http://dx.doi.org/10.14500/aro.12629

# A Comprehensive Review of IoT Attack Detection: Taxonomy, IoT-aware Evaluation, and Research Challenges

Shilan S. Hameed[1†]

[1]Department of Software Engineering, Faculty of Engineering, Koya University, Danielle Mitterrand Boulevard, Koya KOY45, Kurdistan Region – F.R. Iraq

***Abstract*—The lack of security measures in Internet of Things (IoT) systems has made these tiny devices vulnerable to increasingly advanced and evolving cyber-attacks. Attack detection and prevention are one of the most promising approaches to mitigating these attacks. However, these techniques require more computing, memory, and energy than typical IoT devices can provide. In addition, the IoT network is distributed, heterogeneous, and dynamic. These limitations motivate this review to examine the effective use of machine learning and deep learning in detecting attacks on IoT systems. Despite the presence of prior studies on reviewing these techniques, there is still a gap in analyzing attack vectors and assessing the effectiveness of current detection techniques for IoT networks and environments, especially in terms of lightweight and real-time evaluation. In this work, a multidimensional taxonomy of IoT attacks and existing detection techniques is given. The included studies were critically analyzed to evaluate and assess their effectiveness, considering performance metrics, IoT system architecture, datasets, and deployment strategies. The core methodologies of the analyzed studies were examined to guide academia and industry in improving detection techniques. Results showed that most of the proposed techniques in the literature did not address IoT-specific requirements. However, techniques featuring lightweight, real-time, federated, and scalable solutions have been proposed, yet their practical effectiveness remains unvalidated. This review addresses key research gaps and future challenges, emphasizing the need for resource-efficient, adaptable detection methods that align with IoT constraints.**

***Index Terms*—Cyber-attack, Internet of Things, Machine learning, Review, Taxonomy.**

## I. Introduction

Cyber-physical systems (CPS) integrate physical devices with embedded computer systems and are widely applied across various domains, including healthcare, defense, energy systems, and industry (Aouedi, et al., 2022, Harkat, et al., 2024). With the advances of internet technologies such as 5G, 6G, growing the number of interconnected devices, and bringing Artificial Intelligence to the field, a new area is introduced, known as the Internet of Things (IoT) (Dimitrov, 2016). According to recent forecasts, the number of connected IoT devices is expected to reach ~27.1 billion by 2025 (Analytics, 2024). Despite this rapid growth, many IoT devices still operate with minimal security protocols and on open networks, making them especially vulnerable to various cyber-attacks (Othman and Abdullah, 2023). Similarly, when the number of IoT devices increases, the data produced by these devices will significantly increase (Paramesha, Rane and Rane, 2024). The overall annual data volume of related IoT devices globally is expected to approach 79.4 zettabytes (ZB) by 2025 (S. O'Dea, 2020; Jan and Sofi, 2024). The big data produced from the IoT devices is at a higher risk of cyber-attacks (Ahmed, et al., 2025). There are different efforts made in the literature to overcome security and privacy problems in the IoT (Rahim and Chishti, 2025). Intelligent attack and anomaly detection have been promising approaches for conventional networks and recently for the IoT system (Batool, et al., 2024). Nevertheless, the large amount of IoT-generated streaming heterogeneous data and the emergence of new cyber-attacks, and resource-limited IoT devices make the traditional detection systems less effective (Batool, et al., 2024). In the literature, efforts have been made to create IoT-aware attack detection systems, such as reducing the complexity of these techniques, along with using federated and real-time techniques. Therefore, it is crucial to analyze the current methods and highlight their gaps and drawbacks systematically. Furthermore, IoT attacks target multiple system layers and affect more than one security objective related to IoT. Therefore, a multidimensional analysis of IoT attacks is essential to understand their behavior and effects on the IoT system. This is crucial for supporting the development of effective and resilient security and intrusion detection solutions. In conclude, this review focuses on key aspects of IoT security, including attack vectors, machine learning/deep learning (ML/DL) techniques for attack detection, and their performance. A comprehensive taxonomy of cyber-attacks and ML/DL techniques is given.

ARO-The Scientific Journal of Koya University
Vol. XIV, No.1 (2026), Article ID: ARO.12629. 17 pages
DOI: 10.14500/aro.12629
Received: 17 September 2025; Accepted: 26 February 2026
Regular review paper: Published: 24 May 2026
†Corresponding author's e-mail: shilan.sameen@koyauniversity.org

Furthermore, existing approaches are systematically analyzed to highlight their strengths, limitations, and applicability to IoT systems. Hence, this review tries to find the gaps and limitations of the reviewed studies and sheds light on current challenges and future directions.

## II. Related Review Papers

IoT, cybersecurity, and ML/DL are rapidly growing areas in both academic research and industry. Many studies have been published to explore and tackle key challenges in these fields. However, existing reviews exhibit significant methodological gaps in how they categorize and deeply evaluate attack detection techniques and attack types to be compatible with IoT requirements.

For example, a review by (Elrawy, Awad and Hamed, 2018) provided an overview of intrusion detection systems (IDS) developed for the IoT concept, emphasizing the associated methodologies and requirements for developing the IoT-based IDS. However, their study lacked a detailed analysis of attack types and performance evaluation.

(Da Costa, et al., 2019) focused on ML techniques used for computer network security, particularly at the network layer. However, the attacks on the IoT system were not covered. It also heavily relied on general network datasets, narrowing attack types with limited performance assessment.

Similarly, Geetha et al. categorized ML/DL algorithms and discussed their application in attack detection using different tools and applications (Geetha and Thilagam, 2020). However, the review did not show the study's strengths, limitations, and directions. In addition, their work primarily focused on ML/DL, with limited attention given to detailed IoT attack analysis and behavior. (Hussain, et al., 2020) overviewed the IoT attack vectors and the existing ML/DL solutions for their detection. However, it lacked performance evaluation of the studies with limited depth on the attack vector's behavior. Furthermore, (Asharf, et al., 2020) reviewed ML/DL methods for IoT-based IDSs with a discussion on protocols, architecture, and attacks. However, it did not provide detailed taxonomies and a systematic analysis of IoT-aware performance.

In addition, (Merlino and Allegra, 2024) highlighted power-consumption analysis for detecting abnormal IoT device behavior. However, it did not provide a broad multi-vector attack taxonomy. Furthermore, the studies' strengths, limitations, and details of their placement and architecture are not given. (Haque, et al., 2023) reviewed datasets used for attack detection using ML/DL techniques, highlighting experimental findings and future research directions. However, the study was data-driven with limited critical evaluation, and it is biased toward dataset attacks, ignoring the behavior analysis of the attacks.

Therefore, this review attempts to address these gaps by evaluating studies based on IoT-aware compatibility. Furthermore, it gives a multidimensional taxonomy of IoT attacks and ML/DL techniques while analyzing lightweight, real-time, and architectural aspects, followed by each study's strengths and limitations. It also identifies key gaps with future research directions. The comparison of the recent review with previous related studies is listed in Table I.

## III. Methods

In this review, several related topics are elaborated, and hence, the following research questions (RQs) were generated:

1. RQ1: What are the attack types on the IoT system and their multidimensional taxonomies?
2. RQ2: What are the attack detection techniques in the IoT utilizing ML?
3. RQ3: Do the current attack detection techniques for the IoT have reasonable performance and represent the current IoT system based on (lightweight, real-time, architecture, attack types, datasets, and implementation environment)?
4. RQ4: What are the limitations of current studies and future challenges?

A total of 93 papers were used for this review. Among these, seven papers were selected as related review papers. 86 papers were used to answer the above-raised questions. The simplified steps for paper screening and selection are illustrated in Fig. 1.

First, a list of search queries was generated based on multiple keywords. They are used for searching on five different databases and repositories, namely Web of Science, Scopus, Science Direct, Springer Link, and IEEE Xplore. The user queries are as follows:

- (Cyber-attack OR intrusion OR anomaly) AND (IoT OR IoT) AND (ML techniques)
- (Cyber-attack OR intrusion OR anomaly) AND (CPS) AND (ML techniques)
- Cyber-attack AND (IoT OR IoT).

## IV. Results and Discussion

In the following sections, the results of the papers' analysis are given based on each RQ.

### *A. Attack Types on the IoT System and their Multidimensional Taxonomies (RQ1)*

Traditional and 0-day attacks can compromise IoT systems. Also, cryptographic and biometric solutions are often too complex for resource-constrained IoT devices (Hameed, et al., 2021, Alsaleh, Menai and Al-Ahmadi, 2025). Furthermore, the IoT sensor network has ad hoc behavior, implying that any node can enter and exit the network at any time. As a result, node confusion occurs in the IoT sensor network, enabling the attacker to intrude on the connected nodes (Poornima and Paramasivan, 2020).

The IoT attacks can be categorized based on different criteria. Thus, the taxonomy of the attacks is given in multiple ways in this study. They are categorized by IoT layers: perception (sensors and actuators), network (routers and gateways), and application/server layers (Fig. 2). Furthermore, by their impact on security requirements such

TABLE I
THE COMPARISON BETWEEN THE CURRENT REVIEW AND PREVIOUS RELATED REVIEW PAPERS

| References | Detailed and multidimensional taxonomy of IoT attacks | Details of ML methods | ML for attack and anomaly detection | Lightweight and real-time approaches | Evaluating performance and IoT compatibility | Systematic analysis |
|---|---|---|---|---|---|---|
| (Elrawy, Awad and Hamed, 2018) | ☐ | ☐ | ☑ | ◐ | ◐ | ☐ |
| (Da Costa, et al., 2019) | ☐ | ☐ | ☑ | ☐ | ◐ | ☐ |
| (Hussain, et al., 2020) | ◐ | ☑ | ☑ | ☐ | ◐ | ☐ |
| (Geetha and Thilagam, 2020) | ◐ | ☑ | ◐ | ☐ | ☐ | ☐ |
| (Asharf, et al., 2020) | ☑ | ☐ | ☑ | ☐ | ◐ | ☐ |
| (Haque, et al., 2023) | ◐ | ◐ | ☐ | ◐ | ☐ | ☑ |
| (Merlino and Allegra, 2024) | ◐ | ◐ | ◐ | ☐ | ☐ | ☐ |
| This study | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

☐: Not available, ◐: Partially available compared to our study, ☑: Available. ML: Machine learning, IoT: Internet of Things

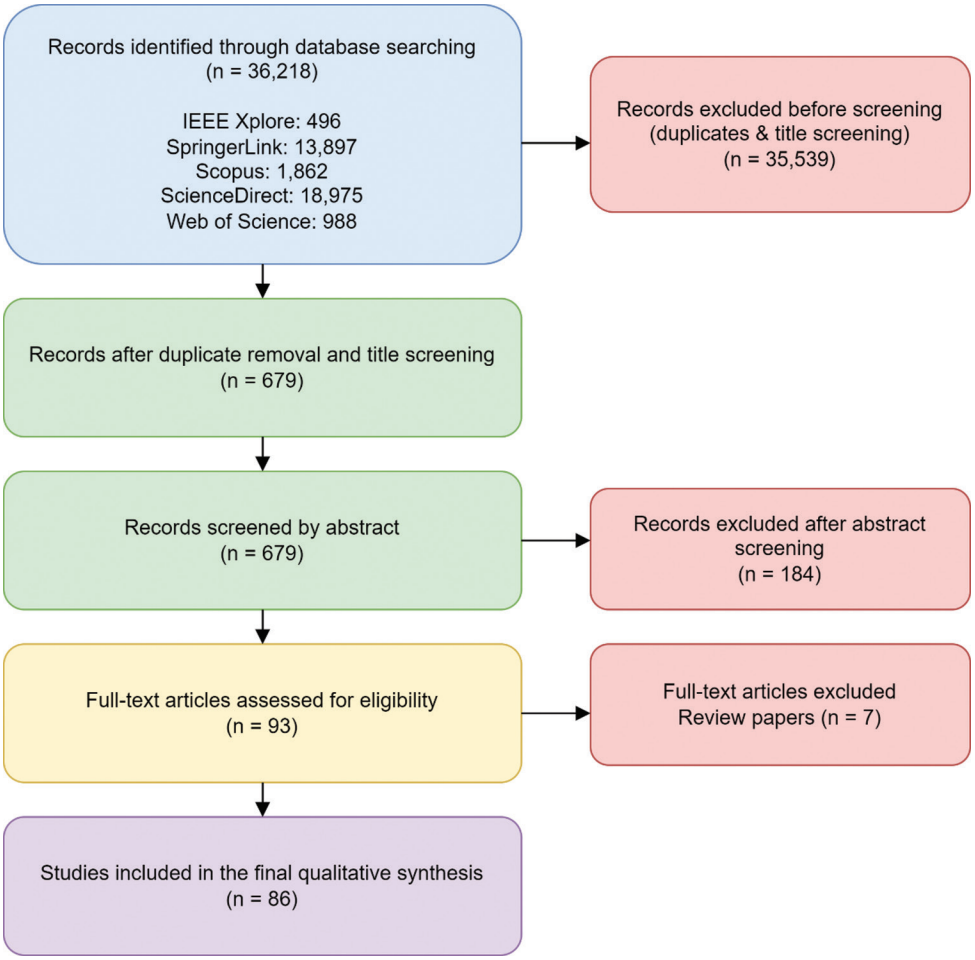


Fig. 1. The steps of paper exclusion following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses standard.

as confidentiality, integrity, and availability (Fig. 3).

*Attacks on confidentiality*

Attacks on confidentiality involve secretly observing, intercepting, or obtaining sensitive information without altering the system or its data. They can be categorized as passive attacks too, as shown in Fig. 3.

a. Eavesdropping attacks: This attack allows adversaries to monitor transmitted data and gather information. Cryptographic techniques prevent this attack, yet they are heavy for IoT devices (Gupta, et al., 2020). Many IoT devices are vulnerable to this attack (Raghunath, et al., 2025).
b. Man-in-the-middle attack (MIM): This attack leads to interception attacks, in which the attacker intercepts the data and resends it at a future time (Alsaleh, Menai and Al-Ahmadi, 2025). The adversary can detect the encryption keys and obtain access to the IoT system and data.
c. Packet analysis attacks: This is achieved by eavesdropping on an encrypted channel and obtaining plain data packets, or simply when the attacker captures transmitting data that

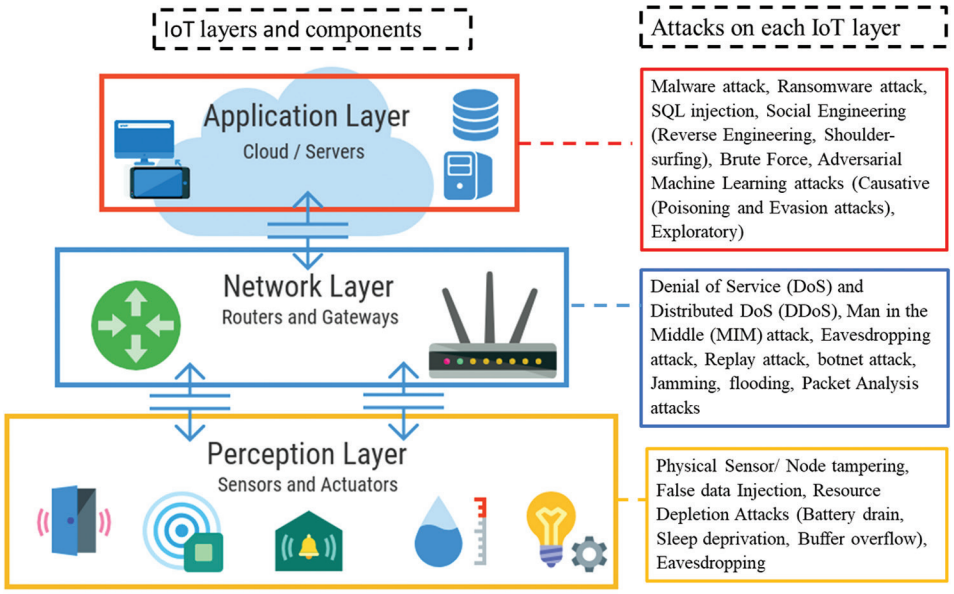


Fig. 2. The Internet of Things layers, their components, and their targeted attacks.

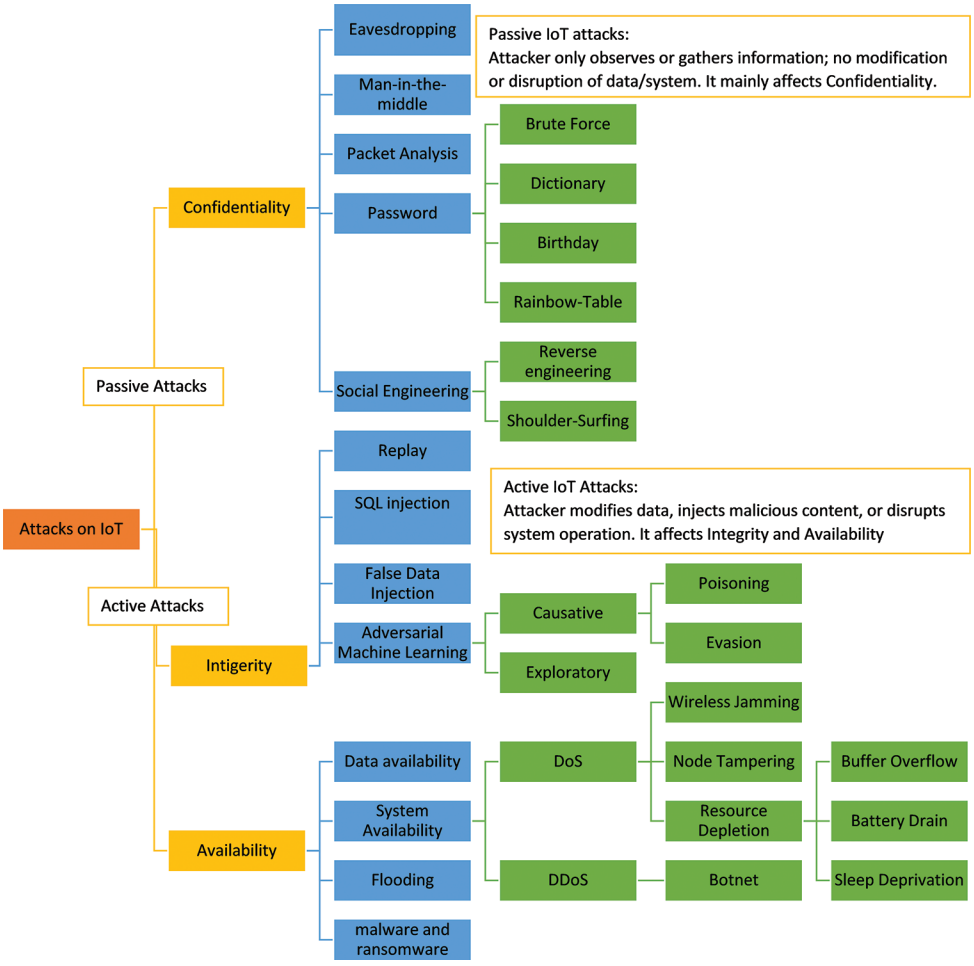


Fig. 3. The taxonomy of internet of things attacks.

is originally unencrypted. The attacker can reveal the user's private information.

d. Password attacks: This type of attack aims to gain the users' and providers' private data by accessing their passwords. A brute force is a password attack in which the attacker tries all possible combinations of passwords to obtain the correct one. Other forms of password attacks include dictionary, birthday, or rainbow-table attacks.

e. Social engineering: Social engineering is not among the technical threats. However, it relies on people's emotions to send back their passwords, names, IDs, and private information (Yaacoub, et al., 2020). This could be by talking with IoT users by voice call, or by sending emails including pictures and links with executable malicious code.
f. Reverse engineering attacks: In this form of attack, the adversary acts like a system technician who is showing help and guidance to fix the problem. As such, he/she could get information about the system's weaknesses.

*Attacks on integrity*

Attacks on integrity are caused by unauthorized modification, injection, or manipulation of data or system operations. They can be considered active attacks too, as shown in Fig. 3.

a. Replay attack: This type of attack is another form of a MIM, in which the attacker repeats or delays the data transmission. This will change the results of data analysis in the IoT databases. Sometimes, the attacker can either capture or manipulate the communicated data by transferring it to another spot. These messages are first collected then replayed to the desired destination (Racherla, et al., 2024).
b. SQL injection attack: Web servers and applications in the IoT use SQL for data manipulation and management in their databases. The attackers manipulate malicious queries to retrieve data related to users' passwords and IDs (Alsaleh, Menai and Al-Ahmadi, 2025; Kumar, Dutta and Pranav, 2024)
c. False data injection attack: This attack may be targeted at the databases, such as the private or public databases, or targeted at the sensor layer (Alsaleh, Menai and Al-Ahmadi, 2025).
d. Adversarial ML attacks: Data analytics at cloud or fog/edge nodes are vulnerable to adversarial attacks. The main objective is to disrupt the classification algorithm by altering the dataset, preventing it from learning an accurate model. This attack can be classified into two types: *Exploratory and causative*. Exploratory attacks exploit system flaws without affecting training, whereas causative attacks interfere with training through dataset manipulation. Causative attacks can also be divided into two types: *Poisoning and Evasion attacks* (Chakraborty, et al., 2018). Poisoning modifies training data with malicious examples, whereas evasion injects harmful data during testing to cause misclassification.

*Attacks on availability*

Attacks on availability behave by disrupting or denying access to systems, services, or data, preventing legitimate users from using them when needed. They can be considered active attacks too, as shown in Fig. 3.

a. Denial of service attacks (DoS): These attacks are generated to prevent system users from accessing the databases and tools (Zhang, 2025; Sinha, et al., 2024). They can be further classified as: wireless jamming attack, node tampering, resource depletion attacks, and battery drain (Mosenia and Jha, 2016; Shen, et al., 2020). Sleep deprivation and buffer overflow attacks can also be listed under this category (Rathore and Park, 2018).
b. Distributed DoS (DDoS): A stronger type of DoS that affects many networks worldwide simultaneously. It can severely disrupt the functionality of IoT devices and services (Othman and Abdullah, 2023; Raghunath, et al., 2025; Roopak, Tian and Chambers, 2020). Its scale is rising every day, with recent IoT DDoS attacks being primarily botnet and flood attacks.
c. Malware: Any malicious software is intended to interrupt or destroy a computer or system while still giving the hackers who installed it unauthorized access (Alsaleh, Menai and Al-Ahmadi, 2025; Al-Shurbaji, et al., 2025). Different types of malware include viruses, trojans, spyware, worms, and rootkits. Mirai is an IoT malware that leads to botnet attacks in the form of DDoS (Olanrewaju-George and Pranggono, 2025; Ahmed, et al., 2025).
d. Ransomware: It is a malicious program that blocks or restricts access to services on an infected device, demanding a ransom, commonly in cryptocurrency such as Bitcoin, for restoration (Hameed, et al., 2022). Crypto and Locker are two common ransomware types. Crypto ransomware encrypts essential files on a server, making them inaccessible to the owner. At the same time, the locker locks the IoT devices until the owner pays a ransom (Hameed, et al., 2022).

*Attacks on multi-pillars*

The above attacks primarily affect one of the CIA security pillars in IoT when they are initiated; however, their impact may extend beyond their success. Therefore, to show the extended impact of these attacks on more than one pillar, Fig. 4 is generated. The attacks in the shared areas indicate that they affect two or all the pillars once they are successful.

### *B. Attack Detection Techniques for IoT Using ML (RQ2)*

Advanced ML/DL approaches learn from enormous IoT data, allowing for the discovery of new attack tendencies

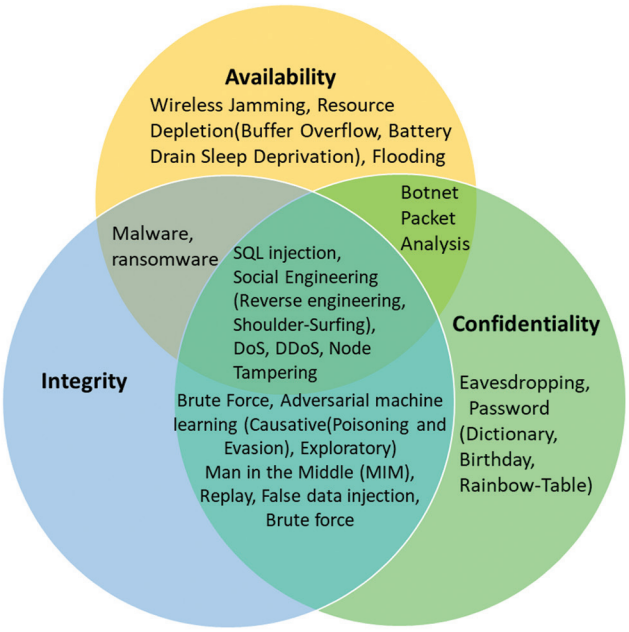


Fig. 4. The extended effect of attacks on multi-pillars.

(Abdullah, et al., 2025). Most of the studies focus on IDSs. An IDS is an agent that can be software or hardware. They can be divided into a host-based detection or a network-based, centralized, or distributed and collaborative (Alshahrani, 2021). Furthermore, they can be divided into signature-based, anomaly-based, or hybrid (Wang, et al., 2018). Signature-based IDSs are fast and efficient; however, they cannot detect new attacks. Anomaly-based IDSs effectively detect new attacks, but are heavy to implement and prone to a high false-positive rate.

In the following sections, the reviewed studies are classified based on the ML techniques and approaches. Furthermore, Table 1 in APPENDIX integrates attack taxonomy, ML model suitability, and detection efficiency into a single decision structure, as identified in Tables II-V.

The taxonomy of these techniques based on the reviewed studies is given in Fig. 5, which can be categorized as follows:

*Feature selection and supervised learning*

Supervised ML is mainly used for either classification, where target classes are known, or regression, where continuous output values are predicted from known input variables. Among these, supervised learning is the most widely used technique for attack detection and classification. Supervised learning is often preferred in IoT attack detection because it works with labeled data, which makes it more accurate and helps reduce false alarms.

Sometimes in the classification process, when the data has a larger number of features compared to its samples, i.e., in high-dimensional data, additional steps are required before classification, which takes advantage of feature selection methods. These methods use the approach of feature impact on the classification process. Any feature that contributes to high classification accuracy, called a discriminant feature, is kept, whereas redundant and irrelevant features are discarded. This improves the accuracy of the classification process and improves its efficiency by reducing complexity (Mohammadi, et al., 2019; Roopak, Tian and Chambers, 2020). The feature selection step is mainly effective in intrusion and attack detection to reduce the complexity of the techniques used in resource-limited devices (Musthafa, et al., 2024).

It was observed that the majority of studies have employed combined feature selection and supervised learning (Table II). They improved accuracy, but often lack complexity analysis and real-time capabilities (Ahmed, et al., 2025; Benmalek and Seddiki, 2025; Karthikeyan, Manimegalai and Rajagopal, 2024). The comparison and further details of such studies are given in Table II.

*Feature selection and unsupervised learning*

When the labels of the datasets are missing and unavailable, ML techniques are used for categorizing and clustering them (Qin, et al., 2019; Lee, Chien and Chang, 2024). Applications of unsupervised learning include fraud detection, anomaly detection (Moustafa, et al., 2021b), and so on. The accuracy of unsupervised learning techniques is highly related to the input datasets, and they are not as accurate as supervised learning. Unsupervised feature selection (reduction)/extraction is used as pre-processing for high-dimensional data reduction and feature transformation as pre-processing, which does not take advantage of class labels, such as singular value decomposition and principal components analysis. Unsupervised methods were not very common among the studies because they are useful for spotting new or unknown threats, but they tend to generate more false positives and demand greater computing power. Studies that implemented feature selection combined with unsupervised learning were (Ahmad, et al., 2019), (Mohammadi, et al., 2019), (Qin, et al., 2019), (Fantacci, et al., 2019), and (Liu, et al., 2018a). Nevertheless, traditional clustering methods struggle with detecting attacks that produce irregular feature space patterns. Density-based clustering algorithms overcome this by detecting clusters based on data density (Lee, Chien and Chang, 2024).

It was found few studies have combined feature selection with supervised and unsupervised learning at the same time for detecting known and unknown attacks, such as (Bostani and Sheikhan, 2017) and (Kumar, et al., 2019). Their details are given in Table III.

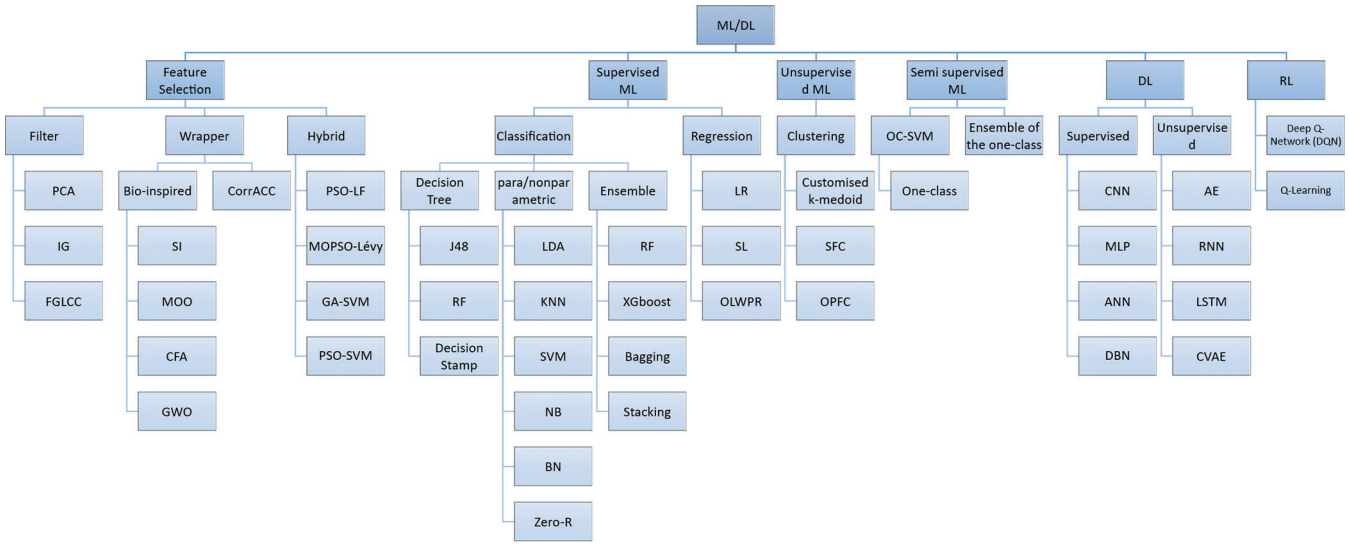


Fig. 5. The taxonomy of machine learning techniques for Internet of Things attack detection.

TABLE II
THE DETAILS OF THOSE STUDIES THAT USED FEATURE SELECTION AND SUPERVISED ML TECHNIQUES

| References | Method | Type of detection | Strengths | Research gaps | Software tools | Data sources |
|---|---|---|---|---|---|---|
| (Alshahrani, 2021) | KNN, RF, LR, XGboost | Signature-based attack detection | High accuracy, Low FPR | Not lightweight, Lacks Complexity metrics, not real-time | python 3.5 | UNSW-NB15 |
| (Moustafa, et al., 2021a) | Multiple classifier | Signature-based IoT attack detection | Distributed, Less time complex, new dataset | Not lightweight lacks complexity metrics | Python | ToN-IoT |
| (Bedi, et al., 2021) | ANN, LR, RF, SVM | Signature-based IoT attack detection. | High accuracy | Not lightweight, lacks complexity metrics, not real-time | Python | DS2OS |
| (Jan, et al., 2019) | (SVM) and using the packet arrival rate | Host-based intrusion detection (HIDS) | Lightweight attack detection, CPU time execution is considered. | Only the DDoS attack, memory allocation is not considered. | MATLAB | CICIDS2017 |
| (Ham, et al., 2014) | Linear SVM | Anomaly-based Malware detection | high accuracy, high TPR, low FPR | High complexity, lacks complexity metrics. | Not available | Not given |
| (Khan, et al., 2019) | AI-based (Statistical) | Anomaly-based Insider attack | Lightweight, improved accuracy, low FP | Lacks complexity metrics. | R programming, NS-2 simulation, | Simulated self-created |
| (Habib, Aljarah and Faris, 2020) | Multi-objective PSO-LF | Anomaly-based Botnet attack detection | Improved accuracy, improved TPR, New real dataset (UCI botnet) | High computational overhead | Weka | IoT Bot net dataset from UCI |
| (Anthi, Williams and Burnap, 2018) | ML-based+Rule based | Hybrid (DoS) attacks detection | Detecting a known and unknown attack, Adaptive | It does not support heterogeneous IoT and lacks a rule-based experiment | Weka | Testbed used, self-created |
| (Maleh, et al., 2015) | SVM | Hybrid (anomaly+ Signature) IDS HIDS | Improved accuracy, Lightweight | High FPR, Computation overhead not calculated, Outdated data | Not available | KDDcup'99 database |
| (Liu, et al., 2018b) | IPSO-SVM | Network- based. (NIDS) | Higher precision, Balanced energy use, Faster convergence | Resource usage not calculated | MATLAB | KDDcup`99 dataset |
| (Pajouh, et al., 2016) | LDA, NB, and modified KNN | Anomaly-based NIDS | Improved detection for low and high attacks | Limited attacks, High computation overhead, outdated dataset | Not available | NSL-KDD dataset |
| (Shafiq, et al., 2020) | Feature selection using (Corraccor) | Signature-based IoT Botnet detection | Improved Accuracy, Precision, Sensitivity (TPR), Specificity (TNR) | FPR not considered, some attacks not detected well, only the accuracy metric, lacks complexity metrics | Weka | Bot-IoT dataset |
| (Oreški and Andročec, 2018) | Data mining pre-processing feature selection | Signature-based intrusion detection NIDS | Feature selection improved efficiency | Outdated dataset | Not available | NSL-KDD |
| (Wang, et al., 2018) | Rabin fingerprint polynomial | Signature-based IDS NIDS | Real network data and simulation are used, and the computation time is reduced | Detection delay still exists, Privacy-preserving affected the efficiency | CanCloud | Self –created Real Network data |
| (Krimmling and Peter, 2014) | ML-based IDS for CoAP IoT devices | intrusion detection-based Hybrid | Usability for CoAP applications, lightweight model | High Training overhead | OMNeT++ simulation with C/C++, application code | Simulation |
| (Amouri, Alaparthy and Morgera, 2018). | DT and iterative LR | Signature and protocol-based | reduced computational overhead | Designed for a specific protocol and specific attacks | Cooja | Simulation dataset |
| (Gupta, et al., 2013) | Swarm intelligence (SI) paradigm | Anomaly-based, Hybrid Intrusion Detection | real-time, Adaptable, Hybrid | It cannot be applied in regions of WSNs that do not use the TCP/IP protocol. No implementation details | Not available | Not available |
| (Roopak, Tian and Chambers, 2020) | Multi-objective optimization method | Signature-based DDoS attack detection NIDS | Improved FPR due to multi-objective feature selection, Improved efficiency | Lacks complexity metrics, using one type of attack | MATLAB | CICIDS2017 |

(*Contd...*)

TABLE II
(*Continued*)

| References | Method | Type of detection | Strengths | Research gaps | Software tools | Data sources |
|---|---|---|---|---|---|---|
| (Bahşi, Nõmm and La Torre, 2018) | DT and feature selection | Signature-based Botnet detection NIDS | Improving efficiency by f. selection, high precision | Lacks Complexity metrics and FPR | Not available | Bot-IoT dataset |
| (Anthi, et al., 2019) | (NB, BN, DT, RF, J48, Zero R, MLP, SL) | Signature-based NIDS | Multiple attack detection | Lacks complexity metrics High training overhead | Weka | Self-created testbed |
| (Poornima and Paramasivan, 2020) | PCA and OLWPR | Anomaly detection at the sensor node | Online, low computation overhead | Lacks Complexity metrics, High error rate | Python | Intel Berkeley Research Lab (IBRL) dataset |
| (Kumar, Gupta and Tripathi, 2021) | Ensemble of DT, NB, and RF | Signature-based IoT network attacks detection | High accuracy, High TPR, Low FPR | High computational overhead, only binary classification | Python | ToN-IoT |
| (Hasan, et al., 2019) | SVM, DT, RF, and ANN | Hybrid detection | Better performance, sufficient metrics used for evaluation | High computational overhead | Pandas, Numpy, Matplotlib, Seaborn, scikit-learn, and Keras | Kaggle dataset DS2OS traffic traces |
| (Ahmed, et al., 2025) | Pearson correlation matrix with random forest (PCM-RF) and XGBoost | Signature-based | Accuracy of 99.39% and an 86% detection rate | High computational overhead limited scalability | Not available | IoTCIC2023 |
| (Benmalek and Seddiki, 2025) | CatBoost combined with PSO | Detection and Classification | Accuracy of 99.85% | needs in real-time detection and not scalable, heavy wrapper- classifier | Python 3.8.10, TensorFlow scikit-learn | RT_IoT2022 |
| (Karthikeyan, Manimegalai, and Rajagopal, 2024) | Firefly algorithm- based feature selection, SVM classification, and GWO-based parameter tuning | Signature NIDS | Accuracy of 99.34% | Can detect only known attacks, an outdated dataset, Heavy model | Not available | NSL-KDD |
| (Luqman, et al., 2025) | RF, SVM, and LSTM | Binary and multiclass Signature | Accuracy of 99.89% and 99.97% | Heavy model | Scikit-learn, numpy, and pandas libraries in Python | UNSW-NB15 and BoTIoT |
| (Raghunath, et al., 2025) | PCA, PSO -SVM | Singtuare, NIDS, Binary class | Accuracy of 98.5% | Outdated dataset | Not available | NSL KDD |

ML/DL: Machine learning/deep learning, DoS: Denial of service attacks, DDoS: Distributed denial of service attacks, IoT: Internet of things, IDS: Intrusion detection systems, PCA: Principal components analysis

TABLE III
The details of those Studies that used Feature Selection with Supervised and Unsupervised ML Techniques

| References | Methods | Type | Strengths | Research gaps | Software tools | Data sources |
|---|---|---|---|---|---|---|
| (Ahmad, et al., 2019) | K-medoid customized clustering | Anomaly detection Sensor node | Acceptable detection rate | Synthetic data is used. Lacks complexity metrics | Network, simulator (NS-2), and R Studio | Simulated dataset |
| (Mohammadi, et al., 2019) | Feature selection (FGLCC) and (CFA) with DT classifier | Signature-based NIDS | Feature selection improved accuracy | Outdated dataset, High resource allocation | Not available | KDD-Cup 99 |
| (Qin, et al., 2019) | PCA and clustering | Anomaly detection Hybrid | Lightweight can detect anomalies that cause slight changes in behavior; autonomous mobile agents are used | Detects only anomalies when largely propagated | Testbed generated | Self-created data, Real IoT data |
| (Fantacci, et al., 2019) | Statistical-based solution | Anomaly-based False data detection | Real-time, energy efficient, suitable for constrained devices, cooperative data IDs among nodes | User privacy problems in the fog layer, Complexity metrics ignored | Raspberry Pi3 | Real IoT dataset using testbed |
| (Liu, et al., 2018a) | (PCA) and (SFC) | Hybrid NIDS | Better adaptability, better detection time | Not lightweight, not accurate for big real-time data | Not available | Not given |
| (Lee, Chien and Chang, 2024) | LSTM and DBSCAN | NIDS | Privacy-preserving and non-IID problem mitigation | Risk of parameter exploitation by an attacker | FedMe framework | CICDDOS2019 |
| (Kumar, et al., 2019) | ML+blockchain | Malware detection | High accuracy and low FPR, real-time | Its failure to tackle the obfuscation methods. | Python programming language | Google Play and the Chinese App Store |

ML: Machine learning, PCA: Principal components analysis

TABLE IV
THE DETAILS OF THOSE STUDIES THAT USED SEMI-SUPERVISED ML TECHNIQUES

| References | Methods | Type | Strengths | Research gaps | Software tools | Data sources |
|---|---|---|---|---|---|---|
| (Moustafa, et al., 2021b) | Ensemble of the one-class classifier using Gaussian Mixture-based Correntropy | Anomaly-based IoT attack detection | Distributed, real-time, Higher accuracy | Recent IoT datasets have not been evaluated, and lack complexity metrics | R and Python languages | NSL-KDD UNSW-NB15 |
| ( Al Shorman, Faris and Aljarah, 2019) | (OC-SVM) and GWO | Anomaly Botnet attack | Improved accuracy, TPR, G-mean, and time of detection | High computational overhead | Anaconda Python framework version 5.2 | N-BaIoT dataset |
| (Eskandari, et al., 2020) | One-class classification | Anomaly-NIDS | Lightweight, low FPR, Multiple attacks | Not effective when the data speed is high | Raspberry Pi 3 Model B, AGILE gateway software, TCPDump, Python | Real datasets, self-created |
| (Garcia-Font, Garrigues and Rifà-Pous, 2017) | rule-based detection and OC-SVM | Hybrid NIDS | Applicability to large-scale WSNs | Not comprehensive to all types of attacks, High resource overhead | R programming language | Simulation dataset |

ML: Machine learning, IoT: Internet of Things, IDS: Intrusion Detection Systems

TABLE V
THE DETAILS OF THOSE STUDIES THAT USED SUPERVISED, UNSUPERVISED DL, AND RL TECHNIQUES

| References | Method | Type | Strengths | Research gaps | Software tools | Data sources |
|---|---|---|---|---|---|---|
| (Gu, et al., 2020) | Entropy-based Reinforcement learning | Signature-based IDS | Efficient in detecting high-rate and low-rate attacks | Lacks complexity metrics | Not available | Real IoT dataset |
| (Balakrishnan, et al., 2019) | (Deep Belief Network) | Signature-based NIDS | More than one type of attack is tested | Predicts only known attacks | Not available | Not given |
| (Parra, et al., 2020) | Cloud-based distributed deep learning | Anomaly-based Botnet attacks detection | Scalable, High detection accuracy, detecting at the device and at the back-end level | High computational overhead | Dell PowerEdge, R630 server, Python3.5.2 | N_BaIoT, PhishTank, OpenPhish, Curlie |
| (Lopez-Martin, et al., 2017) | Conditional Variational Auto-Encoder (ID-CVAE) | Anomaly-based IDS | Low complexity, High detection accuracy, Low latency | High false-positive rate, Training stage uses many resources, Outdated dataset | TensorFlow python package scikit-learn | NSL-KDD dataset |
| (Meidan, et al., 2018) | Deep Autoencoders | Anomaly-based IoT Botnet | Built a new real dataset (UCI botnet), High TPR | Works only for IP-based devices. | Not available | Self-Created IoT botnet |
| (Saeed, et al., 2016) | Recurrent Neural Network (RNN) | Anomaly-based IDS for sensors | High accuracy, minimal performance overhead. | Lacks detail of implementation | Not available | Not given |
| (Sudqi Khater, et al., 2019) | Multi-layer perceptron (MLP) | Hybrid HIDS | Lightweight, New datasets used | Computation overhead is still high | Raspberry Pi | (ADFA-LD) (ADFA-WD) |
| (Thamilarasu and Chawla, 2019) | Deep learning | Integrated Anomaly NIDS | The simulation used with real IoT data used 5 attacks, lightweight | The simulation did not give the same performance as the offline analysis | Scapy, Python, Keras | Self-created, real datasets |
| (Hizal, Cavusoglu and Akgun, 2024) | Convolutional and LSTM-based deep learning | Binary and multiclass attack detection, NIDS | Two-stage models outperformed the baselines. | Lacks complexity metrics | TensorFlow 2.13 and Python 3.11 | CICIoT2023 |
| (Alsaleh, Menai and Al-Ahmadi, 2025) | BiLSTM | Binary and multiclass attack detection, NIDS | Better performance and is suitable for resource-constrained IoT devices | The model is still heavy for edge devices | Scikit-learn (sklearn) library in Python | CICIoT2023 BoT-IoT, WUSTL-IIoT-2021, and Edge-IIoTset |
| (Karunamurthy, et al., 2025) | Chimp optimization algorithm and deep learning | Signature NIDS | Detection accuracy of 95.59% | A compromised local model may send incorrect parameters, high computational overhead in IoT. | Python, PyTorch, SciPy, and NumPy | MQTT dataset |
| (Musthafa, *et al*., 2024) | SVM- bagging and LSTM- stacking | Anomaly-based | Accuracies of 96.92% and 99.77% | Large model size and computationally intensive for IoT | Not available | UNSW-NB15, NSL-KD |

(*Contd*...)

TABLE V
(*Continued*)

| References | Method | Type | Strengths | Research gaps | Software tools | Data sources |
|---|---|---|---|---|---|---|
| (Olanrewaju-George and Pranggono, 2025) | Federated learning with AutoEncoder (AE) | Anomaly detection | Decentralized, enhanced performance and privacy | It faces scalability challenges, especially in large-scale IoT with many devices. | Python | N-BaIoT |
| (Racherla, et al., 2024) | Long-Short-Term-Memory (LSTM) | Anomaly-based | Detection rate of 96.8%, low detection time | It does not encompass a realistic environment, costly | Python and TensorFlow | CIC-IDS2017 |
| (Sinha, et al., 2024) | Hybridization of DNN and DAE | Anomaly-based | 98.97% of F-measure, Faster detection | Not scalable | Python | DS2OS dataset |
| (Zhang, 2025) | Multiple DL models | Anomaly-based | 99.985% accuracy, and 99.54% F1-score | Limited scalability | Python | BoT-IoT dataset |
| (Al-Naday, et al., 2024) | Federated DQN (FDQN) | Anomaly detection and multiclass attack classification | 75–85% detection accuracy; lower data/compute needs | Lacks real-time edge deployment and adversarial robustness analysis | Python | UNSW-NB15/ CIC-IDS2018 |
| (Bachl, et al., 2020). | Actor-Critic reinforcement learning with a three-layer LSTM classifier | Anomaly-based | 75% sparsity (skipping >75% packets) ~99% accuracy | Does not address the adversarial robustness complex | PyTorch | CIC-IDS-2017 |
| (Lalouani and Younis, 2021). | Distributed multi-layer framework (IoT-edge-fog-cloud) | Anomaly detection | Improves response rate, scalability, and fault tolerance | Limited real-world deployment | No available | Simulated EoT network data |
| (Bhargavi and Shiva, 2022). | RL in fog-IoT setups | Man-in-the-Middle (MitM) attack detection in fog-IoT | Low latency, energy use, high accuracy/robustness. | Focuses only on MitM | No available | Simulated fog-IoT with MitM scenarios |
| (Ajao and Apeh, 2023). | Genetic Algorithm-Reinforcement Learning (GARL) | Anomalies in IIoT | 96–99% accuracy; optimizes search space | No evaluation on constrained devices | No available | Simulation-based |
| (Najafli, Toroghi Haghighat and Karasfi, 2024). | Deep Reinforcement Learning-based (DRL) | Anomaly-based | | Dataset-dependent Complex not real IoT datasets | Python | CIC-IDS2018 |

RL: Reinforcement learning, DL: Deep learning, IoT: Internet of Things, IDS: Intrusion Detection Systems

*Semi-supervised learning*

These techniques are used when there is little labeled data in the dataset, whereas the rest of the dataset is unlabeled (Moustafa, et al., 2021b), such as in anomaly detection using behavior analysis (Bezerra, et al., 2019). Semi-supervised models are effective in avoiding adversarial attacks on ML techniques. When the model is introduced to the adversary data, it will avoid misclassification next time (Miyato, et al., 2018). Like supervised learning, there are classification and regression techniques in semi-supervised learning.

It was seen that semi-supervised methods were used in a limited number of studies. They're less commonly used since it's challenging to balance and combine both labeled and unlabeled data effectively. The studies are (Moustafa, et al., 2021b), (Al Shorman, Faris and Aljarah, 2019), (Eskandari, et al., 2020), and (Garcia-Font, Garrigues and Rifà-Pous, 2017). More details of these studies are given in Table IV.

*Supervised and unsupervised DL*

DL is a rapidly developing area within the broader field of ML. DL acts as the human brain, and its performance improves as more data becomes available. Today, DL has achieved an excellent reputation. Similar to traditional ML, DL can be applied in supervised, unsupervised, or semi-supervised settings. Its architectures are typically classified into discriminative and generative models: Discriminative models are mainly used for supervised learning tasks, whereas generative models are better suited for unsupervised learning (Olanrewaju-George and Pranggono, 2025).

Furthermore, with the advancement in computing resources such as high-performance processors and memories, big data handling could be achieved easily. DL has been successfully implemented in Network and IoT security, especially for IDS (Olanrewaju-George and Pranggono, 2025; Zhang, 2025). The details of all the DL-based studies are tabulated in Table V.

*Reinforcement learning (RL)*

RL does not need any learning data, as they learn from practice. The agent "experiments" with the method, and the program reacts to this experiment with incentives or penalties. RL trains agents via trial-and-error to optimize actions in dynamic environments through rewards and penalties. In attack detection for intrusion systems, RL monitors traffic states, flags anomalies as actions, and adapts to evolving threats like 0-day attacks. Recently, several papers have adopted RL for attack detection (Al-Naday, et al., 2024). Other researchers also adopted this technique for dynamic attack detection (Najafli, Toroghi Haghighat and Karasfi, 2024; Bachl, et al., 2020; Lalouani and Younis, 2021; Bhargavi and Shiva, 2022; Ajao and Apeh, 2023).

*Trend and distribution of the studies based on ML techniques*

To better answer RQ2, the studies were categorized by their proposed models. As shown in Fig. 6, most of the studies (45%) have utilized feature selection and supervised learning for detecting known attacks but have failed to detect unknown attacks. DL is the direction of the most recent studies, which was seen in 27% of the studies. RL was used by 11% of studies. Despite their effectiveness in detecting unseen attacks, unsupervised techniques were used in only 8%, and semi-supervised learning in 6%. Fig. 7 shows the evolution from traditional ML approaches to DL, federated learning, and edge-based frameworks from 2017 to 2025 using the reviewed studies.

*E. Do the Current Attack Detection Techniques for IoT have Reasonable Performance and Represent the Current IoT System (RQ3)*

*Lightweight and real-time approaches for attack detection*

Typical IoT devices have limited processing, memory, and energy, which makes data-hungry ML/DL solutions impractical. Therefore, detection techniques should consume minimal processing and network bandwidth while maintaining high accuracy with balanced complexity and overhead. A lightweight approach is when the security solution does not pose overhead on the devices and communication (Oreški and Andročec, 2018; Alsaleh, Menai and Al-Ahmadi, 2025). Some studies explicitly proposed lightweight methods (Karthikeyan, Manimegalai and Rajagopal, 2024; Sinha, et al., 2024), but most of the others have reduced model complexity (Table VI). Nevertheless, several studies claim lightweight models failed to prove and validate with complexity metrics, such as memory, CPU, and communication usage. Instead, they enhanced the detection accuracy and the false-positive rate. Furthermore, those studies that did not propose a lightweight model have reduced the complexity of their model compared to previous works.

Furthermore, in IoT systems, fast detection is significantly essential in reducing the potential impact of an attack and reducing the possibility of spreading to the whole network. Some studies have implemented real-time detection among the reviewed studies, whereas most of the rest of the studies have not used real-time detection. This is shown in Table VI.

*Model architecture and detection placement*

It was seen that while most of the earlier studies used a centralized detection approach, recent studies have used distributed techniques (Al-Naday, et al., 2024), as listed in Table VI.

More recently, edge, fog, and federated learning-based IDS have emerged (Olanrewaju-George and Pranggono, 2025; Karunamurthy, et al., 2025; Alsaleh, Menai and Al-Ahmadi, 2025). Distributed processing is closer to IoT devices in fog and edge computing. Further enhancements are provided by federated learning using collaborative model training, which preserves data privacy and reduces processing load. Recent edge-fog and federated-based studies report improved detection latency, scalability, and comparable or enhanced accuracy, yet with increased communication overhead during model aggregation. Fig. 8 shows the growing use of edge, fog, and federated learning-based approaches among the reviewed studies.

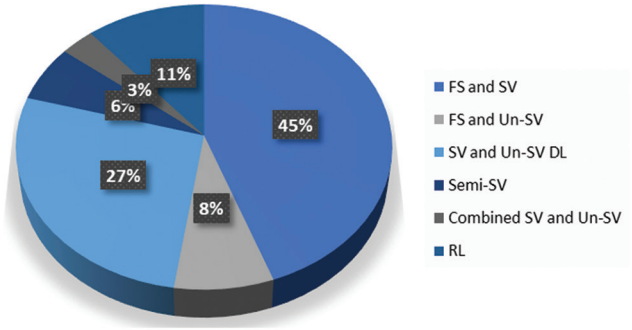


Fig. 6. The distribution of the studies based on different machine learning techniques.

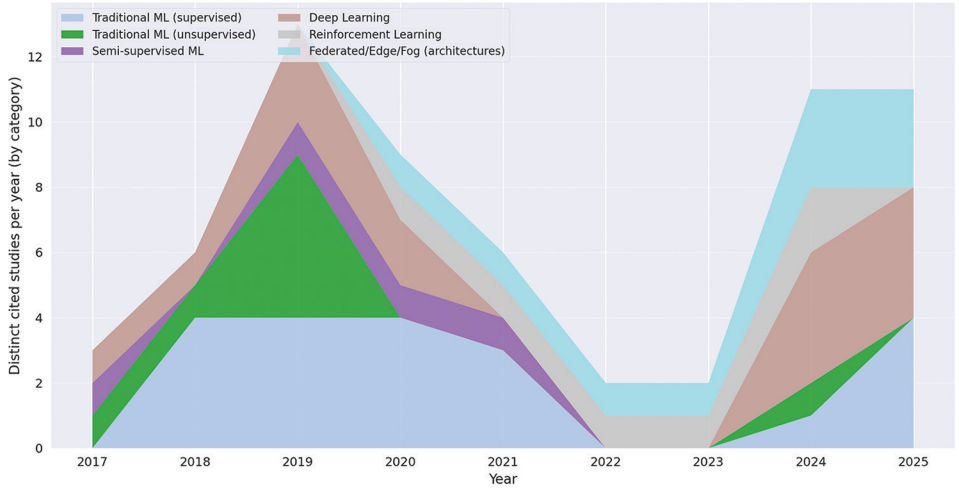


Fig. 7. Evolution of machine learning/deep learning-based Internet of Things attack detection approaches (2017–2025) from the review.

TABLE VI
PAPER CLASSIFICATION BASED ON LIGHTWEIGHT, REAL-TIME, AND DISTRIBUTED FEATURES

| References | Lightweight | Real-time | Distributed |
|---|---|---|---|
| (Ahmad, et al., 2019) | ✗ | ✗ | ✗ |
| (Ahmed, et al., 2025) | ✗ | ✗ | – |
| (Ajao and Apeh, 2023) | – | – | ✓ |
| (Al Shorman, Faris and Aljarah, 2019) | ✗ | ✓ | ✗ |
| (Al-Naday, et al., 2024) | – | – | ✓ |
| (Alsaleh, Menai and Al-Ahmadi, 2025) | ✓` | – | ✗ |
| (Alshahrani, 2021) | ✗ | ✗ | ✓ |
| (Amouri, Alaparthy and Morgera, 2018) | ✗ | ✗ | ✗ |
| (Anthi, Williams and Burnap, 2018) | ✗ | ✓ | ✗ |
| (Anthi, et al., 2019) | ✗ | – | – |
| (Bachl, et al., 2020) | – | – | ✓ |
| (Bahşi, Nõmm and La Torre, 2018) | – | – | ✓ |
| (Balakrishnan, et al., 2019) | ✓ | ✗ | ✗ |
| (Benmalek and Seddiki, 2025) | ✗ | ✗ | – |
| (Bhargavi and Shiva, 2022) | – | – | ✓ |
| (Bostani and Sheikhan, 2017) | ✗ | ✓ | ✓ |
| (Eskandari, et al., 2020) | ✓ | ✗ | ✓ |
| (Fantacci, et al., 2019) | ✓ | ✓ | ✗ |
| (Garcia-Font, Garrigues and Rifà-Pous, 2017) | ✗ | ✗ | ✗ |
| (Gu, et al., 2020) | ✗ | ✗ | ✗ |
| (Habib, Aljarah and Faris, 2020) | ✗ | ✓ | ✗ |
| (Hasan, et al., 2019) | ✗ | ✗ | ✗ |
| (Hizal, Cavusoglu and Akgun, 2024) | ✗ | ✓ | – |
| (Jan, et al., 2019) | ✓ | – | – |
| (Karthikeyan, Manimegalai and Rajagopal, 2024) | ✓ | ✗ | ✗ |
| (Karunamurthy, et al., 2025) | ✗ | – | ✓ |
| (Khan, et al., 2019) | ✓ | – | – |
| (Krimmling and Peter, 2014) | ✓ | ✗ | ✗ |
| (Kumar, Gupta and Tripathi, 2021) | ✗ | ✗ | ✗ |
| (Kumar, et al., 2019) | ✗ | ✗ | – |
| (Lalouani and Younis, 2021) | – | – | ✓ |
| (Lee, Chien and Chang, 2024) | – | – | ✓ |
| (Liu, et al., 2018a) | ✗ | ✗ | ✗ |
| (Liu, et al., 2018b) | ✓ | ✗ | ✗ |
| (Lopez-Martin, et al., 2017) | ✗ | ✗ | ✗ |
| (Luqman, et al., 2025) | ✗ | ✗ | ✗ |
| (Maleh, et al., 2015) | ✓ | – | – |
| (Meidan, et al., 2018) | ✗ | ✓ | ✗ |
| (Mohammadi, et al., 2019) | ✗ | ✗ | ✗ |
| (Moustafa, et al., 2021a) | ✗ | ✗ | ✓ |
| (Moustafa, et al., 2021b) | ✗ | ✓ | ✓ |
| (Musthafa, et al., 2024) | ✗ | ✗ | ✗ |
| (Najafli, Toroghi Haghighat and Karasfi, 2024) | – | – | ✓ |
| (Olanrewaju-George and Pranggono, 2025) | ✗ | ✗ | ✓ |
| (Oreški and Andročec, 2018) | ✓ | ✓ | ✓ |
| (Othman and Abdullah, 2023) | ✗ | ✗ | ✗ |
| (Parra, et al., 2020) | ✗ | ✗ | ✓ |
| (Poornima and Paramasivan, 2020) | ✓ | ✓ | ✗ |
| (Qin, et al., 2019) | ✓ | ✓ | ✓ |
| (Racherla, et al., 2024) | ✗ | ✓ | – |
| (Raghunath, et al., 2025) | ✗ | ✗ | ✗ |
| (Roopak, Tian and Chambers, 2020) | ✗ | ✗ | ✗ |
| (Saeed, et al., 2016) | ✗ | – | – |
| (Shafiq, et al., 2020) | ✗ | ✗ | ✗ |
| (Sinha, et al., 2024) | ✓ | ✗ | ✗ |
| (Sudqi Khater, et al., 2019) | ✓ | ✗ | ✓ |
| (Thamilarasu and Chawla, 2019) | ✗ | – | – |
| (Wang, et al., 2018) | ✓ | ✓ | ✓ |
| (Zhang, 2025) | ✗ | ✗ | ✗ |

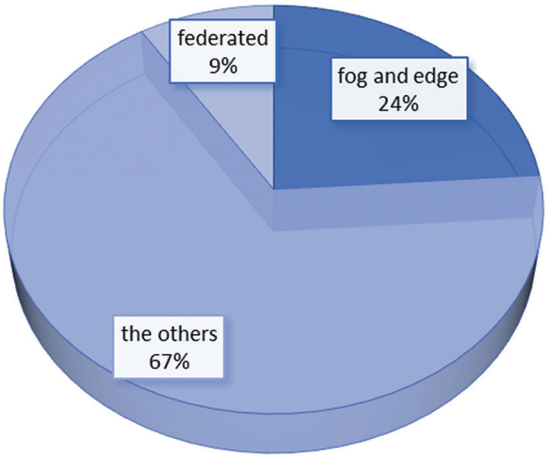


Fig. 8. The ratio of using edge/fog/federated-based approach among the studies.

*Compatible IoT datasets and study environment*

There are three main approaches for IDS validation: First, real-world (experimental) validation, which involves deploying the IDS on physical IoT hardware and real sensors. The second is a simulation using network or IoT simulators/emulators. Third, dataset-based (offline) validation, using benchmark datasets. It was seen that 25% of the studies had used self-created datasets, including simulation and testbed scenarios, as shown in Fig. 9. In addition, it was seen that the majority of the studies use benchmark public datasets, reaching 62% of the studies.

*The studied attack types*

Investigating the studies showed that recent solutions are built for specific attacks, and most of the studies deal with known attacks. However, the possibility of emerging new and 0-day attacks is high, but 0-day attack detection has received less attention. The studied attacks are illustrated in Fig. 10.

### *F. Limitations of Current Studies and Future Challenges (RQ4)*

The research gaps of the studies were discussed previously and presented beside each cited paper in Tables II-VI. These gaps were either explicitly stated by the study or derived from the study's critical analysis. The most frequent gaps are summarized below with possible solutions.

*Overreliance on supervised learning*

Most of the current work focuses on using supervised learning (Ahmed, et al., 2025; Benmalek and Seddiki, 2025; Karthikeyan, Manimegalai and Rajagopal, 2024; Luqman, et al., 2025; Raghunath, et al., 2025), which can detect known attack patterns. However, due to the continuous emergence of novel and 0-day attacks and open-network communication, methods capable of identifying evolving threats remain a critical research challenge.

*Limited consideration of IoT resource constraints*

While many studies focus on improving accuracy, detection rate, and lowering FPR, less attention is given to IoT-specific constraints such as energy consumption, computational overhead, and quality of service (Ahmed, et al., 2025;

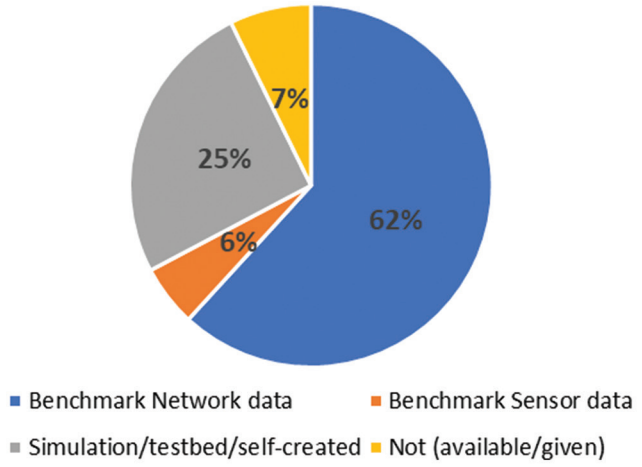


Fig. 9. The ratio of using different types of datasets among the studies.

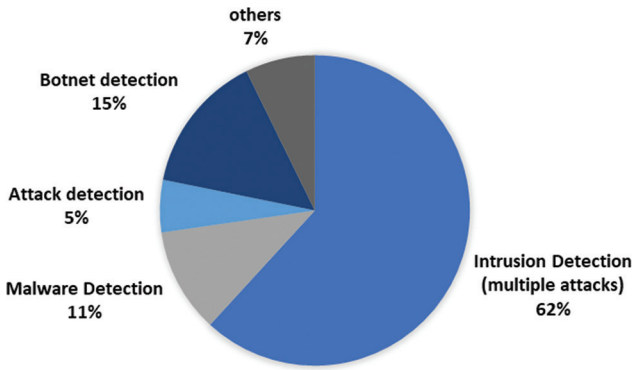


Fig. 10. The ratio of using different types of attacks among the studies.

Benmalek and Seddiki, 2025; Hizal, Cavusoglu and Akgun, 2024; Karunamurthy, et al., 2025; Luqman, et al., 2025; Musthafa, et al., 2024; Olanrewaju-George and Pranggono, 2025; Othman and Abdullah, 2023; Racherla, et al., 2024; Raghunath, et al., 2025; Zhang, 2025). Therefore, a lightweight IDS that requires only a small number of computational operations is needed. Thus, power resources and battery life must be considered in HIDS designs. In addition, when it comes to NIDS, real-time detection should be considered too.

*Privacy concerns in packet inspection–based approaches*

Deep packet inspection (DPI) should be avoided as DPI violates privacy rules (Fantacci, et al., 2019); furthermore, it leads to blocking packets, which may be critical for systems such as industrial and healthcare IoT.

*Federated and distributed computing limitations*

The centralized approaches of attack detection suffer from scalability and latency (Alsaleh, Menai and Al-Ahmadi, 2025; Karthikeyan, Manimegalai and Rajagopal, 2024; Luqman, et al., 2025; Musthafa, et al., 2024; Raghunath, et al., 2025; Zhang, 2025). Nevertheless, federated learning can improve privacy preservation, but it causes non-IID data distribution, communication cost, model convergence, and vulnerability to poisoned local updates (Olanrewaju-George and Pranggono, 2025; Karunamurthy, et al., 2025; Alsaleh, Menai and Al-Ahmadi, 2025). The hybrid architecture of the two techniques represents a promising research direction for tradeoffs.

*Lack of real-world deployment and reproducibility*

The majority of proposed IDS solutions lack validation in real-world applications since they are evaluated in controlled or offline environments. Consequently, their reliability and scalability are not fully understood under dynamic IoT conditions. Moreover, reproducibility and comparison of the studies cannot be investigated due to the limited availability of source code and configuration details.

*Poor generalization across datasets and environments*

Many IDS models are trained and tested on a single dataset or a limited number of scenarios, leading to overfitting and poor generalization when applied to different IoT environments, network configurations, or attack distributions.

*Limited availability of realistic and up-to-date IoT datasets*

Although some IoT datasets contain recent IoT attacks. However, some of these datasets are not publicly available or insufficiently documented. Therefore, researchers tend to use outdated datasets, avoiding requesting data or using less-studied datasets. Thus, generating new public datasets and trying to use new IoT datasets should be considered.

*Security of the IDS itself*

Few studies on poisoning, evasion, or model inversion attacks were reported for adversarial attacks against the IDS model, which led to a significant degradation in the detection performance.

## V. Conclusion

A systematic review was conducted to evaluate the current intrusion and attack detection techniques for IoT systems and networks. This review provides multiple taxonomies of cyber-attacks on the IoT ecosystem. Furthermore, it provides taxonomies of ML and DL techniques for attack detection with critical evaluation based on performance and IoT compatibility. Multiple aspects of each study were analyzed in terms of methods used, their strengths and weaknesses, employed environments, and architectures. The results of this review showed that recently, many promising methods, such as privacy-preserving and distributed federated learning, have been developed, yet these techniques are still tested on conventional network data and cannot fully address IoT-specific challenges, such as limited resources, heterogeneity, and scalability. This emphasizes the need for adaptive, lightweight, context-aware, and reliable solutions which are functioning in dynamic IoT environments. It is recommended that future works take a tradeoff between detection ability and complexity, validate in a real-time way, or use diverse datasets to ensure scalable and secure solutions.

## References

Abdullah, A.A., Mohammed, N.S., Khanzadi, M., Asaad, S.M., Abdul, Z.K., and Maghdid, H.S., 2025. In-depth analysis on machine learning approaches, *Aro the Scientific Journal of Koya University*, 13, pp.190-202.

Ahmad, B., Jian, W., Ali, Z.A., Tanvir, S., and Khan, M.S.A., 2019. Hybrid anomaly detection by using clustering for wireless sensor network, *Wireless Personal Communications*, 106, pp.1841-1853.

Ahmed, N., Ngadi, M.A., Rathore, M.S., and Mahmood, A., 2025. PCM-RF a hybrid feature selection mechanism for intrusion detection system in IoT, *Security and Privacy*, 8, p.e499.

Ajao, L.A., and Apeh, S.T., 2023. Secure edge computing vulnerabilities in smart cities sustainability using petri net and genetic algorithm-based reinforcement learning, *Intelligent Systems with Applications*, 18, p.200216.

Al Shorman, A., Faris, H., and Aljarah, I., 2019. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection, *Journal of Ambient Intelligence and Humanized Computing*, 11, pp.2809-2825.

Al-Naday, M., Dobre, V., Reed, M., Toor, S., Volckaert, B., and De Turck, F., 2024. Federated deep Q-learning networks for service-based anomaly detection and classification in edge-to-cloud ecosystems, *Annales des Telecommunications/ Annals of Telecommunications*, 79, pp.165-178.

Alsaleh, S., Menai, M.E.B., and Al-Ahmadi, S., 2025. A heterogeneity-aware semi-decentralized model for a lightweight intrusion detection system for IoT networks based on federated learning and BiLSTM, *Sensors (Basel)*, 25, p.1039.

Alshahrani, H.M., 2021. CoLL-IoT: A collaborative intruder detection system for internet of things devices, *Electronics*, 10, p.848.

Al-Shurbaji, T., Anbar, M., Manickam, S., Hasbullah, I.H., Alfriehat, N., Alabsi, B.A., Alzighaibi, A.R., and Hashim, H., 2025. Deep learning-based intrusion detection system for detecting IoT botnet attacks: A review, *IEEE Access*, 13, pp.11792-11822.

Amouri, A., Alaparthy, V.T., and Morgera, S.D., 2018. Cross Layer-Based Intrusion Detection Based on Network Behavior for IoT. In: *2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON)*, IEEE, United States, pp.1-4.

Analytics, I., 2024. *How Many IoT Devices are there?* Autobits Labs. Available from: https://autobitslabs.com/how-many-iot-devices-are-there [Last accessed on 2025 Sep 15].

Anthi, E., Williams, L., and Burnap, P., 2018. *Pulse: An Adaptive Intrusion Detection for the Internet of Things. Conference: PETRAS - Living in the Internet of Things Conference*.

Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., and Burnap, P., 2019. A supervised intrusion detection system for smart home IoT devices, *IEEE Internet of Things Journal*, 6, pp.9042-9053.

Aouedi, O., Piamrat, K., Muller, G., and Singh, K., 2022. Federated semisupervised learning for attack detection in industrial internet of things, *IEEE Transactions on Industrial Informatics*, 19, pp.286-295.

Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., and Wahab, A., 2020. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions, *Electronics*, 9, p.1177.

Bachl, M., Meghdouri, F., Fabini, J., and Zseby, T., 2020. SparseIDS: Learning Packet Sampling with Reinforcement Learning*, In: Conference: 2020 IEEE Conference on Communications and Network Security (CNS)*.

Bahşi, H., Nõmm, S., and La Torre, F.B., 2018. Dimensionality reduction for machine learning based iot botnet detection. In: *2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, IEEE, United States, pp.1857-1862.

Balakrishnan, N., Rajendran, A., Pelusi, D., and Ponnusamy, V., 2019. Deep belief network enhanced intrusion detection system to prevent security breach in the internet of things, *Internet of Things*, 14, p.100112.

Batool, S., Abid, M.K., Salahuddin, M.A., Aziz, Y., Naeem, A., and Aslam, N., 2024. Integrating IoT and machine learning to provide intelligent security in smart homes, *Journal of Computing and Biomedical Informatics*, 7, pp.224-238.

Bedi, P., Mewada, S., Vatti, R.A., Singh, C., Dhindsa, K.S., Ponnusamy, M., and Sikarwar, R., 2021. Detection of attacks in IoT sensors networks using machine learning algorithm, *Microprocessors and Microsystems*, 82, p.103814.

Benmalek, M., and Seddiki, A., 2025. Particle swarm optimization-enhanced machine learning and deep learning techniques for internet of things intrusion detection, *Data Science and Management*, 8, pp.423-435.

Bezerra, V.H., Da Costa, V.G.T., Barbon Junior, S., Miani, R.S., and Zarpelao, B.B., 2019. IoTDS: A one-class classification approach to detect botnets in internet of things devices, *Sensors (Basel)*, 19, p.3188.

Bhargavi, K., and Shiva, S.G., 2022. *Man-in-The-Middle attack Explainer for Fog computing using Soft Actor Critic Q-Learning Approach*, Institute of Electrical and Electronics Engineers Inc., United States, pp.100-105.

Bostani, H., and Sheikhan, M., 2017. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach, *Computer Communications*, 98, pp.52-71.

Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., and Mukhopadhyay, D., 2018. *Adversarial Attacks and Defences: A Survey*, [arXiv Preprint].

Da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R., and De Albuquerque, V.H.C., 2019. Internet of Things: A survey on machine learning-based intrusion detection approaches, *Computer Networks*, 151, pp.147-157.

Dimitrov, D.V., 2016. Medical internet of things and big data in healthcare, *Healthcare Informatics Research*, 22, pp. 156-163.

Elrawy, M.F., Awad, A.I., and Hamed, H.F., 2018. Intrusion detection systems for IoT-based smart environments: A survey, *Journal of Cloud Computing*, 7, p.21.

Eskandari, M., Janjua, Z.H., Vecchio, M., and Antonelli, F., 2020. Passban IDS: An intelligent anomaly based intrusion detection system for IoT edge devices, *IEEE Internet of Things Journal*, 7, pp.6882-6897.

Fantacci, R., Nizzi, F., Pecorella, T., Pierucci, L., and Roveri, M., 2019. False data detection for fog and internet of things networks, *Sensors*, 19, p.4235.

Garcia-Font, V., Garrigues, C., and Rifà-Pous, H., 2017. Attack classification schema for smart city WSNs, *Sensors (Basel)*, 17, p.771.

Geetha, R., and Thilagam, T., 2020. A review on the effectiveness of machine learning and deep learning algorithms for cyber security, *Archives of Computational Methods in Engineering*, 28, pp.2861-2879.

Gu, T., Abhishek, A., Fu, H., Zhang, H., Basu, D., and Mohapatra, P., 2020. Towards Learning-Automation IoT Attack Detection Through Reinforcement Learning. In: *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, IEEE, United States, pp.88-97.

Gupta, A., Pandey, O.J., Shukla, M., Dadhich, A., Mathur, S., and Ingle, A., 2013. Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks. *2013 IEEE International Conference on Computational Intelligence and Computing Research*, IEEE, United States, pp.1-7.

Gupta, R., Tanwar, S., Tyagi, S., and Kumar, N., 2020. Machine learning models for secure data analytics: A taxonomy and threat model, *Computer Communications*, 153, pp. 406-440.

Habib, M., Aljarah, I., and Faris, H., 2020. A modified multi-objective particle swarm optimizer-based lévy flight: An approach toward intrusion detection in internet of things, *Arabian Journal For Science And Engineering*, 45, pp.6081-6108.

Ham, H.S., Kim, H.-H., Kim, M.-S., and Choi, M.-J., 2014. Linear SVM-based android malware detection for reliable IoT services, *Journal of Applied Mathematics*, 2014, pp.1-10.

Hameed, S.S., Hassan, W.H., Latiff, L.A., and Ghabban, F., 2021. A systematic review of security and privacy issues in the internet of medical things; The role of machine learning approaches, *PeerJ Computer Science*, 7, p.e414.

Hameed, S.S., Selamat, A., Latiff, L.A., Razak, S.A., and Krejcar, O., 2022. Multi-classification of imbalance worm ransomware in the IoMT system. In:

*New Trends in Intelligent Software Methodologies, Tools and Techniques*, IOS Press, Netherlands.

Haque, S., El-Moussa, F., Komninos, N., and Muttukrishnan, R., 2023. A systematic review of data-driven attack detection trends in IoT, *Sensors (Basel)*, 23, p.7191.

Harkat, H., Camarinha-Matos, L.M., Goes, J., and Ahmed, H.F., 2024. Cyber-physical systems security: A systematic review, *Computers and Industrial Engineering*, 188, p.109891.

Hasan, M., Islam, M.M., Zarif, M.I.I., and Hashem, M., 2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, *Internet of Things*, 7, p.100059.

Hizal, S., Cavusoglu, U., and Akgun, D., 2024. A novel deep learning-based intrusion detection system for IoT DDoS security, *Internet of Things*, 28, p101336.

Hussain, F., Hussain, R., Hassan, S.A., and Hossain, E., 2020. Machine learning in IoT security: Current solutions and future challenges, *IEEE Communications Surveys and Tutorials*, 22, p.1.

Jan, I., and Sofi, S., 2024. Data management for resource optimization in medical IoT, *Health and Technology*, 14, pp.51-68.

Jan, S.U., Ahmed, S., Shakhov, V., and Koo, I., 2019. Toward a lightweight intrusion detection system for the internet of things, *IEEE Access*, 7, pp. 42450-42471.

Karthikeyan, M., Manimegalai, D., and Rajagopal, K., 2024. Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection, *Sci Rep*, 14, p.231.

Karunamurthy, A., Vijayan, K., Kshirsagar, P.R., and Tan, K.T., 2025. An optimal federated learning-based intrusion detection for IoT environment, *Sci Rep*, 15, p.8696.

Khan, A.Y., Latif, R., Latif, S., Tahir, S., Batool, G., and Saba, T., 2019. Malicious insider attack detection in IoTs using data analytics, *IEEE Access*, 8, pp.11743-11753.

Krimmling, J., and Peter, S., 2014. Integration and evaluation of intrusion detection for CoAP in smart city applications. In: *2014 IEEE Conference on Communications and Network Security*, IEEE, United States, pp.73-78.

Kumar, A., Dutta, S., and Pranav, P., 2024. Analysis of SQL injection attacks in the cloud and in WEB applications, *Security and Privacy*, 7, p.e370.

Kumar, P., Gupta, G.P., and Tripathi, R., 2021. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks, *Computer Communications*, 166, pp.110-124.

Kumar, R., Zhang, X., Wang, W., Khan, R.U., Kumar, J., and Sharif, A., 2019. A multimodal malware detection technique for Android IoT devices using various features, *IEEE Access*, 7, pp.64411-64430.

Lalouani, W., and Younis, M., 2021. *Robust Distributed Intrusion Detection System for Edge of Things*, Institute of Electrical and Electronics Engineers Inc., United States.

Lee, Y.C., Chien, W.C., and Chang, Y.C., 2024. FedDB: A federated learning approach using DBSCAN for DDoS attack detection, *Applied Sciences*, 14, p.10236.

Liu, L., Xu, B., Zhang, X., and Wu, X., 2018a. An intrusion detection method for internet of things based on suppressed fuzzy clustering, *EURASIP Journal on Wireless Communications and Networking*, 2018, p.113.

Liu, S., Wang, L., Qin, J., Guo, Y., and Zuo, H., 2018b. An intrusion detection model based on IPSO-SVM algorithm in wireless sensor network, *Journal of Internet Technology*, 19, pp. 2125-2134.

Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., and Lloret, J., 2017. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot, *Sensors*, 17, p.1967.

Luqman, M., Zeeshan, M., Riaz, Q., Hussain, M., Tahir, H., Mazhar, N., and Khan, M.S., 2025. Intelligent parameter-based in-network IDS for IoT using UNSW-NB15 and BoT-IoT datasets, *Journal of the Franklin Institute*, 362, p.107440.

Maleh, Y., Ezzati, A., Qasmaoui, Y., and Mbida, M., 2015. A global hybrid intrusion detection system for wireless sensor networks, *Procedia Computer Science*, 52, pp.1047-1052.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., and Elovici, Y., 2018. N-BaIoT-network-based detection of IoT botnet attacks using deep autoencoders, *IEEE Pervas Comput*, 17(3), pp.12-22.

Merlino, V., and Allegra, D., 2024. Energy-based approach for attack detection in IoT devices: A survey, *Internet of Things*, 27, p.101306.

Miyato, T., Maeda, S.I., Koyama, M., and Ishii, S., 2018. Virtual adversarial training: A regularization method for supervised and semi-supervised learning, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41, pp.1979-1993.

Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., and Karimipour, H., 2019. Cyber intrusion detection by combined feature selection algorithm, *Journal of Information Security and Applications,* 44, pp.80-88.

Mosenia, A., and Jha, N.K., 2016. A comprehensive study of security of internet-of-things, *IEEE Transactions on Emerging Topics in Computing*, 5, pp.586-602.

Moustafa, N., Garg, S., Stinkova, E., Jones, T., and Sioutis, C., 2021a. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets, *Sustainable Cities and Society*, 72, p.102994.

Moustafa, N., Keshk, M., Choo, K.K.R., Lynar, T., Camtepe, S., and Whitty, M., 2021b. DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks, *Future Generation Computer Systems*, 118, pp.240-251.

Musthafa, M.B., Huda, S., Kodera, Y., Ali, M.A., Araki, S., Mwaura, J., and Nogami, Y., 2024. Optimizing IoT intrusion detection using balanced class distribution, feature selection, and ensemble machine learning techniques, *Sensors (Basel)*, 24, p.4293.

Najafli, S., Toroghi Haghighat, A., and Karasfi, B., 2024. A novel reinforcement learning-based hybrid intrusion detection system on fog-to-cloud computing, *Journal of Supercomputing*, 80, pp.26088-26110.

Olanrewaju-George, B., and Pranggono, B., 2025. Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models, *Cyber Security and Applications,* 3, p.100068.

Oreški, D., and Andročec, D., 2018. Hybrid Data Mining Approaches for Intrusion Detection in the Internet of Things. In: *2018 International Conference on Smart Systems and Technologies (SST)*. IEEE, United States, pp.221-226.

Othman, T.S., and Abdullah, S.M., 2023. An intelligent intrusion detection system for internet of things attack detection and identification using machine learning, *Aro the Scientific Journal of Koya University,* 11, pp. 126-137.

Pajouh, H.H., Javidan, R., Khayami, R., Ali, D., and Choo, K.K.R., 2016. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks, *IEEE Transactions on Emerging Topics in Computing*, 7, pp.314-323.

Paramesha, M., Rane, N., and Rane, J., 2024. Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. In: *Artificial Intelligence, Machine Learning, Internet of Things, and Blockchain for Enhanced Business Intelligence*, [SSRN Paper].

Parra, G.D.L.T., Rad, P., Choo, K.K.R., and Beebe, N., 2020. Detecting internet of things attacks using distributed deep learning, *Journal of Network and Computer Applications*, 163, p.102662.

Poornima, I.G.A., and Paramasivan, B., 2020. Anomaly detection in wireless sensor network using machine learning algorithm, *Computer Communications*, 151, pp.331-337.

Qin, T., Wang, B., Chen, R., Qin, Z., and Wang, L., 2019. IMLADS: Intelligent maintenance and lightweight anomaly detection system for internet of things, *Sensors (Basel)*, 19, p.958.

Racherla, S., Sripathi, P., Faruqui, N., Alamgir Kabir, M., Whaiduzzaman, M., and Aziz Shah, S., 2024. Deep-IDS: A real-time intrusion detector for IoT nodes using deep learning, *IEEE Access*, 12, pp.63584-63597.

Raghunath, M.P., Deshmukh, S., Chaudhari, P., Bangare, S.L., Kasat, K., Awasthy, M., Omarov, B., and Waghulde, R.R., 2025. PCA and PSO based optimized support vector machine for efficient intrusion detection in internet of things, *Measurement Sensors*, 37, p.101806.

Rahim, R., and Chishti, M.A., 2025. IoT security innovations: Recent technologies, threats, and solutions, *SN Computer Science*, 6, p.593.

Rathore, S., and Park, J.H., 2018. Semi-supervised learning based distributed attack detection framework for IoT, *Applied Soft Computing,* 72**,** pp. 79-89.

Roopak, M., Tian, G.Y., and Chambers, J., 2020. Multi-objective-based feature selection for DDoS attack detection in IoT networks, *IET Networks*, 9, pp. 120-127.

S. O'dea, S., 2020. *Data Volume of Internet of Things (IoT) Connections Worldwide in 2019 and 2025(in Zettabytes)*. Statista. Available from: https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size [Last accessed on 2021 May 31].

Saeed, A., Ahmadinia, A., Javed, A., and Larijani, H., 2016. Random neural network based intelligent intrusion detection for wireless sensor networks, *Procedia Computer Science,* 80, pp. 2372-2376.

Shafiq, M., Tian, Z., Bashir, A.K., Du, X., and Guizani, M., 2020. IoT malicious traffic identification using wrapper-based feature selection mechanisms, *Computers and Security*, 94, p.101863.

Shen, S., Zhang, K., Zhou, Y., and Ci, S., 2020. Security in edge-assisted internet of things: Challenges and solutions, *Science China Information Sciences,* 63, p.220302.

Sinha, R., Thakur, P., Gupta, S., and Shukla, A., 2024. Development of lightweight intrusion model in industrial internet of things using deep learning technique, *Discover Applied Sciences,* 6, p.346.

Sudqi Khater, B., Wahab, A., Bin, A.W., Idris, M.Y.I.B., Abdulla Hussain, M., and Ahmed Ibrahim, A., 2019. A lightweight perceptron-based intrusion detection system for fog computing, *Applied Sciences,* 9, p.178.

Thamilarasu, G., and Chawla, S., 2019. Towards deep-learning-driven intrusion detection for the internet of things, *Sensors*, 19, p.1977.

Wang, Y., Meng, W., Li, W., Li, J., Liu, W.X., and Xiang, Y., 2018. A fog-based privacy-preserving approach for distributed signature-based intrusion detection, *Journal of Parallel and Distributed Computing,* 122, pp.26-35.

Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R., and Chehab, A., 2020. Securing internet of medical things systems: Limitations, issues and recommendations, *Future Generation Computer Systems*, 105, pp.581-606.

Zhang, H., 2025. Development of an intelligent intrusion detection system for IoT networks using deep learning, *Discover Internet of Things,* 5, p.74.

 http://dx.doi.org/10.14500/aro.12629

# APPENDIX

TABLE I
SYSTEMATIC FRAMEWORK THAT INTEGRATES ATTACK TAXONOMY, ML MODEL SUITABILITY, AND DETECTION EFFICIENCY CONSIDERATIONS

| Attack type (from taxonomy) | CIA | Detection style | Suitable ML/DL models (many per attack) | Feature selection/ optimization | Detection efficiency (Acc/ overhead/real-time) | Datasets+references (author–year) |
|---|---|---|---|---|---|---|
| Eavesdropping | C | Anomaly/Hybrid | OC-SVM; One-class ensemble; Autoencoder (AE); Clustering (k-medoids) | PCA; entropy/ statistics | Low–Med/Low/ Med | Eskandari, et al., 2020 (one-class, real self-created); Moustafa, et al., 2021b (one-class ensemble) |
| Packet analysis | C | Signature+Anomaly | RF; KNN; LR; XGBoost; SVM; AE | CorrACC; PCA; PSO-LF | Med/Med/Med | Alshahrani, 2021; Moustafa, et al., 2021a; Shafiq, et al., 2020 |
| Man-in-the-middle (MitM) | C/I | Signature/Hybrid | RF; SVM; KNN; LSTM; Ensembles (Bagging/ Stacking) | PCA; PSO-SVM; CatBoost+PSO | Med–High/Med/ Med | Luqman, et al., 2025; Benmalek and Seddiki, 2025; Kumar, Gupta and Tripathi, 2021 |
| Password Attacks (brute-force/ dictionary/birthday/ rainbow) | C | Anomaly+Signature | RF; XGBoost; LR; KNN; One-class; MLP | PCA; CorrACC; Pearson corr+RF | High/Low–Med/ High | Ahmed, et al., 2025 (PCM-RF); Alshahrani, 2021; Bedi, et al., 2021 |
| Social engineering | C | Hybrid (rule+ML) | NB; BN; DT/J48; RF; MLP (behavioral models) | IG; feature engineering | Low–Med/Low/ Low | Anthi, Williams and Burnap, 2018 (ML+rule, hybrid IDS); Anthi, et al., 2019 (multi-classifiers) |
| Shoulder-surfing | C | Indirect/Behavioral | NB; SVM; MLP (behavior profiling) | — | Low/Low/Low | — |
| Reverse engineering | C | Indirect/ Malware-focused | SVM; CNN; RNN/ LSTM; DBN | — | Med/Med/Med | Ham, et al., 2014 (SVM malware); Balakrishnan et al., 2019 (DBN); Sinha, et al., 2024 (DNN+DAE) |
| Replay | I | Anomaly/ Semi-supervised | OC-SVM; One-class ensemble; LSTM; AE/ CVAE | PCA; online learning | Med–High/Med/ Med | Garcia-Font, Garrigues and Rifà-Pous, 2017 (rule+OC-SVM); Moustafa, et al., 2021b; Lopez-Martin et al., 2017 (CVAE) |
| SQL injection | I | Signature | DT/J48; RF; XGBoost; LR; MLP | CorrACC; PSO-LF | High/Med/Med | Moustafa, et al., 2021a (multi-classifier); Kumar, Gupta and Tripathi, 2021 (ensemble); Alshahrani, 2021 |
| False data injection (FDI) | I | Anomaly/Hybrid | Statistical; PCA+clustering; SFC; LSTM; MLP | PCA; customized clustering | High/Low–Med/ High | Fantacci, et al., 2019 (real-time, energy efficient); Qin, et al., 2019 (PCA+clustering); Liu et al., 2018a (PCA+SFC) |
| Adversarial ML (Poisoning) | I | Robust training/ detection | Ensembles; FL+AE; robust SVM/RF; anomaly detectors | Feature vetting; GWO/PSO | Med/Med–High/ Med | Olanrewaju-George and Pranggono, 2025 (FL+AE); Karunamurthy, et al., 2025 (FL risk noted); Al Shorman, Faris and Aljarah, 2019 (OC-SVM+GWO) |
| Adversarial ML (Evasion) | I | Robust inference | Ensembles; LSTM; AE; adversarial-aware models | — | Med/Med–High/ Med | Karunamurthy, et al., 2025 (parameter exploitation risk); Lee, Chien and Chang, 2024 (parameter exploitation risk) |
| Protocol Attacks (CoAP/ MQTT) | I | Signature+ Protocol-aware | DT; iterative LR; ML IDS (CoAP); LSTM; RF | PCA | Med–High/Low–Med/Med | Krimmling and Peter, 2014 (CoAP ML IDS); Amouri, Alaparthy and Morgera, 2018 (DT+iterative LR); Karunamurthy, et al., 2025 (MQTT) |
| Insider Attack (data integrity) | I | Anomaly | Statistical AI; lightweight anomaly scoring | — | Med/Low/Med | Khan, et al., 2019 (lightweight statistical AI) |
| DoS | A | Signature/Hybrid | SVM; DT/J48; RF; NB; Ensembles; MLP | PCA; PSO-LF; CorrACC | High/Low–Med/ High | Anthi, Williams and Burnap, 2018 (hybrid DoS); Jan, et al., 2019 (SVM, lightweight); Anthi, et al., 2019 (multi-classifiers) |
| DDoS | A | Signature | RF; XGBoost; Bagging; Stacking; PSO-SVM; LSTM | Multi-objective optimization; PSO-SVM | High/Med/Med | Roopak, Tian and Chambers, 2020 (multi-objective); Musthafa, et al., 2024 (SVM-bagging, LSTM-stacking); Racherla, et al., 2024 (LSTM) |
| Flooding | A | Signature | RF; DT; KNN; LR; XGBoost | Feature selection (CorrACC, PCA) | High/Low–Med/ High | Kumar, Gupta and Tripathi, 2021 (ensemble); Moustafa, et al., 2021a (distributed); Ahmed, et al., 2025 (PCM-RF) |
| Wireless Jamming | A | Anomaly/ Classification | SVM; RF; lightweight DL; online models | — | Med–High/Med/ High | — |
| Resource Depletion | A | Anomaly | OC-SVM; One-class; PCA+OLWPR (online); statistical | PCA; OLWPR | Med/Low/High | Poornima and Paramasivan, 2020 (PCA+OLWPR, online); Eskandari et al., 2020 (lightweight one-class) |
| Battery Drain | A | Anomaly | One-class; AE; RF | PCA | Med/Low/Med | Poornima and Paramasivan, 2020; Qin, et al., 2019 |