, 2020.
- [24] I. Idrissi, M. Azizi, and O. Moussaoui, "IoT security with deep learning-based intrusion detection systems: A systematic literature review," in *2020 4th Int. Conf. Intell. Comput. Data Sci. (ICDS)*, 2020, pp. 1–10.
- [25] M. R. Babu and K. N. Veena, "A survey on attack detection methods for IoT using machine learning and deep learning," in *2021 3rd Int. Conf. Signal Process. Commun. (ICPSC)*, 2021, pp. 625–630.
- [26] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on deep learning approaches for IoT security," *Comput. Sci. Rev.*, vol. 40, p. 100389, 2021.
- [27] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligence techniques for IoT security," *Comput. Netw.*, vol. 206, p. 108771, 2022.
- [28] H. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing Internet of Things security: A survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020.
- [29] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, 2021.
- [30] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma'a, "Machine learning and the Internet of Things security: Solutions and open challenges," *J. Parallel Distrib. Comput.*, vol. 162, pp. 89–104, 2022.
- [31] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 2020.
- [32] Y. Yue, S. Li, P. Legg, and F. Li, "Deep learning-based security behaviour analysis in IoT environments: A survey," *Secur. Commun. Netw.*, vol. 2021, no. 1, p. 8873195, 2021.
- [33] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet Things*, vol. 14, p. 100365, 2021.
- [34] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, p. 3625, 2020.
- [35] K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, 2019.
- [36] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
- [37] S. Zeadally and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," *Int. J. Commun. Syst.*, vol. 33, no. 1, p. e4169, 2020.
- [38] R. Geetha and T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cyber security," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, 2021.
- [39] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep learning for intrusion detection and security of Internet of Things (IoT): Current analysis, challenges, and possible solutions," *Secur. Commun. Netw.*, vol. 2022, no. 1, p. 4016073, 2022.
- [40] A. Salih, S. T. Zeebaree, S. Ameen, A. Alkhyat, and H. M. Shukur, "A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection," in *2021 7th Int. Eng. Conf. (IEC)*, 2021, pp. 61–66.
- [41] K. C. Ravikumar, P. Chiranjeevi, N. M. Devarajan, C. Kaur, and A. I. Taloba, "Challenges in Internet of Things towards the security using deep learning techniques," *Meas. Sens.*, vol. 24, p. 100473, 2022.
- [42] Erfan F, Bellaiche M, Halabi T. Sybil attack defense in blockchain-based industrial IoT systems using decentralized federated learning. *Internet of Things*. 2026 Mar 26:101927.
- [43] M. Alauthman, A. Al-Qerem, A. Almomani, AM. Ishtaiwi, A. Aldweesh, M. Arafah, V. Arya, BB, "Gupta. Enhancing Web of Things Security Using Harris Hawks Optimization with Reinforcement Learning," *International Journal of Cognitive Computing in Engineering*. 2026 Jan 7.

- [44] S. Ramya, U. Ashmitha, M. Rajakumaran, "Improved hypergraph-based authentication scheme with IDS framework for secure IoT systems," *Future Generation Computer Systems*. 2026 Apr 27:108550.
- [45] AA. Abi Sen, AB. Mnaouer, O. Tayan, NM. Bahbouh, "A hybrid framework for IoT attacks detection combining blockchain and deep learning," *Ad Hoc Networks*. 2026 Feb 24:104197.
- [46] S. Sankaran, N. Nedungadi, A. Sharma, "Quantum federated learning for intrusion detection in Industrial Internet-of-Things," *In Quantum Cryptography and Annealing for Securing Industrial IoT* 2026 Jan 1 (pp. 61-75). Syngress.
- [47] R. Rahim, MA. Chishti, "IoT security innovations: Recent technologies, threats, and solutions," *SN Computer Science*. 2025 Jun 28;6(6):593.
- [48] R. Ravish, S. Rangaswamy, PB. Honnavalli, "Future trends in autonomous vehicle safety," *In Autonomous Vehicle Safety Solutions* 2026 Jan 1 (pp. 301-323). Elsevier.
- [49] O. Renuka, N. RadhaKrishnan, BS. Priya, A. Jhansy, S. Ezekiel, "Data privacy and protection: Legal and ethical challenges," *Emerging threats and countermeasures in cybersecurity*. 2025 Feb 17:433-65.
- [50] L. Zolfagharipour and M. H. Kadhim, "A technique for efficiently controlling centralized data congestion in vehicular ad hoc networks," *Int. J. Comput. Netw. Appl.*, vol. 12, no. 2, pp. 267–277, 2025.
- [51] A. Akbari, "The application of radio-frequency identification (RFID) technology in the petroleum engineering industry: Mixed review," *Petroleum Research*. 2025 May 16.
- [52] SK. Khan, N. Shiwakoti, P. Stasinopoulos, M. Warren, "Cybersecurity Regulations for Automated Vehicles: A Conceptual Model Demonstrating the Tragedy of the Commons". *Transportation Research Procedia*. 2025 Jan 1;82:3729-51.