Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/



Research Paper Open Access

Artificial Intelligence Approaches For Iot Security: A Survey on Architecture, Attack Taxonomy, and Intrusion Detection Systems

Rinki Kaur[1], Surendra Kumar Patel[2*]

[1, 2]Dept. of Information Technology, Govt.Nagarjuna P.G. College of Science, Raipur, Chhattisgarh, India
researchrinki25@gmail.com, surendrapatelit2004@gmail.com

ABSTRACT
The Internet of Things (IoT) fast growth has made intelligent and connected environments conceivable, but it has also raised significant security concerns because of the diverse, dynamic, and resource-constrained nature of IoT devices. IoT infrastructure is often the target of evolving attacks that are beyond the capabilities of conventional security measures. Artificial Intelligence (AI), especially Machine Learning (ML) and Deep Learning (DL), has been an effective approach to enhancing IoT security in recent years through intelligent threat detection and intrusion prevention. By examining IoT design, security issues, layer-based attack taxonomy, and the security needs related to different IoT layers, this survey provides a comprehensive evaluation of IoT security. Additionally, it studies the usage of ML and DL algorithms to identify and mitigate intrusions in IoT contexts and looks at AI-driven IDS. Recent AI-based IoT security strategies are compared with an emphasis on detection performance, computational complexity, methodology, and real-world applications. In order to develop innovative, scalable, and efficient security solutions for next-generation IoT devices, the study concludes by highlighting the drawbacks of current approaches and offering suggestions for future research directions.

Keywords: Internet of Things (IoT), Machine Learning (ML), Deep Learning (DL).Artificial Intelligence(AI), Intrusion Detection System(IDS).

1. Introduction

The Internet of Things (IoT) has established into a multidisciplinary environment that connects sensors, actuators, and smart devices in industries including transportation, manufacturing, smart cities, and healthcare. Its mix of sensing, communication, processing, and intelligent services enables networked and automated applications [1], [2], and [3]. However, because of their variety, resource constraints, and dynamic nature, IoT installations present significant security challenges. IoT devices' low computing power and a variety of protocols, open wireless interfaces, and untrusted installations make them particularly vulnerable to attackers[3], [4]. Conventional security solutions may thus be insufficient for IoT scenarios that are resource-constrained and changing quickly.

IoT security is rapidly using artificial intelligence(AI) , especially Machine Learning(ML), and Deep Learning (DL) , to identify threat abnormalities and stop intrusions[2],[4]. IoT data may be scanned by AI-powered techniques to identify patterns associated with known and undiscovered threats. In order to enhance IoT security, ML and DL based Intrusion Detection Systems (IDS) have become crucial[5], [6].

There is not a study that covers all these elements, despite the fact that many studies focus on particular aspects of IoT security, such as security concerns, attack categorization, AI techniques, and IDS. IoT architecture, layer- based attack taxonomy, security needs, AI- driven security strategies, and intrusion detection systems are all thoroughly covered in this survey. The next step is a comparative analysis of recent research. It also cover present problems, limitations, and future goals for AI-enabled IoT security research. The principal contributions are:

- A summary of layer-specific security issues and the architecture of the Internet of Things.

- A methodical categorization of security threats at the application, middle, network, and perception layers.
- A summary and comparison of ML/ DL based IDS and IoT security methods, including performance constraints, research requirements, and prospects for the future.

The remainder of the paper is organized as follows: IoT architecture and Artificial Intelligence are discussed in Section 2. The layer-based attack taxonomy and IoT security standards are covered in Section 3. Section 4 presents AI-based security approaches and intrusion detection systems. The methodology for structured and methodical literature evaluation is described in Section 5. Section 6 contains an up-to-date literature overview and a comparative analysis of existing research. The findings of the literature evaluation are covered in Section 7, and the study is concluded with suggestions for more research in Section 8.

2. IoT and Artificial Intelligence

This section presents the fundamental concepts required to understand AI-driven IoT security. It gives an overview of IoT security-related AI, ML, and DL techniques after introducing IoT and its four-layer architecture. The selected architecture serves as the foundation for the layer-based security analysis in the next section.

2.1. IoT (Internet of Things)

The Internet of Things (IoT) is an interconnected ecosystem of devices that collect, analyze, and share data via communication networks. It combines physical objects, sensors, software, communication protocols, and network infrastructure to enable automated services across a variety of application domains [1], [3].

2.2. Architecture of IoT

IoT uses a multilayer architecture to integrates devices, communication technologies, networking protocols, processing capabilities, and application services. Three-layer, four-layer, and five-layer models have been proposed to meet different application and deployment requirements [10], [8], [7].In this survey, a four-layer architecture comprising Physical, Network, Middle and Application layers is adopted because it provides a consistent basis for analyzing layer-specific security requirements, attacks, and AI-driven security mechanisms.

2.2.1. Physical Layer: Sensors, actuators, controllers, readers, and other IoT devices that sense and collect data from their surroundings make up the physical layer. It is vulnerable to physical and sensing-related security concerns due to its resource-constrained devices and physical contact.[8], [9].

2.2.3. Network Layer: The network layer enables communication between Internet of Things devices and external networks using networking technologies and protocols. In addition to supporting traffic management, routing, forwarding, and data transfer, it is susceptible to DDoS, sinkhole, and selective forwarding attacks. IoT networking settings frequently employ protocols like RPL, CORPL, CARP, and 6LoWPAN [1], [3], [10], [8].

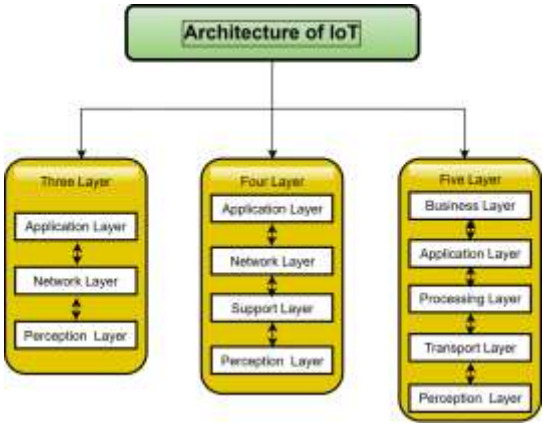


Figure 1:The Layered architecture of IoT (Three, Four, Five layers)

2.2.3. Middleware Layer: The Middle layer provides distributed services for IoT data processing, management, storage, analytics, and interaction between devices and applications. It abstracts hardware-level details and supports and data analysis and AI-based processing. Security at this layer is important for protecting data processing and service delivery against unauthorized access and manipulation [2],[11].

2.2.4. Application Layer: - The Application Layer provides IoT services to users including monitoring, data presentation, device management, notifications and automated control. Protocols including MQTT, XMPP, CoAP, and AMQP support communication at this layer. Security primarily concerns confidentiality, integrity, privacy, and secure service delivery [1],[11],[12], [13].

2.3. Artificial Intelligence

Artificial Intelligence (AI) provides computational techniques for learning, prediction, classification, and intelligent decision-making. AI methods can analyze data, identify abnormal behavior, detect and classify attacks, and support Intrusion Detection Systems (IDS) in IoT secuirty [2],[5],[6]. This survey emphasizes ML and DL methods applied to IoT security and IDS.

2.3.1. Machine Learning

Machine Learning (ML) is a branch of artificial intelligence that permits computational models to learn patterns from data and perform prediction and classification tasks. ML is used for anomaly detection, attack classification, and intrusion detection in IoT security environments. ML methods are categorized as supervised, unsupervised, and reinforcement learning based on their learning process and data requirements [5], [14].

2.3.2. Deep Learning

Deep learning (DL) is a subsection of ML that uses multilayer neural networks to extract complicated symbols from data. It is suitable for IoT security applications, including intrusion detection, attack categorization, and anomaly detection due to its ability to autonomously extract characteristics.[15],[16],[6],[17]. Common deep learning example of CNN, RNN, LSTM, GRU, DNN, GNN, DRL, and GAN used in IoT security.

3. Security in IoT

Because diverse devices, communication protocols, software components, and network connections pose numerous risks, security and privacy are essential needs for the Internet of Things[18],[19], [20]. Threats across the various architectural layers must thus be addressed by IoT security [21]. Heterogeneous and resource constrained context makes protecting IoT systems much more difficult [22],[23].

3.1. Layered-Based Security Attacks Taxonomy

This survey classifies IoT security attacks according to the adopted four-layer architecture: Perception, Network, Middle, and Application. An organized awareness of security risk in IoT systems is provided by the many vulnerabilities and associated attacks found in each tier.

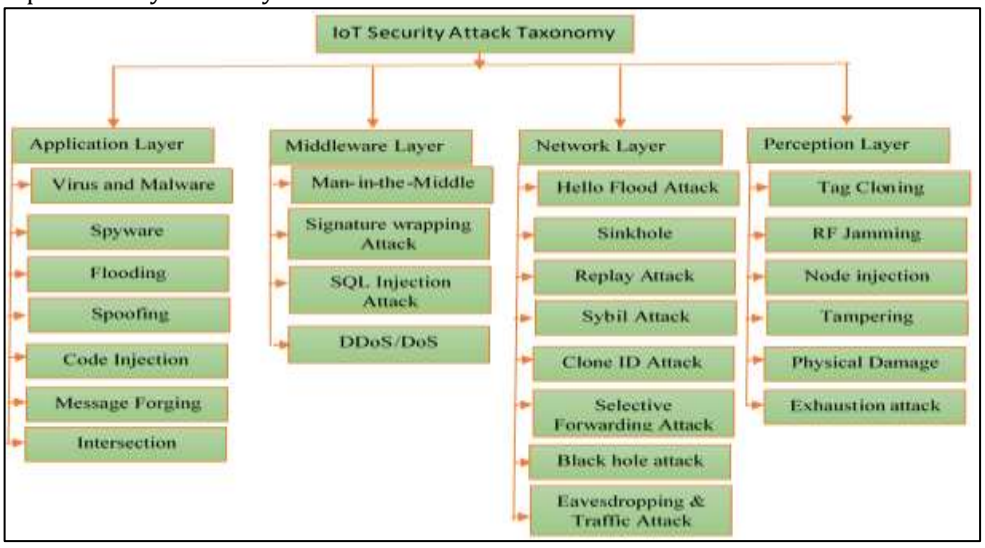


Figure 2:IoT security attack Taxonomy (Layer-based)

Table 1: Layer-wise attack analysis in IoT Environment

Application Layer	**Attack in IoT**	**Attack Description**
	Virus and Malware	Malware such as Trojans, worms, and viruses can compromise IoT devices and threat system security [24], [25],[1].
	Spyware	Spyware secretly collects sensitive information from IoT devices, compromising user privacy [26], [1].
	Spoofing	Spoofing impersonates legitimate nodes or entities, compromising authentication and privacy [27].
	Code Injection	Inserting malicious code, potentially enabling data theft, unauthorized control, and disruption [18], [28].
	Message Forging	Message forging alters or fabricates message , compromising communication integrity.
	Intersection	Intersection attacks compromise privacy by extracting information from multiple sources [29], [19], [20].
Middleware Layer	Man-in-the-Middle attack	Attacker intercepts and potentially manipulate communication between legitimate entries [2].
	Signature Wrapping	Signature wrapping modifies message structures while retaining a valid signature [21].
	SQL Injection	Malicious queries to manipulate databases or obtain sensitive information [23],[22],[30], [31].
	DDoS /DoS Attack	DoS/DDoS attacks generate excessive traffic to exhaust IoT resources and disrupt service availability[32], [33].
Network Layer	Hello Flood Attack	Broadcasts false neighbor or routing information to influence route selection and network connectivity [34],[35].
	Sinkhole Attack	A malicious node advertises false routing information to attract and disrupt network traffic [34],[36]
	Replay Attack	Replay attack retransmits captured messages to mislead nodes and consume resources [37].
	Sybil Attack	Creates multiple false identities to manipulate network operations and trust mechanisms [38],[39], [40].
	Clone ID Attack	Duplicate legitimate IoT node identity to obtain unauthorized access [41].
	Selective Forwarding	A malicious node selectively drops packets, disrupting routing and data delivery [2].
	Blackhole Attack	Attracts network traffic and subsequently drops the forwarded data, compromising communication availability and integrity.
	Eavesdropping & Traffic	Attackers capture or analyze network communications to obtain sensitive information and may use the information for subsequent attacks [42],[1].
Perception Layer	Tag Cloning Attack	Duplicates a legitimate RFID tag identifier, enabling unauthorized authentication and compromising system authenticity [43]. [44].
	RF Jamming	Intentionally interferes with wireless signals, reducing communication performance or preventing normal IoT operation.
	Node Injection	Introduces malicious devices into the IoT topology to intercept or manipulate communication [45],[1].
	Tampering	Involves unauthorized modification, access, damage, or theft of IoT devices and components, compromising their integrity and confidentiality[46].
	Physical damage	Physical damage or destruction of IoT nodes can make service unavailable and may led to network-level disruption [45], [47].

	Exhaustion Attack	Repeated Dos/jamming, Retransmission and MAC collision activity consume battery resources and reduce node lifetime[48]. [1].

3.2. Security requirements of IoT layer based on attack classification:

IoT security requires complementary mechanisms to protect devices, communication, data and services against layer-specific attacks. The main security requirements considered in this survey are authentication, authorization, availability, integrity, confidentiality, and non-repudiation [12], [49], [50], [11].

Table 2: IoT security requirement by layer

Requirement	IoT relevance	Key limitation
Confidentiality [51]	Prevents unauthorized disclosure	Resource constraints
Integrity [11],[52]	Protect data correctness	Lightweight protection
Availability [53]	Maintain service access	DoS/ jamming attacks
Authentication[51]	Verifies identity	Constrained devices
Authorization [11],[54]	Control resource access	Fine-grained access control
Privacy[53]	Protects sensitive information	Data misuse

4. AI–driven security techniques and Intrusion Detection System

This section reviews AI-driven security techniques for protecting IoT systems against cyber threats, with emphasis on their application to attack detection, classification, and intrusion detection.

4.1. Application of Machine Learning in IoT security

IoT security has made substantial use of machine learning techniques to detect intrusion, abnormalities, and threats. Their effectiveness depends on dataset quality, feature selection, computational complexity, and the target IoT environment [5], [14].

Table 3:Study of Machine Learning Algorithms to improve IoT security [56]

Method	Security Application	Key Advantage	Key Limitation
KNN**[55]**	Classification	non-parametric algorithm	Sensitive to Feature distributions
NB **[55]**	Classification	Fast and efficient	Limited to correlated attributes
SVM **[55]**	Classification and Regression	Effective in high-dimensional data	Computational cost for large datasets
RF [56]	Classification and Regression	Robust and reduces overfitting	Limited interpretability
Decision Tree	Attack Classification	Simple and interpretable	Sensitive to feature selection bias
LR **[55]**	Classification	Simple and efficient	Limited for non-linear data
K- means **[55]**	Clustering/ Anomaly Detection	Simple clustering approach	Sensitive to initial parameters
DBSCAN **[55]**	Clustering/ Anomaly Detection	Handles noise and arbitrary clusters	Sensitive to parameter selection

4.2. Application of Deep Learning in IoT security

DL techniques are increasingly applied to IoT security because they can learn complex representations from large scale data. They support intrusion detection, attack classification, anomaly detection, and traffic analysis but their effectiveness depends on sufficient training data and computational resources [6],[17].

Table 4:Representation of Deep Learning algorithms for IoT security by the previous study

Method	Security application	Key Advantage	Key Limitation

CNN **[56]**	Attack detection/ classification	Feature Extraction and Pattern Recognition	High computational and data requirements
LSTM**[56]**	Sequential attack detection	Captures temporal dependencies	Computationally expensive
GRU**[56]**	Attack Detection	Handles nonlinear and temporal data	Hyperparameters optimization
GNN[60]	Network traffic analysis	Network model topology	Training complexity
DNN**[57]**	Intrusion detection	Models complex nonlinear relationships	Gradient/ training issues
RNN**[57]**	Malware/sequence detection	Sequence learning	Difficult for long sequences
DRL**[57]**	Attack/ Intrusion detection	Adaptive decision making	Sampling efficiency
GANs**[57]**	Attack detection/ data generation	Generate additional training data	Convergence and gradient issues
DBNs**[57]**	Intrusion detection	Effective representation learning	Computationally expensive

Table 1: Reported performance of ML and DL based IoT security approaches

Algorithms	**Security Task**	**Reported performance**
[58] RNN-Based Long Short-Term Memory	IoT intrusion detection	Reported Metric
[59] CNN	Cybersecurity threat Detection	Classification accuracy=97.46%
[60] CNN and Gated Recurrent Unit	IoT IDS	F1 score=0.98
[61] DNN	Network intrusion detection	99.66% /99.77%
[62] CNN	Cyber threat detection	99.30% /98.20%
[63] LSTM	IoT IDS	99.5% /99.3%, /99.1%
[64],**[65]** Random Forest	Anomaly Detection, DDoS Detection	99.6% / 99.63%
[66],**[67]** K-NN	IoT device classification , IoT data security	85% / 95%
[68],**[69]** Decision Trees	Multiclass Attack Detection, Botnet Detection	99.92% / 99.89%
[70], **[71]**, **[72]** Support Vector Machine	Malware Detection, Malicious node detection, Data Authentication	99.96% / 90.00% / 99.40%
[73], **[74]** Naïve Bayes	IoT cyber security	96.3% / 78%
[75] PCA	DDoS attack detection	95.24%
[76] K-means clustering	Intrusion Detection	99.94%
[77] Q-learnin g	Malware detection	Improved by 40%

4.3. Attack Detection Methods in IoT Environment Using IDS

This section focuses on the Intrusion Detection System (IDS) in IoT contexts. In terms of IoT deployments situations, it explain IDS and its several variations. To creates IDS that can identify and mitigate IoT network attacks, several researchers have employed machine learning and deep learning techniques.

4.3.1. Intrusion Detection System

An intrusion detection system (IDS) analyzes network or system activity to detect suspicious or unauthorized activities and implement security changes [78],[79]. In IoT contexts, IDS may identify attacks using a variety of design and detection methodologies.

4.3.2. Classification of IDS: -

IDS may be classified by detection mechanism, architecture, target location, and reaction and response.

Table 2:Classification of Intrusion Detection Systems (IDS) in IoT Environments

Classification Basis	IDS Type	Main Characteristics
Based on Architecture	Centralized IDS	A central unit performs analysis [80].
	Distributed IDS	Detection and analysis are distributed among monitoring nodes [80].
Based on Detection Approaches	Signature-based approach	Detects known attacks using predefined patterns
	Anomaly-based Approach	Detects deviation from learned normal behavior
	Graph-Based Approach	Represents network activity using graph structures
	Protocol-Based Approach	Monitors protocol behavior for suspicious activity
Based on Reaction and Response	Active IDS	Automatically responds to detected attacks
	Passive IDS	Detects and reports attacks without direct intervention
Based on Target Location	Host-Based IDS	Monitors individual hosts or endpoints
	Network-Based IDS	Monitors network traffic
	Hybrid IDS	Combines host and network-level information

Research Methodology of Survey: -

This survey adopts a Structured and Systematic Literature Review (SSLR) approach to identify, evaluate, and synthesize research related to AI-driven IoT security. This review examines Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), IoT Security, Intrusion Detection Systems, and IoT Security Attacks. Studies from 2016 to 2025 were evaluated. Initially, 567 papers were extracted from various digital databases and scholarly sources. After applying the selection criteria based on publication time, language relevance, and survey breadth, 262 research were selected as relevant, with 116 papers analyzed in detail. The literature was gathered from reputable academic sources such as Google Scholar, IEEE Xplore, Springer, Wiley, Nature, MDPI, ACM, Elsevier, and other pertinent journal and conference proceedings. The selected studies were analyzed based to their objective, methodologies, key findings, limitations, and relevance to AI-enabled IoT security. The retrieved data were analyzed to identify important research trends, limitations, gaps, and future directions. The selected studies form the basis for the state-of-the-art literature review presented in Section 6.

Table 3:Study Selection Criteria

Criterion	Requirement
Research Scope	IoT security. IoT attacks, AI, ML, DL, and IDS
Publication period	2016-2025
Language	English
Publication Type	Journal and conference publications
Relevance	Direct relevance to AI-driven IoT security

Selection	Studies satisfying the defined scope and relevance criteria

6. State of the Art (Literature Review)

This section examines papers on AI-driven IoT security strategies published between 2016 and 2025 using the SSLR methodology. With an emphasis on attack detection, classification, intrusion detection and mitigation, the literature is examined in terms of research goals, methodologies, key discoveries, constraints, and relevance to IoT security. In addition to highlighting significant research gaps and trends, the paper highlights the development of IoT security research.

6.1. Studies from 2016

In 2016, Gendreau et al. [79] examined IDS and anomaly-based approaches for IoT security, highlighting the importance of intrusion detection while identifying dataset, scalability, and resource constraints as major challenges. Aljami et al. [81] explored selective forwarding attacks and demonstrated that lightweight detection may identify malicious nodes while maintaining quality of service. Tiburski et al.[82] focused on lightweight middleware security and showed that lightweight mechanisms can improve protection at the middleware layer, but empirical validation was limited. T.Lu et al. [83] examined passive attacks and highlighted their potential to compromise communication privacy, while noting the lack of empirical validation.

6.2. Studies from 2017

Research in 2017 expanded toward IoT architecture, security requirements, and attack-specific protection. Yaqoob et al. [8] examine IoT architecture and requirements and identify scalability, interoperability, energy consumption, and security as major challenges, although empirical validation was limited. Kumar et al. [84] investigated XML-wrapping attacks and showed that positional tokens can improve transaction integrity, but evaluation across different applications remained limited. Sunil kumar et al. [85] examined WSN security and identified authentication, confidentiality, integrity and routing attacks, while large-scale solutions remained insufficient. Kamaldeep et al.[86] investigated UDP flooding mitigation and demonstrated that a lightweight Contiki-based defense can reduce flooding impact, although the approach was specific to UDP flooding. Ahmed et al. [87] presented a layered IoT security perspective by mapping attacks and defense across IoT layers, but empirical validation was limited. Sethi et al. [88] provided the foundation of IoT architecture and protocols, although the security coverage was relatively broad. Alvi et al. [89] examined RPL efficiency and highlighted trade-offs among energy consumption, routing stability, and network lifetime, but the evaluation was limited to a specific routing scenario.

6.3. Studies from 2018

In 2018, research increasingly emphasized IoT security challenges, attack taxonomies, malware, IDS, and attack-specific detection. Colakovic et al. [3] examined IoT design and difficulties, including scalability, interoperability, and security, although practical validation was limited. Abul-Ghani et al. [90] proposed a structured layered classification of IoT attacks, providing a foundation for layer-based security analysis, but the work remained largely conceptual. Patel et al. [91] investigated wormhole detection and reported improvements in wormhole identification and network stability, although the approach was attack-specific and had limited scalability. Burhan et al. [7] reviewed IoT architecture and security and identified layer-specific threats and IoT elements, but provided limited empirical validation. Malik et al.[9] reviewed IoT security requirements including authentication, confidentiality, integrity, and privacy. Tahir [24] examined malware categories and detection approaches, although the IoT/WSN focus was limited. Othman et al. [92] classify IDS approaches into signature-based, anomaly-based, and hybrid methods, but provided limited performance evaluation. Sicari et al. [32] investigated DoS mitigation through REATO and demonstrated attack detection and mitigation, although scalability remained a concern. Feng et al. [93] applied machine learning using Random Forest for RF-jamming detection and showed improved performance, but real-world deployment was not extensively evaluated. Ghadimi et al. [28] examined IoT security architecture and defined layered security requirements and trust mechanisms, although scalability testing was limited.

6.4. Studies from 2019

In 2019, research on IoT security increasingly addressed IoT applications, routing attacks, security requirements, machine learning-based resource management, physical layer security, and intrusion detection. Alsh et al. [94] established the general context and objectives of IoT applications; however, the study provided limited depth regarding security aspects. Kfoury et al. [95] explored the detection of RPL routing attacks and found that the approach was effective, albeit with limited generalization

outside the considered context. Hussain et al. [96] investigated the use of machine learning for resource management in IoT networks, emphasizing the potential for traffic, spectrum, and energy control, but implementation and scalability remained significant problems. Haddadpajouh et al. [38] examined IoT security needs, problems, and current solutions, but pointed out shortcomings in real-world validation. Zhang et al. [97] investigated physical layer security and showed that authentication and key generation mechanisms can improve resilience against spoofing and eavesdropping attacks; however, practical validation was limited. Arif et al. [10] examined security threats in vehicular networks and provided a classification of VANET attacks, although the study was specific to VANET environments. Although Kumar et al. [98] provided a comprehensive technological framework for IoT, its security and empirical scope were restricted. Taghanki et al [99] proposed the DEEM sinkhole intrusion detection approach, where lightweight decentralized detection improved network resilience, although the method primarily focused on sinkhole attacks.

6.5. Studies from 2020

In 2020, research on IoT security expanded from general security requirements and attack taxonomies towards specialized intrusion detection, routing attack analysis, deep learning and attack-specific detection mechanisms. Kouliaridis et al. [25] reviewed approaches for mobile malware detection, but the study was mainly oriented towards mobile operating systems rather than a broader environment. Hamza et al. [100] reviewed IoT network security requirement , threats, and countermeasures, but the study had limited empirical validation. Ribera et al. [101] investigated IDS approaches for blackhole and greyhole attacks and showed that a heartbeat-based IDS could improve network reliability; however, the approach remained focused on specific attacks and had limited scalability. Meziane et al. [49] proposed a structured taxonomy for IoT attacks using CTM, although empirical validation was limited. Lee [102] examined IoT cybersecurity and risk management by identifying major cyberattacks and corresponding countermeasures, but the work remained primarily conceptual. Sicato et al [78] analyzed IoT intrusion techniques and classified their strengths and weaknesses, while noting limited real-world validation.

Research during the same period also concentrated on routing and device-level attacks. Boudouaia et al. [103] demonstrated the severe effects of RPL attacks on routing and packet delivery, although the validation of the countermeasure was limited. Alreshoodi et al. [104] investigated internal routing attacks and demonstrated how they affected packet delivery, delay, and network stability, they only offered a cursory assessment of the protection mechanism. M.Emeç et al. [105] used attack simulation to demonstrate the impact of attacks on IoT devices, although the evaluation considered a specific attack scenario. Preda et al. [106] investigated RPL attack simulation and provided a basis for evaluating RPL attack detection, but the work remained simulation-focused. Cakir et al. [107] applied a GRU-based IDS for RPL attacks and demonstrated effective attack detection and prevention; however, comparison with other deep learning models was limited.

Broader reviews and AI-oriented studies further strengthened the security literature. Although Khanam et al. [1] released an IoT security study including attack taxonomy and countermeasures, its scope was conceptually wide. Pal et al. [108] defined structured IoT security requirements but provided limited practical validation. Hlaing et al. [22] addressed SQL-injection detection and demonstrated the ability to detect and block such attacks; however, the approach was restricted to a specific attack type.

6.6. Studies from 2021

In 2021, IoT security research increasingly focused on routing attacks, intrusion detection, deep learning, lightweight security, and attack-specific mitigation techniques. Seth et al. [109] investigated isolation attacks in RPL networks. They proposed a mitigation approach that improved packet delivery and network stability, although the evaluation remained specific to the considered attack and scalability was limited. Alshahrani et al. [110] introduced CoLL-IoT, a collaborative intrusion detection approach that improved attack detection while reducing false positives; however, large-scale validation was limited. ESSope et al. [111] contributed an anomaly detection dataset for IoT and industrial IoT intrusion detection, although its applicability was restricted to the scenario represented in the dataset. Abd Halim et al.[112] examined sinkhole attack detection using a Cooja-based environment, but the approach was mainly oriented towards agriculture-oriented wireless sensor networks.

Deep learning also received increased attention for IoT cybersecurity. Shara [113] studied the use of deep learning for cybersecurity applications, like anomaly and malware detection, and intrusion detection, while the study contained little empirical benchmarking. Alzubaidi et al. [114] studied

deep learning architecture, applications, and challenges, but empirical validation was incomplete. Although the method was domain-specific, Tawfik et al. [115] looked into the usage of deep learning with Software Defined Networking (SDN) for attack detection and prevention in smart home environments. Saleem et al. [116] further discussed deep learning for IoT security, particularly anomaly detection and adaptive security, but practical validation remained limited.

Several studies concentrated on routing and network-level attacks. Sampooram et al. [117] examined wormhole attacks in a LEACH–based network and demonstrated their adverse effects on routing performance, although the analysis was attack-specific. Ambarkar et al.[118] investigated RPL attacks and their effects on packet delivery, latency, and energy consumption, but provided limited mitigation strategies. Ching et al. [119] analyzed RPL performance in terms of energy consumption, communication overhead, and packet delivery, with the study remaining specific to RPL environments. Sinha et al. [120] addressed network denial-of -service attacks and developed a detection approach capable of approximating the attacker's location, although validation across diverse scenarios was limited. Feng et al.[44] proposed a spatiotemporal trajectory-based method for detecting RFID cloning attacks, but its generalization to broader IoT environments was limited.

Other studies addressed broader IoT security environments and attack characteristics. Azrour et al.[50] reviewed major security and communication challenges in IoT environments, while Mishra et al.[121] provided a holistic review of IoT attacks, security mechanisms, and IDS approaches; both studies were primarily survey-based and had limited empirical validation. Kaur et al. [122] classified WSN attacks and analyzed their effects, although the treatment was largely conceptual. Khader et al. [123] surveyed DoS and DDoS threats, their impacts, and countermeasures without empirical testing. Rachit and Bhatt et al.[124] discussed emerging IoT security trends, attacks, and defense mechanisms, but maintain a broad survey scope. Wagle et al.[125] examined lightweight and energy-efficient security mechanisms, although large-scale validation was limited. Xu et al.[126]discussed AI as a paradigm for automation, prediction, and data-driven research, but provided limited empirical application to IoT security.

Overall, the literature indicates a transition towards AI-assisted, collaborative, and lightweight intrusion detection, while attack-specific, dataset- or simulation-dependent, and insufficiently validated in heterogeneous, large-scale environments.

6.7. Studies from 2022

In 2022, research highlighted DL and ML-based IDS, attack detection, protocol security, anomaly datasets, and lightweight mechanisms. Banaamah et al. [127] investigated DL based IDS and reported high attack-detection accuracy in IoT environments; however, the computational requirements of DL models remained a major limitation. Sandur et al. [128] analyzed the 6LoWPAN, CoAP, and RPL protocol stack and highlighted trade-offs among energy consumption, latency, and packet delivery, although the study was protocol-specific. Although the RPL intrusion detection method created by Ribera et al. [129] increased the accuracy of identifying RPL assaults, its applicability to various protocols and heterogeneous IoT environments remained restricted. Although the method was limited to RPL networks, Zahra et al. [130] used machine learning to rank-based wormhole detection and showed accurate detection of RPL routing attacks.

Security modelling and dataset deployment were also addressed during this period. Meziane et al. [11] proposed structured UML-based modelling for IoT security systems, although empirical validation was limited. Dissanayake et al. [131] developed a dataset for denial-of -sleep attacks to support anomaly-based IDS research, but the dataset covered a specific attack category. Aboubakar et al. [132] examined IoT network management and identified major challenges related to scalability, Quality of Service(QoS) and security, while large-scale validation remained limited. Although WSNs were the primary area of discussion, Keerthika et al. [133] studied Denial-of- Service (DDoS) attacks, their effects and responses.

Several studies have studied specialized intrusion detection and mitigation approaches. Savva et al. [134] employed a fuzzy-based IDS for detecting jamming attacks in wireless mesh IoT networks and demonstrated effective detection, but the approach was specific to jamming attacks. Deepavathi et al. [135] investigated secure RPL multicast forwarding and improved multicast security, although the solution remained RPL-specific. Jayalaxmi et al. [136] examined ML and DL based methods for intrusion detection and prevention and emphasized the growing importance of AI in IoT security while noting computational and deployment issue. Tahri et al. [137] used ML for intrusion detection and presented greater attack detection accuracy, yet computational overhead continued a concern. Bharati et al. [138] reviewed the application of ML and DL to IoT security, particularly intrusion

detection, authentication, and privacy, but empirical validation was limited. S.K.B.J. et al. [139] applied an Exponentially Weighted Moving Average (EWMA) based approach for jamming detection and demonstrated improved reliability through lightweight statistical detection; however, the generalization to other environments remained limited. Dominguez-Bolani et al. [140] reviewed IoT architecture and open-source projects, providing an overview of available architecture and tools, although performance evaluation was limited. Rajmohan et al. [51] examined reusable IoT security patterns and architectural solutions, but the work was primarily conceptual. Kiran et al. [141] proposed a trust-based approach for DDoS defense and improved network resilience through node trust evaluation; however, the approach was specific to the RPL environment. Manne et al[142] investigated mitigation of common RPL attacks and demonstrated attack detection and mitigation, although validation across heterogeneous IoT environments was limited. Sun et al. [143] addressed wormhole anomaly detection and demonstrated effective detection, but the approach provided limited coverage of other threat types.

6.8. Studies from 2023

In 2023, research on IoT security increasingly moved towards AI-driven intrusion detection, lightweight ML/ DL approaches, trust management, and intelligent detection of specific attacks. Elhanashi et al [144] reviewed the integration of deep learning into security and highlighted challenges related to scalability and deployment, although empirical validation remained limited. Jahangeer et al.[34] examined network-layer IoT security and identified vulnerabilities related to routing , addressing, and communication, but provided limited cross-layer analysis. Kaveh et al. [145] investigated ML-based intrusion detection for blockhole attacks and showed that detection performance can vary with attack characteristics; however, the study covered a limited range of threats. Konsta et al. [146] reviewed trust management approaches and categorized IoT trust model according to their security role, although large-scale validation remained limited.

The use of AI for adaptive and resource-constrained IoT security also receives greater attention. . Mukha et al. [147] examined lightweight ML/DL based IDS approaches designed for constrained IoT environments, although large-scale validation remained limited. Rao et al. [148] investigated a hybrid ML approach for DoS detection and reported improved detection and reduced false positives, but the approach remained focused on DoS attacks. Noman et al. [31] examined IoT code injection attacks and provided practical analysis of the threats, while cross-layer and hybrid analysis remained limited. Meizane et al. [2] compared AI algorithms for different IoT security tasks and contributed to the evaluation of AI-based detection and classification approaches, although large-scale benchmarking was limited.

Several studies throughout 2023 concentrated on border IoT security necessities and application-specific defense. Taherdoost et al. [149] studied the advantages, challenges and future perception of IoT security, but provided limited technical validation. Although there was little empirical support, Kh- Madhloom et al.[150] looked at security and privacy issues in wireless IoT environments and emphasized scalability and interoperability concerns. Mohsin et al. [151] addressed healthcare IoT security, particularly secure data transmission and patient privacy, but the approach was specific to a healthcare application. Kolhar et al. [152] investigated deep learning for smart vehicle networks and reported environments in detection and adaptability, although generalization across heterogeneous domains remained limited.

Other work provided a broader perspective on AI and IoT security. Patil et al. [153] presented an overview of AI applications, but the technical and empirical depth was limited. Saini[154] reviewed AI applications across different domains, providing a broad introductory perspective rather than a detailed IoT security evaluation. Gupta [155] similarly provided a conceptual overview of AI applications with limited security-specific depth. Rashid et al. [156] reviewed IoT architecture, protocols, and security threats, but remained broad in scope. Tariq et al. [157] reviewed IoT security vulnerabilities, solutions, and future direction, while empirical validation remained limited. Fei et al. [158] provided a systematic review of IoT security vulnerabilities, solutions, and research directions, but also identified the continuing lack of empirical validations.

Attack-specific IDS research continued alongside these broader reviews. Al-Sarawi et al. [159] developed a low-overhead approach for detecting passive sinkhole attacks, although the method was sinkhole-specific. Rehman et al. [160] examined the effect of DoS/ DDoS attacks on IoT performance and reliability, but considered a limited range of attacks. Altaf et al. [161] explored a multigraph neural network and showed great detection accuracy and robustness, despite the approach's computational complexity. Altaf et al[162] then investigated a lightweight Graph Convolutional

Network (GCN) that maintained good detection accuracy while lowering computational cost; nevertheless, comparisons to other DL models were limited. Mazhar et al. [163] demonstrated the efficacy of ML and DL for IoT security, while large-scale validation was limited. Teng et al. [36] proposed a SPA/ Jaya based approach for sinkhole defense and reported improved sinkhole detection and network resilience, but the study provided limited consideration of the evaluation of other routing attacks.

6.9. Studies from 2024

ML/ DL based intrusion and anomaly detection, adaptive security, imbalanced datasets, and optimal deep learning techniques will be the primary areas of focus for IoT security research in 2024. Ghaffari et al. [56] examined the application of ML and DL techniques for IoT security, namely threat mitigation and intrusion and anomaly detection. Although there was no experimental validation, the study demonstrated the promise of intelligent ways for enhancing IoT security. Alwahedi et al. [55] talked about ML and the promise of Large Language Models and generative artificial intelligence for IoT security, but there was no empirical support doe GenAI/LLM based strategies. El- Sofany et al. [5] looked into ML-based IoT security strategies for enhancing resilience and detecting intrusion and anomalies; however, they found little research on DL and LLM-based methods. Talukder et al. [164] investigated ML-based intrusion detection for an imbalanced dataset and demonstrated improved detection performance on a large imbalanced dataset, although computational complexity remained a limitation. Although the evaluation was simulation-based and real-world scalability was not shown, Choudhary et al. [165] looked at a Cooja-based anomaly dataset with optimized deep learning and observed enhanced anomaly identification. Thirumaran et al. [166] proposed an optimized LSTM-based IDS and reported improvements in detection accuracy and convergence, but the computational intensity of the model and its scalability required further validation

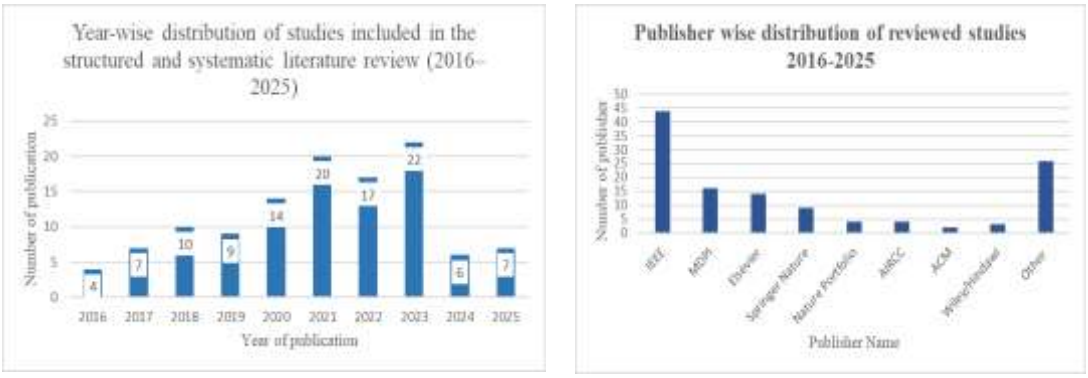
6.10. Studies from 2025

In 2025, research increasingly emphasized advanced ML/ DL based IDS, hybrid deep learning, multiple attack classification, DDoS detection, and practical deployment. Alfahaid et al. [167] reviewed ML, DL, Federated learning and transfer learning for IoT security, and highlighted challenges related to computational cost, adversarial attacks, and interpretability. Yang et al. [168] proposed the FPODL- DDoSAD approach for IoT DDoS detection by combining feature pruning, a Stacked Denoising Autoencoder (SDAE), and optimization techniques. Alharby [169] evaluated several ML classifiers, including RF, GB, NB, DT, and KNN, for detecting DoS, DDoS and Mirai attacks. The study reported high detection accuracy with improved computational efficiency.

Hybrid deep learning approaches were further explored by Jablaoui et al. [170], who developed a CNN-GRU-based IDS that combines spatial and temporal traffic features. The hybrid model outperformed standalone CNN and GRU models, but underrepresented attack classes reduced attack-level recall, and the model required substantial processing time for large datasets. Ali and Al-Sharafi et al. [171] examined machine learning and deep learning algorithms for detecting man-in-the-middle (MitM) attacks. Their findings revealed that RF attained 94% accuracy in sequential traffic analysis, trailing only LSTM. False positives and resource constraints remained problematic, emphasizing the need for more hybrid and real-time assessments. In their review of ML/DL-based IDS methods, datasets, evaluation parameters, and computational problems in IoT intrusion detection, Rehman et al. [172] highlighted the significance of demonstrative datasets and lightweight IDS architecture, as well as continuing problems with computational complexity and false positives. Mallidi and Ramisetty [173] carried out a comprehensive analysis of the literature on AI- based IDS deployment and training, covering cloud, fog, and edge deployment techniques in addition to centralized , distributed, and federated learning. Scalability, dataset appropriateness, and adaptation to IoT. Contexts are still an issue, according to their review.

7. Results and Discussion:

The results of SSLR are presented in this part, with an emphasis on important academic contributions, publishing trends, AI approaches, and their applications in IoT security. The results highlight the evolution of AI-driven IoT security and the major research directions and remaining challenges identified in the reviewed literature. Figure 3 presents the distribution of reviewed studies by publication year and publisher. The year-wise distribution indicates increasing research interest in AI-enabled IoT security, particularly in recent years. The publisher-wise distribution further shows that research in this area is disseminated across multiple established academic sources, reflecting the multidisciplinary nature of IoT security research.



(a) (b)

Figure 3: Distribution of selected studies by (a) publication year and (b) publisher

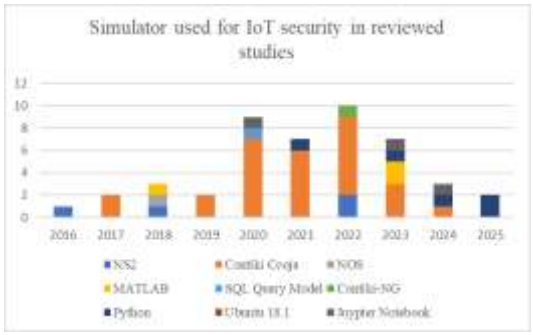


Figure 4: Year-wise usage of simulation platforms and software tools for AI-based IoT security evaluation.

Figure 4 summarizes simulation-based evaluation widely used in the reviewed studies, particularly for constrained and network environments. However, the continued reliance on simulated environments highlights the requirement for greater validation under heterogeneous and real-world deployment situations.

Overall, the SSLR results validate progression from conventional IoT security methods to AI-driven intrusion detection and attack mitigation. ML and DL are gradually used for anomaly and attack classification, while computational efficiency, dataset boundaries, scalability, and real-world validation persist as major challenges. These results demonstrate the need for AI- based security solutions for diverse IoT settings that are lightweight, adaptable, and realistically deployable.

8. Conclusion and Future Direction

8.1. Conclusion

This survey used a Systematic and Structured Literature Review (SSLR) to examine AI-driven methods for enhancing IoT security. The review examines IoT architecture, layer-based attack taxonomy, security standards, and the application of ML and DL methods in IDS. The study retrieved 567 papers; 262 were deemed relevant, and 116 underwent thorough examination. The research shows that between 2016 and 2025, intelligent procedures for lightweight intrusion detection, attack classification, anomaly detection, and mitigation will replace conventional and attack-specific security measures. There are still a number of problems to overcome, such as limited real-world validation, false positives, scalability, dataset quality, and computing needs, while ML and DL techniques show great promise for strengthening IoT security.

In conclusion, the results demonstrate that intelligent approaches can enable more effective IoT security measures, but effective implementation needs striking a balance between detection performance, privacy, scalability, flexibility, and resource efficiency.

8.2. Future Research Directions

Future research should focus on lightweight and computationally efficient models suitable for IoT devices with limited resources, including a scalable and adaptable IDS for diverse and dynamic settings. To enable reliable comparison of security strategies, a standardized and representative benchmark dataset is also required. Privacy, real-world validation, false positives, and new or unidentified risks should all be the focus of future studies. These initiatives may help to create security solutions for diverse IoT contexts that are lightweight, flexible, scalable and realistically deployable.

Conflict of interest

No potential conflict of interest was reported by the author.

References

[1] S. Khanam, I. Ahmedy, M. Idris, M. Jaward, and A. Q. Md. Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," IEEE Access, vol. PP, pp. 1–1, Nov. 2020, doi: 10.1109/ACCESS.2020.3037359.

[2] H. Meziane and N. Ouerdi, "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems," Sci. Rep., vol. 13, no. 1, p. 21255, Dec. 2023, doi: 10.1038/s41598-023-46640-9.

[3] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Comput. Netw., vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.

[4] S. Aslam, "A Review on the Security of IoT Networks: From Network Layer's Perspective", Accessed: May 10, 2024. [Online]. Available: https://www.academia.edu/103866175/A_Review_on_the_Security_of_IoT_Networks_From_Network_Layer_s_Perspective

[5] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," Sci. Rep., vol. 14, no. 1, p. 12077, May 2024, doi: 10.1038/s41598-024-62861-y.

[6] A. Ghaffari, N. Jelodari, S. pouralish, N. derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," Clust. Comput., Apr. 2024, doi: 10.1007/s10586-024-04509-0.

[7] M. Burhan, R. A. Rehman, B.-S. Kim, and B. Khan, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," Sensors, vol. 18, Aug. 2018, doi: 10.3390/s18092796.

[8] I. Yaqoob et al., "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," IEEE Wirel. Commun., vol. 24, Jun. 2017, doi: 10.1109/MWC.2017.1600421.

[9] R. Malik, D. K. Solanki, and D. S. Dalal, "LITERATURE REVIEW ON SECURITY ASPECTS OF IOT," Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, Art. no. 2, Apr. 2018, doi: 10.26483/ijarcs.v9i2.5687.

[10] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," Veh. Commun., vol. 19, no. C, Oct. 2019, doi: 10.1016/j.vehcom.2019.100179.

[11] H. Meziane and N. Ouerdi, "A Study of Modelling IoT Security Systems with Unified Modelling Language (UML)," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 11, 2022, doi: 10.14569/IJACSA.2022.0131130.

[12] H. Meziane, N. Ouerdi, M. Kasmi, and S. Mazouz, "Classifying Security Attacks in IoT Using CTM Method," 2021, pp. 307–315. doi: 10.1007/978-3-030-53440-0_32.

[13] I. Yaqoob, I. Hashem, Y. Mehmood, A. Gani, S. Mokhtar, and S. Guizani, "Enabling Communication Technologies for Smart Cities," IEEE Commun. Mag., vol. 55, Jan. 2017, doi: 10.1109/MCOM.2017.1600232CM.

[14] "(PDF) An Innovative Perceptual Pigeon Galvanized Optimization (PPGO) Based Likelihood Naove Bayes (LNB) Classification Approach for Network Intrusion Detection System." Accessed: Jun. 06, 2024.[Online].Available: https://www.researchgate.net/publication/360330143.

[15] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," Neural Comput., vol. 18, no. 7, pp. 1527–1554, Jul. 2006, doi: 10.1162/neco.2006.18.7.1527.
[16] J. Karhunen, T. Raiko, and K. Cho, "Unsupervised Deep Learning: A Short Review".
[17] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How To Backdoor Federated Learning," in Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics, PMLR, Jun. 2020, pp. 2938–2948. Accessed: Jun. 07, 2024. [Online]. Available: https://proceedings.mlr.press/v108/bagdasaryan20a.html
[18] M. u Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Int. J. Comput. Appl., vol. 111, no. 7, pp. 1–6, Feb. 2015.
[19] E. Erdin, C. Zachor, and M. Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks," IEEE Commun. Surv. Tutor., vol. 17, pp. 1–1, Jul. 2015, doi: 10.1109/COMST.2015.2453434.
[20] S. Ganta, S. Kasiviswanathan, and A. Smith, "Composition Attacks and Auxiliary Information in Data Privacy," Proc. 14th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min. KDD 08, Mar. 2008, doi: 10.1145/1401890.1401926.
[21] WATI, "The Silent Assassins: Understanding Signature Wrapping Attacks," West Advanced Technologies, Inc. Accessed: Jun. 03, 2024. [Online]. Available: https://www.wati.com/the-silent-assassins-understanding-signature-wrapping-attacks/
[22] Z. Hlaing and M. Khaing, A Detection and Prevention Technique on SQL Injection Attacks. 2020, p. 6. doi: 10.1109/ICCA49400.2020.9022833.
[23] "A Detection and Prevention Technique on SQL Injection Attacks | Request PDF." Accessed: Jun. 03, 2024. [Online]. Available: https://www.researchgate.net/publication/339761008_A_Detection_and_Prevention_Technique_on_SQL_Injection_Attacks
[24] R. Tahir, "A Study on Malware and Malware Detection Techniques," Int. J. Educ. Manag. Eng., vol. 8, pp. 20–30, Mar. 2018, doi: 10.5815/ijeme.2018.02.03.
[25] V. Kouliaridis, K. Barmpatsalou, G. Kambourakis, and S. Chen, "A Survey on Mobile Malware Detection Techniques," IEICE Trans. Inf. Syst., vol. E103-D, pp. 204–211, Feb. 2020, doi: 10.1587/transinf.2019INI0003.
[26] "A Study on Malware and Malware Detection Techniques." Accessed: Jun. 02, 2024. [Online]. Available: https://www.researchgate.net/publication/324592375_A_Study_on_Malware_and_Malware_Detection_Techniques.
[27] P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyan, "Secure and Reliable Clustering in Wireless Sensor Networks: A Critical Survey," Comput. Netw., vol. 56, pp. 2726–2741, Jul. 2012, doi: 10.1016/j.comnet.2012.03.021.
[28] Z. Ghadimi, H. Fard, and H. Asadian, Security architecture of the Internet of Things. 2018.
[29] T. Lu, P. Yao, L. Zhao, Y. Li, F. Xie, and Y. Xia, "Towards Attacks and Defenses of Anonymous Communication Systems," Int. J. Secur. Its Appl., vol. 9, no. 1, pp. 313–328, Jan. 2015, doi: 10.14257/ijsia.2015.9.1.30.
[30] M. Nasereddin, A. Alkhamaiseh, M. Qasaimeh, and R. Al-Qassas, "A systematic review of detection and prevention techniques of SQL injection attacks," Inf. Secur. J. Glob. Perspect., pp. 1–14, Oct. 2021, doi: 10.1080/19393555.2021.1995537.
[31] H. A. Noman and O. M. F. Abu-Sharkh, "Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations," Sensors, vol. 23, no. 13, Art. no. 13, Jan. 2023, doi: 10.3390/s23136067.
[32] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "REATO: REActing TO denial of service attacks in the Internet of Things," Comput. Netw., vol. 137, Mar. 2018, doi: 10.1016/j.comnet.2018.03.020.
[33] "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks | PTP Journals & Magazine | IEEE Xplore." Accessed: Jun. 03, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/8932306
[34] A. Jahangeer, S. Bazai, S. Aslam, S. Marjan, M. Anas, and S. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective," IEEE Access, vol. PP, pp. 1–1, Jan. 2023, doi: 10.1109/ACCESS.2023.3246180.

[35] S. Çakır, S. Toklu, and N. Yalçın, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," IEEE Access, vol. 8, pp. 183678–183689, Oct. 2020, doi: 10.1109/ACCESS.2020.3029191.
[36] Z. Teng, M. Li, L. Yu, J. Gu, and M. Li, "Sinkhole Attack Defense Strategy Integrating SPA and Jaya Algorithms in Wireless Sensor Networks," Sensors, vol. 23, p. 9709, Dec. 2023, doi: 10.3390/s23249709.
[37] A. Mitrokotsa, M. Rieback, and A. Tanenbaum, Classification of RFID Attacks. 2008, p. 86.
[38] H. Haddadpajouh, A. Dehghantanha, R. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," Nov. 2019.
[39] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things," Internet Things J. IEEE, vol. 1, pp. 372–383, Oct. 2014, doi: 10.1109/JIOT.2014.2344013.
[40] "Sybil Attack - an overview | ScienceDirect Topics." Accessed: Jun. 03, 2024. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/sybil-attack
[41] "A survey: Attacks on RPL and 6LoWPAN in IoT | Request PDF." Accessed: Jun. 03, 2024. [Online].Available: https://www.researchgate.net/publication/275353396_A_survey_Attacks_on_RPL_and_6LoWPAN_in_IoT
[42] H.-N. Dai, Q. Wang, L. Dong, and R. Wong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas," Int. J. Distrib. Sens. Netw., vol. 2013, Aug. 2013, doi: 10.1155/2013/760834.
[43] C. C. Editor, "Cloned Tag - Glossary | CSRC." Accessed: Jun. 03, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/cloned_tag
[44] Y. Feng, W. Huang, S. Wang, Y. Zhang, and S. Jiang, "Detection of RFID cloning attacks: A spatiotemporal trajectory data stream-based practical approach," Comput. Netw., vol. 189, p. 107922, Apr. 2021, doi: 10.1016/j.comnet.2021.107922.
[45] "Security attacks in IoT: A survey." Accessed: Jun. 03, 2024. [Online]. Available: https://www.researchgate.net/publication/320251025_Security_attacks_in_IoT_A_survey
[46] "How can you prevent physical tampering of your IoT devices?" Accessed: Jun. 03, 2024. [Online]. Available: https://www.linkedin.com/advice/3/how-can-you-prevent-physical-tampering-your-iot-9tm3c
[47] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, Internet of Things: Security vulnerabilities and challenges. 2015, p. 187. doi: 10.1109/ISCC.2015.7405513.
[48] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things," J. Netw. Comput. Appl., vol. 49, pp. 112–127, Mar. 2015, doi: 10.1016/j.jnca.2014.11.011.
[49] H. Meziane, N. Ouerdi, K. Amine, and S. Mazouz, Internet of Things: Classification of attacks using CTM method. 2020, p. 5. doi: 10.1145/3386723.3387876.
[50] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things Security: Challenges and Key Issues," Secur. Commun. Netw., vol. 2021, p. e5533843, Sep. 2021, doi: 10.1155/2021/5533843.
[51] T. Rajmohan, P. H. Nguyen, and N. Ferry, "A decade of research on patterns and architectures for IoT security," Cybersecurity, vol. 5, no. 1, p. 2, Jan. 2022, doi: 10.1186/s42400-021-00104-7.
[52] "A Review of Security in Internet of Things | Request PDF." Accessed: Jun. 04, 2024. [Online]. Available: https://www.researchgate.net/publication/332643942.
[53] "9 Important Security Requirements to Consider for IoT Systems - IoTAC." Accessed: Jun. 04, 2024. [Online]. Available: https://iotac.eu/9-important-security-requirements-to-consider-for-iot-systems/
[54] "(PDF) Internet of Things Security and Privacy." Accessed: Jun. 04, 2024. [Online]. Available: https://www.researchgate.net/publication/309375790_Internet_of_Things_Security_and_Privacy
[55] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," Internet Things Cyber-Phys. Syst., Jan. 2024, doi: 10.1016/j.iotcps.2023.12.003.
[56] A. Ghaffari, N. Jelodari, S. pouralish, N. derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: a survey," Clust. Comput., Apr. 2024, doi: 10.1007/s10586-024-04509-0.

[57] V. Gugueoth, S. Safavat, and S. Shetty, "Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects," ICT Express, vol. 9, no. 5, pp. 941–960, Oct. 2023, doi: 10.1016/j.icte.2023.03.006.
[58] S. K. Singh, Y.-S. Jeong, and J. Park, "A Deep Learning-based IoT-oriented Infrastructure for Secure Smart City," Sustain. Cities Soc., vol. 60, p. 102252, May 2020, doi: 10.1016/j.scs.2020.102252.
[59] F. Ullah et al., "Cyber Security Threats detection in Internet of Things using Deep Learning approach," IEEE Access, vol. PP, pp. 1–1, Aug. 2019, doi: 10.1109/ACCESS.2019.2937326.
[60] "Sensors | Free Full-Text | Sequential Model Based Intrusion Detection System for IoT Servers Using Deep Learning Methods." Accessed: Jul. 14, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/21/4/1113
[61] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Comput. Secur., vol. 92, p. 101752, May 2020, doi: 10.1016/j.cose.2020.101752.
[62] "Electronics | Free Full-Text | An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks." Accessed: Jul. 14, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/9/12/2152
[63] "Deep Learning-Based Intrusion Detection for IoT Networks | IEEE Conference Publication | IEEE Xplore." Accessed: Jul. 14, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/8952154
[64] B. Adhi Tama and K. H. Rhee, "An Integration of PSO-based Feature Selection and Random Forest for Anomaly Detection in IoT Network," MATEC Web Conf., vol. 159, p. 01053, Mar. 2018, doi: 10.1051/matecconf/201815902021.
[65] M. Farukee, M. Shabit, M. Haque, and A. H. M. Sattar, "DDoS Attack Detection in IoT Networks Using Deep Learning Models Combined with Random Forest as Feature Selector," 2021, pp. 118–134. doi: 10.1007/978-981-33-6835-4_8.
[66] M. Arowolo, R. Ogundokun, S. Misra, O. Jonathan, and A. Kadri, "K-Nearest Neighbour Algorithm for Classification of IoT-Based Edge Computing Device," 2022, pp. 161–179. doi: 10.1007/978-3-030-80821-1_8.
[67] C. Guo, R. Zhuang, C. Su, C. Liu, and K.-K. R. Choo, "Secure and Efficient K Nearest Neighbor Query over Encrypted Uncertain Data in Cloud-IoT Ecosystem," IEEE Internet Things J., vol. PP, pp. 1–1, Aug. 2019, doi: 10.1109/JIOT.2019.2932775.
[68] "An Efficient Low Complexity Edge-Cloud Framework for Security in IoT Networks | Request PDF." Accessed: Jul. 13, 2024. [Online]. Available: https://www.researchgate.net/publication/349415304_An_Efficient_Low_Complexity_Edge-Cloud_Framework_for_Security_in_IoT_Networks
[69] M. Alshamkhany, W. Alshamkhany, M. Mansour, S. Dhou, and F. Aloul, Botnet Attack Detection Using Machine Learning. 2020. doi: 10.1109/IIT50501.2020.9299061.
[70] "(PDF) Efficient Detection and Classification of Internet-of-Things Malware Based on Byte Sequences from Executable Files." Accessed: Jul. 13, 2024. [Online]. Available: https://www.researchgate.net/publication/347517490_Efficient_Detection_and_Classification_of_Internet-of-Things_Malware_Based_on_Byte_Sequences_from_Executable_Files
[71] "Detecting malicious nodes via gradient descent and support vector machine in Internet of Things | Request PDF." Accessed: Jul. 13, 2024. [Online]. Available: https://www.researchgate.net/publication/334147458_Detecting_malicious_nodes_via_gradient_descent_and_support_vector_machine_in_Internet_of_Things
[72] "(PDF) A Multi-fusion IoT Authentication System Based on Internal Deep Fusion of ECG Signals."Accessed: Jul. 13, 2024. [Online]. Available: https://www.researchgate.net/publication/355177485_A_Multi-fusion_IoT_Authentication_System_Based_on_Internal_Deep_Fusion_of_ECG_Signals
[73] R. Majeed, N. A. Abdullah, and M. Mushtaq, "IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm," Int. J. Adv. Comput. Sci. Appl., vol. 12, pp. 422–427, Aug. 2021, doi: 10.14569/IJACSA.2021.0120748.
[74] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," J. Supercomput., vol. 74, Oct. 2018, doi: 10.1007/s11227-018-2413-7.

[75] S. Salaria, S. Arora, N. Goyal, P. Goyal, and S. Sharma, "Implementation and Analysis of an Improved PCA technique for DDoS Detection," 2020 IEEE 5th Int. Conf. Comput. Commun. Autom. ICCCA, pp. 280–285, Oct. 2020, doi: 10.1109/ICCCA49541.2020.9250912.
[76] D. Stiawan et al., "Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network," IEEE Access, vol. PP, pp. 1–1, Aug. 2021, doi: 10.1109/ACCESS.2021.3105517.
[77] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in 2017 IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP 2017 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Jun. 2017, pp. 2087–2091. doi: 10.1109/ICASSP.2017.7952524.
[78] J. Sicato, S. K. Singh, S. Rathore, and J. Park, "A Comprehensive Analyses of Intrusion Detection System for IoT Environment," J. Inf. Process. Syst., vol. 16, pp. 975–990, Sep. 2020, doi: 10.3745/JIPS.03.0144.
[79] A. A. Gendreau and M. Moorman, "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things," 2016 IEEE 4th Int. Conf. Future Internet Things Cloud FiCloud, pp. 84–90, Aug. 2016, doi: 10.1109/FiCloud.2016.20.
[80] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and Survey of Collaborative Intrusion Detection," ACM Comput. Surv., vol. 47, May 2015, doi: 10.1145/2716260.
[81] N. M. Alajmi and K. Elleithy, "A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks," in 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA: IEEE, Apr. 2016, pp. 1–6. doi: 10.1109/LISAT.2016.7494104.
[82] R. Tiburski, L. Amaral, E. de Matos, D. Azevedo, and F. Hessel, "The Role of Lightweight Approaches Towards the Standardization of a Security Architecture for IoT Middleware Systems," IEEE Commun. Mag., vol. 54, pp. 56–62, Dec. 2016, doi: 10.1109/MCOM.2016.1600462CM.
[83] T. Lu, P. Gao, L. Zhao, Y. Li, and W. Han, "Towards an Analysis of Passive Attacks on Anonymous Communication Systems," Int. J. Secur. Its Appl., vol. 10, pp. 1–12, Aug. 2016, doi: 10.14257/ijsia.2016.10.8.01.
[84] J. Kumar, B. Rajendran, B. Bindhumadhava, and N. Babu, XML wrapping attack mitigation using positional token. 2017, p. 42. doi: 10.1109/PKIA.2017.8278958.
[85] K. N. SunilKumar and Shivashankar, "A review on security and privacy issues in wireless sensor networks," in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore: IEEE, May 2017, pp. 1979–1984. doi: 10.1109/RTEICT.2017.8256945.
[86] Kamaldeep, M. Malik, and M. Dutta, "Contiki-based mitigation of UDP flooding attacks in the Internet of things," in 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida: IEEE, May 2017, pp. 1296–1300. doi: 10.1109/CCAA.2017.8229997.
[87] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks & defenses," in 2017 International Conference on Communication Technologies (ComTech), Apr. 2017, pp. 104–110. doi: 10.1109/COMTECH.2017.8065757.
[88] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, p. e9324035, Jan. 2017, doi: 10.1155/2017/9324035.
[89] S. Alvi, F. Hassan, and A. Mian, On the Energy Efficiency and Stability of RPL Routing Protocol. 2017. doi: 10.1109/IWCMC.2017.7986578.
[90] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model," Int. J. Adv. Comput. Sci. Appl. IJACSA, vol. 9, no. 3, Art. no. 3, 30 2018, doi: 10.14569/IJACSA.2018.090349.
[91] M. A. Patel and M. M. Patel, "Wormhole Attack Detection in Wireless Sensor Network," in 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore: IEEE, Jul. 2018, pp. 269–274. doi: 10.1109/ICIRCA.2018.8597366.
[92] S. Othman, T. Nabeel, F. Ba-Alwi, and A. Zahary, "Survey on Intrusion Detection System Types," Dec. 2018.

[93] Z. Feng and C. Hua, "Machine Learning-based RF Jamming Detection in Wireless Networks," 2018 Third Int. Conf. Secur. Smart Cities Ind. Control Syst. Commun. SSIC, pp. 1–6, Oct. 2018, doi: 10.1109/SSIC.2018.8556709.
[94] A. Alshammari, "INTERNET OF THINGS OBJECTIVES, BENEFITS, AND APPLICATIONS," Oral Sci. Int., Feb. 2019.
[95] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A Self Organizing Map Intrusion Detection System for RPL Protocol Attacks:," Int. J. Interdiscip. Telecommun. Netw., vol. 11, no. 1, pp. 30–43, Jan. 2019, doi: 10.4018/IJITN.2019010103.
[96] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges," Jul. 21, 2019, arXiv: arXiv:1907.08965. Accessed: Jun. 06, 2024. [Online]. Available: http://arxiv.org/abs/1907.08965
[97] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical Layer Security for the Internet of Things: Authentication and Key Generation," IEEE Wirel. Commun., vol. 26, no. 5, pp. 92–98, Oct. 2019, doi: 10.1109/MWC.2019.1800455.
[98] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," J. Big Data, vol. 6, no. 1, p. 111, Dec. 2019, doi: 10.1186/s40537-019-0268-2.
[99] S. R. Taghanaki, K. Jamshidi, and A. Bohlooli, "DEEM: A Decentralized and Energy Efficient Method for detecting sinkhole attacks on the internet of things," in 2019 9th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran: IEEE, Oct. 2019, pp. 325–330. doi: 10.1109/ICCKE48569.2019.8965177.
[100] A. Hamza, H. Gharakheili, and V. Sivaraman, "IoT Network Security: Requirements, Threats, and Countermeasures," ArXiv, Aug. 2020, Accessed: May 10, 2024. [Online]. Available: https://www.semanticscholar.org/paper/IoT-Network-Security%3A-Requirements%2C-Threats%2C-and-Hamza-Gharakheili/909ec0a8fd521f99f854b19bd1264566f98484af
[101] E. G. Ribera, B. Martinez Alvarez, C. Samuel, P. P. Ioulianou, and V. G. Vassilakis, "Heartbeat-Based Detection of Blackhole and Greyhole Attacks in RPL Networks," in 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal: IEEE, Jul. 2020, pp. 1–6. doi: 10.1109/CSNDSP49049.2020.9249519.
[102] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," Future Internet, vol. 12, no. 9, Art. no. 9, Sep. 2020, doi: 10.3390/fi12090157.
[103] M. A. Boudouaia, A. Abouaissa, A. Benayache, and P. Lorenz, "Divide and Conquer-based Attack against RPL Routing Protocol," in GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan: IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/GLOBECOM42002.2020.9322275.
[104] M. Alreshoodi, "An Experimental Study of IoT Networks Under Internal Routing Attack," Int. J. Comput. Netw. Commun., vol. 12, no. 4, pp. 91–104, Jul. 2020, doi: 10.5121/ijcnc.2020.12406.
[105] M. Emeç and M. H. Özcanhan, "THREE TYPES OF ATTACK SIMULATION ON INTERNET OF THINGS DEVICES," 2020.
[106] M. Preda and V.-V. Patriciu, "Simulating RPL Attacks in 6lowpan for Detection Purposes," in 2020 13th International Conference on Communications (COMM), Bucharest, Romania: IEEE, Jun. 2020, pp. 239–245. doi: 10.1109/COMM48946.2020.9142026.
[107] S. Cakir, S. Toklu, and N. Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," IEEE Access, vol. 8, pp. 183678–183689, 2020, doi: 10.1109/ACCESS.2020.3029191.
[108] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security Requirements for the Internet of Things: A Systematic Approach," Sensors, vol. 20, p. 5897, Oct. 2020, doi: 10.3390/s20205897.
[109] A. D. Seth, S. Biswas, and A. K. Dhar, "Mitigation Technique against Network Isolation Attack on RPL in 6LoWPAN Network," in TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON), Auckland, New Zealand: IEEE, Dec. 2021, pp. 68–73. doi: 10.1109/TENCON54134.2021.9707411.
[110] H. Alshahrani, "CoLL-IoT: A Collaborative Intruder Detection System for Internet of Things Devices," Electronics, vol. 10, p. 848, Apr. 2021, doi: 10.3390/electronics10070848.

[111] I. Essop, J. C. Ribeiro, M. Papaioannou, G. Zachos, G. Mantas, and J. Rodriguez, "Generating Datasets for Anomaly-Based Intrusion Detection Systems in IoT and Industrial IoT Networks," Sensors, vol. 21, no. 4, p. 1528, Feb. 2021, doi: 10.3390/s21041528.
[112] I. H. Abd Halim, M. H. Abdul Azziz, and M. F. Mohd Fuzi, "Sinkhole Attack in IDS: Detection and Performance Analysis for Agriculture-based WSN using Cooja Network Simulator," J. Comput. Res. Innov., vol. 6, no. 2, pp. 173–181, Sep. 2021, doi: 10.24191/jcrinn.v6i2.233.
[113] J. Shara, DEEP LEARNING METHODS FOR CYBERSECURITY. 2021.
[114] L. Alzubaidi et al., "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," J. Big Data, vol. 8, no. 1, p. 53, Mar. 2021, doi: 10.1186/s40537-021-00444-8.
[115] M. Tawfik, N. Al-Zidi, B. Al-sellami, A. Al-Hejri, and S. Nimbhore, Internet of Things-Based Middleware Against Cyber-Attacks on Smart Homes using SoftwareDefined Networking and Deep Learning. 2021. doi: 10.1109/ICCMST54943.2021.00014.
[116] T. J. Saleem and M. A. Chishti, "Deep learning for the internet of things: Potential benefits and use-cases," Digit. Commun. Netw., vol. 7, no. 4, pp. 526–542, Nov. 2021, doi: 10.1016/j.dcan.2020.12.002.
[117] K. P. Sampoornam, S. Saranya, G. K. Mohanapriya, P. Sandhiya Devi, and S. Dhaarani, "Analysis of LEACH Routing Protocol in Wireless Sensor Network with Wormhole Attack," in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India: IEEE, Feb. 2021, pp. 147–152. doi: 10.1109/ICICV50876.2021.9388540.
[118] S. S. Ambarkar and N. Shekokar, "Impact Analysis of RPL Attacks on 6Lo WPAN based Internet of Things network," in 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India: IEEE, Jul. 2021, pp. 1–5. doi: 10.1109/CONECCT52877.2021.9622711.
[119] T. W. Ching, A. H. M. Aman, W. M. H. Azamuddin, H. Sallehuddin, and Z. S. Attarbashi, "Performance Analysis of Internet of Things Routing Protocol for Low Power and Lossy Networks (RPL): Energy, Overhead and Packet Delivery," in 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia: IEEE, Jan. 2021, pp. 1–6. doi: 10.1109/CRC50527.2021.9392475.
[120] S. Sinha and Kruthi. G, "Network layer DoS Attack on IoT System and location identification of the attacker," in 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India: IEEE, Sep. 2021, pp. 22–27. doi: 10.1109/ICIRCA51532.2021.9545071.
[121] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," IEEE Access, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.
[122] R. Kaur and J. Kaur Sandhu, "A Study on Security Attacks in Wireless Sensor Network," in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India: IEEE, Mar. 2021, pp. 850–855. doi: 10.1109/ICACITE51222.2021.9404619.
[123] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," Sustain. Eng. Innov., vol. 3, pp. 23–29, Jan. 2021, doi: 10.37868/sei.v3i1.124.
[124] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: a survey," SN Appl. Sci., vol. 3, no. 1, p. 121, Jan. 2021, doi: 10.1007/s42452-021-04156-9.
[125] S. K. Wagle, A. A. Bazilraj, and K. P. Ray, "Energy efficient security solution for attacks on Wireless Sensor Networks," in 2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), Ernakulam, India: IEEE, Sep. 2021, pp. 313–318. doi: 10.1109/ACCESS51619.2021.9563325.
[126] Y. Xu et al., "Artificial intelligence: A powerful paradigm for scientific research," The Innovation, vol. 2, no. 4, p. 100179, Oct. 2021, doi: 10.1016/j.xinn.2021.100179.
[127] A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," Sensors, vol. 22, no. 21, p. 8417, Nov. 2022, doi: 10.3390/s22218417.
[128] A. Sandur and A. Giri, "Performance Analysis of the merged 6L0WPAN-CoAP and RPL-CoAP with different combination of MAC and RDC layer protocols," in 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India: IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/MysuruCon55714.2022.9972566.

[129] E. Ribera, B. Alvarez, C. Samuel, P. Ioulianou, and V. Vassilakis, "An Intrusion Detection System for RPL-Based IoT Networks," Electronics, vol. 11, p. 4041, Dec. 2022, doi: 10.3390/electronics11234041.
[130] F. Zahra, N. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning," Sensors, vol. 22, no. 18, p. 6765, Sep. 2022, doi: 10.3390/s22186765.
[131] I. Dissanayake, H. D. Weerasinghe, and A. Welhenge, "A generation of dataset towards an Anomaly-Based Intrusion Detection System to detect Denial of Sleep Attacks in Internet of Things (IoT)," in 2022 22nd International Conference on Advances in ICT for Emerging Regions (ICTer), Colombo, Sri Lanka: IEEE, Nov. 2022, pp. 092–097. doi: 10.1109/ICTer58063.2022.10024090.
[132] M. Aboubakar, M. Kellil, and P. Roux, "A review of IoT network management: Current status and perspectives," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 7, pp. 4163–4176, Jul. 2022, doi: 10.1016/j.jksuci.2021.03.006.
[133] M. Keerthika and D. Shanmugapriya, "A Systematic Survey on Various Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks (WSN)," in 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE), MANGALORE, India: IEEE, Dec. 2022, pp. 59–64. doi: 10.1109/ICRAIE56454.2022.10054309.
[134] M. Savva, I. Ioannou, and V. Vassiliou, "Fuzzy-Logic Based IDS for Detecting Jamming Attacks in Wireless Mesh IoT Networks," in 2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet), Pafos, Cyprus: IEEE, Jun. 2022, pp. 54–63. doi: 10.1109/MedComNet55087.2022.9810363.
[135] P. Deepavathi and C. Mala, "EMR-ESD: Ensure Multicast Routing and Enable Secure Data transmission protocol to perform multicast forwarding in RPL based IoT Networks," in 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), Kochi, India: IEEE, Jun. 2022, pp. 1–6. doi: 10.1109/IC3SIS54991.2022.9885612.
[136] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," IEEE Access, vol. 10, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.
[137] R. Tahri, Y. Balouki, A. Jarrar, and L. Abdellatif, "Intrusion Detection System Using machine learning Algorithms," ITM Web Conf., vol. 46, p. 02003, Jan. 2022, doi: 10.1051/itmconf/20224602003.
[138] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," Secur. Commun. Netw., vol. 2022, pp. 1–41, Aug. 2022, doi: 10.1155/2022/8951961.
[139] S. K. B.J and S. C.S, "Jamming Attack Detection Using EWMA in Clustered Wireless Sensor Network," in 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India: IEEE, Jul. 2022, pp. 1–5. doi: 10.1109/ICDSIS55133.2022.9915936.
[140] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, "An overview of IoT architectures, technologies, and existing open-source projects," Internet Things, vol. 20, p. 100626, Nov. 2022, doi: 10.1016/j.iot.2022.100626.
[141] V. Kiran, A. Sardana, and P. Kaur, "Defending Against Ddos Attacks in Rpl Using Subjective Logic Based Trust Approach For IOT," in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India: IEEE, Apr. 2022, pp. 1656–1660. doi: 10.1109/ICACITE53722.2022.9823719.
[142] V. R. J. Manne and S. Sreekanth, "Detection and Mitigation of RPL Routing Attacks in Internet of Things," in 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India: IEEE, Mar. 2022, pp. 481–485. doi: 10.23919/INDIACom54597.2022.9763140.
[143] Y. Sun and Y. Chen, "Detection of Wormhole Attacks in Wireless Sensor Networks Based on Anomaly Detection Algorithms," in 2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China: IEEE, Jan. 2022, pp. 777–782. doi: 10.1109/ICCECE54139.2022.9712659.
[144] A. Elhanashi, P. Dini, S. Saponara, and Q. Zheng, "Integration of Deep Learning into the IoT: A Survey of Techniques and Challenges for Real-World Applications," Electronics, vol. 12, no. 24, Art. no. 24, Jan. 2023, doi: 10.3390/electronics12244925.

[145] A. Kaveh, A. Pettersson, C. Rohner, and A. Johnsson, "On the Impact of Blackhole-Attack Variations on ML-based Intrusion Detection Systems in IoT," in NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA: IEEE, May 2023, pp. 1–4. doi: 10.1109/NOMS56928.2023.10154213.
[146] A. M. Konsta, A. L. Lafuente, and N. Dragoni, "Trust Management for Internet of Things: A Systematic Literature Review," Sep. 25, 2023, arXiv: arXiv:2211.01712. Accessed: Jun. 02, 2024. [Online]. Available: http://arxiv.org/abs/2211.01712
[147] G. A. Mukhaini, M. Anbar, S. Manickam, T. A. Al-Amiedy, and A. A. Momani, "A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in Internet of Things networks," J. King Saud Univ. - Comput. Inf. Sci., vol. 36, no. 1, p. 101866, Jan. 2024, doi: 10.1016/j.jksuci.2023.101866.
[148] G. S. Rao, M. Harshitha, V. R. Joshitha, S. S. Sravya, and M. V. Priya, "DoS Attack Detection in Wireless Sensor Networks (WSN) Using Hybrid Machine Learning Model," in 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India: IEEE, Mar. 2023, pp. 384–388. doi: 10.1109/SPIN57001.2023.10117098.
[149] H. Taherdoost, "Security and Internet of Things: Benefits, Challenges, and Future Perspectives," Electronics, vol. 12, no. 8, Art. no. 8, Jan. 2023, doi: 10.3390/electronics12081901.
[150] J. kh-madhloom and G. Alawadi, "LITERATURE REVIEW AND COMPREHENSIVE EVALUATION SECURITY AND PRIVACY IN WIRELESS NETWORK AND INTERNET OF THINGS (IOT)," vol. 13, Oct. 2023.
[151] J. Mohsin and S. Albermany, "Proposing an IOT Secure Framework for Monitoring COVID-19 Patients," in 2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT), Al-Muthana, Iraq: IEEE, Jul. 2023, pp. 263–266. doi: 10.1109/AICCIT57614.2023.10217893.
[152] M. Kolhar and S. M. Aldossary, "A Deep Learning Approach for Securing IoT Infrastructure with Emphasis on Smart Vertical Networks," Designs, vol. 7, no. 6, Art. no. 6, Dec. 2023, doi: 10.3390/designs7060139.
[153] N. Patil, S. Patel, and S. D. Lawand, "Research Paper On Artificial Intelligence And It's Applications," J. Adv. Zool., vol. 44, Dec. 2023, doi: 10.53555/jaz.v44iS8.3544.
[154] N. Saini, "RESEARCH PAPER ON ARTIFICIAL INTELLIGENCE & ITS APPLICATIONS," vol. 8, no. 4, 2023.
[155] R. Gupta, "Research Paper on Artificial Intelligence," Int. J. Eng. Comput. Sci., vol. 12, pp. 25654–20656, Feb. 2023, doi: 10.18535/ijecs/v12i02.4720.
[156] T. Rashid and S. Mustafa, "A Review on IoT: Layered Architecture, Security Issues and Protocols," Int. J. Comput. Sci. Netw. Secur., vol. 23, no. 9, pp. 100–110, Sep. 2023, doi: 10.22937/IJCSNS.2023.23.9.13.
[157] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," Sensors, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.
[158] W. Fei, H. Ohno, and S. Sampalli, "A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions," ACM Comput. Surv., vol. 56, no. 5, p. 111:1-111:40, Nov. 2023, doi: 10.1145/3625094.
[159] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, "Passive Rule-Based Approach to Detect Sinkhole Attack in RPL-Based Internet of Things Networks," IEEE Access, vol. 11, pp. 94081–94093, 2023, doi: 10.1109/ACCESS.2023.3310242.
[160] S. Rehman, S. Manickam, and N. Firdous, Impact of DoS/DDoS attacks in IoT environment: A study. 2023. doi: 10.1063/5.0150000.
[161] T. Altaf, X. Wang, W. Ni, G. Yu, R. Liu, and R. Braun, "A new concatenated Multigraph Neural Network for IoT intrusion detection," Internet Things, vol. 22, p. 100818, May 2023, doi: 10.1016/j.iot.2023.100818.
[162] T. Altaf, X. Wang, W. Ni, R. Liu, and R. Braun, "NE-GConv: A Lightweight Node Edge Graph Convolutional Network for Intrusion Detection," Comput. Secur., vol. 130, p. 103285, May 2023, doi: 10.1016/j.cose.2023.103285.
[163] T. Mazhar et al., "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," Brain Sci., vol. 13, no. 4, p. 683, Apr. 2023, doi: 10.3390/brainsci13040683.

[164]Md. A. Talukder et al., "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," J. Big Data, vol. 11, no. 1, p. 33, Feb. 2024, doi: 10.1186/s40537-024-00886-w.
[165] V. Choudhary, S. Tanwar, and T. Choudhury, "Generating IoT Specific Anomaly Datasets Using Cooja Simulator (Contiki-OS) and Performance Evaluation of Deep Learning Model Coupled with Aquila Optimizer," J. Comput. Sci., vol. 20, no. 4, pp. 365–378, Apr. 2024, doi: 10.3844/jcssp.2020.365.378.
[166] V. W. Thirumaran, N. Joseph, and U. Srikanth, "Levy Flight – Pelican Optimization Algorithm Based Refined Long Short-Term Memory for Network Intrusion Detection System," Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 3, Art. no. 3, Mar. 2024.
[167] A. Alfahaid, E. Alalwany, A. M. Almars, F. Alharbi, E. Atlam, and I. Mahgoub, "Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey," Sensors, vol. 25, no. 11, p. 3341, May 2025, doi: 10.3390/s25113341.
[168] E. Yang, S. Jeong, and C. Seo, "Harnessing feature pruning with optimal deep learning based DDoS cyberattack detection on IoT environment," Sci. Rep., vol. 15, no. 1, p. 17516, May 2025, doi: 10.1038/s41598-025-02152-2.
[169] M. Alharby, "Evaluating machine learning approaches for multiple attack classification with improved computational efficiency in IoT networks," Sci. Rep., vol. 15, no. 1, p. 39914, Nov. 2025, doi: 10.1038/s41598-025-23711-7.
[170] R. Jablaoui, O. Cheikhrouhou, M. Hamdi, and N. Liouane, "Deep learning enabled intrusion detection system for IoT security," EURASIP J. Wirel. Commun. Netw., vol. 2025, no. 1, p. 66, Aug. 2025, doi: 10.1186/s13638-025-02477-6.
[171] M. A. Ali and S. A. H. Al-Sharafi, "Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation," Discov. Internet Things, vol. 5, no. 1, p. 48, Apr. 2025, doi: 10.1007/s43926-025-00104-w.
[172] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," Cyber Secur. Appl., vol. 3, p. 100082, Dec. 2025, doi: 10.1016/j.csa.2024.100082.
[173] S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review," Discov. Internet Things, vol. 5, no. 1, p. 8, Jan. 2025, doi: 10.1007/s43926-025-00099-4.

AUTHORS



Dr. Surendra Kumar Patel is currently working as an Assistant Professor in the Department of Information Technology at the Government. N.P.G. College of Science, Raipur, India. He has published more than 40 research papers. His main research focuses on Grid Computing, Cloud Computing, IoT, AI, etc. He has more than 15 years of teaching experience and 12 years of research experience. One Ph.D. candidate has been awarded under his supervision, and currently, three research scholars are pursuing their Ph.D. under their guidance.



Ms. Rinki Kaur received her Master of Philosophy from Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India, in 2013, a Master's degree in Computer Applications at Chhattisgarh Swami Vivekanand University, Bhilai, Chhattisgarh, India, in 2010, a Bachelor's degree in Computer Science from Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India, in 2007. Currently pursuing Ph.D. from Pt. Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India. Her research interests include the Internet of Things (IoT), machine learning, and deep learning.