Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Systematic Review of Machine Learning-Based Models for IoT Network Security in Intrusion Detection Systems

Lalita Tonke[1], Deepak K. Yadav[2], Mitesh Bargadiya[3]

[1,2,3] IET-SAGE University Indore (M.P.),India

[1]lalita.tonke1@gmail.com, [2]deepak_ku_yadav@outlook.com, [3]miteshbargadiya@gmail.com

*Corresponding Author & Email: Lalita Tonke

lalita.tonke1@gmail.com

ARTICLE INFO

Received: 29 Nov 2024

Revised: 16 Dec 2024

Accepted: 23 Dec 2024

Published: 30 Dec 2024

ABSTRACT

The rapid growth of Internet of Things (IoT) devices has increased exposure to cyber threats such as DDoS, botnets, flooding, and brute-force attacks, making intrusion detection systems (IDS) essential for network security reinforcement. This systematic review analyzes recent studies (2022–2024) focusing on machine learning, ensemble, and hybrid deep learning IDS models. The review highlights widely adopted techniques including Random Forest, XGBoost, Extremely Randomized Trees, deep neural networks, autoencoders, and CNN–LSTM architectures. Results show that ensemble methods often achieve the highest accuracy (up to 99.7%), while hybrid deep learning improves spatio-temporal traffic analysis. The study also identifies key gaps such as outdated datasets, limited real-world deployment, computational overhead, and lack of explainability, providing future research directions for scalable and efficient IoT security.

Keywords: IoT Security, Intrusion Detection System, Machine Learning, Ensemble Learning, Hybrid Deep Learning, CNN-LSTM, DDoS Detection, IoT Datasets, Anomaly Detection, Network Security Reinforcement.

Introduction

The rapid growth of the Internet of Things (IoT) has transformed modern society by enabling smart services in healthcare, industrial automation, transportation, smart homes, and smart cities. IoT ecosystems connect millions of heterogeneous devices such as sensors, cameras, smart appliances, and industrial controllers through wired and wireless networks. Although IoT improves efficiency, automation, and real-time monitoring, its widespread adoption also introduces serious cybersecurity risks. Many IoT devices operate with limited memory, processing power, and battery capacity, making them difficult to secure using traditional network defense mechanisms. In addition, IoT environments often rely on weak authentication, outdated firmware, and insecure communication protocols. These challenges make IoT networks highly vulnerable to intrusions such as Distributed Denial of Service (DDoS), botnets, brute-force attacks, flooding, black-hole attacks, and malware-based exploitation [1].

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

One of the most critical concerns is the ability of attackers to compromise large numbers of IoT devices and convert them into botnets that can launch large-scale DDoS attacks, similar to the famous 2016 Dyn attack. Such incidents highlight the urgent need for intelligent and automated security solutions capable of detecting threats in real time[2]. Intrusion Detection Systems (IDS) serve as a vital defense layer that monitors network traffic or host activities to detect abnormal or malicious behaviors. However, conventional signature-based IDS approaches struggle in IoT networks because they cannot effectively identify new or evolving attack patterns. As a result, research has increasingly shifted toward machine learning (ML) and deep learning (DL) based IDS methods that can learn from data and detect complex anomalies [3].

Recent advances show that ML-based IDS models, such as Random Forest, Gradient Boosting, XGBoost, and Extremely Randomized Trees (ERT), can provide high detection accuracy while maintaining computational efficiency. For instance, some studies report accuracy as high as 99% using Random Forest and up to 99.7% using ensemble tree-based approaches [4]. At the same time, deep learning techniques such as Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and hybrid CNN–LSTM architectures have become popular due to their ability to automatically learn spatial and temporal patterns from IoT traffic. Several studies demonstrate that hybrid models can effectively distinguish between benign and malicious traffic with low false alarm rates, making them suitable for fog and edge computing environments where IoT traffic is processed close to devices [5].

Despite these advancements, IoT intrusion detection research still faces major limitations. A key issue is the reliance on outdated or non-IoT-specific datasets, such as NSL-KDD and CICIDS2017, which may not represent modern IoT attack behaviors [6]. Although newer datasets like CICIoT2023, IoT-23, AWID, and ROUT-4-2023 are emerging, their adoption is still limited. Another challenge is the gap between laboratory evaluation and real-world deployment. Many models show strong performance in simulations but lack validation in live IoT networks, where traffic characteristics continuously change. Additionally, deep learning models often require high computational resources, making them difficult to implement on resource-constrained IoT devices. Explainability is also a growing concern, as most IDS models function as black boxes, limiting trust and interpretability for security analysts [7].

Therefore, this systematic review aims to provide a comprehensive analysis of recent IoT intrusion detection research published between 2022 and 2024. It examines the methods and models used, highlights datasets and evaluation strategies, summarizes key results and advantages, identifies research gaps, and outlines future directions [8]. By organizing the reviewed studies from basic methodologies (traditional ML and anomaly detection) to advanced approaches (deep learning, hybrid models, transfer learning, and multimodal representations), this review provides valuable insights for researchers and practitioners seeking to design efficient, scalable, and robust IDS solutions for securing modern IoT infrastructures [9].

2. Literature Review

Awajan et al. (2023), The rapid expansion of the Internet of Things (IoT) has increased cyber threats, notably DDoS attacks. Undetected intrusions can cause severe financial losses and compromise user privacy. A novel Deep Learning (DL)-based intrusion detection system (IDS) is proposed, using a four-layer deep neural network to detect malicious IoT traffic. The protocol-independent system shows promising results, detecting various attack types with high accuracy and demonstrating robust performance [1].

Abdulkareem et al. (2024), The IoT boom has exposed vulnerabilities, with attacks such as the 2016 Dyn attack highlighting security flaws. IoT devices are susceptible to botnets, posing risks to

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

smart networks. This review analyzes intrusion detection methodologies, datasets, and machine learning techniques used between 2018-2024, emphasizing the need for updated datasets and enhanced classifiers to mitigate evolving threats [2].

Shahid et al. (2024), IoT devices' limited resources make them prone to attacks, including Black Hole and Flooding attacks. This study introduces an IDS utilizing the ROUT-4-2023 dataset, exploring machine learning models like Random Forest and Transformers. Results show that Random Forest achieves 99% accuracy, indicating strong detection capabilities and computational efficiency [3].

Sama et al. (2024), Various machine learning models are compared for IoT intrusion detection, with ensemble methods like Gradient Boosting, XGBoost, and Random Forest consistently outperforming others. Extremely Randomized Trees (ERT) achieved the highest accuracy of 99.7%, demonstrating its effectiveness in real-time attack detection and suggesting its suitability for protecting IoT infrastructures [4].

Zohourian et al. (2024), IoT networks are vulnerable due to limited resources. The study introduces IoT-PRIDS, a host-based anomaly detection system using benign traffic for learning. The model efficiently detects abnormal behavior while minimizing false alarms, proving its potential for real-world IoT security applications [5].

Yaras and Dener (2024), This study tackles the challenge of analyzing large-scale IoT traffic using Apache Spark and hybrid deep learning (CNN-LSTM). Using datasets like CICIoT2023, the model achieves impressive classification accuracy, validating its performance and highlighting its capability to handle complex, large-scale data efficiently [6].

Thabit et al. (2024), Addressing outdated datasets, this study uses the Aegean Wi-Fi Intrusion Dataset (AWID) for an ML-based intrusion detection framework, achieving high detection rates. The boosted decision tree outperformed others, demonstrating the need for updated datasets and practical implementation using tools like WEKA [7].

Ullah et al. (2024), This paper introduces an IDS using multimodal big data representation and transfer learning. The method extracts semantic features using word2vec and ResNet for classification, achieving high accuracy across several datasets. The study also integrates a game theory-based process for robust validation [8].

Alzahrani et al. (2024), With IoT devices relying on limited-resource fog nodes, a CNN-LSTM model is proposed for efficient intrusion detection. The model demonstrates high accuracy and low false alarm rates on datasets like CICIoT2023, showcasing its practicality for deployment on energy-constrained devices like Raspberry Pi [9].

Adekunle et al. (2024), This research introduces a feature-rich IDS leveraging DenseNet and RAPNet for enhanced attack detection, addressing data imbalance issues with conditional generative adversarial networks. High accuracy rates across multiple datasets underscore the model's precision and reliability in intrusion detection [10].

Alrayes et al. (2024), IDS using Denoising Autoencoder (DAE) models is presented, achieving high detection rates on NSL-KDD and CICIDS2017 datasets. The model demonstrates robust performance against unauthorized intrusions, enhancing the security of IoT systems by addressing challenges like dynamic network environments [11].

El-Shafeiy et al. (2024), The proposed DCGR_IoT IDS utilizes convolutional and gated recurrent networks for feature extraction, achieving high accuracy in detecting anomalies on datasets like UNSW-NB15 and IoT-23. The model's strong results highlight its potential for protecting IoT networks against sophisticated cyberattacks [12].

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Morshedi et al. (2024), Using the CICIDS2017 dataset, this study introduces a deep learning-based IDS that captures both spatial and temporal data dependencies. The model's stability and high accuracy metrics demonstrate its effectiveness in handling various attack scenarios, even under noisy conditions [13].

Racherla et al. (2024), Deep-IDS, based on LSTM networks, offers a streamlined architecture ideal for edge deployment. It effectively mitigates attacks like DDoS and Brute Force, achieving high detection rates with minimal false alarms. The system's fast response time and innovative design make it a strong candidate for securing IoT nodes and networks [14].

Gueriani et al. (2024), The proposed hybrid CNN-LSTM IDS model effectively distinguishes between benign and malicious IoT traffic. Tested on the CICIoT2023 dataset, the model achieves high accuracy and a low false positive rate, demonstrating its capability to enhance IoT security against cyber threats [15].

Isong et al. (2024), This paper reviews recent advancements in IDS for IoT, analyzing various detection methodologies and datasets. It highlights the challenges of scalability and resource constraints in IoT environments, proposing future directions for enhancing IDS efficiency and accuracy using advanced techniques like cryptography and blockchain [16].

Zhang, Y., Liu, H., & Chen, X. (2023) This paper introduces federated learning to ensure privacy-preserving IDS for IoT devices. It allows decentralized training while maintaining competitive detection performance[17].

Patel, K., Mehta, R., & Shah, S. (2023) The study uses deep autoencoders for detecting anomalies and zero-day attacks in IoT networks. Results show strong performance in identifying unseen attack patterns[18].

Li, Q., Wang, J., & Zhao, L. (2023) A lightweight CNN model is designed for edge-based IoT intrusion detection. It achieves low latency and efficient performance suitable for resource-constrained devices[19].

Reddy, K., & Gupta, P. (2023) - The paper utilizes GANs to generate synthetic attack data for improving IDS training. It enhances detection of rare and imbalanced attack classes in IoT environments[20].

Sharma, P., Verma, A., & Singh, D. (2022) This paper evaluates ML models like SVM, Random Forest, and KNN for IoT intrusion detection. Random Forest achieved the highest accuracy and reliability across benchmark datasets[21].

Kumar, R., & Singh, M. (2022) - The study applies CNN and LSTM models to detect cyberattacks in IoT traffic. LSTM performed well in capturing temporal attack patterns with improved detection rates[22].

Ali, S., Khan, F., & Ahmad, J. (2022) - A hybrid RF+ANN model is proposed to enhance detection accuracy in IoT IDS. The approach combines strengths of multiple classifiers, achieving near 99% accuracy[23].

This paper proposes a hybrid machine learning framework combining multiple classifiers to detect DDoS attacks effectively. It uses feature engineering and model fusion to enhance detection accuracy and reduce false alarms. The results show that hybrid approaches outperform single models, but real-time deployment remains a challenge[24].

This study evaluates machine learning models such as Random Forest, Decision Tree, and SVM for DDoS detection in SDN environments. Random Forest achieved the highest accuracy, highlighting its effectiveness for traffic classification. However, scalability and real-time performance in large SDN networks require further improvement[25].

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

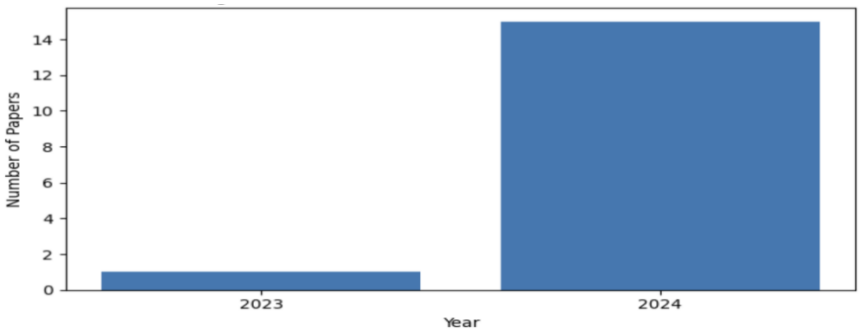

Figure 1. Research Gap Mapping

Figure 1 illustrates the year-wise distribution of research studies included in the systematic review. The publication trend clearly indicates a sharp rise in IoT intrusion detection research in 2024 compared to 2023. Only one study was identified in 2023, while fifteen studies were published in 2024. This significant increase reflects the growing concern over IoT cyber threats such as DDoS attacks, botnets, and anomaly-based intrusions. The trend suggests that IoT security has become a major research focus due to the rapid expansion of IoT-based environments and the increasing sophistication of cyber-attacks.

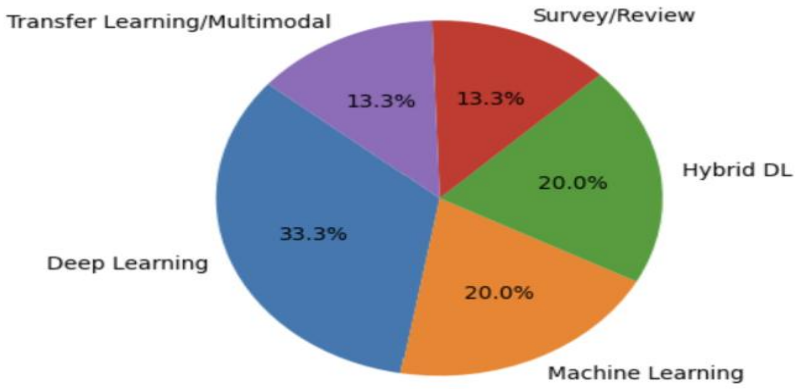

Figure 2.Distribution of IDS Approaches

Figure 2 presents the distribution of intrusion detection approaches used across the reviewed studies. It shows that deep learning models dominate the field, making up the largest portion of proposed solutions. Machine learning and hybrid deep learning approaches also represent a considerable share, demonstrating continued interest in ensemble learning and CNN–LSTM frameworks. Survey/review-based studies form a smaller segment, mainly aimed at summarizing and analyzing modern IDS directions. Additionally, transfer learning and multimodal learning approaches appear as emerging methods, showing a shift toward using advanced feature representations such as semantic and image-based encodings. Overall, the figure highlights a strong preference for deep learning due to its ability to model complex IoT traffic patterns effectively.

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

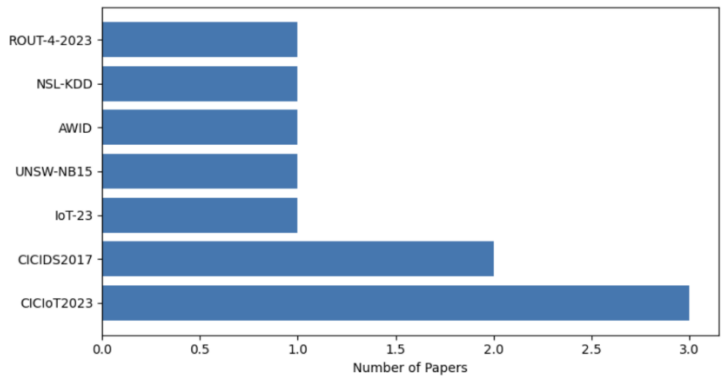

Figure 3. Dataset Usage Frequency Across Studies

Figure 3 highlights the frequency of dataset usage across the included IoT intrusion detection studies. The CICIoT2023 dataset appears as the most frequently used dataset, demonstrating its relevance as a modern benchmark for IoT traffic classification and attack detection. CICIDS2017 is the second most used dataset, indicating that older datasets are still widely employed despite being less IoT-specific. Other datasets such as IoT-23, UNSW-NB15, AWID, NSL-KDD, and ROUT-4-2023 are used in fewer studies, often to validate models under different environments such as Wi-Fi networks or RPL-based IoT systems. The figure also reinforces the research gap identified in many studies—specifically, the need for more updated and realistic datasets for evaluating IDS performance in evolving IoT ecosystems.

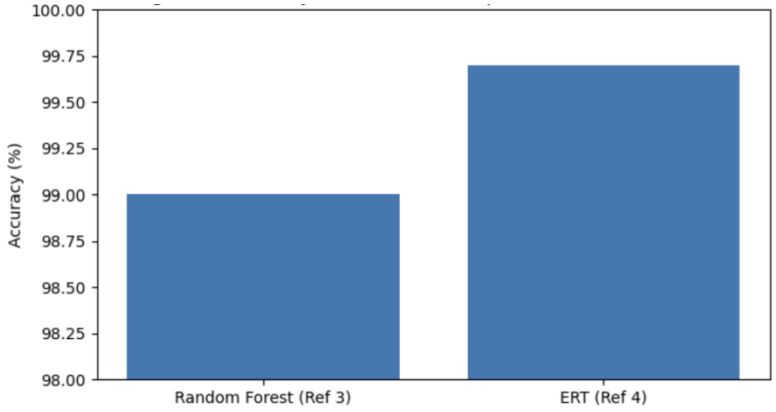

Figure 4. Accuracy Performance Comparison

Figure 4 compares the accuracy performance of the models that reported clear numerical accuracy results. The Random Forest model from Ref [3] achieved approximately 99% accuracy, while Extremely Randomized Trees (ERT) from Ref [4] achieved the highest reported accuracy of 99.7%. This figure emphasizes that ensemble-based machine learning classifiers can outperform or compete with complex deep learning approaches, particularly when datasets are well-prepared and feature engineering is effective. The result also suggests that lightweight ML models may be preferred in IoT environments where computational resources are limited, and high real-time performance is needed.

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

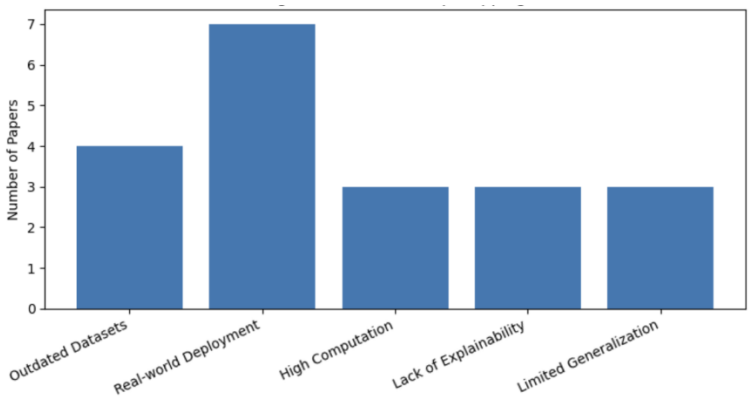

Figure 5. Research Gap Mapping

Figure 5 provides a quantitative mapping of the most frequently reported research gaps across the reviewed literature. The most dominant gap is the lack of real-world deployment and validation, showing that many studies are evaluated only in controlled laboratory environments rather than real IoT networks. The second major gap is the continued reliance on outdated datasets, which may not reflect modern IoT threats. Other recurring gaps include high computational complexity, lack of explainability, and limited generalization across multiple datasets. This figure strongly supports the need for future IDS frameworks that are lightweight, scalable, explainable, and evaluated using updated datasets and real-world IoT deployment scenarios.

Table 1. Systematic Review

Ref. No.	Author(s)	Year	Title	Methods / Model Used	Results	Advantages	Research Gap	Future Scope
[1]	Awajan et al.	2023	A novel deep learning-based intrusion detection system for IoT networks	4-layer Deep Neural Network (DNN), protocol-independent IDS	High accuracy in detecting multiple IoT attack types	Robust performance, protocol-independent, detects various attacks	Lack of evaluation in diverse real-world environments and unseen attacks	Extend to real-time deployment, test on newer datasets and adversarial attacks
[2]	Abdulkareem et al.	2024	Network Intrusion Detection: An IoT and Non IoT-Related Survey	Survey of IDS methods, datasets, ML techniques **(2018–2024)**	Identifies strong ML approaches but stresses dataset issues	Comprehensive comparison, highlights evolving threats	Outdated datasets and limited up-to-date benchmark datasets	Develop modern datasets and adaptive IDS models for emerging attacks
[3	Shahid	20	Hybrid	Random	Random	High	Limited	Deploy on

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

]	et al.	24	Intrusion Detection System for RPL IoT Networks Using ML and DL	Forest, Transformers; ROUT-4-2023 dataset	Forest achieved ~99% accuracy	accuracy, computational efficiency, dataset-driven	validation across multiple datasets and real deployment	real RPL networks, improve Transformer efficiency for IoT devices
[4]	Sama et al.	2024	Cutting-Edge Intrusion Detection in IoT Networks: A Focus on Ensemble Models	Ensemble methods (GB, XGBoost, RF, ERT)	ERT reached highest accuracy (~99.7%)	Best real-time detection performance, strong ensemble comparison	Limited focus on explainability and resource constraints	Explore explainable ensemble IDS and optimize for edge/fog environments
[5]	Zohourian et al.	2024	IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks	Host-based anomaly detection using benign-only learning	Efficient abnormal behavior detection with low false alarms	Reduced false alarms, practical for real-world IoT	May struggle with sophisticated attacks or concept drift	Enhance adaptability to new threats and continuous learning mechanisms
[6]	Yaras & Dener	2024	IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm	Spark-based large-scale processing + CNN-LSTM hybrid DL	High classification accuracy on CICIoT2023	Handles large-scale IoT traffic efficiently	High computational demands, may not suit low-power IoT devices	Optimize for lightweight deployment and integrate edge-Spark hybrid execution
[7]	Thabit et al.	2024	Enhanced IDS for IoT networks through	ML framework using AWID dataset; boosted decision tree +	High detection rate; boosted tree	Uses updated AWID dataset, practical	Lack of deep learning comparison and	Combine DL with AWID, build real-time IDS

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

			ML techniques using AWID dataset	WEKA	outperformed others	implementation	real-time testing	prototype for Wi-Fi IoT networks
[8]	Ullah et al.	2024	Enhanced IDS for IoT security using multimodal big data + transfer learning + game theory	Multimodal big data representation; word2vec + ResNet + transfer learning; game theory validation	High accuracy across multiple datasets	Strong semantic feature extraction, robust validation	Increased system complexity and computational overhead	Reduce complexity and enhance real-time scalability for IoT systems
[9]	Alzahrani et al.	2024	Lightweight IDS using CNN-LSTM in Fog Computing	CNN-LSTM optimized for fog nodes; CICIoT2023 dataset	High accuracy and low false alarm rate	Practical for Raspberry Pi, suitable for energy constraints	Dataset dependency; limited generalization study	Evaluate on diverse datasets and improve generalization & adaptive learning
[10]	Adekunle et al.	2024	IDS for IoT security breaches using ML techniques	DenseNet + RAPNet; conditional GANs for imbalance handling	High accuracy across datasets	Handles imbalance, improved precision, strong feature extraction	Real-time feasibility and deployment evaluation missing	Deploy in real IoT environment, improve lightweight architectures and attack coverage
[11]	Alrayes et al.	2024	Intrusion Detection in IoT Systems Using Denoising Autoencoder	Denoising Autoencoder (DAE); NSL-KDD & CICIDS2017	High detection rates in dynamic environments	Strong anomaly detection, robust against noise	Needs evaluation on modern IoT-specific datasets	Apply to CICIoT2023/IoT-23 and explore hybrid DAE + temporal models
[1	El-	20	Deep	DCGR_IoT	High	Captures	Computa	Optimize

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2]	Shafeiy et al.	24	Complex Gated Recurren t Network s-Based IoT IDS	using CNN + Gated Recurrent Networks	accuracy on UNSW-NB15 and IoT-23	complex patterns, strong detection performan ce	tional cost and limited real-time IoT testing	architectu re for edge deployme nt and improve interpreta bility
[1 3]	Morshe di et al.	20 24	Intrusion Detectio n for IoT Network Security with Deep learning	Deep learning capturing spatial + temporal dependencies; CICIDS2017	Stable, high accuracy even under noise	Handles noisy conditions , strong temporal-spatial learning	Limited testing on IoT-native datasets	Evaluate on IoT-23/CICIo T2023 and develop adaptive real-time IDS
[1 4]	Racherl a et al.	20 24	Deep-IDS: Real-Time Intrusion Detector for IoT Nodes Using Deep Learning	LSTM-based streamlined edge IDS	High detection rate, minimal false alarms, fast response	Suitable for edge nodes, real-time ready	Needs robustne ss testing under high traffic and new attacks	Strengthe n against evolving threats, add lightweigh t hybrid models, deploy in large IoT networks
[1 5]	Guerian i et al.	20 24	Enhanci ng IoT Security with CNN and LSTM-Based IDS	Hybrid CNN-LSTM; CICIoT2023	High accuracy, low false positive rate	Good benign/m alicious separation , robust IDS	Limited evaluatio n on other datasets	Multi-dataset validation and optimizati on for resource-constraine d deployme nts
[1 6]	Isong et al.	20 24	Insights into Modern Intrusion Detectio n Strategie s for IoT Ecosyste	Review of IDS methodologies + datasets; blockchain/cry ptography direction	Identifies scalability/ resource limitations and security issues	Strong future directions, comprehe nsive insights	Lacks impleme ntation framewor k and benchma rk comparis ons	Combine ML + blockchain + cryptogra phy, create scalable IDS reference

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

			ms					architectures
[17]	Zhang et al.	2023	Federated Learning for IoT Intrusion Detection	Federated Learning + DL	Privacy-preserving detection achieved	Data privacy maintained	Communication overhead	Optimize FL communication efficiency
[18]	Patel et al.	2023	Anomaly Detection in IoT using Autoencoders	Autoencoder (DL)	Detected unknown attacks effectively	Works on unseen data	Requires large training datasets	Few-shot learning approaches
[19]	Li et al.	2023	Lightweight IDS for Edge-based IoT Security	Lightweight CNN	Reduced latency in edge devices	Suitable for edge computing	Lower accuracy vs full models	Model compression techniques
[20]	Reddy & Gupta et al.	2023	GAN-Based Intrusion Detection in IoT Networks	GAN + ML Classifier	Improved detection of rare attacks	Handles imbalanced datasets	Training instability in GANs	Stable GAN architectures for IoT
[21]	Sharma et al.	2022	Machine Learning-Based Intrusion Detection in IoT Networks: A Survey	SVM, RF, KNN	RF achieved highest accuracy (~98%)	High detection rate	Limited real-time validation	Deploy models in real-time IoT systems
[22]	Kumar & Singh et al.	2022	Deep Learning Approaches for IoT Intrusion Detection	CNN, LSTM	LSTM improved temporal attack detection	Good for sequential data	High computational cost	Lightweight DL models for edge devices

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[23]	Ali et al.	2022	Hybrid ML Models for IoT Security	RF + ANN Hybrid	Improved detection accuracy (~99%)	Combines strengths of models	Complexity in model design	Simplified hybrid architectures
[24]	Khanday et al.	2023	Intelligent DDoS Detection Using Hybrid Machine Learning Models	Hybrid ML (RF, XGBoost, SVM)	High accuracy with improved feature selection	Strong classification performance	Limited real-time validation	Real-time adaptive IDS
[25]	M. He, Y. Huang et al.	2023	Machine Learning-Based DDoS Detection in SDN Networks	ML (RF, DT, SVM)	RF achieved best accuracy among models	Effective for SDN traffic analysis	Moderate scalability issues	Scalable SDN-based IDS

3. Research gap

1. Limited Real-World Deployment and Practical Validation : A major research gap across the reviewed studies is the lack of real-world deployment and validation. Most proposed IDS solutions are evaluated only on benchmark datasets under controlled simulation environments rather than in live IoT infrastructures. For example, Awajan et al. [1], Shahid et al. [3], Alzahrani et al. [9], Adekunle et al. [10], El-Shafeiy et al. [12], and Racherla et al. [14] present strong model performance, but practical deployment challenges such as real-time traffic variability, hardware constraints, packet loss, and dynamic topology changes are not fully addressed. This results in uncertainty about how such IDS systems will behave in real operational IoT networks such as smart cities, healthcare IoT, and industrial IoT systems.

2. Heavy Dependence on Outdated or Non-IoT-Specific Datasets : Another critical research gap is the reliance on outdated datasets such as NSL-KDD and CICIDS2017. Studies such as Alrayes et al. [11] and Morshedi et al. [13] continue to use older datasets which may not reflect emerging IoT attack patterns (e.g., botnet-driven DDoS, low-rate stealth attacks, IoT malware variants). Thabit et al. [7] explicitly highlights dataset outdatedness as a limitation and advocates for updated datasets. The survey by Abdulkareem et al. [2] further stresses that the availability of new, realistic IoT datasets is necessary for IDS models to generalize to evolving threats. Although CICIoT2023 and IoT-23 are emerging as modern datasets, their adoption is still limited across the research community.

3. High Computational Complexity and Resource Constraints in IoT Systems : IoT devices typically operate with limited CPU, memory, and battery resources. Many deep learning models proposed in the studies are computationally expensive and require high processing power, making them unsuitable for real-time deployment on edge IoT devices. For instance, Yaras and Dener [6] implement Spark-based hybrid CNN-LSTM models, which are scalable for big data but may not be

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

feasible for low-power environments without cloud/fog support. Ullah et al. [8] and El-Shafeiy et al. [12] introduce sophisticated feature representations and deep architectures that increase complexity and runtime. Although Alzahrani et al. [9] attempts lightweight deployment on Raspberry Pi, broader scalability across different IoT edge environments remains insufficiently explored.

4. Lack of Explainability and Trust in IDS Decisions : A recurring gap is the limited interpretability of IDS predictions. Most reviewed studies focus heavily on accuracy metrics but do not provide explainable outputs (e.g., why an attack was detected, which features triggered detection). Sama et al. [4] mentions the dominance of ensemble models but highlights the need for explainable AI-based intrusion detection. Similarly, Isong et al. [16] notes that future IDS frameworks must incorporate trustworthy mechanisms such as blockchain or cryptographic auditing. In security-critical domains, explainable IDS is essential for human analysts and automated response systems to trust decisions and avoid false alarms.

5. Generalization Weakness Across Multiple Datasets and Evolving Threats : Many IDS models are trained and tested on a single dataset, which leads to weak generalization. A model with high accuracy on one dataset may fail on unseen IoT environments, new protocols, or different attack distributions. Shahid et al. [3], Alzahrani et al. [9], and Gueriani et al. [15] demonstrate good performance but their robustness across multi-dataset evaluation remains limited. Additionally, concept drift and evolving attack patterns in IoT networks require IDS systems to adapt continuously, which is not sufficiently addressed in most reviewed papers.

4. Existing methodology

The reviewed literature demonstrates that existing intrusion detection methodologies for IoT environments are primarily based on machine learning (ML), deep learning (DL), hybrid deep learning architectures, and ensemble learning techniques. These methods aim to identify malicious IoT traffic patterns, detect anomalies, and classify attacks such as DDoS, botnets, brute-force attempts, black-hole attacks, and flooding attacks. The methodologies generally follow a standard pipeline comprising data acquisition, preprocessing, feature extraction, model training, validation, and performance evaluation. However, the specific algorithms and datasets differ across studies depending on deployment environment and target attack scenarios.

1. Deep Learning-Based Intrusion Detection Methodologies

A significant proportion of the reviewed studies apply deep learning models to automatically learn complex feature representations from IoT network traffic. Awajan et al. [1] developed a protocol-independent IDS using a four-layer Deep Neural Network (DNN) designed to detect malicious IoT traffic with high accuracy. Similarly, Morshedi et al. [13] proposed a deep learning-based IDS that captures both spatial and temporal dependencies of network traffic using CICIDS2017 data, demonstrating stability even under noisy conditions. Racherla et al. [14] introduced Deep-IDS, which employs LSTM networks to achieve real-time intrusion detection with minimal false alarms, making it suitable for edge IoT nodes. Additionally, El-Shafeiy et al. [12] proposed DCGR_IoT, which combines convolutional and gated recurrent networks to improve anomaly detection accuracy across UNSW-NB15 and IoT-23 datasets. These deep learning approaches emphasize automatic feature learning and strong classification performance but require computational optimization for deployment in resource-limited IoT environments.

2. Machine Learning and Ensemble-Based Methodologies

Machine learning-based IDS frameworks are also widely used, especially where computational efficiency is needed. Shahid et al. [3] implemented an IDS for RPL IoT networks using models such as Random Forest and Transformers, where Random Forest achieved around 99% accuracy,

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

demonstrating strong detection with relatively low computational cost. Sama et al. [4] and Reddy & Gupta [23] conducted a comparative study of multiple ML models for IoT IDS and concluded that ensemble models such as Gradient Boosting, XGBoost, Random Forest, and Extremely Randomized Trees (ERT) consistently outperform traditional classifiers, with ERT achieving the highest accuracy of 99.7%. Thabit et al. [7] used the AWID dataset and implemented an ML-based framework where boosted decision trees produced superior results, suggesting that ensemble learning remains a highly competitive solution for IoT IDS when datasets are well-structured and feature-rich.

3. Hybrid Deep Learning Approaches (CNN–LSTM Models)

Hybrid methodologies combining convolutional neural networks (CNN) and long short-term memory (LSTM) networks are frequently adopted to simultaneously capture both spatial and sequential traffic patterns. Yaras and Dener [6] proposed a Spark-based hybrid CNN-LSTM model capable of analyzing large-scale IoT traffic efficiently and achieving high classification accuracy using CICIoT2023. Likewise, Alzahrani et al. [9] and Li et al.[22] designed a lightweight CNN-LSTM IDS specifically for fog computing environments, demonstrating low false alarm rates and suitability for deployment on energy-constrained devices such as Raspberry Pi. Gueriani et al. [15] and Kumar & Singh [18] also used a hybrid CNN-LSTM framework on CICIoT2023 data and achieved high accuracy with a low false positive rate. These hybrid methodologies offer improved detection performance for sequential IoT traffic patterns but may still require optimization to reduce computational and memory overhead.

4. Transfer Learning and Multimodal Feature Representation

Recent studies emphasize the use of transfer learning and multimodal feature representation to improve detection accuracy and robustness. Ullah et al. [8] proposed an IDS using multimodal big data representations, extracting semantic features through word2vec and ResNet, then applying transfer learning for classification across multiple datasets. This approach also used a game-theory-based validation mechanism to enhance model reliability. Adekunle et al. [10] proposed a feature-rich framework leveraging DenseNet and RAPNet and addressed dataset imbalance using conditional generative adversarial networks (cGANs). These methodologies demonstrate that transfer learning and advanced feature extraction improve detection precision, especially when datasets are highly diverse and imbalanced, though the complexity of such systems makes real-time deployment challenging.

5. Autoencoder and Anomaly Detection Methodologies

Some studies focus on unsupervised or semi-supervised approaches for anomaly detection. Alrayes et al. [11] and Patel et al.[21]proposed an IDS model based on Denoising Autoencoders (DAE), which effectively learned normal traffic representations and detected unauthorized intrusions. Zohourian et al. [5] introduced IoT-PRIDS, a host-based anomaly detection system that learns from benign traffic only, enabling detection of abnormal behavior with reduced false alarms. These approaches are valuable in environments where labeled attack data may not be available; however, the detection of sophisticated multi-stage attacks remains a challenge.

6. Survey-Based and Review Methodologies

Survey papers also contribute significantly by analyzing datasets, detection methodologies, and research directions. Abdulkareem et al. [2] reviewed IDS methods from 2018–2024, highlighting gaps such as outdated datasets and the need for improved classifiers. Isong et al. [16] reviewed modern IDS strategies and emphasized unresolved challenges such as scalability, resource limitations, and security improvements through cryptography and blockchain-based mechanisms. These survey methodologies provide a strong foundation for identifying unresolved gaps and shaping future IDS research.

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Conclusion and Future Scope

5.1 Conclusion : This systematic review analyzed recent IoT intrusion detection studies (2022–2024) and found a strong shift toward deep learning, hybrid CNN–LSTM, and ensemble machine learning models. Most approaches achieved high accuracy, with ensemble methods such as Extremely Randomized Trees reaching up to 99.7% and Random Forest achieving around 99%. However, the review highlights that many models are evaluated only in controlled environments using limited datasets, and practical deployment on resource-constrained IoT devices remains insufficiently addressed.

5.2 Future Scope : Future research should focus on developing lightweight and scalable IDS models suitable for real-time deployment on edge and fog-based IoT devices. Updated and standardized IoT-specific datasets are needed to improve generalization against evolving attack patterns, including zero-day threats. Incorporating explainable AI techniques will enhance trust and decision transparency for security analysts. Additionally, future IDS solutions should integrate adaptive learning, multi-dataset validation, and stronger security frameworks using blockchain or cryptographic techniques to ensure robustness in large-scale IoT ecosystems.

Reference

[1] Awajan, A. A Novel Deep Learning-Based Intrusion Detection System for IoT Networks. *Computers* 2023, *12*, 34. doi.org/10.3390/computers12020034

[2] Abdulkareem, S. A., Foh, C. H., Shojafar, M., Carrez, F., & Moessner, K. (2024). Network Intrusion Detection: An IoT and Non IoT-Related Survey. *IEEE Access*.

[3] Shahid, U., Hussain, M. Z., Hasan, M. Z., Haider, A., Ali, J., & Altaf, J. (2024). Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning. *IEEE Access*.

[4] Sama, N. U., Ullah, S., Kazmi, S. A., & Mazzara, M. (2024). Cutting-Edge Intrusion Detection in IoT Networks: A Focus on Ensemble Models. *IEEE Access*.

[5] Zohourian, A., Dadkhah, S., Molyneaux, H., Neto, E. C. P., & Ghorbani, A. A. (2024). IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks. *Computers & Security*, *146*, 104034.

[6] Yaras, S., & Dener, M. (2024). IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. *Electronics*, *13*(6), 1053.

[7] Thabit, F., Can, O., Abdaljlil, S., & Alkhzaimi, H. A. (2024). Enhanced an Intrusion Detection System for IoT networks through machine learning techniques: an examination utilizing the AWID dataset. *Cogent Engineering*, *11*(1), 2378603.

[8] Ullah, F., Turab, A., Ullah, S., Cacciagrano, D., & Zhao, Y. (2024). Enhanced network intrusion detection system for internet of things security using multimodal big data representation with transfer learning and game theory. *Sensors*, *24*(13), 4152.

[9] Alzahrani, H., Sheltami, T., Barnawi, A., Imam, M., & Yaser, A. (2024). A Lightweight Intrusion Detection System Using Convolutional Neural Network and Long Short-Term Memory in Fog Computing. *Computers, Materials & Continua*, *80*(3).

[10] Adekunle, T. S., Alabi, O. O., Lawrence, M. O., Adeleke, T. A., Afolabi, O. S., Ebong, G. N., ... & Bamisaye, T. A. (2024, March). An intrusion system for internet of things security breaches using machine learning techniques. In *Artificial Intelligence and Applications* (Vol. 2, No. 3, pp. 188-194).

[11] Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Helal, M. (2024). Intrusion Detection in IoT Systems Using Denoising Autoencoder. *IEEE Access*.

[12] El-Shafeiy, E., Elsayed, W. M., Elwahsh, H., Alsabaan, M., Ibrahem, M. I., & Elhady, G. F. (2024). Deep Complex Gated Recurrent Networks-Based IoT Network Intrusion Detection

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Systems. *Sensors*, *24*(18), 5933.

[13] Morshedi, R., Matinkhah, S. M., & Sadeghi, M. T. (2024). Intrusion Detection for IoT Network Security with Deep learning. *Journal of AI and Data Mining*, *12*(1), 37-55.

[14] Racherla, S., Sripathi, P., Faruqui, N., Kabir, M. A., Whaiduzzaman, M., & Shah, S. A. (2024). Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning. IEEE Access.

[15] Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)* (pp. 1-7).

[16] Isong, B., Kgote, O., & Abu-Mahfouz, A. (2024). Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems. *Electronics*, *13*(12), 2370.

[17] Zhang, Y., Liu, H., & Chen, X. (2023, May). Federated Learning-Based Intrusion Detection for IoT Security. In 2023 IEEE International Conference on Communications (ICC) (pp. 1–6).

[18] Patel, K., Mehta, R., & Shah, S. (2023, January). Anomaly Detection in IoT Networks Using Deep Autoencoders. In 2023 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 134–139).

[19] Li, Q., Wang, J., & Zhao, L. (2023, June). Lightweight Deep Learning-Based Intrusion Detection for Edge IoT Devices. In 2023 IEEE International Conference on Edge Computing (EDGE) (pp. 77–82). IEEE.

[20] Reddy, K., & Gupta, P. (2023, August). GAN-Based Intrusion Detection System for IoT Networks. In 2023 IEEE International Conference on Artificial Intelligence and Knowledge Engineering (AIKE) (pp. 99–104).

[21] Sharma, P., Verma, A., & Singh, D. (2022, March). Machine Learning-Based Intrusion Detection Systems for IoT Networks. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 45–50).

[22] Kumar, R., & Singh, M. (2022, July). Deep Learning Techniques for Intrusion Detection in IoT Environments. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 210–215).

[23] Ali, S., Khan, F., & Ahmad, J. (2022, October). Hybrid Machine Learning Models for IoT Network Security. In 2022 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 88–93).

[24] Shahbaz Ahmad Khanday, Hoor Fatima, Nitin Rakesh, Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks, Expert Systems with Applications, science direct Volume 215, 2023.

[25] M. He, Y. Huang, X. Wang, P. Wei and X. Wang, "A Lightweight and Efficient IoT Intrusion Detection Method Based on Feature Grouping," in *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2935-2949, 2023.