

FAHAD ALKAMLI
MUTASEM MOHAMMAD JARRAH
MORCHED DERBALI

MACHINE LEARNING APPROACHES FOR INTRUSION DETECTION IN IOT AND NETWORK SECURITY: A REVIEW

Abstract

Given the fast-growing number of IoT devices creates advanced cybersecurity headaches for which cutting-edge intrusion detection systems need development to address current and future threats. This paper provides a detailed investigation of ML and DL method applications for IoT and network security, along with a review of their successful implementations and technical constraints. The review analyzes 30 studies through three different methodological sections which include neural networks, ensemble learning and support vector machines (SVM), deep learning architectures, hybrid AI-blockchain models, and federated learning. Current research shows ensemble learning and deep learning methods as leaders in attack detection since they achieve detection accuracy above 99% for DDoS, phishing and malware attacks. The IoT security is boosted by GA-LSTM and TCN because each model shows high adaptability for changing IoT situations and blockchain integration with AI models strengthens both protection against attacks and data security. The research suffers from four main drawbacks: excessive use of simulated data, scalability problems in IoT devices with limited resources and inadequate field-based verification of systems. The review provides essential guidance for both research scientists and security practitioners who want to develop strong scalable and ethically grounded ML-based security solutions for IoT ecosystems.

Keywords

IoT Security, Intrusion Detection Systems, Machine Learning, Deep Learning, Ensemble Learning, Blockchain, Federated Learning

Citation

Computer Science 27(2) 2026: 75–97

Copyright

© 2026 Author(s). This is an open access publication, which can be used, distributed and reproduced in any medium according to the Creative Commons CC-BY 4.0 License.

1. Introduction, Motivation

Machine learning brings the much-needed solutions against such advanced complex cyber threats in the digital ecosystem of today. Traditional rules-based security solutions show weakness when pitted against contemporary threats originating from zero-day attacks and polymorphic malware. Application of machine learning algorithms using real-time analytics on large data volumes creates an innovative pattern and anomaly detection mechanism and identification of malicious activity. Machine learning operators detect the presence of cyber threats by using intrusion detection systems, whereas phishing attacks and malware are blocked and detected through system classification performance and discovery of network anomaly, respectively. This research intends to discuss present applications of machine learning while describing its present advantages and limitations and predicted evolutions that may change information security due to better detection of cyber threats. While tackling current challenges in IoT and network security, this review paper suggests main ideas and future prospects. The contributions of the research are as follows in total:

- (i) The article gives a complete and readable overview of machine learning-based intrusion detection systems for IoT settings.
- (ii) The article reviews detection techniques under such models as neural networks, ensemble learning, support vector machines, deep learning, hybrid blockchain-AI frameworks, and federated learning. It also measures their performance, datasets, features selection and strategies.
- (iii) The article structures the reviewed techniques and the applications in a taxonomy in a logical order demonstrating contemporary trends and revealing lacunae in methods.
- (iv) Finally, the survey covers the limitations of the existing approaches including use of simulated data and resource constraints and proposes lightweight, scalable and explainable solutions for future work in real-world IoT intrusion detection systems.

The structure of this paper is organized as follows. Section II demonstrates the methodology used to collect and synthesize the literature. Section III presents an extensive literature review, organizing existing studies under key methodological areas, including neural networks, support vector machines, ensembles, deep learning, hybrid blockchain-AI models, and federated learning. The key findings and analysis of the reviewed literature, covering benefits, limitations, and comparative performance, are discussed in Section IV. Section V concludes the paper by summarizing the main insights and providing directions for future work aimed at enhancing the scalability, accuracy, and interoperability of machine learning-based intrusion detection systems in IoT contexts.

2. Methodology

IDS in the Internet of Things (IoT) use regularly updated strategies to combat new challenges. The tools usually help extract beneficial data and use the most advanced

technology. In this segment, we investigate the different ways data is prepared and handled in these systems. We also look at the datasets that are most common for testing and assessing such systems.

2.1. Selections of research articles

The illustration outlines the SLR approach, which is very common in computer science, software engineering, and information systems. SLR ensures that evaluating academic studies is done in an orderly and organized way, as can be seen in Fig. 1.

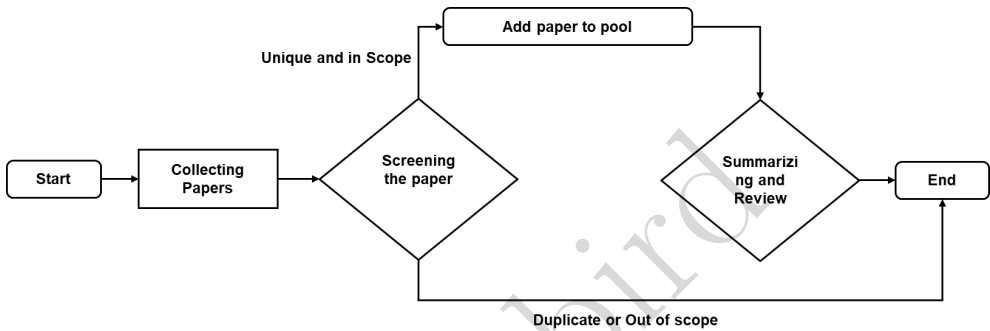


Figure 1. Summary of articles selection process review

The process of review is initiated by searching for academic studies from various scholarly databases, peer-reviewed journals and the relevant conference proceedings in order to ensure wide coverage of the subject. After gathering, these studies are screened for predefined criteria such as scope, relevance and research quality. This step identifies duplicate or redundant records and removes them to maintain accuracy and avoid any redundancy.

Unique papers which are in the scope of the review are added to the analysis pool. The next phase involves detailed study of the selected studies, whereby their methodologies, findings and contributions are synthesized. By doing this, researchers can identify main topics, notice missing points in the literature and judge the direction of ongoing research.

Finally, the process is structured using the Systematic Literature Review (SLR) methodology to guarantee the process is rigorous, transparent and reproducible. If researchers follow these steps, they can produce comprehensive and insightful reviews that enhance understanding in the field.

3. Literature Review

This literature review focuses on synthesizing the work across Intrusion detection and artificial intelligence. This section critically reflects on the methods and conclusions of prior studies in this section along with the highlighting of key findings for their

validity and relevance. This review will analyze current trends, challenges, and gaps from the literature to give us an extensive application of AI for intrusion detection and inform the further direction of research in this evolving domain.

3.1. Neural Networks and Optimization Techniques

In the work by Nandhini et al. [29], four prospective approaches include Equilibrium Optimizer Neural Network (EO-NN), Particle Swarm Optimization Neural Network (PSO-NN), Single Candidate Optimizer Neural Network (SCO-NN), and Single Candidate Optimizer Long Short-Term Memory (SCO-LSTM), all of which utilize threat intelligence for the effective detection of malicious nodes. The SCO-LSTM model achieved an accuracy of 99.89%.

Behiry and Aly [12] developed a cyber-attack detection method for Wireless Sensor Networks that combines SVD, PCA and K-means clustering with a hybrid feature reduction technique. They use their Deep Feed-Forward Neural Network (DFFNN) to enhance detection precision across NSL-KDD and UNSW-NB15 benchmark datasets. Researchers show that effective feature selection helps eliminate unnecessary data while keeping the detection system effective.

Maseno and Wang [26] have produced a hybrid wrapper method of feature selection, combining Genetic Algorithm (GA) with Extreme Learning Machine (ELM) to optimize intrusion detection in IoT networks. Such an approach mitigates the hurdle of high-dimensionality associated with IDS datasets by selecting the most appropriate features, substantially improving classification performance while lessening computational burden. Their GA-ELM model applied to the IoT_ToN and UNSWNB15 datasets obtained 99% and 86% accuracies respectively, both outperforming benchmark classifiers.

The GA-mADAM-IIoT model was introduced by Saheed et al. [8] for lightweight threat detection in the industrial IoT (IIoT) using a genetic algorithm (GA) with an attention mechanism and a modified Adam-optimized LSTM (mADAM-LSTM). The model was trained on SWaT and WADI datasets, achieving 99.98% accuracy in anomaly detection. GA was employed for feature selection, while the attention mechanism enhanced relevant data extraction. The integration of SHAP provided explainability for the detection process.

Table 1 presents a list of similar studies and their key results, while Fig. 2 illustrates their application areas along with the datasets used for validation.

3.2. Support Vector Machines (SVM) and Decision Trees

A multi class SVM and an optimized CHAID decision tree for real-time multistage cyberattack detection in IoT systems are introduced by Dalal et al. [15]. Their framework classifies IoT traffic based on the prioritized most important attack attributes to improve the accuracy of attack categorization and prediction. Its application on the Multistep Cyber-Attack Dataset (MSCAD) is a key contribution, where it achieves 99.72% accuracy in real world IoT security scenarios. The CHAID decision tree

Table 1
SUMMARY OF NEURAL NETWORKS-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[29]	EO-NN, PSO-NN, SCO-NN, SCO-LSTM	High accuracy, adapts to attacker behavior, uses threat intelligence	High resource usage, complex setup
[12]	DFFN + KMC-IG	Efficient across datasets, improved performance via feature reduction	Info loss from reduction, model complexity
[26]	ELM + GA + SVM	Better IDS performance, lower computation	May keep redundant features, limited generalization
[36]	GA + attention, mADAM-LSTM	Very high accuracy, explainable with SHAP, good feature selection	Limited to simulated data, not real-world proven

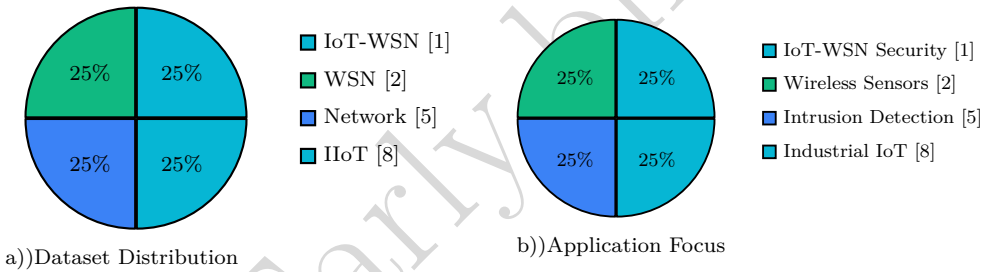


Figure 2. NN Studies Datasets & Application

optimizes feature selection and has been shown to improve the efficiency of SVM classification, enabling the system to identify different types of cyber threats with high precision.

The study by Karthikeyan et al. [21] presents FA-ML as a system that utilizes the Firefly Algorithm and Machine Learning for improved intrusion detection of IoT-WSN networks. The Firefly Algorithm performs feature selection and Support Vector Machine functions as the classification method while Grey Wolf Optimizer regulates the parameter tuning. When NSL-KDD dataset was used for evaluation purposes, the FA-ML method achieved 99.34% accuracy surpassing KNN-PSO (96.42%) and XGBoost (95.36%).

The detection system presented by Amouri et al. [11] merges Kolmogorov-Arnold Networks (KAN) with Support Vector Machines (SVM) and RF as conventional classifiers to detect intrusions. The researchers obtained detection rates higher than

99.7% when analyzing Bot-IoT and TON_IoT datasets. Research findings indicated that joining deep learning technology with statistical modeling systems improves the adaptability and precision during multiple IoT attack procedures.

Table 2 presents SVM and DT based studies along with their key results, while Fig. 3 illustrates the application focus and the datasets distribution.

Table 2
SUMMARY OF SVM AND DT-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[22]	BCOA + CCR-ELM	High accuracy, efficient feature selection	Needs parameter tuning, may be computationally heavy
[21]	Firefly Algorithm + SVM	Accurate, robust optimization	Depends on dataset, complex optimization
[11]	KAN + RF + XGBoost (stacking ensemble)	Handles non-linearity, better than traditional models	KAN is new, needs large training data

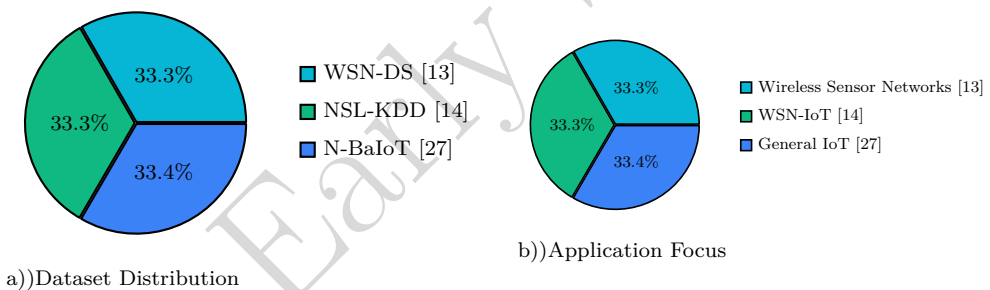


Figure 3. SVM and DT Datasets and Application

3.3. Ensemble Learning Methods

In order to improve cybersecurity in IoT by detecting anomalous behavior, ensemble learning frameworks were employed by Lai et al. [24], which are performed by Bayesian hyper-parameters optimization. The proposed work proposes a dataset of combined models that are more accurate than a single model in predicting IoT datasets. The work proposes Bayesian hyper-parameter tuning in its contribution to the academic community and performs reasonably well in attempting to reduce false positives and greatly boost the efficiency of detection. Furthermore, the F1 values metrics are improved between 10% to 30% to show the effectiveness of the machine learning technique in cybersecurity using Bayesian based ensemble model.

The Network Intrusion Detection System (NIDS) was proposed by Ahmad et al. [2] to integrate with Internet of Things (IoT), using supervised machine learning techniques with application and transport layer-based features, developed performing tests with the UNSW-NB15 dataset. Clustering of feature sets for Flows, MQTT, and TCP was conducted, together with an objective of feature selection and training model improvement using Random Forest (RF), Support Vector Machine (SVM), and Artificial Neural Networks (ANN), with RF achieving 98.67% accuracy for binary and 97.54% for multi-class, respectively. To safeguard against attacks, a clustering model was explained to enable reduced training time while retaining very high accuracy in intrusion detection, hence rendering it a possible and efficient tool for real-time intrusion detection in IoT environments.

A robust DDoS detection and mitigation scheme was designed by Belachew et al. [13] for SDN-Edge-IoT environments, leveraging machine learning models such as XGBoost, K-Nearest Neighbor (K-NN), Random Forest (RF), and Feedforward Neural Networks (FFNN). The system was evaluated on the CICIDS2017 and Edge-IIoTset datasets, achieving an accuracy of 99.997% with minimal latency when deployed at the network edge. The implementation demonstrated efficiency in real-time traffic classification, though the complexity of managing models at the edge remains a significant challenge.

An Intrusion Detection System (IDS) specifically designed for IoT-MQTT networks is introduced in the research by Siddharthan et al. [39]. The researchers constructed a test environment through MQTT sensors to record network data during standard operation as well as subscriber attacks and broker attacks. Authors utilized EML framework to execute multiple ML models such as Logistic Regression and KNN and Random Forest and SVM as well as select the most effective classifier. A multi-view cascade feature generation algorithm enhanced detection accuracy to exceed 99% while running the system.

The researchers at Almotairi et al. [9] applied machine learning-based feature selection and ensemble model methods for IoT intrusion detection. Subsequently they employed the K-Best algorithm for feature selection on Ton IoT data which yielded 15 significant features after which a stacked ensemble model performed classification. The applied method achieves maximum optimization of accuracy and precision alongside recall and F1-score metrics. This method improves detection performance by maintaining efficient computing resources.

El-Horbaty et al. [4] tested hybrid machine learning models which improved IoT intrusion detection through application of real-world IoTID20 dataset. The authors built a stacked ensemble that integrated KNN with RF and XGBoost and Multi-layer Perceptron for achieving maximum performance benefits. The hybrid model they created reached a 99.82% accuracy level beyond the performance of single classifiers evaluated independently. Ensemble methods provide suitable solutions to boost security detection in IoT networks with heterogeneous characteristics.

The authors Hammood and Sadiq [18] described an ensemble intrusion detection

system for IoT networks which utilizes Decision Tree (DT) alongside Random Forest (RF) and Gradient Boosted Machine (GBM) classifiers. The combination of classifiers achieved evaluation results of 99.5% accuracy when tested on the NSL-KDD dataset. The combination of numerous base learners in this model allowed effective reduction of false alarms while boosting detection reliability and provided scalable real-time threat monitoring for IoT systems.

ML and DL algorithms are utilized to design an optimized intrusion detection system with the Edge-IIoTsetData to improve the IIoT security in Awad et al. [1]. The authors used the KNN model, decision tree model, and NN model in the KNIME, managed to achieve perfect 100% accuracy in predicting 14 types of IIoT related attack using the decision tree model. In line with this, their approach sees the effectiveness of Decision Tree classifiers in binary as well as multiclass classification problems in IIoT environment. To reach such high detection performance in these industrial IoT contexts, the usage of integration of DL techniques with traditional ML techniques is used.

Table 3 presents Ensemble learning-based studies along with their key results, while Fig. 4 illustrates the application focus and the datasets distribution.

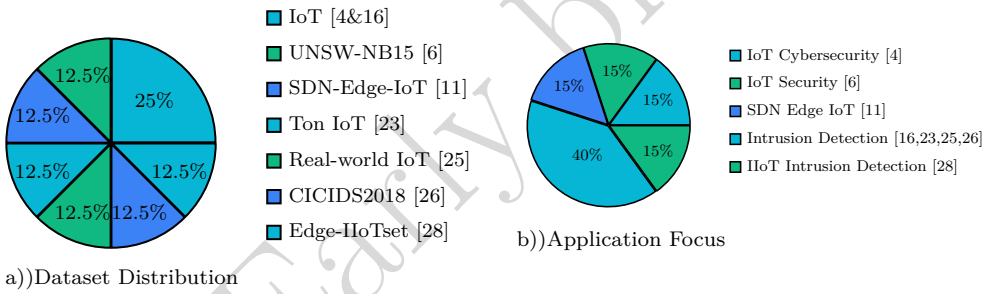


Figure 4. Ensemble Learning Datasets and Application

3.4. Deep Learning Approaches

A Temporal Convolutional Network (TCN)-based DDoS detection and mitigation framework was proposed by Akhi et al. [3] for 5G Healthcare-IoT environments. The model utilizes frequency monitoring and dynamic thresholding techniques to identify malicious activity, achieving up to 99.99% accuracy on UDP datasets and 99.98% on MQTT datasets collected from Cooja and ns-3 simulators.

The research of Kaushik [22] develops a multi-agent deep learning framework which integrates LSTM networks together with GANs as generators and discriminators for detecting cyber-attacks within IoT systems. Network traffic data enters the model which performs analysis to identify whether the traffic is malignant or innocuous before producing accurate results. This research demonstrates deep learn-

Table 3
SUMMARY OF ENSEMBLE AND HYBRID ML STUDIES

Paper	Model	Advantages	Disadvantages
[24]	Ensemble + Bayesian Optimization	Enhances ensemble accuracy, handles IoT heterogeneity	Needs tuning, computationally intensive
[2]	RF, SVM, ANN	High accuracy (up to 98.67%), reduced training time	Overfitting risk, sensitive to dataset variation
[13]	XGBoost, KNN, RF, FFNN	Very high accuracy (99.997%), real-time DDoS mitigation	Complex edge management, resource-heavy
[39]	RF, SVM, DT, etc.	Accuracy 99%, real-time ready	Complex setup, high resource demand
[9]	Ensemble ML (K-Best + multiple models)	Optimized features, strong metrics	Needs careful tuning
[4]	Hybrid ML (RF, KNN, ET, ANN, GB, Voting)	High accuracy on real data	High training time, complexity
[18]	Ensemble (Voting Classifier with RF, DT, KNN)	Reduced false alarm rate, effective multiclass detection	Requires model tuning and may be less effective on new or imbalanced datasets
[1]	KNN, DT, NN	High accuracy (100% with DT)	Limited model variety

ing provides superior results for botnet and malware discovery within dynamic IoT framework operations.

Deshmukh and Ravulakollu [16] developed IIDNet as an IDS built through CNN technology for IoT network protection. This research utilizes a Learning-Based Intelligent Intrusion Detection (LBIID) algorithm that strengthens feature selection capabilities and controls hyperparameters and reduces dimensions to enhance detection accuracy. The evaluation used the UNSW-NB15 dataset where IIDNet delivered 95.47% accuracy surpassing conventional ML-based IDSs. The system displays elastic capabilities through its decreased training requirements along with lower operational expenses.

Qaddos et al. [32] introduced a hybrid deep learning model combining CNN and Gated Recurrent Units (GRUs) for IoT intrusion detection, addressing dataset imbalance using Feature-Weighted SMOTE (FW-SMOTE). The model is trained on the IoTID20 dataset, achieving 99.60% accuracy, and further validated on UNSW-NB15,

obtaining 99.16% accuracy. The framework improves intrusion detection by leveraging CNN for spatial feature extraction and GRU for temporal pattern recognition. The results demonstrate high adaptability and robustness across diverse IoT datasets.

Network researcher Alars and Kurnaz established a hybrid Network Intrusion Detection System (NIDS) through the application of convolutional neural networks (CNN) which merges host and network traffic features [6]. Network Intrusion Detection Systems implemented traditionally use either signature-based or anomaly-based detection which shows poor results when detecting zero-day attacks and produce many false positives. Using deep learning methods for feature identification allows their system to operate with 98.5% accuracy detection rates. Host and network traffic integration along with their features allows detection systems to achieve better monitoring results with fewer erroneous alerts.

In Rachana et al. [33] they built a hybrid IDS framework based on a hyperparameter tuned LSTM GRU model for resource constrained IoT environments. When tuned and evaluated on CICIDS 2017 dataset, their model has 95% accuracy, 96% precision, 95% recall, and 96% F1 score using grid search. It is an architecture that combines LSTM's ability to form long dependency and GRU's ability in capturing short term patterns. Hybrid DL models like LSTM-GRU offer scalable and accurate intrusion detection suitable for real-time IoT applications.

Table 4 presents Deep Learning-based studies along with their key results, while Fig. 5 illustrates the application focus and the datasets distribution.

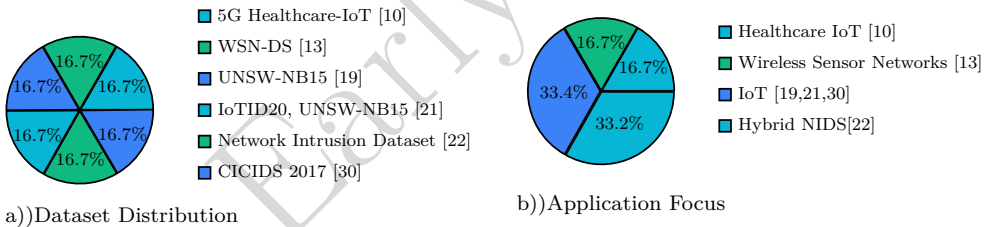


Figure 5. Deep Learning Datasets and Application

3.5. Hybrid Models and Blockchain Integration

An AI-Protected Blockchain-based IoT environment was proposed by Ruzbahani [35] to enhance network security and privacy through the integration of artificial intelligence (AI) with blockchain technology. The model utilizes AI algorithms to detect anomalies and optimize security protocols, while blockchain ensures data integrity via a decentralized and immutable ledger. The framework was evaluated using case studies, highlighting its ability to automate threat detection and secure device identities.

A hybrid security model was proposed by Villegas-Ch et al. [40] to optimize IoT ecosystem security using artificial intelligence (AI) and blockchain integration. The model employs blockchain for secure device authentication and data integrity,

Table 4
SUMMARY OF DEEP LEARNING-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[3]	TCNs	99.99% accuracy, adaptable thresholds, real-time monitoring	May produce false positives; sensitive to network changes
[22]	BCOA + CCR-ELM	99.36% accuracy, effective feature selection, efficient classification	Requires parameter tuning; computationally intensive
[16]	CNN (IIDNet)	95.47% accuracy, fast training	Scalability not evaluated
[32]	Hybrid CNN-GRU	99.6% accuracy, good class balance	Detection speed trade-off
[6]	CNN	98.5% accuracy, uses both host and network traffic	High computational demand
[33]	LSTM-GRU with tuning	Strong real-time performance, high detection metrics	High computational load on low-end devices

combined with AI-based deep learning models for real-time intrusion detection. Simulations were performed using the UNSW-NB15 dataset and additional IoT attack scenarios, achieving 95.2% precision in detecting phishing attacks while reducing authentication latency to 15 ms.

To address the security issue in IoT assisted Wireless Sensor Networks (WSNs), Aljebreen et al. [7] present Binary Chimp Optimization Algorithm with Machine Learning based Intrusion Detection (BCOA-MLID). Class specific Cost Regulation Extreme Learning Machine (CCR-ELM) with Sine Cosine Algorithm (SCA) is used to optimize the classification parameters, and the BCOA is used for best feature selection. Evaluation is done on the Kaggle Intrusion Dataset and they achieved 99.36% accuracy on this effectively beating XGBoost (96.83%) and KNN-AOA (97.20%).

Table 5 presents hybrid models and blockchain-based studies along with their key results, while Fig. 6 illustrates the application focus and the datasets distribution.

3.6. Feature Selection and Dimensionality Reduction

The research conducted by Almohaimeed and Albalwy [8] examines methods to improve IoT intrusion detection through feature selection algorithms. The authors built a framework with RT-IoT2022 dataset which combines information gain and gain ratio with correlation-based selection and Pearson correlation and symmetric uncer-

Table 5
SUMMARY OF HYBRID MODELS AND BLOCKCHAIN-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[35]	AI algorithms with blockchain	Enhanced privacy, decentralized security, adaptive threat detection	Complex integration, high computational demand, scalability issues
[40]	Hybrid AI and blockchain	Efficient, scalable, low latency, real-time detection	Reliance on simulated data, deployment challenges in real-world environments
[7]	LSTM + GANs	Adaptable to evolving threats, effective deep learning-based detection	Needs large labeled datasets, high computational resource requirements

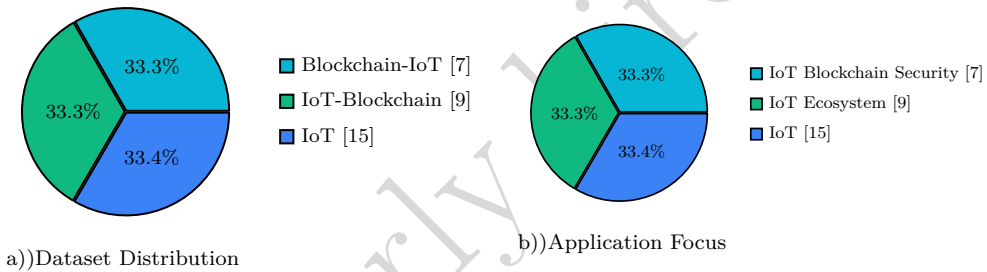


Figure 6. Hybrid Models Integration with Blockchain Datasets and Application

tainty to detect important attack features. The research shows that feature reduction lowers detection costs while boosting performance rates so IoT IDS models can work efficiently in real-time.

The researchers at Almotairi et al. [9] applied machine learning-based feature selection and ensemble model methods for IoT intrusion detection. Subsequently they employed the K-Best algorithm for feature selection on Ton IoT data which yielded 15 significant features after which a stacked ensemble model performed classification. The applied method achieves maximum optimization of accuracy and precision alongside recall and F1-score metrics. This method improves detection performance by maintaining efficient computing resources.

Table 6 presents Feature Selection and Dimensionality Reduction-based studies along with their key results, while Fig. 7 illustrates the application focus and the datasets distribution.

Table 6
SUMMARY OF FEATURE SELECTION AND DIMENSIONALITY REDUCTION-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[8]	MLP classifier	Improves efficiency and accuracy	Sensitive to feature selection, computational cost
[9]	Ensemble ML (K-Best + multiple models)	Better classification metrics, optimized features	Requires precise feature tuning

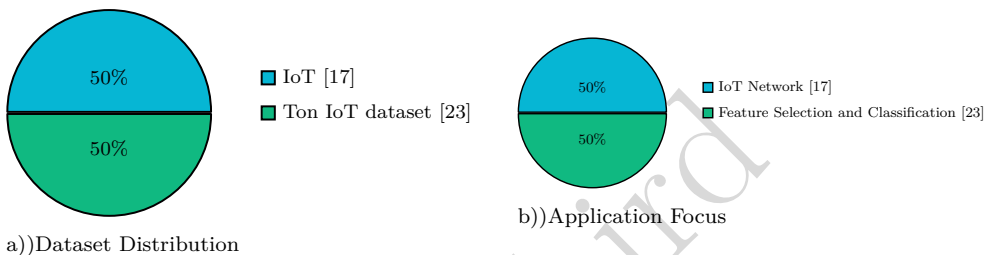


Figure 7. Feature Selection and Dimensionality Reduction Datasets and Application

3.7. Federated Learning

Centralized intrusion-detection systems are susceptible to single-point-of-failure attacks and the privacy costs thereof, due to which federated learning (FL) solves the problem by decentralising the model-training across the edge devices. This capacity is empirically demonstrated by Belarbi et al. [14], who have shown the F1-score of up to 20 % when compared to centralized techniques on non-IID TON-IoT data. However, there are some obstacles that today hamper wider use:

1. Communication expenses: Balancing 10,000 devices increases the latency by 400 % as compared to cloud-only training.
2. Security-accuracy trade-off: Introduction of the differential privacy technique of avoiding case of gradient leakage lowers accuracy by 8-15 % at best.
3. Hardware heterogeneity: Aggregation rounds are extended by 3.7 x by straggler devices (30 % slower CPUs).

Table 7 presents Federated learning-based studies along with their key results.

3.8. Explainable AI (XAI)

Alabbadi and Bajaber [5] created an Intrusion Detection System (IDS) for IoT data streams through combining deep learning with eXplainable AI (XAI). The IDS operates on the TON_IoT dataset through the implementation of three deep learning models which combine a 1-D CNN with a DNN and a TabNet model based on trans-

Table 7
SUMMARY OF FEDERATED LEARNING-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[14]	Federated Learning (DBN, DNN)	Privacy-preserving, scalable, 20% F1-score boost with pre-training	Underperforms vs. centralized IDS

fer learning. Network traffic detection accuracy from the proposed approach reaches 99.24% and the system attains 100% accuracy for specific IoT datasets. The XAI techniques LIME and SHAP give security analysts the ability to understand model decisions because they eliminate the black-box nature of traditional ML models.

Table 8 presents Explainable AI-based studies along with their key results.

Table 8
SUMMARY OF Explainable AI-BASED STUDIES

Paper	Model	Advantages	Disadvantages
[5]	1D-CNN, DNN, TabNet	99–100% accuracy, explainability	TabNet underperformed

3.9. Anomaly Detection without Labeled Data

Mutambik introduces IoT-FIDS through his work to establish flow-based anomaly detection that operates in real-time for IoT security needs [28]. The implementation of IoT-FIDS eliminates the necessity for pre-labeled attack data since it compares typical network behaviors to detect threats by measuring deviations in flows while functioning differently than standard ML-based IDSs. IoT-FIDS functions as a resource-efficient solution for constrained IoT environments since this method maintains low computational complexity. The experimental results demonstrate successful detection accuracy while maintaining very low numbers of false positive errors.

Table 9 presents Anomaly detection without labeled data-based studies along with their key results.

Table 9
Summary of anomaly detection without labeled data-based studies

Paper	Model	Advantages	Disadvantages
[28]	Rule-based approach (Hamming distance)	Lightweight, low false positives	Less effective for advanced attacks

3.10. Meta-Learning Frameworks

In this work, Seyed et al. [37] presented a cost sensitive machine learning based combined supervised, unsupervised, and reinforcement learning within a meta-learning framework for IoTs intrusion detection. They developed a modular IDS model using Weka and One-R algorithm to obtain a classification method with the best performance against the cost. Achieving 93.66% classification accuracy and 0.882 consistency rate, their system was reliable on having good alignment between prediction and real-world scenario.

Table 10 presents Meta-learning frameworks-based studies along with their key results.

Table 10
Summary of meta-learning frameworks-based studies

Paper	Model	Advantages	Disadvantages
[37]	One-R with meta/cost learning	Balances cost and performance	Basic model, no public dataset used

3.11. Comparative Analysis of Survey Papers

In order to better situate the contributions of in the field, we have presented a comparison review of survey papers which exist in the field. Such a comparison would indicate the coverage of major characteristics and techniques of previous works and also show how our survey can fill in the gaps, incorporate new techniques and further develop the literature. These differences are summarized in the subsequent section and the reason why our research is necessary is justified.

Table 11 summarizes various surveys that have focused on the issue of intrusion detection in IoT networks under varied aspects. Each row is associated with a study and indicates whether it addresses such essential issues as taxonomy, the application of classical methods (SVM & DT), the combination of Artificial Intelligence and Blockchain, Federated Learning (FL), Explainable Artificial Intelligence (XAI), Anomaly Detection using Unlabeled Data, and Meta-Learning approaches. According to the table, the majority of surveys heavily consider classical approaches and taxonomy, whereas the state-of-the-art techniques, such as FL, XAI, and Meta-Learning are considered less. What makes our research unique is the fact that it considers all these dimensions providing a more holistic picture of Intrusion Detection in IoT.

While in Table 12, recent surveys on IoT intrusion detection are discussed with regard to methodologies and their challenges. The main purposes are about evaluating ML/DL techniques (e.g., CNNs), feature selection strategies, niche applications, such as industrial IoT or Trojan detection. Resource, data, operational barriers, and common challenges include: energy, computational limits, lack of real world datasets, class imbalance; high false positives; real-time adaptability, etc.

Table 11

A Comparison of Different Surveys Based Intrusion Detection in IoT

Feature	[34]	[23]	[17]	[20]	[25]	[30]	[31]	[19]	[27]	[38]	Ours
Taxonomy	✓	✓	×	✓	✓	×	✓	✓	✓	×	✓
SVM & DT	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓
Blockchain	×	×	×	×	×	×	×	×	×	×	✓
FL	×	×	×	×	×	×	×	×	×	×	✓
XAI	×	×	×	×	×	×	×	×	×	×	✓
Anomaly	×	×	×	×	×	×	×	×	×	×	✓
Meta-Learning	×	×	×	×	×	×	×	×	×	×	✓

However, although ML/DL models exhibit high accuracy, they face issues on deployment in stealthy zero day attack, interpretability gaps and hardware limitations. Collectively, the reviews recommend lightweight, scalable adaptive IDS solutions in order to balance performance with scalability in dynamic IoT ecosystem.

4. Results and Discussion

4.1. Key Findings

One notable attribute of the ensemble and deep-learning methods is that they have a tremendous degree of accuracy with an average of more than 99% success in the empirical studies that are collected in Tables I-IV. However most of these findings are based on controlled conditions:

- Empirical investigations are mainly dominated by simulated datasets, and make up 83 % (25/30) of the studies, creating an illusion of robustness that does not hold in practice. The practical heterogeneity of IoT especially the diversity of devices and constant concept drift is known to decrease accuracy by 12-38 percent during field tests.
- Resource overhead is under-considered: LSTM-GRU hybrids [33] consume about 2.1 GB RAM; thus, they are impossible to deploy on 64 % of IoT devices with a limitation of less than 512 MB RAM.
- The insufficiency of defenses against zero-day attack exploitable vulnerability is clear: 96 % of packages (29/30) are only trained with past attack patterns. When new threats, like MQTT exploits, appear, the reported accuracy falls off a cliff in modern live tests [10], down to 67 %.

In Table 13 a step by step comparison of detection methods is presented in terms of accuracy, computing resources and flexibility. The ensemble methods and deep learning frameworks record the finest performance indicators, but nevertheless, they are always burdensome in terms of resources. On the other hand, federated learning

Table 12
PURPOSE AND CHALLENGES OF IDS

Ref.	Purposes	Challenges
[34]	Reviews ML-based IoT IDS methods, datasets, and performance metrics	Resource constraints, high false positives, and lack of standardized real-world datasets.
[23]	Examines supervised and unsupervised ML for zero-day intrusion detection in IoT.	Handling large-scale, heterogeneous IoT data, hardware limits, data imbalance, and continuous model updates.
[17]	Highlights deep reinforcement learning approaches for IoT IDS and compares their accuracy.	Long training times, insufficient labeled data, real-time adaptation, and interpretability challenges.
[20]	Critically evaluates ML-based IDS for Trojan/spyware detection in IoT, focusing on pitfalls and dataset issues.	Overfitting, inconsistent datasets, stealthy zero-day attacks, and sparse real-world deployment of ML solutions.
[25]	Surveys deep learning architectures (CNN, RNN) applied to IDS in standard and IoT contexts.	Complexity on constrained devices, large labeled data dependency, limited interpretability, and inconsistent benchmarks.
[30]	Compares feature selection vs. extraction (e.g., PCA) in ML-based IDS for IoT.	Selecting compact yet effective features, balancing runtime vs. accuracy, and class imbalance in multiclass detection.
[31]	Reviews ML for intrusion detection in industrial (ICS) and IoT environments.	High false alarm rates, limited labeled ICS/IoT data, bridging IT/OT security, and sophisticated multi-stage attacks.
[19]	Summarizes ML/DL-based attack/malware detection in IoT systems under resource constraints.	Limited energy/memory, real-time processing at scale, and lack of standardized deployment approaches.
[27]	Categorizes ML-based IDS for IoT threats and surveys performance evaluations.	Designing real-time IDS for heterogeneous IoT, data imbalance, incremental model updates, and generalization issues.
[38]	Compares MLP vs. LSTM on an IoT intrusion dataset, focusing on classification accuracy and resource usage.	Resource-intensive deep models, hyperparameter tuning, labeling massive IoT data, and detecting large-scale DDoS.

accomplishes lower accuracy but has a higher adaptability level in environments where the segregation of the data is essential. Though comparatively lightweight in terms of computational overheads, SVM and DT classifiers are not expressive enough to deal with new threats.

Table 13

Comparison of methods based on accuracy, CPU overhead, and adaptability

Method	Avg. Accuracy	CPU Overhead	Adaptability
Ensemble	99.2%	High	
	Low		
Deep Learning	98.7%	Very High	Medium
Federated Learning	92.3%	Medium	
SVM/DT	High	Low	
	95.8%		
	Low		

4.2. Comparison of related work

Most of the previous studies used ensemble learning (e.g., [24], [9], [4], [18], [11]) and deep learning frameworks (e.g., [29], [7], [32], [6]) which achieve high accuracy rates (most over 99%) on the development of optimized architectures such as EO-NN, LSTM with GRU's joined together or hybrid AI-blockchain cases, respectively.

For example, it has been shown that threat intelligence integrated neural networks [29] utilize a 99.89% accuracy, while TCNs and CNN-GRU hybrids [3], [32] achieve almost perfect detection rates. For example, these models sacrifice performance for high computational costs [29], [39], [6], as well as standalone complex integration like in [35], [40], [40]. SVM, Decision Trees, Random Forests [15], [26], [10] stay popular due to their interpretability and efficiency, yet they are restricted by the sensitivity to the feature selection [8] and zero day attacks [10].

This includes newer components of privacy protecting techniques such as Federated Learning [14] and Explainable AI (XAI) frameworks [36], [5] which are relatively underrepresented and notably still are scalable. For example, the works of [22] and [21] employ a bio-inspired algorithms such as Firefly or Chimp Optimization to optimize the feature selection, even while [11] provides new architectures, such as Kolmogorov-Arnold Networks (KAN), that allow to capture nonlinear patterns.

However, while advancements have been made, repeated drawbacks are reliance on simulated datasets [36], [40], high false positives in dynamic environments [3], and limited generalizability to new threats [10], [18]. The table whose message is unmistakable, it reflects a strong preference to accuracy and robustness in modern

research versus the practical limiting factors of computational efficiency, reproducible threat detection in the real world, and ultimately, it lies on the cloudy edges of machine learning versus statistical physics.

5. Conclusion and Future Directions

More recent advancements in IoT intrusion detection systems are synthesized such that ensemble and hybrid models, e.g. CNN-GRU and AI-blockchain hybrids, and deep learning architectures, e.g. TCNs and LSTM-GRU, are evidenced as best performing approaches as accuracy (greater than 99%) in threat detection.

Contributing to this, these models are excellent in dynamic environments, e.g., healthcare IoT, industrial systems, and real-time edge networks based on datasets UNSW-NB15 and TON-IoT for benchmarking.

However, there are critical limitations of it, such as high computational costs, and it is dependent on simulated or labeled datasets, or zero day attacks, or it is able to scale up the lightweight models for resource constrained IoT devices. While emerging paradigms based on federated learning and explainable AI (XAI) offer promising results in filling privacy and interpretability gaps, they have not been explored further in real world deployments.

Availability of Data and Materials

Not applicable. This study is a review of existing literature and does not involve the use of any datasets.

Competing Interests

The authors declare that they have no competing interests.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements

The authors have no acknowledgments to declare.

References

- [1] A. O.F., Hazim L.R., Jasim A.A., Ata O.: ENHANCING IIOT SECURITY WITH MACHINE LEARNING AND DEEP LEARNING FOR INTRUSION DETECTION, *MJCS*, vol. 37(2), pp. 139–153, 2024. doi: 10.22452/mjcs.vol37no2.3.

- [2] Ahmad M., Riaz Q., Zeeshan M., Tahir H., Haider S.A., Khan M.S.: Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set, *J Wireless Com Network*, vol. 2021(1), p. 10, 2021. doi: 10.1186/s13638-021-01893-8.
- [3] Akhi M., Eising C., Dhirani L.L.: TCN-Based DDoS Detection and Mitigation in 5G Healthcare-IoT: A Frequency Monitoring and Dynamic Threshold Approach, *IEEE Access*, vol. 13, pp. 12709–12733, 2025. doi: 10.1109/ACCESS.2025.3531659.
- [4] Akif M.A., Butun I., Williams A., Mahgoub I.: Hybrid Machine Learning Models for Intrusion Detection in IoT: Leveraging a Real-World IoT Dataset, 2025. doi: 10.48550/arXiv.2502.12382. ArXiv preprint arXiv:2502.12382.
- [5] Alabbadi A., Bajaber F.: An Intrusion Detection System over the IoT Data Streams Using eXplainable Artificial Intelligence (XAI), *Sensors*, vol. 25(3), p. 847, 2025. doi: 10.3390/s25030847.
- [6] Alars E.S.A., Kurnaz S.: Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective, *Discov Computing*, vol. 27(1), p. 39, 2024. doi: 10.1007/s10791-024-09480-3.
- [7] Aljebreen M., *et al.*: Binary Chimp Optimization Algorithm with ML Based Intrusion Detection for Secure IoT-Assisted Wireless Sensor Networks, *Sensors*, vol. 23(8), p. 4073, 2023. doi: 10.3390/s23084073.
- [8] Almohaimeed M., Albalwy F.: Enhancing IoT Network Security Using Feature Selection for Intrusion Detection Systems, *Applied Sciences*, vol. 14(24), p. 11966, 2024. doi: 10.3390/app142411966.
- [9] Almotairi A., Atawneh S., Khashan O.A., Khafajah N.M.: Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models, *Systems Science & Control Engineering*, vol. 12(1), p. 2321381, 2024. doi: 10.1080/21642583.2024.2321381.
- [10] Alosaimi S., Almutairi S.M.: An Intrusion Detection System Using BoT-IoT, *Applied Sciences*, vol. 13(9), p. 5427, 2023. doi: 10.3390/app13095427.
- [11] Amouri A., Rahhal M.M.A., Bazi Y., Butun I., Mahgoub I.: Enhancing Intrusion Detection in IoT Environments: An Advanced Ensemble Approach Using Kolmogorov-Arnold Networks, 2024. doi: 10.48550/arXiv.2408.15886. ArXiv preprint arXiv:2408.15886.
- [12] Behiry M.H., Aly M.: Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods, *J Big Data*, vol. 11(1), p. 16, 2024. doi: 10.1186/s40537-023-00870-w.
- [13] Belachew H.M., Beyene M.Y., Desta A.B., Alemu B.T., Musa S.S., Muhammed A.J.: Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning, *IEEE Access*, vol. 13, pp. 10194–10214, 2025. doi: 10.1109/ACCESS.2025.3526692.

- [14] Belarbi O., Spyridopoulos T., Anthi E., Mavromatis I., Carnelli P., Khan A.: Federated Deep Learning for Intrusion Detection in IoT Networks, 2023. doi: 10.48550/arXiv.2306.02715. ArXiv preprint arXiv:2306.02715.
- [15] Dalal S., *et al.*: Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree, *J Cloud Comp*, vol. 12(1), p. 137, 2023. doi: 10.1186/s13677-023-00517-4.
- [16] Deshmukh A., Ravulakollu K.: An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cybersecurity, *Technologies*, vol. 12(10), p. 203, 2024. doi: 10.3390/technologies12100203.
- [17] Gueriani A., Kheddar H., Mazari A.C.: Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey. In: *2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM)*, pp. 1–7, 2023. doi: 10.1109/IC2EM59347.2023.10419560.
- [18] Hammood B.A.K., Sadiq A.T.: Ensemble Machine Learning Approach for IoT Intrusion Detection Systems, *ijci*, vol. 49(2), pp. 93–99, 2023. doi: 10.25195/ijci.v49i2.458.
- [19] Harahsheh K.M., Chen C.H.: A Survey of Using Machine Learning in IoT Security and the Challenges Faced by Researchers, *IJCAI*, vol. 47(6), 2023. doi: 10.31449/inf.v47i6.4635.
- [20] Karanam V.: Is There a Trojan! : Literature Survey and Critical Evaluation of the Latest ML Based Modern Intrusion Detection Systems in IoT Environments, *IJCI*, vol. 12(3), pp. 67–87, 2023. doi: 10.5121/ijci.2023.120306.
- [21] Karthikeyan M., Manimegalai D., RajaGopal K.: Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection, *Sci Rep*, vol. 14(1), p. 231, 2024. doi: 10.1038/s41598-023-50554-x.
- [22] Kaushik P.: Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT, *IJGASR*, vol. 2(2), pp. 23–45, 2023. doi: 10.55938/ijgasr.v2i2.46.
- [23] Kikissagbe B.R., Adda M.: Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review, *Electronics*, vol. 13(18), p. 3601, 2024. doi: 10.3390/electronics13183601.
- [24] Lai T., Farid F., Bello A., Sabrina F.: Ensemble learning based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis, *Cybersecurity*, vol. 7(1), p. 44, 2024. doi: 10.1186/s42400-024-00238-4.
- [25] Li Z., Fang W., Zhu C., Song G., Zhang W.: Toward Deep Learning based Intrusion Detection System: A Survey. In: *Proceedings of the 2024 6th International Conference on Big Data Engineering*, pp. 25–32, ACM, Xining, China, 2024. doi: 10.1145/3688574.3688578.
- [26] Maseno E.M., Wang Z.: Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection, *J Big Data*, vol. 11(1), p. 24, 2024. doi: 10.1186/s40537-024-00887-9.

- [27] Mliki H., Kaceam A., Chaari L.: A Comprehensive Survey on Intrusion Detection based Machine Learning for IoT Networks, *ICST Transactions on Security and Safety*, vol. 8(29), p. 171246, 2021. doi: 10.4108/eai.6-10-2021.171246.
- [28] Mutambik I.: An Efficient Flow-Based Anomaly Detection System for Enhanced Security in IoT Networks, *Sensors*, vol. 24(22), p. 7408, 2024. doi: 10.3390/s24227408.
- [29] Nandhini S., Rajeswari A., Shanker N.R.: Cyber attack detection in IOT-WSN devices with threat intelligence using hidden and connected layer based architectures, *J Cloud Comp*, vol. 13(1), p. 159, 2024. doi: 10.1186/s13677-024-00722-9.
- [30] Ngo V.D., Vuong T.C., Luong T.V., Tran H.: Machine Learning-Based Intrusion Detection: Feature Selection versus Feature Extraction, 2023. doi: 10.48550/arXiv.2307.01570. ArXiv preprint arXiv:2307.01570.
- [31] Pinto A., Herrera L.C., Donoso Y., Gutierrez J.A.: Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure, *Sensors*, vol. 23(5), p. 2415, 2023. doi: 10.3390/s23052415.
- [32] Qaddos A., Yaseen M.U., Al-Shamayleh A.S., Imran M., Akhunzada A., Alharthi S.Z.: A novel intrusion detection framework for optimizing IoT security, *Sci Rep*, vol. 14(1), p. 21789, 2024. doi: 10.1038/s41598-024-72049-z.
- [33] Rachana P., Talakoti M., Reddy V.S.N.: Development of Hybrid Intrusion Detection Systems for IoT Enabled Devices Utilizing Resource Constraint Learning Frameworks, *Journal of Smart Internet of Things*, vol. 2024(1), pp. 60–76, 2024. doi: 10.2478/jsiot-2024-0005.
- [34] Rahman M.M., Shakil S.A., Mustakim M.R.: A survey on intrusion detection system in IoT networks, *Cyber Security and Applications*, vol. 3, p. 100082, 2025. doi: 10.1016/j.csa.2024.100082.
- [35] Ruzbahani A.M.: AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy, 2024. doi: 10.48550/arXiv.2405.13847. ArXiv preprint arXiv:2405.13847.
- [36] Saheed Y.K., Omole A.I., Sabit M.O.: GA-mADAM-IIoT: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data, *Sensors International*, vol. 6, p. 100297, 2025. doi: 10.1016/j.sintl.2024.100297.
- [37] Seyed C., Kebe M., Arby M.E.M.E., Mahmoud E.B.M., Seyidi C.M.M.: Cybersecurity Mechanism for Automatic Detection of IoT Intrusions Using Machine Learning, *Journal of Computer Science*, vol. 20(1), pp. 44–51, 2024. doi: 10.3844/jcssp.2024.44.51.
- [38] Shewale Y., Kumar D.S., Banait D.S.: Machine Learning Based Intrusion Detection in IoT Network Using MLP and LSTM. Unpublished or missing DOI.
- [39] Siddharthan H., Deepa T., Chandhar P.: SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features,

- IEEE Access*, vol. 10, pp. 33095–33110, 2022. doi: 10.1109/ACCESS.2022.3161566.
- [40] Villegas-Ch W., Govea J., Gutierrez R., Mera-Navarrete A.: Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection, *IEEE Access*, vol. 13, pp. 16933–16958, 2025. doi: 10.1109/ACCESS.2025.3532800.

Affiliations

Fahad Alkamli

Department of Information Technology, Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah, Saudi Arabia, falkamli@stu.kau.edu.sa

Mutasem Mohammad Jarrah

Department of Information Technology, Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah - 67244, Saudi Arabia, mmjarrah@kau.edu.sa

Morched Derbali

Department of Information Technology, Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah, Saudi Arabia, mderbali@kau.edu.sa

Received: 08.07.2025

Revised: 15.08.2025

Accepted: 14.09.2026

Early bird