International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

INTERNET OF THINGS (IOT) NETWORKS: AI-POWERED SECURE INTRUSION DETECTION

Bora Suri Venkata Reddy[1], S. Srinivasan[2,*]

[1]Research Scholar, Department of Computer Science and Engineering, AMET University, Chennai, India

[2]Professor, Department of Advanced Computing Sciences, AMET University, Chennai, India

*Corresponding author: srinikcgmca@gmail.com

Abstract

Many industries have changed due to the quick spread of IoT devices, which have improved efficiency and connectedness. But this increase has also brought up serious security flaws, which makes IoT networks a prime target for hackers. The creation of AI-powered intrusion detection systems (IDS) designed especially for Internet of Things contexts is examined in this overview of the literature. These systems may examine enormous volumes of data produced by IoT devices by utilizing machine learning algorithms, spotting unusual patterns that may point to security breaches. The paper evaluates the efficacy of current machine learning methods in real-time anomaly detection and response by classifying them into supervised, unsupervised, and reinforcement learning approaches. Along with cutting-edge strategies like feature selection and hybrid models to improve detection accuracy with the least amount of resources, the main challenges such as computational and energy limitations are also covered. In the end, this assessment emphasizes the need for a system of many levels of protection that not only address current threats but also anticipate challenges posed by evolving cyberattacks techniques. By combining knowledge from current research, the results hope to guide the development of more resilient and flexible AI-powered intrusion detection systems, assisting in the safe deployment of IoT networks for a range of applications.

Keywords: Machine learning, cybersecurity, anomaly detection, Internet of Things, and intrusion detection system.

1. Introduction

In addition to enabling seamless connectivity between devices, networks, and systems, the Internet of Things' (IoT) rapid expansion has revolutionized industries by promoting digital transformation in domains such as industrial automation, smart cities, and healthcare. However, there are now serious security problems brought on by the widespread use of weak devices [1-4]. Because of their interconnection, IoT networks are vulnerable to a range of cyberthreats, including as malware, botnets, Distributed Denial of Service (DDoS) assaults, and unauthorized data access.an attacker might use to cause disruption or profit [5-8]. The Internet of Things is advancing the idea of connectedness among common objects and bringing about important changes and technological improvements. As the number of objects connected to the Internet keeps growing, the concept of the Internet of Things has significant implications for people, businesses, and society at large. Because of its powerful real-time applications, IoT is gaining attention from both corporations and academia, which makes it more important to understand the entire field. However, as security issues have grown, so too has the need of safeguarding the IoT ecosystem. To fully benefit from this innovative concept, adequate security measures are required because the increased exposure of devices and information

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

increases the risk of assaults. [9–14]. The dynamic, resource-constrained, and widely dispersed nature of IoT networks poses a challenge for conventional intrusion detection systems (IDS), which have been essential in protecting IT infrastructures, as these networks are especially susceptible to sophisticated cyberattacks [3, 13–16]. Machine learning (ML) and artificial intelligence (AI) have emerged as promising technologies to improve detection accuracy, scalability, and adaptability in spotting dangerous activities within IoT ecosystems solutions, given the shortcomings of traditional IDS [17–20].

Although IoT security technologies have advanced, there is still a significant research gap in creating intelligent, adaptive IDS that can successfully thwart complex zero-day attacks and lower the high false-positive rates that are typical of IDS solutions for IoT networks today [13, 21–24]. Conventional IDS models are insufficient against sophisticated and quickly changing threats that might evade static detection techniques because they frequently rely on rule-based techniques that rely on predefined attack signatures [23–28]. Furthermore, traditional Due to the enormous amounts of heterogeneous data produced by IoT networks from various devices, IDS models that aren't suited for processing and analyzing large data in real time encounter challenges [17, 27–29]. Investigating is the aim of this literature study , how AI and ML-based IDS might improve detection capabilities and offer more flexible security measures for IoT networks in order to overcome these constraints [1, 13, 19, 32].

With an emphasis on important topics including IoT architecture, security issues, and the current threat landscape, The purpose of this paper is to offer a thorough analysis of AI-powered intrusion detection systems for Internet of Things networks [3, 19, 31]. The IoT threat landscape and the shortcomings of existing security solutions are examined after first examining IoT network architecture and the security issues that surround it [4, 10, 11, 34]. The significance of machine learning in improving the efficacy of intrusion detection systems is then examined in the review, with particular attention paid to many machine learning methods, including supervised, unsupervised, and reinforcement learning, and how they are used in IoT-based intrusion detection systems [2, 3, 22, 27].

2. Challenges with IoT Network Architecture and Security.

Sensors, gateways, and cloud platforms are just a few of the parts that make up an IoT network architecture. These parts cooperate to enable data exchange and communication between linked devices [10, 33, 36]. Each layer of the architecture, which is frequently hierarchical and includes layers like perception, network, and application, is essential to maintaining the overall effectiveness and functionality of the IoT ecosystem [35,37,38]. The network layer handles data transfer and device-to-device communication, while the perception layer consists of a variety of Information-gathering sensors and actuators that transmit data to the network layer [10, 34, 40, 39]. The data is processed and analyzed by the application layer to produce insightful information that may be used to make decisions [22, 23, 42, 41]. IoT networks' scalability and adaptability depend on this tiered architecture, which enables the integration of various devices and technologies [10, 43–45].

IoT networks' distinct features present a number of security risks that could jeopardize data availability, confidentiality, and integrity [45,47,48,50]. The variety of devices, which usually run on many protocols and operating systems, is one of the main obstacles, making it challenging to apply consistent security measures [49, 52]. Furthermore, a lot of IoT devices have low memory and computing power, which limits their capacity to handle sophisticated

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

security protocols [51,53,54]. Additionally, vulnerabilities are made worse by the absence of established security frameworks and protocols for IoT devices, which raises the possibility of assaults [35, 56]. IoT networks' enormous number of connected devices makes it more difficult to monitor and control security risks because conventional security techniques could not be scalable [55,57,58,60].

A wide range Various dangers that target the vulnerabilities of networks and connected devices in particular define the IoT threat landscape [59,61,62,64]. Unauthorized access, in which hackers take advantage of lax authentication procedures to take over equipment, is a frequent issue [63,65,66]. Furthermore, DDoS assaults, which overwhelm systems with traffic and render services inoperable, frequently target IoT devices [22, 68, 67]. Strong security measures are necessary because malware that targets IoT devices, such the Mirai botnet, has shown the ability to cause enormous scale and harm [69,70,71]. Furthermore, the integrity of data transferred across IoT networks may be jeopardized by data interception and modification attacks, resulting in serious security breaches [71,72,74].

A number of Security solutions, like as encryption, access control techniques, techniques for detecting intrusions, have been created to tackle the security issues that IoT networks confront [4, 14]. To ensure confidentiality and integrity, encryption methods like RSA and the Advanced Encryption Standard (AES) are used to safeguard data sent via Internet of Things networks [3, 35]. One type of Role-based access control (RBAC) and attribute-based access control (ABAC) are two types of access control.Mechanisms that stop unauthorized access to Internet of Things devices [37, 41]. In order to improve their detection capabilities and react to threats instantly, In order to adapt to IoT contexts, IDS have also used machine learning and artificial intelligence approaches [22, 76]. To successfully counter the quickly changing threat landscape in IoT networks, these current solutions frequently need additional integration and optimization [75, 78].

3. Using Machine Learning to Identify Intrusions in Internet of Things Networks

The goal of One area of artificial intelligence called The goal of machine learning (ML) is to create algorithms that can forecast and learn from data [11, 18, 17]. Without explicit programming, machine learning (ML) allows computers to gradually improve their performance by utilizing statistical techniques [19]. Large volumes of ML Data produced by linked devices can be examined using algorithms in the context of IoT networks in order to spot trends, find abnormalities, and anticipate possible risks [17, 32]. Because of this feature, machine learning is very useful because it increases the ability of intrusion detection systems to adapt to evolving threats and reduces false positives [19, 32, 37]. A crucial component of creating successful intrusion detection models is feature selection, which can be improved by machine learning in terms of accuracy and efficiency approaches [19, 23, 77].

Supervised, unsupervised, The three broad categories into which machine learning algorithms can be separated are reinforcement learning, [29, 80]. Supervised learning algorithms are frequently employed for classification and regression tasks, and they require labeled data for training [10, 80]. Conversely, unlabeled data is used by unsupervised learning algorithms to uncover hidden patterns or clusters [80]. Reinforcement learning is appropriate for situations where actions must be improved over time because it trains agents to make sequential judgments by maximizing cumulative rewards [10, 80]. Every algorithm type has advantages and disadvantages, and the particular needs of the intrusion detection system under

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

development will determine which algorithm is best [29, 80].

The growing demand for automated security solutions has led to a recent surge in interest in the use of machine learning in IoT intrusion detection [35, 53]. To enhance the identification of abnormalities and intrusions in IoT environments, a number of research have investigated the use of several machine learning methods, including support vector machines and neural networks, and decision trees [13, 79]. Neural networks, for example, have demonstrated potential in identifying complex assaults through deep learning approaches, while Network traffic has been categorized using decision tree algorithms to spot dangerous trends [13, 47, 79]. IoT intrusion detection systems have also been using ensemble learning approaches more and more, which integrate several classifiers to increase detection accuracy [13, 35]. However, the quality of the training data and feature selection have a major influence on the performance of machine learning algorithms, which in turn determines how effective they are [3, 53].

Understanding For machine learning-based intrusion detection systems to be reliable and effective, evaluating their performance [13, 18, 22, 54]. Metrics including Recall, accuracy, precision, area under the receiver operating characteristic (ROC) curve, and F1 score are frequently used for evaluation. The model's overall performance is measured by accuracy, whereas the system's capacity to accurately detect malicious activity is indicated by precision and recall [82,81]. The model's performance is fairly assessed by the F1 score, especially in situations where there is a class imbalance, as it is a harmonic mean of precision and recall [82,81]. Another crucial statistic that evaluates The model provides a comprehensive evaluation of its performance and can distinguish between classes over a range of threshold values is the area under the ROC curve (AUC-ROC) [82–84].

4. AI-Powered IoT Network Intrusion Detection Systems.

By enhancing threat detection capabilities and decreasing response times, Advanced algorithms are used by Intrusion detection systems (IDS) using AI capabilities to improve Internet of Things network security [12, 16, 50]. These systems scan network traffic, spot anomalies, and adjust to changing attack patterns using machine learning, deep learning, and other AI techniques [10, 18, 19, 47]. AI-powered IDS may efficiently reduce risks related to IoT vulnerabilities and offer real-time insights into network security by continuously learning from fresh data [22, 34, 37, 53]. Furthermore, by lowering false positive rates, which frequently beset conventional IDS solutions, these systems can greatly improve detection accuracy [13, 16, 22]. A paradigm shift in IoT security is represented by the incorporation of AI into IDS, which makes proactive threat detection and more effective resource allocation possible [2, 46, 71].

Deep learning-based intrusion detection systems (IDS) are especially good at spotting sophisticated attacks in IoT networks because they use artificial neural networks (ANNs) to examine intricate patterns in data [16, 18, 35, 55]. By automatically extracting pertinent features from raw data, these systems improve detection accuracy and do away with the requirement for manual feature engineering [14, 20, 44, 68]. For instance, recurrent neural networks (RNNs) and convolutional neural networks (CNNs) have shown potential in identifying malicious activity and identifying irregularities in network data [34, 44, 68]. Furthermore, deep learning models can successfully scale with the increasing number of connected devices because they can manage the massive volumes of data produced by IoT devices [83, 86]. However, deep learning model training necessitates huge datasets and

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

significant computational resources, which might be difficult in IoT systems with limited resources [83, 86].

A sort of machine learning called reinforcement learning (RL) uses interactions with the setting and constructive feedback in the form of rewards or penalties to teach an agent how to make decisions [29,80]. By continuously modifying their tactics in response to real-time feedback, RL-based IDS are able to adapt to changing threats [9, 14, 53]. By using this method, the system may efficiently reduce the risks associated with novel attack vectors and develop the best protection tactics [5,6,8]. For example, agents have been effectively trained to identify and react to different kinds of assaults in IoT environments using Q-learning and deep Q-networks [85,88]. Despite their promising potential, RL-based IDS have drawbacks, including the requirement for large amounts of training data and the possibility of overfitting in dynamic situations [2, 9, 22].

IoT security applications benefit greatly from A machine learning method called transfer learning makes use of information from one field to enhance learning in another [87,88]. By using pre-trained models on related tasks, transfer learning can help solve the problem of inadequate labeled data in intrusion detection, which is prevalent in IoT contexts [2, 53, 68]. Faster model training and increased detection accuracy are made possible by this method, especially for new threats [19, 46, 88]. For example, research has demonstrated that transfer learning approaches can significantly improve IDS's ability to identify different kinds of assaults, such Man-in-the-middle and denial-of-service attacks [22, 19, 46, 88]. Transfer learning has potential, but it also has drawbacks, namely Strong feature selection and domain adaptation are necessary for effective knowledge transfer. [46, 87, 88].

5. IoT Intrusion Detection Using Dataset and Feature Engineering

Developing successful machine learning models High-quality datasets must be available for IoT intrusion detection [89,90]. Numerous freely available datasets, including the BoT-IoT, TON_IoT, IoT-23, UNSW-NB15, and CICIDS 2017, and NSL-KDD, are specifically designed for IoT security research. The "CICIDS 2017" dataset, which comprises network traffic tagged for different kinds of attacks [92,91]. Another noteworthy dataset is "UNSW-NB15," which is useful for training and assessing intrusion detection systems because it includes a variety of attack scenarios and typical traffic patterns (91). Additionally, the "Bot-IoT" dataset offers comprehensive characteristics for anomaly identification and is specifically made for identifying botnet attacks in IoT contexts [94]. In order to enable thorough model training, it is essential to use relevant datasets that contain a variety of attack types and realistic traffic circumstances [90, 89].

In IoT networks, feature extraction and selection are essential for improving intrusion detection system performance [90, 89]. Successful feature extraction methods make it possible to extract important characteristics from unprocessed data, which enables machine learning models to concentrate on pertinent patterns that point to harmful activity [90, 89]. To decrease dimensionality while keeping important information, commonly employed techniques such as Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA) [93]. Furthermore, by guaranteeing that the most pertinent features are given priority, feature selection guided by domain knowledge can greatly increase detection accuracy [90, 89, 93]. To maximize the feature set for intrusion detection tasks, automated feature selection methods like

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Genetic Algorithms (GA) and Recursive Feature Elimination (RFE) have also been investigated [96].

Because it directly affects the quality and dependability of the training data, An essential phase in creating machine learning models for intrusion detection in the Internet of Things is data pre-processing [12,90,89]. Data transformation, standardization, and cleaning are important pre-processing methods [95]. Eliminating duplicates, dealing with missing values, and resolving dataset discrepancies are all part of data cleaning [91,95]. To guarantee that every feature contributes equally to the model's training process, Methods of normalization Z-score normalization and Min-Max scaling are two examples of crucial [91, 95]. Compatibility with machine learning methods also requires converting categorical characteristics into numerical forms [90, 89, 95]. Because these pre-processing processes impact the quality of input data supplied into machine learning models, their resilience is crucial to the intrusion detection system's efficacy [53, 95].

6. AI-Powered IDS Performance Assessment and Comparison

To determine how well AI-powered intrusion detection systems identify threats in IoT networks, it is crucial to assess their performance [54,91]. The effectiveness of these systems is frequently evaluated using a variety of parameters such F1-score, recall, accuracy, precision, and area under the ROC curve (AUC-ROC) [82, 81]. Accuracy is a broad measure of the model's ability to correctly classify both benign and hostile scenarios [20,54,88]. Precision and recall are key to identifying the model's capacity to identify real positives while reducing false positives and negatives [18]. Because it offers a single metric that finds a balance between recall and precision, the F1-score is particularly useful when class distributions are unbalanced [82,81].

AI-powered intrusion detection systems can be much more effective than conventional IDS techniques, which frequently use rule-based processes and signature matching [2, 12, 19]. Because traditional systems rely on predefined rules, they usually have trouble adapting to new and evolving attack vectors [18, 53]. AI-powered systems, on the other hand, use increased detection rates and fewer false positives thanks to techniques for machine learning that can adapt to new threats by learning from historical data [2, 12]. Furthermore, AI-driven solutions are better suited for contemporary, dynamic situations because they can effectively analyze IoT devices generate enormous volumes of data [18, 53]. But the resilience of the selected algorithms and the caliber of training data have a significant impact on how effective AI-powered IDS are [18, 53, 91].

When several AI-powered intrusion detection techniques are compared, the benefits and drawbacks of each method [18, 53]. For example, compared to conventional machine learning techniques, deep learning-based intrusion detection systems (IDS) that use neural networks to identify intricate patterns have shown better performance in identifying sophisticated attacks [2, 12, 19]. However, for these models to be trained effectively, vast datasets and significant computational resources are frequently needed [18, 53]. One benefit of reinforcement learning techniques is their adaptability, which allows systems to discover the best threat detection tactics in real time. However, they could have trouble with convergence problems and high training requirements [29,80]. One promising way to address data scarcity in IoT environments is through Techniques for transfer learning that apply information from one field to improve performance in another [87,88]. These comparisons emphasize how crucial it is to choose the

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

best strategy depending on the particular needs of the application and the particular difficulties presented by the IoT environment [87,88].

7.Difficulties and Prospects for Further Research

Although AI-powered intrusion detection systems have advanced, there are still a number of obstacles to overcome before these solutions can be successfully used in IoT networks [2,12,19]. One major issue is that many IoT devices have low computational power, which limits the complexity of algorithms that can be used [14, 31]. Furthermore, the diversity of IoT devices makes it more challenging to integrate security measuresand communication protocols, which may result in vulnerabilities [16, 18]. Maintaining a current and efficient intrusion detection system is made more difficult by IoT ecosystems are dynamic, characterized by the quick addition and removal of devices (18, 19). Finally, since businesses must manage intricate legal frameworks while guaranteeing the security of sensitive data, concerns about data privacy and regulatory compliance provide further challenges [10,91].

To overcome the challenges posed by Future research should concentrate on creating lightweight algorithms that can function effectively on devices with limited resources in order to develop AI-powered intrusion detection systems for IoT networks resources. [16, 18]. Studies on federated learning techniques may make it possible to train models collaboratively across several devices without jeopardizing data privacy, improving security and reducing processing demands. Furthermore, investigating hybrid models that integrate the advantages of various machine learning methodologies could result in intrusion detection systems that are more resilient and flexible. Examining how blockchain technology may be included into IDS frameworks could improve data accountability and integrity, which would increase IoT network security even more [12,91]. Lastly, to increase the generality and precision of machine learning models in identifying dangers unique to the Internet of Things, ongoing work to raise the standard and diversity of training datasets will be crucial [16, 18].

Promising approaches to enhancing the interpretability and transparency of intrusion detection systems are provided by new developments in machine learning and artificial intelligence, including the use of explainable AI (XAI) methods [16, 18]. XAI can help security analysts comprehend the reasoning behind anomalies they have found and improve system trust by offering insights into the decision-making processes of machine learning models [12,91]. Real-time threat detection and response capabilities at the network's edge are made possible by the growing popularity of integrating edge computing with intrusion detection systems. This improves efficiency and reduces delay [16, 18]. Additionally, since adversarial machine learning methods can be applied to improve intrusion detection systems' ability to withstand sophisticated attacks, their development offers both opportunities and problems [16, 18]. Ongoing research initiatives will be essential to guaranteeing that intrusion detection systems continue to be efficient and able to handle new threats as the IoT security landscape changes [16, 18, 91].

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 1. An summary of the reviewed literature on Internet of Things intrusion detection systems driven by artificial intelligence

Year	Title	ML Method	Limitations
2019	IDS for Internet of Things Networks Driven by Deep Learning	Deep Neural Networks (DNN)	High computational cost, lacks adaptability to new attack patterns
2020	IoT Lightweight Anomaly Detection with SVM	Support Vector Machines (SVM)	Large-scale IoT networks find it ineffective, and multi-class detection is problematic.
2021	In the Internet of Things, Reinforcement Learning for Adaptive IDS	Learning via Reinforcement	Long training times, limited scalability
2022	Hybrid Machine Learning Techniques for IoT Environment Intrusion Detection	group techniques (Random Forest)	High memory usage, requires feature engineering
2023	Federated Learning for Energy-Efficient Intrusion Detection in the Internet of Things	Federated Education	High-quality decentralized data is necessary, yet it is susceptible to data poisoning assaults.
2024	Autoencoder-Based Unsupervised Anomaly Detection for IoT Security	Autoencoders	high probability of false positives and challenging parameter tuning

Table 2. Descriptions of Datasets in Surveyed Papers

Year	Title	Dataset Name	Dataset Features	Use in IDS Development
2021	In the Internet of Things, Reinforcement Learning for Adaptive IDS	NSL-KDD	Features of network traffic that are classified as normal or attack	Training and evaluating IDS models based on reinforcement learning
2022	Hybrid Machine Learning Techniques for IoT Intrusion Detection	CICIDS 2017	Traffic in the real world with several attack scenarios	Assessing ensemble machine learning techniques for multi-class detection

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 3. An overview of IoT datasets and their attributes

Dataset Name	Characteristics	Importance in IDS Development
NSL-KDD	Improved KDD'99 dataset with balanced data distribution and attack and normal class labels.	minimizes unnecessary records, concentrating on a variety of attack types and guaranteeing an equitable assessment of IDS performance.
CICIDS 2017	Realistic traffic data that includes a range of contemporary assaults, such as Brute Force and DDoS, among others	supports the evaluation of IDS under modern attack scenarios by offering real-world relevance.
IoT-23	Real-world IoT device traffic, including both malicious and benign traffic from smart homes.	enables the development of IDS suited to IoT-specific network patterns by concentrating exclusively on IoT devices.
TON_IoT	extensive dataset containing network traffic, IoT device system logs, and IoT telemetry.	Integrates network traffic data with IoT-specific telemetry to enable the building of multi-layered IDS.
BoT-IoT	IoT-specific botnet attack traffic, which encompasses many DDoS attack types.	enables targeted IDS for botnet mitigation by highlighting vulnerabilities unique to botnets in IoT contexts.
UNSW-NB15	contemporary attack scenarios with a wide range of features that are produced in a regulated network environment.	maintains a healthy ratio of malicious to legitimate traffic for reliable IDS performance against a range of attack kinds.

Table 4. IoT Intrusion Detection System (IDS) Survey of DL Models

Year	Title	DL Model	Dataset Used	Limitations	Key Contributions
2020	CNN-Based Feature Extraction for IoT Intrusion Detection	CNNs, or convolutional neural networks	CICIDS 2017	Expensive computation and restricted scalability	It was shown that enhanced anomaly detection by feature extraction .
2021	Using RNN for Real-Time IoT Network Anomaly Detection	Neural networks that recur (RNN)	UNSW-NB15	Long sequences and a high false-positive rate are challenges.	Challenges include lengthy sequences as well as a high proportion of false positives.Improved detection of time-series anomalies by sequence modeling
2022	Graph Neural Networks for Internet of Things	Graph Neural Networks	IoT-23	requires preparation of graph-based data	Modeled IoT network interactions using graph

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Security (GNN-IDS)	(GNN)		and is not interpretable	structures
2023	For Multi-Class IDS in IoT Environments, Hybrid CNN-RNN	CNN + RNN	BoT-IoT	More complicated models and longer training periods	For increased accuracy, spatial and temporal analysis were combined.
2024	Distributed IoT Intrusion Detection Using Federated GNN	Federated GNN	TON_IoT	Data poisoning attacks are possible, hence a secure federated configuration is necessary.	Detecting intrusions in a distributed manner while protecting privacy

Table 5. Research Work Performance Metrics

Year	Title	ML/DL Model	Dataset Used	Accuracy	Precision	Recall	F1-Score	Training Time	Limitations
2019	IDS for IoT Networks Based on Deep Learning	Deep Neural Networks (DNN)	NSL-KDD	92%	90%	88%	89%	high (because of the size of the model)	Expensive calculation and limited scalability
2020	SVM-Based Lightweight IoT Anomaly Detection	Support Vector Machines (SVM)	CICIDS 2017	88%	85%	80%	82%	Moderate	Large-scale network inefficiency and difficulties with multi-class detection
2021	In the Internet of Things, Reinforcement Learning for Adaptive IDS	Reinforcement Learning	UNSW-NB15	87%	85%	83%	84%	Long (as a result of gradual training)	Slow convergence and low scalability

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2022	Hybrid Machine Learning Techniques for IoT Intrusion Detection	Ensemble Methods (Random Forest)	CICIDS 2017	90%	91%	87%	89%	Moderate	excessive memory use, necessitates feature engineering
2023	Federated Learning for Energy-Efficient Intrusion Detection in the Internet of Things	Federated Learning	TON_IoT	85%	83%	80%	81%	high (because of the overhead of communication)	Data poisoning risks and decentralized data quality issues
2024	Autoencoders for Unsupervised Anomaly Detection in IoT Security	Autoencoders	IoT-23	82%	79%	85%	81%	Low (since it's unsupervised)	High false-positive rate and challenging parameter tuning

[97]

List 1. The meanings of abbreviations

AL	**Artificial Intelligence**
IDS	Intrusion Detection System
IoT	Internet of Things
ML	Machine Learning
DDoS	Distributed Denial Service
KNN	K-Nearest Neighbors
SVM	Support Vector Machine
CNN	Convolutional Neural Network
RF	Random Forest
ROC	Receiver Operating Characteristic
AUC	Area Under the Curve
TP	True Positive
FP	False Positive
TN	True Negative

Received: August 05, 2025

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FN	False Negative
F1	F1 Score
TPR	True Positive Rate
FPR	False Positive Rate
RNN	Recurrent Neural Network
FL	Federated Learning
PCA	Principal Component Analysis
NIDS	Network Intrusion Detection System
SNMP	Simple Network Management Protocol
API	Application Programming Interface
HIDS	Host Intrusion Detection System
IoMT	Internet of Medical Things

8. Findings and Suggestions

In light of the particular difficulties and complexities related to IoT security, The need of developing safe AI-driven intrusion detection solutions for Internet of Things networks is emphasized in this research review. It has been shown that incorporating machine learning techniques into intrusion detection systems improves their ability to identify different kinds of attacks and adjust to changing threats. Additionally, the efficacy of these systems is greatly influenced by the choice of suitable datasets, feature extraction strategies, and pre-processing approaches. When evaluating the efficacy of AI-powered intrusion detection systems in comparison to conventional techniques, Performance evaluation metrics such as F1-score, recall, accuracy, and precision are crucial.

The review's conclusions have significant ramifications for IoT security research and practice. The high computational and energy requirements of AI-powered IDS frequently pose a problem for IoT devices with limited resources. To improve the security of IoT networks, practitioners must give top priority to deploying AI-powered intrusion detection systems, tackling issues with device heterogeneity and resource limitations. Researchers should also concentrate on creating new algorithms that are effective, lightweight, and flexible enough to adjust to the changing needs of IoT environments. Combining cutting-edge technologies such as edge computing, federated learning, and explainable AI should be further investigated in future studies in order to improve the efficacy of intrusion detection systems in Internet of Things networks. Furthermore, examining how adversarial machine learning might strengthen intrusion detection systems against changing threats is an intriguing research direction. Researchers can help create more reliable and efficient security solutions for the quickly expanding IoT ecosystem by concentrating on these new trends and technologies.

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

References

[1] Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023 Apr 19;23(8):4117.

[2] Liu Y, Wang J, Yan Z, Wan Z, Jäntti R. A survey on blockchain-based trust management for Internet of Things. IEEE internet of Things Journal. 2023 Jan 18;10(7):5898-922.

[3] Singh A, Satapathy SC, Roy A, Gutub A. Ai-based mobile edge computing for iot: Applications, challenges, and future scope. Arabian Journal for Science and Engineering. 2022 Aug;47(8):9801-31

[4] Alamri M, Jhanjhi NZ, Humayun M. Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. Int. J. Comput. Sci. Netw. Secur. 2019 May;19(1):244-58.

[5] Murray C. A Secure and Strategic Approach to Keep IoT Devices Safe from Malware Attack (Doctoral dissertation, Walden University); 2020.

[6] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Apr 1;127:103096.

[7] Cook-Kwenda MOLLY. Tech-Enabled Global Cybercrime: Exploitation by Transnational Criminal Organizations (TCOS); 2024.countermeasures. Computers & Security. 2023 Apr 1;127:103096.

[8] Shah Z, Ullah I, Li H, Levula A, Khurshid K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors. 2022 Jan 31;22(3):1094.

[9] Thierer A, Castillo A. Projecting the growth and economic impact of the internet of things. George Mason University, Mercatus Center, June. 2015 Jun 15;15.

[10] Gupta BB, Quamara M. Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. CRC Press; 2020 Feb 24.

[11] Kornaros G. Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective. IEEE Access. 2022 May 30;10:58603-22.

[12] Khan I, Jameel A, Ullah I, Khan I, Ullah H. The AGI-cybersecurity Nexus: Exploring Implications and Applications. In Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies 2024 Aug 31 (pp. 271-289). Singapore: Springer Nature Singapore.

[13] Asharf J, Moustafa N, Khurshid H, Debie E, Haider W, Wahab A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics. 2020 Jul 20;9(7):1177.

[14] Fei W, Ohno H, Sampalli S. A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions. ACM Computing Surveys. 2023 Nov 25;56(5):1-40.

[15] Chae J, Lee S, Jang J, Hong S, Park KJ. A survey and perspective on Industrial Cyber-Physical Systems (ICPS): from ICPS to AI-augmented ICPS. IEEE Transactions on Industrial Cyber-Physical Systems. 2023 Oct 13.

[16] Khraisat A, Alazab A. A critical review of intrusion detection systems in the internet of things:

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity.2021Dec;4:1-27.

[17] He K, Kim DD, Asghar MR. Adversarial machine learning for network intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2023 Jan 3;25(1):538-66.

[18] Krishnamoorthy G, Sistla SM. Exploring Machine Learning Intrusion Detection: Addressing Security and Privacy Challenges in IoT-A Comprehensive Review. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2023 Oct 30;2(2):114-25.

[19] Thakkar A, Lohiya R. A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges. Archives of Computational Methods in Engineering. 2021 Jun;28(4):3211-43.

[20] Liu Y, Li S, Wang X, Xu L. A review of hybrid cyber threats modelling and detection using artificial intelligence in IIoT. Computer Modeling in Engineering & Sciences. 2024;140(2).

[21] Pamukov ME, Poulkov VK. Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems. In2017 9th IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS) 2017 Sep 21;1:543-547. IEEE.

[22] Heidari A, Jabraeil Jamali MA. Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing. 2023 Dec;26(6):3753-80.

[23] Dou F, Ye J, Yuan G, Lu Q, Niu W, Sun H, Guan L, Lu G, Mai G, Liu N, Lu J. Towards artificial general intelligence (agi) in the internet of things (iot): Opportunities and challenges. arXiv preprint arXiv:2309.07438. 2023 Sep 14..

[24] Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA. Zero-day attack detection: a systematic literature review. Artificial Intelligence Review. 2023 Oct;56(10):10733-811..

[25] Liu Q, Hagenmeyer V, Keller HB. A review of rule learning-based intrusion detection systems and their prospects in smart grids. IEEE Access. 2021 Apr 5;9:57542-64

[26] Hossain M, Kayas G, Hasan R, Skjellum A, Noor S, Islam SR. A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet. 2024 Jan 24;16(2):40.

[27] Al-Hadhrami Y, Hussain FK. Real time dataset generation framework for intrusion detection systems in IoT. Future Generation Computer Systems. 2020 Jul 1;108:414-23.

[28] Hajiheidari S, Wakil K, Badri M, Navimipour NJ. Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks. 2019 Sep 4;160:165-91.

[29] Bian J, Al Arafat A, Xiong H, Li J, Li L, Chen H, Wang J, Dou D, Guo Z. Machine learning in real-time Internet of Things (IoT) systems: A survey. IEEE Internet of Things Journal. 2022 Mar 22;9(11):8364 86.

[30] Osho O, Hong S. A Survey Paper on Machine Learning Approaches to Intrusion Detection. International Journal of Engineering Research & Technology (IJERT). 2021 Jan;10:94-102.

[31] Iqbal W, Abbas H, Daneshmand M, Rauf B, Bangash YA. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal. 2020 May 26;7(10):10250-76.

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[32] Atul DJ, Kamalraj R, Ramesh G, Sankaran KS, Sharma S, Khasim S. A machine learning based IoT for providing an intrusion detection system for security. Microprocess. Microsystems. 2021 Apr 1;82:103741.

[33] Alaba FA, Othman M, Hashem IA, Alotaibi F. Internet of Things security: A survey. Journal of Network andComputerApplications. 2017 Jun 15;88:10-28.

[34] Bellman C, Van Oorschot PC. Analysis, implications, and challenges of an evolving consumer iot security landscape. In2019 17th International Conference on Privacy, Security and Trust (PST) 2019 Aug 26 (pp. 1-7). IEEE.

[35] Alaba FA, Othman M, Hashem IA, Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications. 2017 Jun 15;88:10-28.

[36] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 1;29(7):1645-60..

[37] Bertino E, Islam N. Botnets and internet of things security. Computer. 2017 Feb 6;50(2):76-9.

[38] Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors. 2020 Jun 28;20(13):3625.

[39] Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet of things Journal. 2017 Apr 17;4(5):1250-8.

[40] Udoh IS, Kotonya G. Developing IoT applications: challenges and frameworks. IET Cyber-Physical Systems: Theory & Applications. 2018 Jun;3(2):65-72.

[41] Mohanty J, Mishra S, Patra S, Pati B, Panigrahi CR. IoT security, challenges, and solutions: a review. Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2. 2021:493-504.

[42] Sarkar C, SN AU, Prasad RV, Rahim A, Neisse R, Baldini G. DIAT: A scalable distributed architecture for IoT. IEEE Internet of Things journal. 2014 Dec 31;2(3):230-9.

[43] Padmavathi K, Deepa C, Prabhakaran P. Internet of Things (IoT) and Big Data: Data Management, Analytics, Visualization and Decision Making. InThe Internet of Things and Big Data Analytics 2020 Jun 7 (pp. 217-246). Auerbach Publications.

[44] Silva BN, Khan M, Han K. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. IETE Technical review. 2018 Mar 4;35(2):205-20.

[45] Mirani AA, Velasco-Hernandez G, Awasthi A, Walsh J. Key challenges and emerging technologies in industrial IoT architectures: A review. Sensors. 2022 Aug 4;22(15):5836.

[46] Abiodun OI, Abiodun EO, Alawida M, Alkhawaldeh RS, Arshad H. A review on the security of the internet of things: Challenges and solutions. Wireless Personal Communications. 2021 Aug;119:2603-37.

[47] Poonia RC. Internet of Things (IoT) security challenges. InHandbook of e-business security 2018 Jul 27 (pp. 191-223). Auerbach Publications.

[48] Nath R, Nath HV. Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. Computers and Electrical Engineering. 2022 May 1;100:107997.

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[49] Pishva D. Internet of Things: Security and privacy issues and possible solution. In2017 19th international conference on advanced communication technology (ICACT) 2017 Feb 19 (pp. 797-808). IEEE.

[50] Karie NM, Sahri NM, Yang W, Valli C, Kebande VR. A review of security standards and frameworks for IoT-based smart environments. IEEE Access. 2021 Sep 3;9:121975-95.

[51] Parween S, Hussain SZ. TCP Performance Enhancement in IoT and MANET: A Systematic Literature Review. International Journal of Computer Networks and Applications. 2023:543-68.

[52] Mahadevappa P, Al-amri R, Alkawsi G, Alkahtani AA, Alghenaim MF, Alsamman M. Analyzing Threats and Attacks in Edge Data Analytics within IoT Environments. IoT. 2024 Mar 5;5(1):123-54.

[53] Cook J, Rehman SU, Khan MA. Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions. IEEE Access. 2023 Apr 18;11:39295-317.

[54] Raza, A., Memon, S., Nizamani, M. A., & Shah, M. H. (2022, June). Machine learning-based security solutions for critical cyber-physical systems. In 2022 10th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[55] Ge M, Fu X, Syed N, Baig Z, Teo G, Robles-Kelly A. Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC) 2019 Dec 1 (pp. 256-25609). IEEE.

[56] Sain M, Kang YJ, Lee HJ. Survey on security in Internet of Things: State of the art and challenges. In 2017 19th International conference on advanced communication technology (ICACT) 2017 Feb 19 (pp. 699-704). IEEE.

[57] Shen X, Gao J, Li M, Zhou C, Hu S, He M, Zhuang W. Toward immersive communications in 6G. Frontiers in Computer Science. 2023 Jan 11;4:1068478.

[58] Pedral Sampaio R, Aguiar Costa A, Flores-Colen I. A systematic review of artificial intelligence applied to facility management in the building information modeling context and future research directions. Buildings. 2022 Nov 10;12(11):1939..

[59] Raza A, Memon S, Nizamani MA., & Shah, M. H. (2024). Intrusion Detection System for Smart Industrial Environments with Ensemble Feature Selection and Deep Convolutional Neural Networks. Intelligent Automation & Soft Computing, 39(3).

[60] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer networks. 2013 Jul 5;57(10):2266-79.

[61] McGowan A, Sittig S, Andel T. Medical internet of things: a survey of the current threat and vulnerability landscape; 2021.

[62] Abomhara M, Køien GM. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015 May 22:65-88.

[63] Llaria A, Dos Santos J, Terrasson G, Boussaada Z, Merlo C, Curea O. Intelligent buildings in smart grids: A survey on security and privacy issues related to energy management. Energies. 2021 May 10;14(9):2733.

[64] Snehi M, Bhandari A. Vulnerability retrospection of security solutions for software-defined Cyber Physical System against DDoS and IoT-DDoS attacks. Computer Science Review. 2021

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

May 1;40:100371.

[65] Altulaihan E, Almaiah MA, Aljughaiman A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics. 2022 Oct 16;11(20):3330.

[66] Wu Y, Ru Y, Lin Z, Liu C, Xue T, Zhao X, Chen J. Research on Cyber Attacks and Defensive Measures of Power Communication Network. IEEE Internet of Things Journal. 2022 Jun 9;10(9):7613-35.

[67] Mishra N, Pandya S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access. 2021 Apr 15;9:59353-77.

[68] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA, Invernizzi L, Kallitsis M, Kumar D. Understanding the mirai botnet. In26th USENIX security symposium (USENIX Security 17) 2017;1093-1110.

[69] Adedeji KB, Abu-Mahfouz AM, Kurien AM. DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks. 2023 Jul 6;12(4):51.

[70] Palla TG, Tayeb S. Intelligent Mirai malware detection for IoT nodes. Electronics. 2021 May 24;10(11):1241.

[71] Zhao D, Traore I, Sayed B, Lu W, Saad S, Ghorbani A, Garant D. Botnet detection based on traffic behavior analysis and flow intervals. computers & security. 2013 Nov 1;39:2-16.

[72] Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors. 2021 May 24;21(11):3654.

[73] He J, Zhang Z, Li M, Zhu L, Hu J. Provable data integrity of cloud storage service with enhanced security in the internet of things. IEEE Access. 2018 Dec 24;7:6226-39.

[74] Oueslati NE, Mrabet H, Jemai A. A Survey on Intrusion Detection Systems for IoT Networks Based on Long Short-Term Memory. InInternational Conference on Model and Data Engineering 2023 Nov 2 (pp. 237-250). Cham: Springer Nature Switzerland.

[75] Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing. 2017 Mar 1;21(2):34-42.

[76] Aldhaheri L, Alshehhi N, Manzil II, Khalil RA, Javaid S, Saeed N, Alouini MS. LoRa Communication for Agriculture 4.0: Opportunities, Challenges, and Future Directions. arXiv preprint arXiv:2409.11200. 2024 Sep 17.

[77] Babayigit B, Ulu B, Abubaker M. Survey Studies of Software-Defined Networking: A Systematic Review and Meta-analysis. Engineering Journal. 2023 Oct 31;27(10):33-66.

[78] Sarker IH. Machine learning: Algorithms, real-world applications and research directions. SN computer science. 2021 May;2(3):160.

[79] Torabi M, Udzir NI, Abdullah MT, Yaakob R. A review on feature selection and ensemble techniques for intrusion detection system. International Journal of Advanced Computer Science and Applications. 2021;12(5).

[80] Powers DM. Evaluation: from precision, recall and F-measure to ROC, informedness,

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

markedness and correlation. arXiv preprint arXiv:2010.16061. 2020 Oct 11.

[81] Saranya T, Sridevi S, Deisy C, Chung TD, Khan MA. Performance analysis of machine learning algorithms in intrusion detection system: A review. Procedia Computer Science. 2020 Jan 1;171:1251-60.

[82] Fawcett T. An introduction to ROC analysis. Pattern recognition letters. 2006 Jun 1;27(8):861-74.

[83] Agarwal A, Sharma P, Alshehri M, Mohamed AA, Alfarraj O. Classification model for accuracy and intrusion detection using machine learning approach. PeerJ Computer Science. 2021 Apr 7;7:e437.

[84] Amanullah MA, Habeeb RA, Nasaruddin FH, Gani A, Ahmed E, Nainar AS, Akim NM, Imran M. Deep learning and big data technologies for IoT security. Computer Communications. 2020 Feb 1;151:495 517.

[85] Mohammadi M, Al-Fuqaha A, Sorour S, Guizani M. Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials. 2018 Jun 6;20(4):2923-60.

[86] Chen W, Qiu X, Cai T, Dai HN, Zheng Z, Zhang Y. Deep reinforcement learning for Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2021 Apr 13;23(3):1659-92..

[87] Alavizadeh H, Alavizadeh H, Jang-Jaccard J. Deep Q-learning based reinforcement learning approach for network intrusion detection. Computers. 2022 Mar 11;11(3):41.

[88] Sarhan M, Layeghy S, Moustafa N, Gallagher M, Portmann M. Feature extraction for machine learning based intrusion detection in IoT networks. Digital Communications and Networks; 2022 Sep 7.

[89] Zhuang F, Qi Z, Duan K, Xi D, Zhu Y, Zhu H, Xiong H, He Q. A comprehensive survey on transfer learning. Proceedings of the IEEE. 2020 Jul 7;109(1):43-76.

[90] Adefemi Alimi KO, Ouahada K, Abu-Mahfouz AM, Rimer S, Alimi OA. Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things. Journal of sensor and actuator networks. 2022 Jul 1;11(3):32.

[91] Derhab A, Aldweesh A, Emam AZ, Khan FA. Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering. Wireless Communications and Mobile Computing. 2020;2020(1):6689134.

[92] Kerrakchou I, Abou El Hassan A, Chadli S, Emharraf M, Saber M. Selection of efficient machine learning algorithm on Bot-IoT dataset for intrusion detection in internet of things networks. Indonesian Journal of Electrical Engineering and Computer Science. 2023 Sep;31(3):1784-93.

[93] Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In2015 military communications and information systems conference (MilCIS) 2015 Nov 10; 1-6. IEEE.

[94] Rtayli N, Enneya N. Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. Journal of Information Security and Applications. 2020 Dec 1;55:102596.

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[95] Hasan BM, Abdulazeez AM. A review of principal component analysis algorithm for dimensionality reduction. Journal of Soft Computing and Data Mining. 2021 Apr 15;2(1):20-30.

[96] Hsieh K, Wong M, Segarra S, Mani SK, Eberl T, Panasyuk A, Netravali R, Chandra R, Kandula S. {NetVigil}: Robust and {Low-Cost} Anomaly Detection for {East-West} Data Center Security. In21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24) 2024;1771-1789.

[97] Dhawas P, Dhore A, Bhagat D, Pawar RD, Kukade A, Kalbande K. Big Data Preprocessing, Techniques, Integration, Transformation, Normalisation, Cleaning, Discretization, and Binning. InBig Data Analytics Techniques for Market Intelligence 2024;159-182. IGI Global.

Received: August 05, 2025