East Journal of Computer Science
ISSN: 3079-9406

Volume 1, Issue 4
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejcs.Vol1.Iss4.187

A Comprehensive Review of Learning-Based Anomaly Detection Techniques in IoT Security Systems

***Sulaiman Muhammed Sulaiman*[*,1], *Wafaa Mustafa Abduallah*[2]**

[1]Department of Information Technology Management, Technical College of Administration, Duhok Polytechnic University, Duhok, Kurdistan, Iraq- sulaiman.muhammed@dpu.edu.krd

[2]Department of Cyber Security Engineering, Technical College of Engineering, Duhok Polytechnic University, Kurdistan Region, Iraq- Wafaa.abduallah@dpu.edu.krd

*Corresponding Author.

Received: 19/08/2025, **Revised**: 21/08/2025, **Accepted**: 07/09/2025, **Published**: 20/09/2025

Abstract:

The Internet of Things (IoT) is increasingly integrated into critical systems such as healthcare, transportation, and smart cities, making it a prime target for cybersecurity threats. As traditional intrusion detection systems (IDS) struggle to handle the volume and diversity of IoT-generated data, machine learning (ML) and deep learning (DL) techniques have emerged as promising solutions. Unlike previous surveys, this review systematically analyzes and compares recent studies published between 2022 and 2025, focusing on ML/DL approaches, datasets, and evaluation metrics for anomaly detection in IoT environments. Key techniques such as convolutional neural networks (CNNs), long short-term memory (LSTM) networks, autoencoders, and hybrid models are examined with respect to their strengths, limitations, and suitability across IoT domains. The review also highlights preprocessing techniques such as feature selection, principal component analysis (PCA), oversampling (e.g., SMOTE), and federated learning (FL), which are essential for handling imbalanced and distributed data. Furthermore, the paper discusses commonly used datasets, evaluation metrics, and emerging research challenges. This work provides researchers and practitioners with updated insights and practical guidance for selecting appropriate algorithms, datasets, and evaluation metrics when developing scalable and secure IDS for modern IoT networks.

Keywords: IoT anomaly detection, Intrusion Detection System, Deep Learning, Federated Learning and security.

1- Introduction

The rapid expansion of the Internet of Things (IoT) has significantly impacted various sectors, including healthcare, smart cities, and industrial automation. With the ongoing advancement of network technologies such as 5G and mobile connectivity, forecasts predict the deployment of billions of connected devices in the near future. Given that, due to real-time data dissemination and automation, IoTs tend to become highly dynamic and distributed, it makes them face some of the most critical security challenges that urgently require to be addressed [1] .

Conventional rule-based IDSs are not appropriate anymore to cope with complexity requirements of IoT networks, against sophisticated attacks as they cannot satisfy the collider interception problem. Consequently, machine learning (ML) and deep learning (DL) have yielded better contribution to developing robust anomaly detection mechanisms [2]. Models evolved using DL approaches such as Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), and Autoencoders are especially showed more accuracy because of the fact that they possess to classify new pattern, minimize false positives, and trained smoothly with high-dimensional data [3]. Although these methods are superior in many ways, DL methods are computationally costly and are less appropriate for lightweight IoT devices. Recent research studies recommend hybridization strategies, i.e., integrating DL with federated (or else traditional) learning in order to enhance efficiency and scalability of the learning process [4] .

Alternate technologies are enabled for security of IoT industrial environment, (i.e., IoT, 5G, and AI) are not the only ones that must be accounted for such environment. Edge computing and Distributed Ledger Technology (DLT) are also considered as important enablers for the industrial be secure IoT by means of a decentralized environment. Such technologies improve immediate processing and data certainty and obsolesce dependence on

centralized servers [5] . However, the security risks of sensitive and non-sensitive IoT data are still severe, including Distributed Denial of Service (DDoS) attacks, spoofing, malware and so on.

In addition to ML and DL advancements, several enabling technologies have been explored in the context of IoT security. For instance, 5G networks enhance anomaly detection systems by providing high bandwidth and low-latency communication for large-scale IoT deployments. Edge computing allows IDS models to be executed closer to IoT devices, reducing latency and improving real-time detection of malicious activities [6]. Similarly, Distributed Ledger Technology (DLT) provides decentralized trust mechanisms that can complement anomaly detection by ensuring data integrity and secure communication among IoT nodes. While these technologies are not anomaly detection techniques themselves, they provide the infrastructure that strengthens the applicability, efficiency, and resilience of ML/DL-based IDS solutions [7].

Another approach for IDS implements recently Federated Learning (FL), key difference concepts of Traditional cloud-based AI training poses privacy risks due to the transfer of sensitive IoT data. Federated Learning (FL) addresses this by training models locally on trusted edge devices and sharing only model parameters, not raw data. This decentralized approach enhances data privacy while enabling accurate and secure attack detection [8] . Threats and attacks income with diversity effects and damage, IoT layer architecture include three layers each one with specific function. Figure-1 represented IoT layers along with attacks for each one. There is an imperative to deal with the increasing sophistication of IoT security problems. High demand for smart adaptive and distributed anomaly detection techniques, which can in the context of real-time processing. Deep learning methods, but also more generic when used, adopted with decentralized structures, have been developed as viable techniques to safeguard IoT systems from ongoing cyber-physical threats [9] .

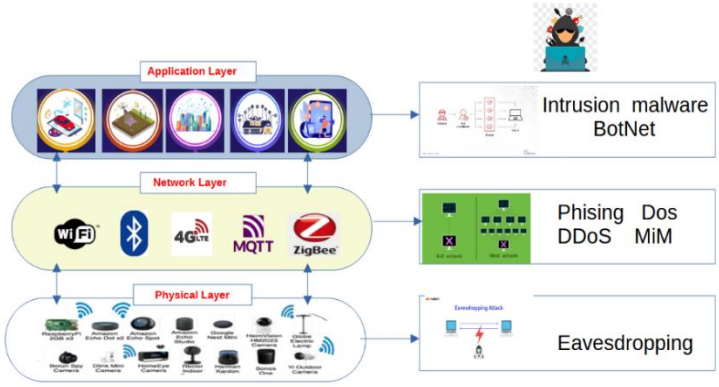

Figure 1: Architecture of IoT layers & Attacks [10]

The rest of this review is organized as follows: Section 2 reviews machine learning and deep learning approaches for intrusion detection in IoT. Section 3 presents commonly used datasets. Section 4 provides a critical analysis of the literature, and Section 5 concludes with key findings and directions for future research.

2. Related Works

In recent years with the large scale IoT deployment the accessible of IoT devices for Inflicting harm have been sharply increase from attackers simultaneously by the rapid growth of IoT applications. leading to the investigation of intelligent IDSs as a defense mechanism. There are many research studies that recommend machine learning (ML) and constrained deep learning (DL) methods to advance anomaly detection and also to enhance classification accuracy, and can accommodate the dynamic environment of IoT networks. This section summarizes and classifies recent projects from the last three years, by concentrating on models created for the purpose of intrusion detection in IoT systems. The review is organized according to the methodological focus of

the studies, including feature selection, hybrid DL architectures, ensemble learning and real-time prevention systems, as well as their applied datasets, evaluation metrics, and major contributions.

2.1 Machine Learning and Deep Learning Approaches for IDS in IoT

Several recent works, adopted different ML and DL approaches to create smart IDS in IoT. These approaches address various issues, such as feature selection, anomaly detection, and hybrid model creation. This section categorizes and reviews relevant literature from the past three years under four key themes:

2.1.1 Feature Selection and Dimensionality Reduction

Studies in this section are used machine learning algorithms for feature selection and classifying. In [11], the core of this study lies in integration (PCA) Principal Component Analysis to enhance dimensionality reduction and feature selection with (MLP) Multi Layers Perceptron for classifying. PCA reduced the original 44 features (35 network + 8 biometric + 1 label) to 14 essential ones, optimizing computational efficiency by reducing training time from 154.5 seconds to 67.4 seconds, and classification using MLP which achieved highest performance, compared to Support Vector Machine (SVM), K-Nearest Neighbors. (KNN) , and Naïve Bayes classifiers. DL learning algorithms produces significant effects in feature engineering and attacks classifying regard IDS models in [12] , developed novel intrusion detection system for IoT networks using a 1D CNN for feature extraction and a prototypical network as a few-shot learning classifier. Two datasets—MQTT-IoT-IDS2020 and CICIDS2017—were used to evaluate the model. Experiments included varying N-way K-shot scenarios with emphasis on support-query Euclidean distance learning.

2.1.2 Deep Learning and Hybrid Architectures

The authors in [13], introduced AttackNet model, a robust deep learning model designed within Industrial Internet of Things (IIoT) environments. they employed a hybrid architecture that combines Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU), the model leverages both spatial and temporal feature learning to effectively detect and classify botnet attacks. model underwent rigorous evaluation using the N_BaIoT dataset, achieving a testing accuracy outperforming several state-of-the-art models by a notable margin. For more enhancement of IDS in [14] , proposed a next-generation intrusion detection system (IDS) tailored for IoT-based Electric Vehicle Charging Stations (EVCS), that integrates CNN, LSTM, and GRU models. The methodology focused on capturing both spatial and temporal characteristics of network traffic through a hybrid framework, enhanced by sophisticated preprocessing techniques applied to the Edge-IIoTset dataset. The accuracy showed that model obtained a superior level in binary class classifying than other six class and fifteen. When towards technological advancements, malicious activities have become increasingly widespread. So, these systems face inherent vulnerabilities and needs more advanced security solutions that can successfully recognize and counteract threats within the network.

Combine of multiple ML algorithms showed interesting results regards anomaly detection in IoT system in [15] , viewed the ensemble voting classifier (DRX) that combines Decision Tree, Random Forest, and eXtreme Gradient Boosting (XGBoost) for intrusion detection in IoT networks. The model was trained and tested using three benchmark datasets: NSL-KDD, UNSW-NB15, and CIC-IDS2017. It followed a five-step machine learning pipeline, including SMOTE-based preprocessing and 10-fold cross-validation. Another Hybrid Deep Learning (HDL**)** methods introduced POAHDL-MDC in [16] , combining Stacked Autoencoder (SAE) and Bi-LSTM for malicious URL detection. The model focusing on Text data by utilize FastText for word embedding and employs the Political Optimization Algorithm (POA) for hyperparameter tuning. Pre-processing and feature engineering enhance the input data before classification. In order to reducing computational time and operational cost when adopting DL and FL in [17], proposes an efficient anomaly detection framework tailored for federated learning, utilizing separable convolution and convergence acceleration. It addresses key challenges in FL, including limited device resources, communication efficiency, and privacy preservation, making it suitable for decentralized anomaly detection scenarios. In the same context in [18] contributes an edge-optimized FL framework for anomaly detection that balances privacy, efficiency, and accuracy in 5G IoT settings. Its main novelty lies in real-time detection with reduced overhead, validated on standard network intrusion datasets.

2.1.3 Ensemble and Voting Techniques

To achieve a thorough reading and a more profound comprehension of attacks mechanisms by utilizing DL models, in [19] , identify location spoofing attacks and predicting the Time-of-Arrival (ToA) based on signal power received from a single access point. they employed two models MLP multi-layer perceptron and LSTM long short-term memory trained using simulated datasets. The method incorporated signal feature extraction and centralized data aggregation to improve the accuracy of spoofer localization. incremental learning methods used to reduce computation time in contrary increase efficiency of models by train only for new attacks not repeat whole model for pre-trained datasets, in [20] , research introduce Gradient Boosting Decision Trees GBDT-IL, depend on incremental learning concepts, the framework built upon Gradient Boosting Decision Trees for the detection of botnet traffic in Internet of Things (IoT) environments. The model incorporates an improved Fisher Score algorithm to facilitate optimal feature selection and employs a pruning strategy to mitigate overfitting. Furthermore, GBDT-IL effectively addresses concept drift in streaming data through a dynamic sliding window mechanism.

Algorithm 1 Dynamic Access Control Algorithm

```
Require: p : Network Packet
  r ← RandBetween(1, 2)
  while p ≠ 0 do
      s_t ← Sequence(p, t)
      d ← LSTM(s_t)
      if d is benign then
          IoTNode(d)
      else if d is malicious then
          r ← RandBetween(r, r+r)
          ip ← IPScan(Source(p))
          RouterAPI.AccessControl(ip, false, r)
          Discard(d)
      end if
  end while
```

Figure 2: DAC algorithm [20] .

2.1.4 Security-Aware Systems and Real-Time Prevention

Kalis2.0 framework in [21] , uniquely integrates a SECaaS-based model with a comprehensive context discovery mechanism and dynamic detection strategy selection. This positions Kalis2.0 as a significant advancement in enabling scalable, adaptive, and context-sensitive security for heterogeneous and evolving IoT environments. Alongside developing smart IDS in order detecting malicious packets it necessary to take prevent action such as in [22] , proposed an LSTM-based Intrusion Detection system integrated with a Dynamic Access Control (DAC) algorithm. DAC works as smart firewall located on output of LSTM that make automatically responds to attacks by blocking, in somehow detects real time IoT devices. Figure-2 show DAC algorithm for block network packets attacks.

Table 1 presents a comprehensive comparison for recently methodologies utilized in IDS and anomaly detection. it showed multiple aspects of comparing between methods. Headline of columns are selected according to the used datasets by researcher, methodologies and obtained accuracy after selecting distinct methods for training and testing.

Table1: IDS Methodologies Comparison

I, year	Detection Technique	Methodology	Datasets	Results/ Accuracy	Attack types
[1], 2023	Monitoring	FL & DNN	N-BaIoT and WUSTL & Kitsune datasets	97%	

					BASHLITE or Mirai attacks
[2], 2022	IDS	LSTM, CNN, Autoencoders, and SVMs	real-world data with simulation	99%	DDoS UDP flooding
[3], 2022	IDS	LSTM	UNSW-NB15	98.63%	FAR false alarm rate
[23], 2024	IDS	FL	CICIoT2023	97.65%	TCP SYN Flood
[5], 2024	IDS healthcare devices	Multi-Step Deep Q Learning Network	simulation	99.24%	malware & DDoS
[6], 2022	IDS in ICN network	ML	synthetic dataset	97%	DoS attacks
[7], 2023	IDS	HDL CNN and LSTM	CICIoT2023' and 'TON_IoT	98.75%	DDoS
[9], 2024	Enhance Feature selection in IDS	DT & GB	InSDN	99.99	DDoS attacks
[11], 2023	IDS healthcare devices	PCA with MLP	WUSTL-EHMS 2020 data sets	96%	Man-in the-meddle - attack
[19], 2024	IDS	Sky Mote XM1000 sensor boards	Real experiments IoT adopters in cloud and local network	97%	Smurf and ICMP Flood attacks
[13], 2024	IDS	CNN-GRU	N-BOTNET	Acc-99.7	BotNet
[14], 2024	IDS for EVCS	CNNs LSTM and GRU	Edge-IIoTset	97.44%	anomaly detection
[12], 2024	IDS	CNN	MQTT-IoT2020 and CICIDS2017	99.44%	
[17], 2025	IDS	FL & Separable Convolution	Public datasets	98.5%	Anomaly Detection
[18], 2025	IDS	CNN/MLP & FL	NSL-KDD - CIC-IDS 2017 - IoT-23	92%	Anomaly Detection
[19], 2023	IDS	MLP and LSTM	simulation	96%	Spoofing attacks
[15], 2024	classifier	DT -RF & XGBoost	NSL-KDD, UNSWNB15, and CIC-IDS2017 datasets	99%	anomaly detection
[20], 2024	Drift Detection for botnet detection	GBDT	BoT-IoT, N-BaIoT, MedBIoT, and MQTTSet datasets	99.81%	zombie network
[21], 2024	IDS	LSTM	BoT-IoT	98%	DDoS
[16], 2023	URL detection	HDL Bi- LSTM & Autoencooder	ISCX-URL2016	Acc-99.31%,	URL
[24], 2024	Botnet Detection	GIN	Chord datasets and P2P	99.9%	BoTNet

3. Used Datasets for IoT Intrusion Detection

In the field of IoT security, datasets play a crucial role in developing and evaluating machine learning (ML) and deep learning (DL) models for detecting multiple threats and attacks such as Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS). In many research authors employs multiple benchmark datasets to enhance the reliability and robustness of intrusion detection systems (IDS). These datasets serve as essential tools for evaluating machine learning-driven security approaches, helping researchers develop robust, scalable, and adaptive intrusion detection systems capable of mitigating evolving cybersecurity threats in IoT environments. Table 2 view popular datasets that are adopted by researchers in IDS models[13].

Table 2: Popular IDS Datasets**.**

Dataset	Purpose	No.of Records	No. of Features	Attack Types	Source
NSL-KDD	Intrusion Detection	148,517	41	DoS, R2L, U2R, Probe	[15]
UNSW-NB15	Cybersecurity Network Traffic	2,540,044	49	Fuzzers, Backdoor, Exploits, Worms	[23]
CIC-IDS2017	Real-world Attack Simulation	2,830,743	78	Brute Force, DDoS, Infiltration	[24]
BoT-IoT	IoT Security Botnet Attacks	72 million	46	DDoS, Keylogging, Data Exfiltration	[25]
IoTID20	IoT Network Anomaly Detection	625,783	36	MITM, DoS, Mirai Botnet	[26]

Each datasets have distinct purpose and utilization according to model of deep learning or machine learning. Besides, selecting appropriate datasets considered as initial action of developing model for achieve right preprocessing and minimize complexity. In term of IoT there are many benchmarks' datasets play crucial role for developing IDS models considering the heterogeneity of IoT sensors devices data, the real time stream data and attacks kinds that affects IoT systems[15].

specific data characteristics and security requirements generated by various IoT domains, so far, process of dataset selection yielded critical impacts on model performance and relevance. For instance, IoTID20 and UNSW-NB15 offer a broad mix of network traffic that nominate to become well-suited for evaluating models in industrial or smart city environments, include diverse attacks and high-volume communication [11]. In another hands, TON_IoT-Healthcare and MedBIoT datasets major focused on healthcare applications, in order to capture specialized traffic patterns and domain-specific threats such as spoofing and data tampering in medical devices. These datasets reflect more stringent privacy concerns and device heterogeneity. Therefore, selecting appropriate dataset that aligns with IoT domain target present better generalizability, threat coverage, and realistic evaluation of intrusion detection systems[20].

4. Literature Analysis

As previously discussed, researchers have proposed a wide range of deep learning approaches to address anomaly detection and intrusion detection systems (IDS) in IoT environments. This section surveys the state of the art, critically discussing the pros and the cons of the existing models, including the security challenges of IoT-based solutions. The presentation is divided into two sections:

4.1 Limitations of Previous Studies

While several works have been done to handle IoT anomaly detection and intrusion detection limitations, many are still not met, with the increasing variety of cyberattacks. For example, [12] showed that DL-based IDS models

even have a hard time identifying new attack types like zero-days. In addition, even the with highest accuracy, this tends to make these models overly complicated for real-time or resource-constrained deployment.

In term of IoT networks as in [7] , the examination was limited to SDN-based IoT networks and did not investigate different network architecture(s).

Their work also highlighted optimization difficulties and the high computational complexity of traditional feature selection methods. Moreover, IoT devices' inherent limitations in memory and processing power increase the risk of vulnerabilities in their security protocols.

In [11] investigated threats like Man-in-the-Middle MITM, spoofing, and data injection in IoMT networks; however, their dataset excluded other significant attack types. While the use of PCA improved classification performance, it introduced the risk of losing subtle yet important features during dimensionality reduction, potentially affecting the detection of less common threats.

From a comparative standpoint, CNN-based models [11], at feature extraction but require large labeled datasets and are sensitive to adversarial attacks. Recurrent Neural Network (RNN) and LSTM models, as used by [7] , are better suited for modeling temporal dependencies in sequential IoT traffic but tend to be slower and less scalable. Combine PCA and deep classifiers as hybrid models which considered by [12], improve efficiency, but at the cost of reducing feature sensitivity. In contrast, federated learning-based methods provide better privacy and scalability through not sharing centralized data aggregation. Nevertheless, their corresponding accuracies are usually degraded due to the lack of IID data distribution. across edge clients.

4.2 Standalone Verses Hybrid Approaches

Purely ML and DL techniques specify the proportions of contributions of individual features in comparison to hybrid models. These models present more accepted performance by taking advantage of a number of methods. For instance, hybrid systems that combine feature selection methods like (PCA, or autoencoders) with deep classifiers methods (CNNs, MLPs) resort a hidden layer for feature extraction, followed by a deep classifier. can usually offer better dimensionality reduction and better detection performance. These models is especially useful to exploit high dimensional IoT data. However, they may added computation and tuning complexity.

In contrast, standalone DL models (e.g., CNNs or RNNs) are less sensitive to carry out deployment and fine-tuning, resulting in poorer performance even when dealing with noisy or redundant input features. In general, the hybrid approaches are appropriate for cases requiring the highest performance and interpretability) due to their relative simplicity, where the single stand-alone DL models are more favorable in real-time or resource-limited applications. The models learned with deep networks have better recognition performance, such as the ensemble networks, transformers-based model, and stack of deep CNN, but it always needs a larger dataset, longer training time, and higher computing resources.

These requirements may constrain their applicability in real time or resource limited IoT scenarios. On the other hand, lightweight models or simple architectures such as (shallow CNNs or pruned networks) may also be used to achieve fast inference and energy efficient processing, while potentially giving up detection accuracy, especially in complex or emergent attack patterns. Hence, the cost and benefit of a model should be trad-off towards model complexity without losing operational feasibility, which is evidenced in IDS solutions for edge devices or decentralized IoT ecosystems.

4.2 IoT Security Challenges

- **Generalization:** this diversity of IoT devices results in a data diversity in format, type, and scale: from numerical sensor readings to video surveillance feeds, etc. It is difficult to design a unified model that is applicable for all of them. Dealing with this symptom will need multimodal preprocessing pipelines that are customized for each data type.

- **IoT Constraints:** Most IoT devices have limited computational power, memory, and energy. Deploying large, high-complexity models on such devices is impractical. A pragmatic solution is the offloading of

heavy computing to cloud or edge hands, with help of some technologies, like cascading or federated learning approaches that enable updates on individual or federated learning strategies that support updates of model port. without retraining or pre-processing.

- **Type of Attacks:** It is vital that the nature of an attack is accepted in a way that it will continue. DL-based methods are highly scalable and versatile with promising potential in the real-time anomaly and intrusion detection. Their capacity to learn a hierarchy of features allows for generalization and increases the resilience of detection of established and new threats.

Consequently, it can be concluded that deep learning seems to offer a promising direction to construct intelligent, autonomous and effective detection systems in such complex and dynamic IoT environments.

5. Conclusion

Security issues have become a critical problem in a wide range of technologies in the past. Artificial Intelligence (AI), and more specifically machine learning (ML) and deep learning (DL), thereby contributes significantly to the field of intrusion detection system(IDS) and anomaly detection models. This study provided a broad depiction of the various threats that are looming over the IoT systems and the algorithms and methodologies to detect and classify the received activity as malicious or benign is a key factor in developing smart firewalls and intelligent defense systems. ML and DL techniques have been shown to be effective in the classification of the attacks. Moreover, federated learning (FL) has recently been recognized as a feasible approach to mitigate IoT's performance and privacy limitations since it enables the local model updates without transmitting the raw data. Nevertheless, in spite of the above-mentioned progresses, more development is needed to handle the special needs of IoT especially in data generalization, latency and low computational capability of devices. For **Future work**, it is suggested that, innovative preprocessing methods according to different types of heterogeneous data can improve detection sensitivity. Furthermore, federated learning (FL) can help alleviate resource limitations by enabling model training on edge devices, thus reducing the use of bandwidth and central processing capacity. The combination of FL with lightweight models and incremental learning can further speed up training and make the IDS more appropriate for real-time application in resource-limited IoM.

References:

[1] T. Sauter and A. Treytl, "IoT-Enabled Sensors in Automation Systems and Their Security Challenges," *IEEE Sens Lett*, vol. 7, no. 12, pp. 1–4, Dec. 2023, doi: 10.1109/LSENS.2023.3332404.

[2] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," Aug. 01, 2022, *Elsevier B.V.* doi: 10.1016/j.iot.2022.100568.

[3] Y. Wang, X. Du, Z. Lu, Q. Duan, and J. Wu, "Improved LSTM-Based Time-Series Anomaly Detection in Rail Transit Operation Environments," *IEEE Trans Industr Inform*, vol. 18, no. 12, pp. 9027–9036, 2022, doi: 10.1109/TII.2022.3164087.

[4] M. A. Ferrag *et al.*, "Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices," *IEEE Access*, vol. 12, pp. 23733–23750, 2024, doi: 10.1109/ACCESS.2024.3363469.

[5] I. C. Lin, P. C. Tseng, P. H. Chen, and S. J. Chiou, "Enhancing Data Preservation and Security in Industrial Control Systems through Integrated IOTA Implementation," *Processes*, vol. 12, no. 5, May 2024, doi: 10.3390/pr12050921.

[6] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq, and K. K. Wong, "Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare," *IEEE Access*, vol. 10, pp. 37064–37081, 2022, doi: 10.1109/ACCESS.2022.3163580.

[7] M. F. Saiyed and I. Al-Anbagi, “Flow and unified information-based DDoS attack detection system for multi-topology IoT networks,” *Internet of Things (Netherlands)*, vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100976.

[8] M. S. Ahmad and S. M. Shah, “A lightweight mini-batch federated learning approach for attack detection in IoT,” *Internet of Things (Netherlands)*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2024.101088.

[9] A. Garcés-Jiménez *et al.*, “Industrial Internet of Things embedded devices fault detection and classification. A case study,” *Internet of Things (Netherlands)*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2023.101042.

[10] V. Gugueoth, S. Safavat, and S. Shetty, “Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects,” Oct. 01, 2023, *Korean Institute of Communications and Information Sciences*. doi: 10.1016/j.icte.2023.03.006.

[11] A. Judith, G. J. W. Kathrine, S. Silas, and A. J, “Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices †,” *Engineering Proceedings*, vol. 59, no. 1, 2023, doi: 10.3390/engproc2023059139.

[12] T. Althiyabi, I. Ahmad, and M. O. Alassafi, “Enhancing IoT Security: A Few-Shot Learning Approach for Intrusion Detection,” *Mathematics*, vol. 12, no. 7, Apr. 2024, doi: 10.3390/math12071055.

[13] H. Nandanwar and R. Katarya, “Deep learning enabled intrusion detection system for Industrial IOT environment,” *Expert Syst Appl*, vol. 249, Sep. 2024, doi: 10.1016/j.eswa.2024.123808.

[14] D. Kilichev, D. Turimov, and W. Kim, “Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models,” *Mathematics*, vol. 12, no. 4, Feb. 2024, doi: 10.3390/math12040571.

[15] A. H. Farooqi, S. Akhtar, H. Rahman, T. Sadiq, and W. Abbass, “Enhancing Network Intrusion Detection Using an Ensemble Voting Classifier for Internet of Things,” *Sensors*, vol. 24, no. 1, Jan. 2024, doi: 10.3390/s24010127.

[16] M. Aljebreen, F. S. Alrayes, S. S. Aljameel, and M. K. Saeed, “Political Optimization Algorithm with a Hybrid Deep Learning Assisted Malicious URL Detection Model,” *Sustainability (Switzerland)*, vol. 15, no. 24, Dec. 2023, doi: 10.3390/su152416811.

[17] B. Jiang, G. Wang, X. Cui, F. Luo, and J. Wang, "Lightweight anomaly detection in federated learning via separable convolution and convergence acceleration," *Internet of Things*, vol. 25, 2025.

[18] M. J. C. S. Reis, "Edge-FLGuard: A Federated Learning Framework for Real-Time Anomaly Detection in 5G-Enabled IoT Ecosystems," *Applied Sciences*, vol. 15, no. 12, Art. no. 6452, 2025.

[19] W. Aldosari, “Deep Learning-Based Location Spoofing Attack Detection and Time-of-Arrival Estimation through Power Received in IoT Networks,” *Sensors*, vol. 23, no. 23, Dec. 2023, doi: 10.3390/s23239606.

[20] R. Chen, T. Dai, Y. Zhang, Y. Zhu, X. Liu, and E. Zhao, “GBDT-IL: Incremental Learning of Gradient Boosting Decision Trees to Detect Botnets in Internet of Things,” *Sensors*, vol. 24, no. 7, Apr. 2024, doi: 10.3390/s24072083.

[21] A. Rullo, D. Midi, A. Mudjerikar, and E. Bertino, “Kalis2.0 - A SECaaS-Based Context-Aware Self-Adaptive Intrusion Detection System for IoT,” *IEEE Internet Things J*, vol. 11, no. 7, pp. 12579–12601, Apr. 2024, doi: 10.1109/JIOT.2023.3333948.

[22] M. Alazab, A. Awajan, H. Alazzam, M. Wedyan, B. Alshawi, and R. Alturki, “A Novel IDS with a Dynamic Access Control Algorithm to Detect and Defend Intrusion at IoT Nodes,” *Sensors*, vol. 24, no. 7, Apr. 2024, doi: 10.3390/s24072188.

[23] D. Hamouda, M. A. Ferrag, N. Benhamida, H. Seridi, and M. C. Ghanem, “Revolutionizing intrusion detection in industrial IoT with distributed learning and deep generative techniques,” *Internet of Things (Netherlands)*, vol. 26, Jul. 2024, doi: 10.1016/j.iot.2024.101149.

[24] L. Yin, W. Chen, X. Luo, and H. Yang, “Efficient Large-Scale IoT Botnet Detection through GraphSAINT-Based Subgraph Sampling and Graph Isomorphism Network,” *Mathematics*, vol. 12, no. 9, May 2024, doi: 10.3390/math12091315.

[25] Q. Wang, H. Jiang, J. Ren, H. Liu, X. Wang, and B. Zhang, “An intrusion detection algorithm based on joint symmetric uncertainty and hyperparameter optimized fusion neural network,” *Expert Syst Appl*, vol. 244, Jun. 2024, doi: 10.1016/j.eswa.2023.123014.

[26] S. Li, Y. Cao, S. Liu, Y. Lai, Y. Zhu, and N. Ahmad, “HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN,” *Expert Syst Appl*, vol. 238, Mar. 2024, doi: 10.1016/j.eswa.2023.122198.

[27] D. T. Nguyen and K. H. Le, “The robust scheme for intrusion detection system in Internet of Things,” *Internet of Things (Netherlands)*, vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100999.

[28] S. Rahman, S. Pal, S. Mittal, T. Chawla, and C. Karmakar, “SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security,” *Internet of Things (Netherlands)*, vol. 26, Jul. 2024, doi: 10.1016/j.iot.2024.101212.