Iraqi Journal of Intelligent Computing and Informatics (IJICI)
Vol. 4, 2. December 2025, pp. 212~226
ISSN: 2791-2868, DOI: 10.52940/ijici.v4i2.141

Cyber Attack Detection System for Internet of Things Using Machine Learning: A Review

Zainab hani hadi[1], Haider m. al-mashhadi[2]
[1,2] Department of Computer Science, Basra University, Basra, Iraq

Article Info

Article history:

Received November 16, 2025
Revised December 9, 2025
Accepted December 29, 2025

Keywords:

Detection,
Explainable AI,
Federated Learning.
Internet of Things,
Intrusion,
Anomaly Detection,
Cybersecurity.

ABSTRACT

With the explosive growth of the Internet of Things (IoT), intrusion detection systems have been challenged with new and complex cybersecurity problems that they are ill equipped to handle. Therefore, in the recent work ML-methods were highlight as one of the appropriate solution that can be used for assuring intelligent and adaptive (real-time) perceiving an online cyberattacks attacking IoT environments. To the best of our knowledge, no specific systematic review paper has been published on ML-based intrusion detection techniques in IoT systems; thus, this study aims to provide an overview and comparison of such methods with respect to underlying methodologies, datasets utilized for experimentation purpose, performance metrics that have been evaluated upon and deployment challenges faced out. Although the available works mainly focus on enhancing detection performance, important characteristics of scalable estimation and robustness, light computation load, interpretable model design as well as adaptability to diverse IoT environments still need to be further investigated. Solutions to these limitations are important in realizing practical and effective intrusion detection solutions for next generation of IoT networks.For the period 2020–2025, the latest developments are reviewed, and a unified classification is proposed for ML based IoT intrusion detection technologies, based on learning models and operational contexts. The contributions included in this study are a systematic comparative analysis of ML models also IoT security datasets, providing insights into future research directions towards hybrid, interpretable, and privacy-preserving frameworks in the field of ML for cyber IoT security, and identifying important open issues related to resource limitations and model interpretability.

Corresponding Author:

zainab hani hadi
Department of Computer Science, Basra University, Basra, Iraq
Email: pgs.zainab.hani@uobasrah.edu.iq

1. INTRODUCTION

The Internet of Things (IoT) is impacting modern industries, from healthcare and manufacturing to smart cities. This is achieved by connecting billions of devices that automatically collect and exchange data. However, this massive interconnection has also led to an cyberattacks expansion, exposing IoT systems to a cyber threats variety. IoT devices are particularly vulnerable to cyberattacks such as denial-of-service attacks, malware, identity theft, also data leaks due to their limited computing resources, heterogeneous architecture, and weak security settings [1].

The capabilities of IoT environments surpass those of traditional intrusion detection systems designed for conventional networks due to their dynamic nature also limited resources. Many solutions are

inadequate for rapidly evolving IoT systems because they cannot detect new or zero-day attacks. Machine learning technologies have garnered significant attention due to their ability to automatically assess network behavior and detect unusual or malicious patterns in real time [2] [3].

Despite advancements in ML based intrusion detection techniques, current research faces several challenges. Critical factors like scalability, ease of processing, interpretability, and real time applicability within limited contexts of the Internet of Things are sometimes overlooked in favor of detection accuracy [4] [5].

Most studies on the use of ML in IoT security focus on specific learning models or legacy approaches. The period from 2020 to 2025 saw the emergence of new, more interpretable, lightweight, also hybrid models that sought to balance efficiency and performance. This review, by integrating and restructuring supervised, semi supervised, and unsupervised learning techniques into a single framework, reveals persistent gaps in learning that maintain privacy, scalability, and adaptability. It also offers insights into how ML enabled IoT intrusion detection frameworks are evolving toward more intelligent also distributed architectures [6] [7].

2.REVIEW METHODOLOGY

This survey follows a systematic and elaborate methodology to guarantee that a comprehensive, transparent and academically rigorous study of machine learning techniques for intrusion detection in IoT is conducted. The process is structured into four main steps: search strategy, study selection criteria, categorisation of approaches and analytical evaluation.

1. Research Strategy

The survey includes the peer-reviewed studies which were published from 2018 to 2025 during which the IoT technologies have been emerged exponentially and consequently machine learning-based intrusion detection systems have become more popular. A predefined search strategy was employed to obtain the eligible studies. The main keywords were the IoT, cybersecurity, ML, anomaly detection, intrusion detection, explainable artificial intelligence and federated learning. These words were chosen to encompass a wide end of research about traditional/in emerging security areas in IoT network.

2. Inclusion Criteria

Studies that proposed machine learning-based or hybrid machine learning-based approaches for detecting IoT breaches were included, as well as research that evaluated models using available IoT security datasets (such as UNR-IDD, NSL-KDD, KDDCup99, MQTT-IoT-IDS, and CIC-IoT).

3. Classification and Analysis Method

The selected studies were classified into three groups (unsupervised and semi-supervised learning methods, supervised learning methods, and hybrid and lightweight machine learning models). The following aspects of each study were analyzed in terms of the methodology used, computational efficiency, suitability for IoT endpoint devices, as well as the ability to detect zero-day attacks, scalability, and deployment feasibility.

4. Limitations of the Review

This review has several limitations, including the fact that the variation in datasets and evaluation criteria across studies complicates direct performance comparisons. Consequently, the review focuses on machine learning-based intrusion detection systems, leaving other areas, such as blockchain-based IoT security, outside its scope.

3. CYBERATTACKS IN IOT NETWORKS

Cyberattacks are intentional actions aiming at violating integrity, confidentiality, and availability of information systems. In IoT, such attacks take advantage of inherent weaknesses in the device/thing ecosystem like small computational capabilities, non-standardized security protocols or massive deployment [8]. Despite many works on each type of attack, there is still lacking a systematic framework to take into account the heterogeneity and IoT networks dynamism. However, most of the current solutions are tailored only toward traditional networks and do not address specific challenges in IoT, including real time data stream ing, mobility, etc. resource constraints. To make matters worse, most of the detection algorithms are reactive rather than proactive, so they have a very narrow window in which to mitigate an ongoing attack. Types of Cyberattacks:

1. DoS and DDoS Attacks

DoS attack is A situation where a system can no longer process legitimate service requests at the desired level because its resources are bombarded by unfair or malicious resource utilization. This sort of attack is often kicked off by malware installed on attacker-controlled devices. Distributed Denial-of-Service (DDoS) attacks operate in a similar manner but use multiple compromised systems or devices, typically become part of a botnet, to overwhelm the targeted system. Typical DoS and DDoS attacks include the ping-of-death, smurf attacks, teardrop attacks, and TCP-SYN flood attack etc. It is very difficult to prevent such attacks since both

legitimate and malicious traffic use the same ports and protocols. To prevent such threat, companies might use an (IDS) and DDoS protection service or size up to meet a potential surge traffic [9].

2. Man-in-the-Middle (MitM) Attack

Man-in-the-Middle describes the method a hacker would use to intercept and impersonate both the client and server — so that they can access sensitive data. This category of attack enables the opponent to eavesdrop, record and sometimes change the transmitted data. Typical MitM attack vectors are session hijacking, IP spoofing and eves-dropping the communication channels. Defence measures can involve the use of intrusion detection systems, suspicious network activity alerts in real time and virtual private networks (VPNs), an additional layer of security when using public Wi-Fi to access private networks.

3. Phishing Attacks

Phishing Phishing involves fraudulent mails that pretend to come from a genuine source. "This is primarily to steal information, like passwords and personal information. Attackers often use emails containing malicious URLs or bogus sites to dupe users into sharing data. Methods used include phishing, spear-phishing, pharming, and whaling. Users and companies can mitigate the threat of phishing by using sand-boxing, carefully examining email headers, considering URLs prior to clicking on links, and training knowledge for employees [8].

4. Drive-by Download Attacks

Drive-by download Software that is installed without a user's knowledge through drive-by downloads installed behind-the-scenes, the victim visiting a malicious web site or viewing an email message containing malware and the installation ranks happen completely automatically. In these attacks, attackers typically conceal malicious code in a reputable website with methods such as malicious JavaScript, an iFrame hidden from view, or cross site scripting (XSS). After infecti, the malware looks for holes in the OS or applications. What steps can be taken to help prevent this from happening: Firewalls, Web filtering software, keeping up with patches and to protect from ransomware place all important data on a separate domain slave accounts from regular usage accounts [8].

5. Password Attacks

Passwords are the typical authentication mechanism and hence attractive to attackers. Password attacks seek unauthorized access by breaking the passwords using methods such as dictionary attacks). bruteforce, password sniffing and software exploits. Such mitigation measures could involve the requirement for a strong password or regular changes, combining character types that are difficult to guess. Employing multi-factor authentication and is more secure against all these attacks [8].

6. SQL Injection AttacksSQL injection attacks target weaknesses in web applications to execute malicious SQL statements on backend databases. This can lead to unauthorized access specifically on sensitive data and the manipulation of, or loss of the data. Developers don’t escape SQL statements or allow an apostrophe in the input. Prevention strategies are input validation, parameterized queries and employing WAFs to detect and block malicious behaviors [8].

7. Cross-Site Scripting (XSS) XSS attacks are used to inject code (typically JavaScript) into a trusted website or web application. The malicious code could then harvest users' cookies, session tokens or other sensitive information and send them to a server controlled by the attackers, who could use it to gain unauthorized access. XSS attacks may be categorized as three types: reflected, persistent and DOM-based. Prevention is a process to validate input, encode output and then implement content security policy to "tell" the browser that input should be treated like data not code [8].

8. Eavesdropping Attacks

One type of eavesdropping attack, also referred to as a sniffing attack, involves an attacker attempting to read the traffic on the network. This may include any sensitive information such as passwords or credit card numbers. These attacks can be passive (eavesdropping on network traffic) or active (posing as a legitimate device to snatch data). PrecautionsDesensitization by using encryption, virtual private networks, firewalls, antivirus software and the non-use of public networks for sensitive communication adequate resources to address PIB29 exist [8].

9. Birthday Attacks

A birthday attack is inspired by the birthday paradox of probability theory. It is directed against hashing because it finds two Input which lead to an identical hash. This allows an attacker to hijack or create

messages without being detected. Prevention against birthday attacks: To prevent the received message from being broken, use strong collision resistant hash function and longer hash length [8].

10. Malware Attacks

Malware and Malicious Software Malware describes any software that is installed on a machine without the user's knowledge. Today's malware encompasses viruses, worms, trojans, spyware and adware. Malware can disrupt system operations, trick you into downloading malware, siphon sensitive information, and fleece users for dimes. Common types include:

• Virus: Attaches itself to programs and reproduces when files are executed or downloaded.
• Worms: Self-replicating malware that spreads unassisted over networks.
• Trojans: Deceptively designed to seem harmless, they carry out their nasty deeds, albeit without self-replication.
• Cryptojacking Malware Uses the victim's computing power to mine cryptocurrency.
• Spyware – Monitor user activities and Sends information to its attackers [8].

4. CYBERSECURITY

Cybersecurity A science to protect digital resources from unauthorized access, service disruption and data manipulation. The first objective of it, is to safeguard information systems in traditional IT environments using strong security controls that maintain the confidentiality, integrity, and availability. Yet, with the advent of IoT came fundamental deviations in terms of security assumptions when it comes to traditional IT setup. IoT devices are a highly diverse collection of devices and often have limited computing, memory and power resources. These limitations make robust security difficult to realize on IoT devices and allow for increased vulnerabilities to cyber-attacks of IoT systems. As a result, security solutions for IoT should infer device diversity, long-term connection, and decentralized networks. Therefore, it is important to understand the differences between classic cybersecurity and IoT security in order to create effective protection mechanisms for today's distributed systems.

Transitioning from traditional IT environments to the IoT, conventional cybersecurity controls (e.g., secure authentication, continuous monitoring, regular system maintenance) are frequently by themselves no longer enough. Notwithstanding the aforesaid precautions, the IoT devices are still at risk of being compromised owing to low processing capabilities, obsolete firmware and no security online. Therefore, a new security perspective is essential for ensuring the protection of IoT systems where the conventional requirements such as availability, integrity and confidentiality are preserved while coping with bounded devices supports: communication protocols and distribution networks topologies [10].

A combination of technical and organizational measures is implemented throughout the entire life cycle of information systems in order to ensure cybersecurity. The extremely growing machine-to-machine communication, the increased amount of sensor data generation and penetration of connectivity technologies in IoT environments result in an elevated system complexity. Traditional security monitoring methods are insufficient for dealing with the overwhelming amount of IoT traffic. This limitation has motivated the use of machine learning (ML) methods for analyzing network behavior and identifying anomalies in real-time. Of these methods, they are a good complement to traditional security measures and work especially well in situations where inspections are difficult apply manually, effectively serving as advanced intruder detection systems [11].

Protection of corporate infrastructure such as networks, endpoints, applications, and data repositories is one of the most important responsibilities of cybersecurity [12]. The proliferation of IoT installations has dramatically increased the attack surface based on the sheer number of devices, variety of operating systems, vendor distinctiveness and different communication protocols. Such diversity elevates the potential for malware dissemination, protocol-based attacks (e.g., identity spoofing and packet forging), or unauthorized access to a system [13]. Thus, IoT security requires multiple layers of protection ranging from secure communication facilities, firmware validation and device security up to network-based IDS/IPS [14].

The CIA (Confidentiality, Integrity, and Availability) security triad has assumed the point of departure for capturing IoT security requirements as shown in Figure(1). Confidentiality prevents unauthorized access to sensor data and communication channels, and integrity protects transmitted information against tampering or modification. Availability is very important in the context of IoT deployments where operations at scale could potentially be affected by unavailability caused by hardware failures or security attacks, e.g., distributed-denial-of-service (DDoS).

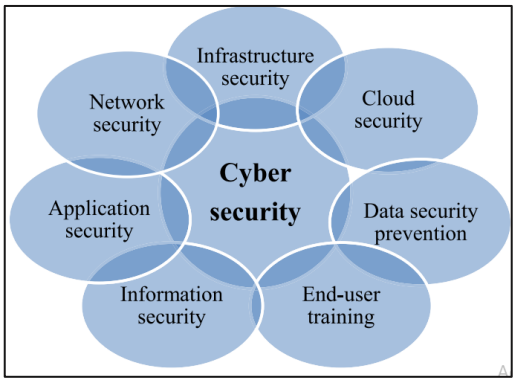

Figure 1: Security triangle (CIA).

5. ML IN IOT CYBERSECURITY

ML is an essential element in enabling intelligent and automated cybersecurity in (IoT) environments. It contributes to discovering hidden patterns within massive data streams, enabling abnormal behaviors identification, the detection of new threats, also human intervention the reduction [5]. Recent studies have classified ML-based intrusion detection methods in IoT networks into three major models: supervised, and unsupervised, supervised, semi- depended on their reliance on tagged data and their ability to adapt to diverse IoT environments [11]. Supervised learning achieves high accuracy in detecting known attacks but difficulty with unprecedented threats. Semi-supervised methods address the limitations of tagged data through hybrid and active learning, while unsupervised methods are characterized by their ability to detect zero-day attacks without prior knowledge, although they may have a higher false-point rate [16]. Recent trends suggest integrating these models within hybrid frameworks that gather their advantages, employing federated learning to protect privacy, explainable AI to enhance transparency, and focusing on lightweight, edge-deployment models to increase efficiency also performance in distributed systems [17]. Figure (2) illustrates the classification of ML methods for detecting IoT intrusion.

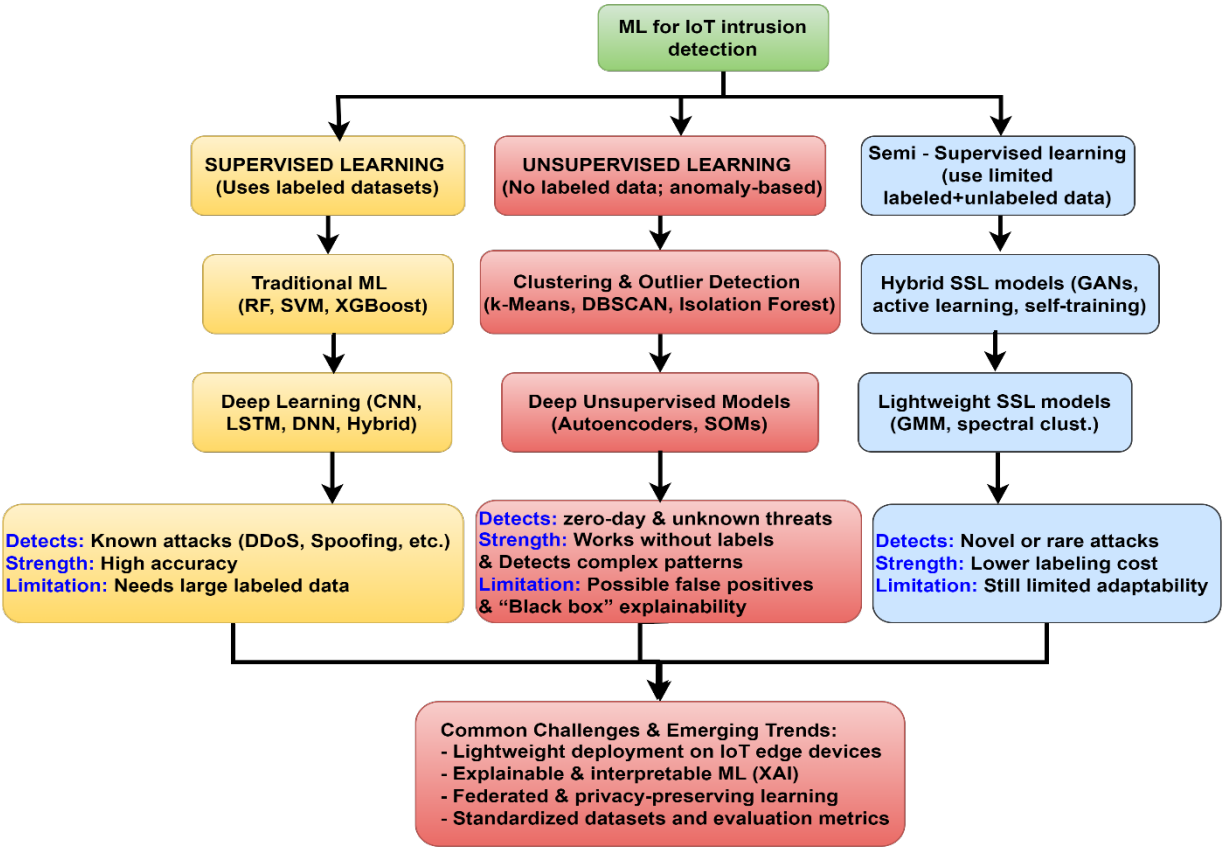

Figure 2: ML Approaches for IoT Intrusion Detection

With the increasing vulnerabilities and attack vectors in IoT, ML techniques have been extensive used for detection and malicious activities prevention at different layers to secure the networks as well as devices connected to it. ML is the cornerstone in today's IoT security solutions, providing an automated and adaptive approach to identify, predict, and counteract cyber-attacks[18]. In the literature, ML techniques can be mainly classified into three main categories: unsupervised, supervised, and semi-supervised; each method having its own advantages and drawbacks when applied in IoT networks.

Challenges and Research Gaps Although ML based approaches have proven to be promising, there are several key challenges in using them for IoT security. The majority of these models are proposed and analyzed under ideal conditions, which cannot adapt to the dynamic, heterogeneous and distributed environment in real IoT networks. Moreover, the current works usually focus on the detection accuracy and ignore other important constraints that include both latency, energy and scalability. Finally, the connection of ML models to live IoT systems is yet unexplored which in turn restricts the translation of research findings into valid and operational solutions.

In general, ML holds great potential to enhance efficiency and the accuracy of IoT cyberattack detection and also to con- tribute in devising more resilient security mechanisms for IoT devices. The intelligent smart device is capable of altering its own intelligent state and behavior, in which degree of intelligence is changed or characteristic of the change process can be learned as a driving force for operation on the basis of such learning, is referred to as ML, and it is one of realism physical object system solution. ML refers to the general process of learning useful information from data, generated by humans as well machines (robots). Its methods have two applications: regression and classification. In an IoT based company, artificial intelligence (ML) is also used to provide security services. Use of ML in cyberattack detection problems has increased [18]. Various applications of ML are applied in network security. Most of today's passive security approaches are based on a quantitative evaluation, which does not inherently provide the exactness of the systems. In the wireless scenarios, strong security demands enormously complex mathematics operations that are time-consuming [19]. As ML techniques offer capabilities for and contributing towards IoT security an efficient use, to take these solutions forward need strategies that can balance the trade-offs of accuracy, efficiency and real time feasibility and to build standardized benchmarks that reflect both diversity and evolution of threats in IoT networks. Overcoming these challenges is also essential in enabling the development of intelligent, adaptive, and scalable cybersecurity systems that can protect IoT infrastructures efficiently.

The following sub-sections detail supervised, semi-supervised, and unsupervised ML approaches for cyberattack discovery in IoT devices and systems.

5.1 Supervised Learning Techniques for IOT Security:

How Labeled Data Can Be Used to Perform Robust Threat Detection The scope of the IoT unsurprisingly evolves alongside its corporate use case sectors remain dominant. Contrary to semi-supervised methods, datasets to develop models that are able to classify and detect known threats with high accuracy. Recent studies have concentrated on improving performance, efficiency and flexibility of such models in order to deal with evolving challenges in IoT security.

1. Ensemble Methods for Multi-Class Attack Detection

Supervised learning is very good at classifying these sets of known attacks using labelled data. In [20], three used Random Forest (RF) and XGBoost to detect spoofing, Denial of Service (DoS), and Mirai-based attacks on the IoTID20 dataset. Multi-class classification accuracy of the model was equal to 99.2%, which indicates that ensemble methods can manage multi-threat patterns effectively. Analysis of the feature importance also indicated that packet size and protocol type were important elements to discriminate between benign and malicious traffic. While the results are excellent, the study relied on traditional algorithms, which may limit performance with complex data. The lack of real-world testing of the methodology on direct data from IoT devices leads to lower reliability in real-world performance. Furthermore, the method was not compared to modern feature selection techniques, and no analysis was provided of difficult-to-detect attack types.

2. Intrusion Detection with Deep Learning (DL) in Real Time

In [21]This study addresses the development of an (IDS) using deep learning techniques on the UNR-IDD dataset. Four main Convolutional Neural Network (CNN) models were used to extract spatial patterns from the network data: ANN/MLP as a traditional classification model, RNN/ Long Short-Term Memory (LSTM) for attack chronology analysis, and a hybrid CNN+LSTM model combining spatial and temporal feature analysis. The hybrid model performed best with an accuracy of 96.2%. Strengths of the study included the comprehensive testing and comparison of four diverse (DL) models, the use of a hybrid model, and the use of a modern and realistic dataset (UNR-IDD) containing multiple attacks Strengths of the study included the

comprehensive testing and comparison of four diverse (DL) models, the use of a hybrid model, and the use of a modern and realistic dataset (UNR-IDD) containing multiple attacks. Weaknesses included the lack of comparison with classical methods or advanced ML algorithms such as XGBoost or Random Forest, the absence of model complexity analysis (memory, FLOPs, training time), the failure to test the model's performance against novel attacks (zero-day attacks), and the lack of data imbalance correction techniques (oversampling, SMOTE).

3. Hybrid Models for Spatio-Temporal Analysis

In, [21]This study explored the problem of (IDSs) using ML and DL techniques, comparing the performance of several algorithms, including KNN, SVM, (RF), Naïve Bayes, Decision Trees, and some DL models such as MLP and CNN. The study relied on the NSL-KDD and KDDCup99 datasets to train models and measure the accuracy and classification of attack types. Tree algorithms (such as (RF) and Decision Tree) outperformed the other traditional algorithms, with (RF) achieving the highest classification accuracy (approximately 95–97%). DL models performed well but not as well due to the lack of hyperparameter adjustments or insufficient data preprocessing. The study indicated the potential for improved performance using more advanced deep networks. A key strength of the study was its systematic comparison of several ML and DL algorithms on the same dataset. The weaknesses included the greater focus on very old data (KDD99), which does not represent modern attacks, and the failure to compare the study with modern advanced models such as GRU, LSTM, and Transformer-based IDS.

4. Lightweight Detection for Resource-Constrained Devices

In order to reduce computer power consumption while retaining high attack detection accuracy, this study [22], provides a lightweight (IDS) for (IoT) scenarios that makes use of artificial neural networks (ANNs). The ToN-IoT telemetry dataset, which includes actual data from IoT sensors exposed to nine distinct kinds of attacks, was utilized by the researchers. Both binary (attack/normal) and multi-class (attack type) classifications were carried out. In ideal circumstances, binary classification accuracy reached 91%–92%. The model performed quite well in multi-class classification, with accuracy ranging from 91% to 100% for the majority of assault types. In terms of time complexity, the ANN model was substantially lighter than other models like (RF) and LSTM. The creation of an IDS appropriate for devices with low processing power—a critical component in the IoT field—as well as the use of a contemporary and realistic dataset are two of this study's main strengths. The model was only tested on ToN-IoT, which restricts the results' generalizability, and it did not employ Temporal Features, which were among its flaws.

Table 1. Summary Of Supervised ML Methods for Cyber Attack Detection in IOT**.**

Refs.	Detection method	Attacks Types	Feature Selection/Classification Methods	Datasets
[23]	Multi-class classification 99.2% Accuracy	Spoofing, DoS, Mirai	XGBoost, Random Forest	IoTID20
[24]	Real-time traffic analysis 98.5% F1-Score	MQTT DDoS, Brute Force	Deep Neural Network (DNN)	CIC-IoT2023
[25]	Explainable AI (SHAP) 97.8% Detection Rate	Ransomware, Injection	LightGBM, XGBoost	TON_IoT
[26]	Spatio-temporal analysis 99.1% Accuracy	Botnet (Mirai)	Hybrid CNN-LSTM	BoT-IoT
[27]	Lightweight payload analysis 96.3% Accuracy	MQTT Flooding	Logistic Regression + Principal Component Analysis (PCA)	MQTTset

5.2 Semi-Supervised Learning (SSL) Methods in IoT Security

Recent trends on semi-supervised learning in IoT security: addressing the lack of labeled Data Sens.

Data Given the increasing sophistication of cyberthreats for IoT and limited labeled data, (SSL) has proven to be an essential technique in developing robust detection systems. Current research efforts aim to utilize the numerous since-born, naturally occurring non-labeled data in IoT networks, complemented with scarce labeled datasets to train high- precision models for discerning novel and rare attacks.

1. SSL for Zero-Payload and Low-and-Slow Attack Detection: Zero-payload and low-and-slow attacks are among sophisticated attack techniques that traditional tactics cannot easily detect, due to the absence of known malicious payloads they bear or their traffic patterns resembling normal flow. In [28], a hybrid framework using Semi-Supervised Generative Adversarial Networks (GANs) was introduced. Use the model on a small set of labeled attack data (e.g., DDoS attacks over MQTT protocol), co-located in virtual private cloud VXRs, and combined with unlabelled network flow data. Model was evaluated on MQTT-IoT-IDS2020 dataset and achieved 98.7% accuracy in detecting novel attacks surpassing both supervised models that did not generalized well for these threat conditions.
2. Adaptation for Lightweight IoT Protocols The recent research trends focus on creating light weight SSL models to fit into the memory and processing requirements of (IoT) devices. In [29], a semi-supervised model, using GMMs and Spectral Clustering was proposed. When applied to CoAP protocol data to detect eavesdropping and spoofing attacks, the model performances were evaluated on the CIC-IoT2023 dataset. PartialNest achieved an F1-Score of 96.5% with a reduction of 40% in computational cost when compared to DL models for running on IoT gateways.
3. Iterative Learning and Active Discovery: Rather than only querying randomly labeled unlabeled data, recent approaches use AL to select the most informative set of k unlabeled samples for inducing model.
   improvement. In [30], an SSL-AL framework to enable anomaly detection in IIoT systems was designed. The model is initialized with a small number of labeled data followed by iteratively querying a human annotator to label instances in which the model is most uncertain about (inspired by Active Learning strategies such as Least Confidence). The model's performance on the IIoT-Malware-2022 dataset presented accuracy close to that of fully supervised methods (99.1%), while utilizing 20% of annotated data than previously required.
4. Self-Training with Lightweight Base Classifiers Self-training, whose model labels high-confidence unlabeled data for expanding training set—recently being revived by deployment of lighter weight classifiers. In [30] a LightGBM classifier was used as the base model in a self-training loop. This technique was then used to the TON_IoT dataset for ransomware attacks detection in smart home. "The study in [30]reported that the accuracy increased rapidly over several training cycles, rising from about 92% to 98.3% within a short training duration."

   Recent research discussed above indicates that SSL in IoT security is moving from primitive models to more complex and adaptive designs, as depicted by: (i) An increasing number of use cases and end-to-end scenarios, original proposals only focused on point-to-point communications.

· A look at current attacks against IoT protocols themselves.
· Computational efficiency to deploy models on devices with limited resources.
· Smart data selection heuristics, e.g., Active Learning, in order to make the most of every labeled example.

Table 2. Summary Of Semi-Supervised ML Methods for Cyber Attack Detection in IOT**.**

Refs.	Detection method	Attacks Types	Feature Selection/Classification Methods	Datasets
[28]	Generative Model-based Anomaly Detection	Zero-Payload DDoS attacks on the MQTT protocol	Semi-Supervised GAN (SSGAN)	MQTT-IoT-IDS2020
[29]	Lightweight Anomaly Detection	Eavesdropping and Spoofing attacks on the CoAP protocol	Gaussian Mixture Models (GMM) and Spectral Clustering	CIC-IoT-2023

[30]	Attack detection using a Least Confidence query strategy	Malware and unusual attacks in Industrial IoT (IIoT)	Semi-Supervised Learning with Active Learning (SSL with AL) using an SVM classifier	IIoT-Malware-2022
[30]	Iterative high-confidence classification for threat detection	Ransomware attacks in smart home environments	Self-Training with a LightGBM base classifier	TON_IoT
[31]	Fully unsupervised anomaly detection, used to reduce reliance on labeled data [7]	Botnet attacks (e.g., Mirai)	Isolation Forest and One-Class SVM (OCSVM)	IoT-23 (One of the most famous modern datasets)
[32]	Attack detection via network traffic behavior analysis	DDoS and Scanning attacks from Mirai botnet	Semi-Supervised Multi-Layer Perceptron (MLP)	N-BaIoT (Network-based IoT)

5.3 Unsupervised ML methods in IoT security

1. Clustering Techniques for Attack Classification: Clustering algorithms are widely used to group similar network behaviors, identifying deviations that may indicate an attack [33]. Spatial clustering technology was used for density-based noise-based (DBSCAN) applications to analyze network flow data from smart home devices. A key advantage of this technique is that it does not require pre-specifying the number of clusters, making it ideal for detecting unknown attack patterns. The IoT-23 dataset was used in its evaluation, and it successfully identified distinct clusters of network behavior, isolated Mirai robotic network activity, and examined sensors with 95.1% variance, demonstrating high coherence and cluster separation.

2. Anomaly detection using isolation mechanisms: Isolation-based algorithms excel at detecting rare events by isolating anomaly values in the feature space [34] . The study proposed a lightweight Isolation Forest (iForest) model, deployed on the Internet of Things (IoT) portal. The model was trained on typical network traffic metrics (packet size, frequency, protocol) from devices in the TON_IoT dataset. It demonstrated high effectiveness in detecting slow and low-intensity DDoS attacks, as well as data leakage attempts, achieving an F1 score of 93.5% with minimal computational load, making it suitable for real-time detection on endpoints.

3. Auto encoders for Deep Anomaly Detection: Auto-encoders are unsupervised deep learning models used to learn a compact representation of normal network traffic. Any large reconstruction error indicates an anomaly [35] . The study designed a convolutional autoencoder (CAE) to process the headers of sequential network packets. The model was trained on intact traffic from an N-BaIoT dataset, and by identifying patterns it couldn't accurately reconstruct, it was able to detect botnet activity. The method achieved a 98.2% detection (call) rate for Mirai and Bashlite attacks, demonstrating the power of deep learning in capturing complex temporal features without the need for classifications.

4- Self Organized Maps (SOMs) for Visual Intrusion Detection: To detect anomalies, SOMs provide a visual method by transforming high dimensional data into a low dimensional representation and monitoring behavior of IoT devices [36]. Normal processes cluster together on map, while attacks appear as anomalies. The self organizing map successfully captured and detected spoofing and retransmission attacks with 91.8% accuracy when tested on IoT sensor data, providing security analysts with a more interpretable view of network threats.

Unsupervised learning is indispensable for proactive IoT security, capable of identifying zero-day attacks and sophisticated threats without need for labeled data. The trend is moving towards:
· Hybrid models: Improved accuracy by combining the strengths of different unsupervised technologies.
· Explanability: Making the decisions of black box models easy to explain for security professionals.
· Extreme mitigation: Building highly efficient algorithms that can operate on the most resource-restricted IoT nodes, with detection going to the edge of the network.
Reducing false positives, as well as process of controlling false positives and actual malicious activity, are essencial challenges.

Table 3. Summary Of Unsupervised ML Methods for Cyber Attack Detection In IOT

Refs.	Detection method	Type of Attacks	Feature Selection/Classification Methods	Datasets
[33]	Clustering-based Anomaly Detection	Botnet (Mirai), Scanning	Density-Based Spatial Clustering (DBSCAN)	IoT-23
[34]	Isolation-based Outlier Detection	Low-and-Slow DDoS, Data Exfiltration	Isolation Forest (iForest)	TON_IoT
[35]	Anomaly Detection (Reconstruction Error)	Botnet (Mirai, Bashlite)	Convolutional Autoencoder (CAE)	N-BaIoT Deep
[36]	Visual Anomaly Detection & Clustering	Spoofing, Replay Attacks	Self-Organizing Maps (SOM)	Custom IoT Sensor Data
[37]	Hybrid Clustering & Proximity-based Detection	DDoS, Port Scan, Infiltration	Local Outlier Factor (LOF), k-Means	CICIDS2017
[38]	One-Class Classification	MQTT-based Publish Flooding	One-Class Support Vector Machine (OCSVM)	MQTTset

5.4 Critical Analysis of Previous Studies

Even though supervised, semi-supervised, and unsupervised machine-learning approaches have been utilized in several studies for IoT intrusion detection, a thorough review of the literature reveals some important findings: Benefits of Previous Research

1. Many supervised models have good detection accuracy when trained on well-labeled datasets such as IoTID20, BoT-IoT, and CIC-IoT2023.
2. Hybrid architectures (like CNN-LSTM) effectively capture spatiotemporal relationships in IoT traffic.
3. Semi-supervised and unsupervised methods offer better generalization for detecting novel or rare attacks when there is limited labeled data.

Limitations and Weaknesses
1. Because many supervised models rely heavily on specific datasets, they cannot be applied to a variety of IoT scenarios.
2. Many studies choose ideal laboratory conditions over noise, concept drift, and the real-time constraints of IoT environments.
3. SSL and unsupervised techniques often show high false positive rates, especially when network behavior fluctuates over time.
4. Few studies actually evaluate memory footprint, latency, also energy consumption on real IoT devices, despite lightweight models the suggestion.

Every study agrees that ML significantly improves intrusion detection performance when compared to traditional rule-based IDSs. Everyone acknowledges that IoT data is dynamic, varied, and often unlabeled, hence, new models must be lightweight and adaptable. The best machine learning paradigm is a topic of debate, some contend that supervised models are the most accurate, while others emphasize SSL or unsupervised models for spotting novel attacks.

6. DATASETS FOR IOT BASED INTRUSION DETECTION

The choice of suitable datasets is an important issue when designing and evaluating IDS for the IoT. A good dataset should mimic real traffic, cover different attack scenarios and exhibit diverse features to represent the reality of IoT environments. This paper provides a summary of most used datasets in the context of IoT IDS research, their characteristics and academic references.

- TON_IoT Dataset One of the most complete datasets designed for IoiRS environment is TON_IoT dataset by the University of New South Wales (UNSW) [39]. This union of multiple data sources is network traffic, telemetry from IoT

sensors, and operating system logs. This variety allows for the comparison of various ML and DL models.

There have been some attempts to diagnose the pitfalls associated with TON_IoT such as discrepancies across feature sets in different versions of TON_IoT and the necessity for its standardization. The traffic flows are captured by the CICFlowMeter, with different subsets of features. It has been pointed out by previous works1 that we may overestimate models if they are trained and tested on same dataset enumeration so cross-dataset analysis is crucial [39].

- CICIoT2023 Dataset

  The CICIoT2023 was produced by Canadian Institute for Cybersecurity (CIC) and intends to replicate an actual IoT network environment [40]. It consists of 105 IoT devices and traffic for 33 attacks grouped into types of seven: DDoS, DoS, Scan, Web-based, Brute Force, Spoofing and Mirai.

  Dataset is available to the public and has several representations which are suitable for (ML/DL) based IDS development. This is one the few (or maybe the unique) datasets that actually represents real IoT network traffic and not a synthetic simulation.

- IoTID20 Dataset

  There is very little work going on considering SDN-based IoT Botnet attack detection The IoTID20 dataset is designed specifically for botnet attacks in IoT network [41]. It has flow-based network features which are helpful to detect malicious patterns using ML methodology. It is frequently used to test models that address binary or multi-class IoT traffic classification.

- MQTT-IoT-IDS2020 Dataset

  The MQTT-IoT-IDS2020 dataset is specifically developed for IoT networks operating based on the MQTT protocol, a popular IoT communication protocol [42]. It includes the packet-based, unidirectional flow and bidirectional flow representation that network traffic datasets have typically shown and it overcomes the lack of MQTT-specific intrusion data in available datasets.

- Standard Benchmark datasets (NSL-KDD, UNSW-NB15, Bot-IoT)

  While not intended for IoT, a set of classic intrusion detection datasets (e.g., NSL-KDD, UNSW-NB15 and Bot-IoT) is often used as reference baselines in the field of IoT IDS[43].

  These data are also frequently enriched by crafting them for simulating IoT environments or by complementing them with other IoT designed datasets to produce better coverage.

  One such example is UNSW-NB15, which is a widely enhanced dataset for ML and DL models training against IoT datasets. Bot-IoT is also on massive botnet attacks and potentially combine with TON_IoTs so as to obtain more diversity.

7. ISSUES IN IOT INTRUSION DETECTION WITH MACHINE LEARNING

As much as ML has a promise in improving IoT-IDS, there are few challenges constraining the effective use of such technologies. Data quality and availability are the first main challenges. In an IoT context, data are noisy, incomplete and heterogeneous. Furthermore, the absence of labeled data for rare attacks and class imbalance problem diminishes the effectiveness of supervised models [43].

Another issue is the constrained resources of IoT devices. Low processing power and memory of devices make it difficult to deploy complicated ML models. Meanwhile, concerted effort is required for real-time analysis of intrusion detection, which further increases the burden [44].
Scale and heterogeneity are also major challenges. IoT networks being comprised a devices large number of with diverse communication protocols, the surrounds are always changing over time. The use of static and small datasets results in non-generalizable models [45].
In addition, intelligent IoT (IIoT) systems are targets of the ever-increasing more complex and advanced cyberattacks, such as zero-day and adversarial attacks. They are not solving the threat because traditional methods will fail against new threats and ML models could be blind towards patterns they have never been trained on [46].
Privacy, security and explainability are and other concerns. Many ML models are (black boxes) which makes it challenging for security analysts to interpret the model outputs. Privacy protecting approaches, such as federated learning [47], are in raise.
No common standard for evaluation and benchmark. Divergent studies use different datasets and evaluation metrics, so it is difficult to compare results in a fair manner.

8.COMPARISON WITH EXISTING SURVEYS

As for the survey works on applying ML techniques to intrusion detection systems in IoT, there have been some studies. But most of these critiques appear to have shortcomings in their comprehensiveness and depth of analysis. There are survey works available in the literature dealing with traditional supervised approaches (e.g., SVM [3], Random Forests (RF), K -Nearst Neighbors(KNN) etc.); however, they typically focus on detection accuracy. In such solutions, they in general ignore several crucial challenges such as scalability, model interpretability and computation efficiency, that play an important role in resource-constrained IoT deployments.
A few of recent surveys published included coverage about some deep learning (DL) techniques, but they often were not organized in a systematic way in the sense that it was hard to know where they corresponded to be within supervised, semi-supervised or unsupervised learning. Such lacking prevents from a comprehensive consideration of the pros and cons of alternatives in various IoT scenarios.
However, the present work proposes a systematic analytical and classification framework that can be applied to various ML-based intrusion detection methods. It supports emerging opportunities such as hybrid learning models, explainable AI and federated learning to improve the security of IoT while ensuring data privacy. This work does not present an extensiv e study of dataset properties but explicitly tackles the most important issues that are relevant to our proposal, including insufficient computational resources, imbalance distributions and mismatched evaluation procedures. Accordingly, this survey has more extensive and future perspective on ML-based intrusion detection in IoT environment than the previous work published.

9.CONCLUSION

The use of ML technology has become essential for improving IoT security due to the ongoing rise in cyberattacks and the growing complexity of smart device ecosystems. An examination of recent literature from 2020 to 2025 leads to multi-important conclusions. The most of studies concur that when labeled data is available, supervised learning models provide the highest accuracy rates. Unsupervised and semi-supervised approaches typically offer greater adaptability and the detection of new attacks, but they have issues with lower accuracy and tuning difficulty. In addition to including performance-enhancing strategies such as dimensionality reduction, data rebalancing, and transaction hyper-optimization, recent advancements are moving toward creating hybrid and lightweight models that fit the constrained capabilities of IoT devices.

The studies have a multi of flaws in common that indicate a glaring research deficit. Large datasets that are disconnected from operational realities are most models' foundation. Interpretability, practical applicability to edge devices with limited resources, and power consumption while operation have all been the subject of a small number of studies. Many studies simply use accuracy criteria to assess performance, ignoring other measures that are more crucial in real-world settings, like response times and false positive rates.

In this paper, we offer a judicious review of state-of-the-art research, point out its methodological short comings and contrast heterogeneous approaches on the real-world deployment level. It emphasizes the practical point of view from real-time requirement, computational efficiency and accuracy trade-off, hybrid

learning model designing as well as cross device joint working mechanism. In light of the results, various research implications are suggested.

First, future works should ensure to evaluate on realistic and complete datasets including a full range of IoT communication protocols instead of over-constrained or synthetic data. Second, research is required on the fusion of neuro-symbolic artificial intelligence and lightweight deep learning models to improve interpretability while respecting cybersecurity and regulatory constraints.

These results demonstrate the increasing need for intrusion detection approaches which satisfy operational requirements, such as being lightweight, interpretable and scalable (but also privacy-friendly), while at the same time achieving high accuracy. This article provides strong impetus for addressing important research paths that could improve the efficiency on intelligent threat detection system in a massive and evolving IoT environment.

REFERENCES

[1] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review," Sep. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics13183601.

[2] Satyajit. Chakrabarti and H. Nath. Saha, *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) : 7th-9th January, 2019, University of Nevada, Las Vegas, NV, USA*. IEEE, 2019.

[3] A. Haider, M. A. Khan, A. Rehman, M. Ur Rahman, and H. S. Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Computers, Materials and Continua*, vol. 66, no. 2, pp. 1785–1798, 2020, doi: 10.32604/cmc.2020.013910.

[4] M. Li *et al.*, "Cognitive IoT and Edge Computing for Intrusion Detection with Federated TinyML," in *2025 IEEE 6th Annual World AI IoT Congress, AIIoT 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 677–684. doi: 10.1109/AIIoT65859.2025.11105231.

[5] M. N. Alatawi, "SAFEL-IoT: Secure Adaptive Federated Learning with Explainability for Anomaly Detection in 6G-Enabled Smart Industry 5.0," *Electronics (Switzerland)*, vol. 14, no. 11, Jun. 2025, doi: 10.3390/electronics14112153.

[6] J. Alsamiri and K. Alsubhi, "Internet of Things Cyber Attacks Detection using Machine Learning," 2019. [Online]. Available: www.ijacsa.thesai.org

[7] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," Jul. 01, 2020, *MDPI AG*. doi: 10.3390/electronics9071177.

[8] L. Florido-Benítez, "The types of hackers and cyberattacks in the aviation industry," Dec. 01, 2024, *Springer*. doi: 10.1007/s12198-024-00281-9.

[9] Z. ElSayed, A. Abdelgawad, and N. Elsayed, "CryptoDNA: A Machine Learning Paradigm for DDoS Detection in Healthcare IoT, Inspired by Cryptojacking Prevention Models," in *Proceedings of the International Florida Artificial Intelligence Research Society Conference, FLAIRS*, Florida Online Journals, University of Florida, May 2025. doi: 10.32473/flairs.38.1.138680.

[10] K. Joseph Ajeigbe, H. Agoro, O. Emma, and J. Doe, "Security Vulnerability Detection Using Machine Learning," 2024. [Online]. Available: https://www.researchgate.net/publication/390492680

[11] J. C. Rosero and I. Dusparic, "Explainable Multi-Objective Reinforcement Learning: challenges and considerations."

[12] M. L. Rodríguez-deArriba, A. L. Nocentini, E. Menesini, and V. Sánchez-Jiménez, "Dimensions and measures of cyber dating violence in adolescents: A systematic review," May 01, 2021, *Elsevier Ltd*. doi: 10.1016/j.avb.2021.101613.

[13] A. Desai and S. Khorgade, "Machine Learning in Cyber Security", doi: 10.51583/IJLTEMAS.

[14] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[15] F. Jaidi, S. Ksibi, and A. Bouhoula, "An Internet of Medical Things Cyber Security Assessment Model (IoMT-CySAM)," *Cureus*, Oct. 2025, doi: 10.7759/cureus.94639.

[16] Jay Kumar Jain, Akhilesh A. Waoo, and Dipti Chauhan, "A Literature Review on Machine Learning for Cyber Security Issues," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 374–385, Dec. 2022, doi: 10.32628/cseit228654.

[17] N. A. Qahtani, "Hybrid Swarm Intelligence and Deep Neural Networks for Real-Time IoT Intrusion Detection." [Online]. Available: https://www.researchgate.net/publication/395714137
[18] C. Al Harake, D. Alrijjal, D. Al Rijjal, and J. Al Daghma, "IoT Cyber Attack Detection Using Machine Learning." [Online]. Available: https://www.researchgate.net/publication/391458631
[19] S. Ali *et al.*, "6G White Paper on Machine Learning in Wireless Communication Networks," Apr. 2020, [Online]. Available: http://arxiv.org/abs/2004.13875
[20] K. Albulayhi, Q. A. Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method," *Applied Sciences (Switzerland)*, vol. 12, no. 10, May 2022, doi: 10.3390/app12105015.
[21] S. Sadhwani, M. A. H. Khan, R. Muthalagu, and P. M. Pawar, "BiLSTM-CNN Hybrid Intrusion Detection System for IoT Application," Jan. 03, 2024. doi: 10.21203/rs.3.rs-3820775/v1.
[22] R. A. A. Saleh, L. Al-Awami, M. Ghaleb, and A. A. Abudaqa, "Lightweight Intrusion Detection for IoT Systems Using Artificial Neural Networks," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, Springer Science and Business Media Deutschland GmbH, 2025, pp. 45–59. doi: 10.1007/978-3-031-64954-7_3.
[23] K. Albulayhi, Q. A. Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method," *Applied Sciences (Switzerland)*, vol. 12, no. 10, May 2022, doi: 10.3390/app12105015.
[24] A. H. Ali Ahmed, W. Jin, and M. A. Hussein Ali, "Artificial Intelligence Models for Predicting Mechanical Properties of Recycled Aggregate Concrete (RAC): Critical Review," 2022, *Japan Concrete Institute*. doi: 10.3151/jact.20.404.
[25] B. Omarov *et al.*, "CNN-BiLSTM Hybrid Model for Network Anomaly Detection in Internet of Things." [Online]. Available: www.ijacsa.thesai.org
[26] R. A. A. Saleh, L. Al-Awami, M. Ghaleb, and A. A. Abudaqa, "Lightweight Intrusion Detection for IoT Systems Using Artificial Neural Networks," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, Springer Science and Business Media Deutschland GmbH, 2025, pp. 45–59. doi: 10.1007/978-3-031-64954-7_3.
[27] B. I. Farhan and A. D. Jasim, "Survey of Intrusion Detection Using Deep Learning in the Internet of Things," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp. 83–93, 2022, doi: 10.52866/ijcsm.2022.01.01.009.
[28] L. Liu, W. Zhai, F. Wang, Y. Ding, W. Lu, and W. Meng, "Federated Semi-Supervised and Semi-Asynchronous Learning for Anomaly Detection in IoT Networks," May 2025, [Online]. Available: http://arxiv.org/abs/2308.11981
[29] B. Williams and L. Qian, "Semi-Supervised Learning for Intrusion Detection in Large Computer Networks," *Applied Sciences (Switzerland)*, vol. 15, no. 11, Jun. 2025, doi: 10.3390/app15115930.
[30] A. Singh, Z. Mushtaq, H. A. Abosaq, S. N. F. Mursal, M. Irfan, and G. Nowakowski, "Enhancing Ransomware Attack Detection Using Transfer Learning and Deep Learning Ensemble Models on Cloud-Encrypted Data," *Electronics (Switzerland)*, vol. 12, no. 18, Sep. 2023, doi: 10.3390/electronics12183899.
[31] Y. Meidan *et al.*, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," May 2018, doi: 10.1109/MPRV.2018.03367731.
[32] Q. Xin, Z. Xu, L. Guo, F. Zhao, and B. Wu, "IoT traffic classification and anomaly detection method based on deep autoencoders," *Applied and Computational Engineering*, vol. 69, no. 1, pp. 64–70, Jul. 2024, doi: 10.54254/2755-2721/69/20241511.
[33] R. Bekkouche, M. Omar, R. Langar, and B. Hamdaoui, "Ultra-Lightweight and Secure Intrusion Detection System for Massive-IoT Networks."
[34] I. Apostol, M. Preda, C. Nila, and I. Bica, "Iot botnet anomaly detection using unsupervised deep learning," *Electronics (Switzerland)*, vol. 10, no. 16, Aug. 2021, doi: 10.3390/electronics10161876.
[35] M. Chovanec, L. Vokorokos, and A. Baláž, "Intrusion detection system using self organizing map," *Acta Electrotechnica et Informatica No. 1*, vol. 6, p. 1, 2006, [Online]. Available: https://www.researchgate.net/publication/228530209
[36] T. Talaei Khoei and N. Kaabouch, "A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems," *Information (Switzerland)*, vol. 14, no. 2, Feb. 2023, doi: 10.3390/info14020103.
[37] "A Comparative Study of Supervised vs. Unsupervised Learning Techniques for Real-Time Intrusion Detection in Cybersecurity Networks." [Online]. Available: https://www.researchgate.net/publication/396389868
[38] Y. Yin *et al.*, "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," *J Big Data*, vol. 10, no. 1, Dec. 2023, doi: 10.1186/s40537-023-00694-8.

[39] K. Kuchar, E. Holasova, R. Fujdiak, and J. Misurec, "Exploring the Landscape and Severity of Distributed Denial of Service Attacks." [Online]. Available: https://ssrn.com/abstract=4955404
[40] A. A. Raskovalov, N. Gabdullin, and V. Dolmatov Kryptonite, "Investigation and rectification of NIDS datasets and standratized feature set derivation for network attack detection with graph neural networks", doi: 10.48550/arXiv.2212.13994.
[41] E. Ghiasvand, "Resilience Against APTs: A Provenance-Based Dataset and Attack Detection Framework," 2019.
[42] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Cluster Comput*, vol. 26, no. 6, pp. 4069–4083, Dec. 2023, doi: 10.1007/s10586-022-03810-0.
[43] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)," in *Lecture Notes in Networks and Systems*, Springer Science and Business Media Deutschland GmbH, 2021, pp. 73–84. doi: 10.1007/978-3-030-64758-2_6.
[45] M. A. Ferrag *et al.*, "Edge Learning for 6G-enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses," Feb. 2024, [Online]. Available: http://arxiv.org/abs/2306.10309
[46] M. B. Suthar and S. Khara, "Enhancing IoT Security through Machine Learning-Based Intrusion Detection Systems," *Indian J Sci Technol*, vol. 18, no. 35, pp. 2884–2896, Oct. 2025, doi: 10.17485/IJST/v18i35.684.
[47] E. Ghiasvand, S. Ray, S. Iqbal, S. Dadkhah, and A. A. Ghorbani, "CICAPT-IIOT: A provenance-based APT attack dataset for IIoT environment," Jul. 2024, [Online]. Available: http://arxiv.org/abs/2407.11278