AI-DRIVEN SECURE INTRUSION DETECTION FOR INTERNET OF THINGS (IOT) NETWORKS

Abstract

The rapid proliferation of Internet of Things (IoT) devices has transformed various sectors, enhancing connectivity and efficiency. However, this surge has also introduced significant security vulnerabilities, making IoT networks attractive targets for cyber threats. This literature review investigates the development of AI-powered intrusion detection systems (IDS) tailored specifically for IoT environments. By leveraging machine learning algorithms, these systems can analyze vast amounts of data generated by IoT devices, identifying anomalous patterns indicative of potential security breaches. The review categorizes existing machine learning techniques, including supervised, unsupervised, and reinforcement learning approaches, assessing their effectiveness in real-time anomaly detection and response. Furthermore, the Key challenges, including computational and energy constraints, are discussed, alongside advanced approaches like feature selection and hybrid models to enhance detection accuracy with minimal resources. Ultimately, this review highlights the necessity for a multi-layered security framework that not only addresses current threats but also anticipates future challenges posed by evolving cyberattack methodologies. By synthesizing insights from recent studies, the findings aim to inform the design of more robust and adaptive AI-powered IDS, contributing to the secure implementation of IoT networks across diverse applications.

Keywords: Internet of Things, Intrusion detection system, machine learning, cybersecurity, anomaly detection

Introduction

The rapid expansion of the Internet of Things (IoT) has revolutionized industries by enabling seamless connectivity among devices, networks, and systems, fostering digital transformation in sectors like healthcare, smart cities, and industrial automation, while also introducing significant security concerns due to the proliferation of vulnerable devices (1-4). This interconnectedness exposes IoT networks to a broad range of cyber threats, including malware, botnets, Distributed Denial of Service (DDoS) attacks, and unauthorized data access, which attackers can exploit for financial or disruptive purposes (5-8). The concept of interconnectivity among commonplace objects is being built by the IoT, which is bringing forth huge developments and technological advancements. The idea of the IoT has enormous ramifications for individuals, businesses, and society as a whole because to the rapidly increasing number of objects connected to the Internet. IoT is attracting interest from academics and businesses because of its potent real-time applications, which increase the need to comprehend the whole range of the area. Nonetheless, protecting the IoT ecosystem has grown in importance as a result of growing security concerns. Adequate security measures are necessary to fully utilize the advantages of this novel idea since devices and information are becoming more exposed, which raises the possibility of attacks. (9-13). Traditional intrusion detection systems (IDS) have been pivotal in securing IT infrastructures, but they struggle to cope with the dynamic, resource-constrained, and highly distributed nature of IoT networks, which are particularly vulnerable to advanced cyberattacks (4, 14-16). Given the limitations of

conventional IDS, AI and machine learning (ML) have emerged as promising technologies to enhance detection accuracy, scalability, and adaptability in identifying malicious activities within IoT ecosystems (17-20).

Despite advancements in IoT security technologies, a critical research gap remains in developing adaptive, intelligent IDS capable of effectively countering sophisticated zero-day attacks and reducing high false-positive rates, common in current IDS solutions for IoT networks (14, 21-23). Traditional IDS models often rely on rule-based methods, which depend on predefined attack signatures, making them inadequate against rapidly evolving and sophisticated threats that can bypass static detection methods (24-27). Additionally, IoT networks generate vast amounts of heterogeneous data from various devices, posing challenges for conventional IDS models that are not optimized for real-time big data processing and analysis (18, 28-30). This literature review aims to explore how AI and ML-based IDS can address these limitations by enhancing detection capabilities and providing more adaptive security measures for IoT networks (2, 14, 20, 31).

This review is structured to provide a comprehensive examination of AI-powered IDS for IoT networks, focusing on key areas such as IoT architecture, security challenges, and the current threat landscape (4, 20, 32). It begins by exploring IoT network architecture and its associated security challenges, followed by an analysis of the IoT threat landscape and the limitations of current security solutions (3, 9, 12, 33). The review then explores the role of machine learning in enhancing the effectiveness of IDS, focusing on various machine learning algorithms, such as supervised, unsupervised, and reinforcement learning, and their application in IoT-based intrusion detection systems (1, 4, 21, 28).

IoT Network Architecture and Security Challenges

IoT network architecture comprises various components, including sensors, gateways, and cloud platforms, which work collaboratively to facilitate communication and data exchange among connected devices (9, 34, 35). The architecture is often hierarchical, consisting of layers such as perception, network, and application, where each layer plays a vital role in ensuring the overall functionality and efficiency of the IoT ecosystem (36-38). The perception layer includes various sensors and actuators that collect and transmit data to the network layer, while the network layer is responsible for data transmission and communication between devices (9, 33, 39, 40). The application layer processes and analyzes the data to derive meaningful insights, which can be utilized for decision-making (21, 24, 41, 42). This layered architecture is essential for the scalability and flexibility of IoT networks, allowing for the integration of diverse devices and technologies (10, 43-45).

The unique characteristics of IoT networks pose several security challenges that can compromise data integrity, confidentiality, and availability (46-49). One of the primary challenges is the heterogeneity of devices, which often run on different operating systems and protocols, making it difficult to implement uniform security measures (50, 51). Additionally, many IoT devices have limited processing power and memory, restricting their ability to support complex security protocols (52-54). Furthermore, the lack of standardized security frameworks and protocols for IoT devices exacerbates vulnerabilities, leading to increased risks of cyberattacks (36, 55). The vast number of connected devices in IoT networks also complicates monitoring and managing security threats, as traditional security measures may not scale adequately (56-59).

The IoT threat landscape is characterized by a diverse array of threats that specifically target the vulnerabilities of connected devices and networks (60-63). Common threats include unauthorized access, where attackers exploit weak authentication mechanisms to gain control over devices (64-66). Additionally, IoT devices are often susceptible to DDoS attacks, which can incapacitate services by overwhelming systems with traffic (21, 67, 68). Malware targeting IoT devices, such as the Mirai botnet, has demonstrated the potential for massive scale and damage, emphasizing the need for robust security measures (69-71). Moreover, data interception and manipulation attacks can compromise the integrity of the data transmitted across IoT networks, leading to significant security breaches (72-74).

Various security solutions have been developed to address the security challenges faced by IoT networks, including encryption, access control mechanisms, and intrusion detection systems (3, 13). Encryption techniques, such as Advanced Encryption Standard (AES) and RSA, are employed to protect data transmitted over IoT networks, ensuring confidentiality and integrity (4, 36). Access control mechanisms, including role-based access control (RBAC) and attribute-based access control (ABAC), are implemented to restrict unauthorized access to IoT devices (38, 42). IDS have also been adapted for IoT environments, utilizing machine learning and AI techniques to enhance their detection capabilities and respond to threats in real time (21, 75). However, these existing solutions often require further optimization and integration to effectively combat the rapidly evolving threat landscape in IoT networks (76, 77).

Machine Learning for Intrusion Detection in IoT Networks

Machine learning (ML) is a subset of artificial intelligence that focuses on developing algorithms that can learn from and make predictions based on data (12, 17, 18). By leveraging statistical techniques, ML enables systems to improve their performance over time without being explicitly programmed (20). In the context of IoT networks, ML algorithms can analyze vast amounts of data generated by connected devices to identify patterns, detect anomalies, and predict potential threats (18, 31). This capability makes ML particularly valuable for intrusion detection systems, as it enhances their ability to adapt to evolving threats and reduce false positives (20, 31, 38). Additionally, ML techniques can be employed to improve the efficiency and accuracy of feature selection, a critical aspect of developing effective intrusion detection models (20, 24, 78).

Machine learning algorithms can be broadly classified into three categories: supervised, unsupervised, and reinforcement learning (30, 79). Supervised learning algorithms require labeled data for training and are commonly used for classification and regression tasks (9, 79). In contrast, unsupervised learning algorithms work with unlabeled data to discover hidden patterns or groupings within the data (79). Reinforcement learning involves training agents to make sequential decisions by maximizing cumulative rewards, making it suitable for applications where actions must be optimized over time (9, 79). Each type of algorithm has its strengths and weaknesses, and the choice of algorithm depends on the specific requirements of the intrusion detection system being developed (30, 79)

The application of machine learning in IoT intrusion detection has gained significant attention in recent years, driven by the increasing need for automated security solutions (36, 54). Numerous studies have explored the use of various ML algorithms, such as decision trees, support vector

machines, and neural networks, to improve the detection of anomalies and intrusions in IoT environments (14, 80). For instance, decision tree algorithms have been employed to classify network traffic and identify malicious patterns, while neural networks have shown promise in detecting complex attacks through deep learning approaches (14, 48, 80). Additionally, ensemble learning techniques, which combine multiple classifiers to improve detection accuracy, have been increasingly adopted in IoT intrusion detection systems (14, 36). However, the effectiveness of machine learning approaches is heavily dependent on the quality of the training data and feature selection, which can significantly impact their performance (4, 54).

Evaluating the performance of machine learning-based intrusion detection systems is crucial for understanding their effectiveness and reliability (14, 17, 21, 53). Common evaluation metrics include accuracy, precision, recall, F1 score, and area under the receiver operating characteristic (ROC) curve. Accuracy measures the overall performance of the model, while precision and recall provide insights into the system's ability to correctly identify malicious activities (81, 82). The F1 score is a harmonic mean of precision and recall, offering a balanced assessment of the model's performance, especially in scenarios with class imbalance (81, 82). The area under the ROC curve (AUC-ROC) is another important metric that assesses the model's ability to distinguish between classes across various threshold values, providing a comprehensive evaluation of its performance (81-83).

AI-Powered Intrusion Detection Systems for IoT Networks

AI-powered intrusion detection systems (IDS) leverage advanced algorithms to enhance the security of IoT networks by improving threat detection capabilities and reducing response times (11, 15, 49). These systems utilize machine learning, deep learning, and other AI techniques to analyze network traffic, identify anomalies, and adapt to evolving attack patterns (9, 17, 20, 48). By continuously learning from new data, AI-powered IDS can effectively mitigate risks associated with IoT vulnerabilities and provide real-time insights into network security (21, 33, 38, 54). Moreover, these systems can significantly enhance the accuracy of detection, reducing false positive rates that often plague traditional IDS solutions (14, 15, 21). The integration of AI into IDS represents a paradigm shift in IoT security, enabling proactive threat detection and more efficient resource allocation (1, 45, 72).

Deep learning-based IDS utilize artificial neural networks (ANNs) to analyze complex patterns in data, making them particularly effective for identifying sophisticated attacks in IoT networks (15, 17, 36, 56). These systems can automatically extract relevant features from raw data, eliminating the need for manual feature engineering and improving detection accuracy (13, 19, 43, 67). For example, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have shown promise in detecting anomalies in network traffic and classifying malicious activities (33, 43, 67). Moreover, deep learning models can handle large volumes of data generated by IoT devices, allowing them to scale effectively with the growing number of connected devices (84, 85). However, the training of deep learning models requires substantial computational resources and large datasets, which can be challenging in resource-constrained IoT environments (84, 85).

Reinforcement learning (RL) is a type of machine learning where an agent learns to make decisions by interacting with its environment and receiving feedback in the form of rewards or penalties (30, 79). RL-based IDS can adaptively respond to evolving threats by continuously updating their strategies based on real-time feedback (10, 13, 54). This approach enables the system to learn optimal defense strategies and effectively mitigate risks associated with new attack vectors (5-7). For instance, Q-learning and deep Q-networks have been successfully employed to train agents to recognize and respond to various types of attacks in IoT environments (86, 87). Although RL-based IDS offer promising capabilities, they also face challenges, such as the need for extensive training data and the risk of overfitting in dynamic environments (1, 10, 21).

Transfer learning is a machine learning approach that leverages knowledge gained from one domain to enhance learning in another, making it particularly useful for IoT security applications (88, 87). In the context of intrusion detection, transfer learning can address the challenge of limited labeled data, which is common in IoT environments, by utilizing pre-trained models on related tasks (1, 54, 67). This approach allows for faster model training and improved detection accuracy, particularly for emerging threats (20, 45, 87). For instance, studies have shown that transfer learning techniques can effectively enhance the performance of IDS in detecting various attack types, including denial-of-service and man-in-the-middle attacks (21, 20, 45, 87). Despite its potential, transfer learning also presents challenges, such as domain adaptation and the need for robust feature selection to ensure effective knowledge transfer (45, 88, 87).

Dataset and Feature Engineering for IoT Intrusion Detection

The availability of high-quality datasets is crucial for developing effective machine learning models for IoT intrusion detection (89,90). Various publicly available datasets cater specifically to IoT security research, such as the NSL-KDD, CICIDS 2017, UNSW-NB15, BoT-IoT, TON_IoT, IoT-23. The 'CICIDS 2017' dataset, which includes labeled network traffic for various attack types (91,92). Another notable dataset is the 'UNSW-NB15', which contains a diverse range of attack scenarios and normal traffic patterns, making it valuable for training and evaluating intrusion detection systems (92). Furthermore, the 'Bot-IoT' dataset is designed specifically for detecting botnet attacks in IoT environments, providing rich features for anomaly detection (93). The selection of appropriate datasets is critical, as they need to represent realistic traffic scenarios and encompass various attack types to facilitate comprehensive model training (89, 90).

Feature extraction and selection play a vital role in enhancing the performance of intrusion detection systems in IoT networks (89, 90). Effective feature extraction techniques enable the identification of critical attributes from raw data, allowing machine learning models to focus on relevant patterns that indicate malicious activities (89, 90). Methods such as Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are commonly employed to reduce dimensionality while retaining essential information (94). Moreover, the use of domain knowledge to guide feature selection can significantly improve detection accuracy by ensuring that the most relevant features are prioritized (89, 90, 94). Automated feature selection techniques, such as Recursive Feature Elimination (RFE) and Genetic Algorithms (GA), have also been explored to optimize the feature set for intrusion detection tasks (95).

Data pre-processing is a critical step in the development of machine learning models for IoT intrusion detection, as it directly impacts the quality and reliability of the training data (11, 89, 90). Key pre-processing techniques include data cleaning, normalization, and transformation (96). Data cleaning involves removing duplicates, handling missing values, and addressing inconsistencies in the dataset (92, 96). Normalization techniques, such as Min-Max scaling and Z-score normalization, are essential for ensuring that all features contribute equally to the model's training process (92, 96). Additionally, transforming categorical features into numerical formats is necessary for compatibility with machine learning algorithms (89, 90, 96). The effectiveness of the intrusion detection system heavily relies on the robustness of these pre-processing steps, as they determine the quality of input data fed into machine learning models (54, 96).

Performance Evaluation and Comparison of AI-Powered IDS

Evaluating the performance of AI-powered intrusion detection systems is essential for understanding their effectiveness in identifying threats within IoT networks (53, 92). Various metrics, including accuracy, precision, recall, F1-score, and area under the ROC curve (AUC-ROC), are commonly used to assess the performance of these systems (81, 82). Accuracy provides a general measure of the model's ability to classify both normal and malicious instances correctly (19, 53, 87). Precision and recall are crucial in understanding the model's ability to detect true positives while minimizing false positives and negatives, respectively (17). The F1-score is particularly useful in scenarios with imbalanced class distributions, as it provides a single metric that balances precision and recall (81, 82).

The effectiveness of AI-powered intrusion detection systems can be significantly enhanced compared to traditional IDS approaches, which often rely on rule-based mechanisms and signature matching (1, 11, 20). Traditional systems typically struggle to adapt to new and evolving attack vectors due to their reliance on predefined rules (17, 54). In contrast, AI-powered systems leverage machine learning algorithms that can learn from historical data and adapt to emerging threats, resulting in improved detection rates and reduced false positives (1, 11). Additionally, AI-driven solutions can efficiently analyze large volumes of data generated by IoT devices, making them more suitable for modern, dynamic environments (17, 54). However, the effectiveness of AI-powered IDS is highly dependent on the quality of training data and the robustness of the chosen algorithms (17, 54, 92).

The comparison of various AI-powered intrusion detection approaches highlights the strengths and weaknesses of different techniques (17, 54). For instance, deep learning-based IDS, which employ neural networks to capture complex patterns, have demonstrated superior performance in detecting sophisticated attacks compared to traditional machine learning methods (1, 11, 20). However, these models often require substantial computational resources and large datasets for effective training (17, 54). Reinforcement learning approaches offer the advantage of adaptability, enabling systems to learn optimal strategies for threat detection in real-time. Nonetheless, they may struggle with extensive training requirements and convergence issues (30, 79). Transfer learning techniques, which leverage knowledge from one domain to improve performance in another, have emerged as a promising solution to overcome data scarcity issues in IoT environments (88, 87). These comparisons highlight the importance of selecting the most appropriate approach based on specific application requirements and the unique challenges of the IoT landscape (88, 87).

Challenges and Future Research Directions

Despite the advancements in AI-powered intrusion detection systems, several challenges remain in effectively implementing these solutions within IoT networks (1,11,20). One significant challenge is the limited computational resources available in many IoT devices, which constrains the complexity of algorithms that can be deployed (13,32). Additionally, the heterogeneity of IoT devices and communication protocols complicates the integration of security measures, leading to potential vulnerabilities (15, 17). The dynamic nature of IoT environments, characterized by the frequent addition and removal of devices, presents further challenges in maintaining an up-to-date and effective intrusion detection system (17, 20). Finally, issues related to data privacy and regulatory compliance pose additional obstacles, as organizations must navigate complex legal frameworks while ensuring the security of sensitive information (11, 92).

To address the challenges facing AI-powered intrusion detection systems for IoT networks, future research should focus on developing lightweight algorithms that can operate efficiently on resource-constrained devices (15, 17). Research on federated learning approaches could enable collaborative model training across multiple devices without compromising data privacy, enhancing security while minimizing computational burdens. Additionally, exploring hybrid models that combine the strengths of different machine learning techniques may lead to more robust and adaptable intrusion detection systems. Investigating the integration of blockchain technology into IDS frameworks could provide improved data integrity and accountability, further enhancing security in IoT networks (11, 92). Finally, continuous efforts to improve the quality and diversity of datasets used for training will be essential to enhance the generalization and accuracy of machine learning models in detecting IoT-specific threats (15, 17).

Emerging trends in AI and machine learning, such as the utilization of explainable AI (XAI) techniques, offer promising avenues for improving the transparency and interpretability of intrusion detection systems (15, 17). By providing insights into the decision-making processes of machine learning models, XAI can help security analysts understand the rationale behind detected anomalies and enhance trust in the system (11, 92). The integration of edge computing with intrusion detection systems has also gained traction, enabling real-time threat detection and response capabilities at the network's edge, thereby reducing latency and improving efficiency (15, 17). Furthermore, the development of adversarial machine learning techniques presents both challenges and opportunities, as they can be employed to improve the resilience of intrusion detection systems against sophisticated attacks (15, 17). As the landscape of IoT security continues to evolve, ongoing research efforts will be critical in ensuring that intrusion detection systems remain effective and capable of addressing emerging threats (15, 17, 92).

Conclusion and Recommendation

This literature review highlights the significance of designing secure AI-powered intrusion detection systems for IoT networks, emphasizing the unique challenges and complexities associated with IoT security. The integration of machine learning techniques into intrusion detection systems has demonstrated improved performance in detecting various attack types and adapting to evolving threats. Furthermore, the selection of appropriate datasets, feature extraction methods, and pre-processing techniques plays a crucial role in the effectiveness of these systems.

Performance evaluation metrics such as accuracy, precision, recall, and F1-score are essential in assessing the effectiveness of AI-powered intrusion detection systems compared to traditional methods.

The findings of this review have important implications for both practice and research in the field of IoT security. AI-powered IDS often face resource constraints, with high computational and energy demands that are challenging for resource-limited IoT devices. Practitioners must prioritize the implementation of AI-powered intrusion detection systems to enhance the security of IoT networks, addressing the challenges related to resource constraints and device heterogeneity. Additionally, researchers should focus on developing novel algorithms that are lightweight, efficient, and capable of adapting to the dynamic nature of IoT environments. Future research should continue to explore the integration of advanced technologies such as federated learning, explainable AI, and edge computing to enhance the effectiveness of intrusion detection systems in IoT networks. Moreover, investigating the role of adversarial machine learning in fortifying intrusion detection systems against evolving threats presents an exciting avenue for exploration. By focusing on these emerging trends and technologies, researchers can contribute to the development of more robust and effective security measures for the rapidly growing IoT landscape.

Table 1: Summary of Surveyed Papers on AI-Powered Intrusion Detection Systems for IoT

Year	Title	ML Method	Limitations
2019	Deep Learning-Based IDS for IoT Networks	Deep Neural Networks (DNN)	High computational cost, lacks adaptability to new attack patterns
2020	Lightweight Anomaly Detection in IoT Using SVM	Support Vector Machines (SVM)	Ineffective for large-scale IoT networks, struggles with multi-class detection
2021	Reinforcement Learning for Adaptive IDS in IoT	Reinforcement Learning	Long training times, limited scalability
2022	Hybrid ML Approaches for Intrusion Detection in IoT Environments	Ensemble methods (Random Forest)	High memory usage, requires feature engineering

2023	Energy-Efficient Intrusion Detection Using Federated Learning in IoT	Federated Learning	Vulnerable to data poisoning attacks, requires high-quality decentralized data
2024	Unsupervised Anomaly Detection with Autoencoders for IoT Security	Autoencoders	High false-positive rate, difficulty in parameter tuning

Table2: **Datasets Described in Surveyed Papers**

Year	Title	Dataset Name	Dataset Features	Use in IDS Development
2021	Reinforcement Learning for Adaptive IDS in IoT	NSL-KDD	Network traffic features, labeled as normal or attack	Training and testing reinforcement learning-based IDS models
2022	Hybrid ML Approaches for Intrusion Detection in IoT Environments	CICIDS 2017	Real-world traffic with multiple attack scenarios	Evaluating ensemble ML methods for multi-class detection

Table 3: Summary of IoT Datasets and Their Characteristics

Dataset Name	Characteristics	Importance in IDS Development
NSL-KDD	Improved version of the KDD'99 dataset; balanced data distribution; labeled normal and attack classes.	Reduces redundant records, ensuring a fair evaluation of IDS performance and focusing on diverse attack types.
CICIDS 2017	Realistic traffic data; contains a variety of modern-day attacks, including DDoS, Brute Force, and more	Provides real-world relevance, supporting the evaluation of IDS under contemporary attack scenarios
IoT-23	Traffic from real IoT devices; includes benign and	Focuses specifically on IoT devices, enabling the creation of IDS tailored to IoT-specific network patterns.

	malicious traffic from smart home environments.	
TON_IoT	Comprehensive dataset with IoT telemetry, network traffic, and system logs from IoT devices.	Facilitates multi-layered IDS development by integrating IoT-specific telemetry and network traffic data.
BoT-IoT	IoT-specific botnet attack traffic; includes multiple types of DDoS attacks.	Highlights botnet-specific vulnerabilities in IoT environments, allowing targeted IDS for botnet mitigation.
UNSW-NB15	Modern attack scenarios; generated in a controlled network environment; diverse feature set.	Ensures a balance between normal and malicious traffic for robust IDS performance across various attack types.

Table 4: Survey of DL Models for IoT Intrusion Detection Systems (IDS)

Year	Title	DL Model	Dataset Used	Limitations	Key Contributions
2020	IoT Intrusion Detection Using CNN-Based Feature Extraction	Convolutional Neural Networks (CNN)	CICIDS 2017	High computational cost, limited scalability	Demonstrated improved feature extraction for anomaly detection
2021	RNN for Real-Time Anomaly Detection in IoT Networks	Recurrent Neural Networks (RNN)	UNSW-NB15	Struggles with long sequences, high false-positive rate	Struggles with long sequences, high false-positive rate Enhanced time-series anomaly detection using sequence modeling

2022	GNN-IDS: Graph Neural Networks for IoT Security	Graph Neural Networks (GNN)	IoT-23	Requires graph-based data preprocessing, lacks interpretability	Leveraged graph structures to model IoT network relationships
2023	Hybrid CNN-RNN for Multi-Class IDS in IoT Environments	CNN + RNN	BoT-IoT	Increased model complexity, longer training time	Combined spatial and temporal analysis for enhanced accuracy
2024	Federated GNN for Distributed IoT Intrusion Detection	Federated GNN	TON_IoT	Vulnerable to data poisoning attacks, requires secure	Distributed intrusion detection with privacy-preserving models

				federated setup	

Table 5: Performance Metrics of Research Works

Year	Title	ML/DL Model	Dataset Used	Accuracy	Precision	Recall	F1-Score	Training Time	Limitations
2019	Deep Learning-Based IDS for IoT Networks	Deep Neural Networks (DNN)	NSL-KDD	92%	90%	88%	89%	High (due to large model size)	High computational cost, poor scalability

2020	Lightweight Anomaly Detection in IoT Using SVM	Support Vector Machines (SVM)	CICIDS 2017	88%	85%	80%	82%	Moderate	Ineffective for large-scale networks, struggles with multi-class detection
2021	Reinforcement Learning for Adaptive IDS in IoT	Reinforcement Learning	UNSW-NB15	87%	85%	83%	84%	Long (due to training over time)	Limited scalability, slow convergence
2022	Hybrid ML Approaches for Intrusion Detection in	Ensemble Methods (Random Forest)	CICIDS 2017	90%	91%	87%	89%	Moderate	High memory usage, requires feature engineering

	IoT Environments								
2023	Energy-Efficient Intrusion Detection Using Federated Learning in IoT	Federated Learning	TON_IoT	85%	83%	80%	81%	High (due to communication overhead)	Vulnerable to data poisoning, decentralized data quality challenges
2024	Unsupervised Anomaly Detection with	Autoencoders	IoT-23	82%	79%	85%	81%	Low (due to unsupervised nature)	High false-positive rate, difficulty in tuning parameters

	Autoencoders for IoT Security								

(97)

List 1: Abbreviations and their meanings

AI	Artificial Intelligence
IDS	Intrusion Detection System
IoT	Internet of Things
ML	Machine Learning
DDoS	Distributed Denial Service
KNN	K-Nearest Neighbours
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
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
DPI	Deep Packet Inspection

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

References

1. 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.

2. 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.

3. 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.

4. 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.

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

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

7. 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.

8. Cook-Kwenda, M.O.L.L.Y., 2024. Tech-Enabled Global Cybercrime: Exploitation by Transnational Criminal Organizations (TCOS).

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

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. Khraisat A, Alazab A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity. 2021 Dec;4:1-27.

16. 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.

17. 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.

18. 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.

19. 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).

20. 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.

21. 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.

22. 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 (Vol. 1, pp. 543-547). IEEE.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. Bhuiyan MN, Rahman MM, Billah MM, Saha D. Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Internet of Things Journal. 2021 Mar 1;8(13):10474-98.

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

37. 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.

38. 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.

39. 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.

40. 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.

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

42. 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.

43. 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.

44. 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.

45. 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.

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

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.

58. Raza, A., Memon, S., Nizamani, M. A., & 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).

59. 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

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

61. 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.

62. 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.

63. 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.

64. 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.

65. 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 May 1;40:100371.

66. 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

67. 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.

68. 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.

69. 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 (pp. 1093-1110).

70. 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..

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

72. 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.

73. 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.

74. 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.

75. 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.

76. 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.

77. 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.

78. 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).

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

80. 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.

81. Powers DM. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. arXiv preprint arXiv:2010.16061. 2020 Oct 11.

82. 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.

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

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.

89. 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.

90. 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.

91. 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.

92. 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 (pp. 1-6). IEEE.

93. 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.

94. 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.

95. 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.

96. 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 (pp. 159-182). IGI Global.

97. 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 (pp. 1771-1789).