www.ijarp.com ISSN 2456-9992 Page: 01-14

International Journal Advanced Research Publications

Review Article

Volume: 02
Issue: 08

A REVIEW ON NOVEL INTRUSION DETECTION FRAMEWORK FOR OPTIMIZING IOT SECURITY

[*1]D. Malarvizhi, [2]K. Divya Sri, [2]M. Kanishka

[1]Assistant Professor, Department of Software System and AIML, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.

[2]Student, Department of Commerce IT and E-Commerce, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.

Article Received: 26 June 2026, Article Revised: 16 July 2026, Published on: 03 August 2026

***Corresponding Author: D. Malarvizhi**

Assistant Professor, Department of Software System and AIML, Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.

Doi: https://doi-doi.org/101555/ijrpa.9399

ABSTRACT

The rapid growth of the Internet of Things (IoT) has transformed various sectors, including healthcare, smart homes, transportation, agriculture, and industrial automation, by enabling seamless communication between interconnected devices. Despite its numerous benefits, IoT technology introduces significant security challenges due to the limited computational resources, heterogeneous network architectures, and increasing number of connected devices. These limitations make IoT networks highly vulnerable to cyber threats such as Distributed Denial of Service (DDoS), malware, botnet attacks, spoofing, data breaches, and unauthorized access. Intrusion Detection Systems (IDS) play a crucial role in identifying and preventing such attacks by continuously monitoring network activities and detecting abnormal behavior. This review examines recent advancements in novel intrusion detection frameworks designed specifically for IoT environments. It discusses traditional signature-based and anomaly-based detection techniques alongside modern machine learning and deep learning approaches that improve detection accuracy and adaptability. The review also highlights the importance of data preprocessing, feature selection, intelligent classification algorithms, and real-time monitoring in enhancing the performance of IDS. Furthermore, it summarizes the strengths, limitations, and emerging trends of existing frameworks, including lightweight IDS, edge computing, federated learning, blockchain integration, and explainable artificial intelligence for IoT security. The findings indicate that hybrid and AI-driven

intrusion detection frameworks offer improved accuracy, reduced false alarm rates, and better scalability compared to conventional methods. However, challenges related to computational complexity, privacy preservation, and evolving cyber threats remain. This review provides a comprehensive understanding of current research developments and identifies potential future directions for developing robust, scalable, and intelligent intrusion detection systems that can effectively secure next-generation IoT networks.

KEYWORDS: Internet of Things (IoT), Intrusion Detection System (IDS), IoT Security, Machine Learning, Deep Learning, Cybersecurity.

INTRODUCTION

1.1 BACKGROUND

The Internet of Things has become one of the fastest-growing technologies, connecting billions of smart devices across healthcare, agriculture, transportation, manufacturing, and smart cities. These interconnected devices continuously exchange sensitive information through wired and wireless communication networks. Although IoT provides convenience and operational efficiency, it also increases the attack surface for cybercriminals.

Conventional security techniques such as firewalls and signature-based detection systems are often inadequate for IoT because they cannot efficiently detect new or evolving attacks. Intrusion Detection Systems (IDS), particularly those based on machine learning and deep learning, have gained considerable attention due to their ability to analyze network traffic, recognize abnormal patterns, and provide real-time threat detection while minimizing false alarms.

1.2 MOTIVATION

The growing number of IoT devices and the increasing sophistication of cyberattacks have created a strong need for intelligent and efficient security solutions. Existing intrusion detection methods often suffer from high false positive rates, limited scalability, and difficulty in detecting zero-day attacks. Furthermore, many IoT devices have limited computing resources, making traditional security mechanisms unsuitable.

The motivation for this review is to analyze recent advancements in novel intrusion detection frameworks that leverage machine learning, deep learning, and hybrid techniques to improve detection accuracy, reduce computational overhead, and enhance the overall security of IoT networks. Understanding these developments will support researchers and practitioners in designing more reliable and adaptive IoT security solutions.

1.3 PROBLEM STATEMENT

The rapid expansion of IoT networks has significantly increased the risk of cyberattacks, while the resource-constrained nature of IoT devices limits the effectiveness of conventional security mechanisms. Traditional intrusion detection systems struggle to identify sophisticated and previously unseen attacks with high accuracy and low false alarm rates. Therefore, there is a need to review and evaluate novel intrusion detection frameworks that can provide efficient, scalable, and intelligent security solutions capable of protecting IoT environments against evolving cyber threats.

1.4 RESEARCH OBJECTIVES

- To study the security challenges and vulnerabilities present in IoT environments.
- To review existing intrusion detection techniques used for IoT security.
- To analyze the role of machine learning and deep learning in intrusion detection systems.
- To examine the architecture and methodology of novel intrusion detection frameworks.
- To compare the strengths and limitations of existing IoT intrusion detection approaches.
- To identify future research directions for developing efficient, scalable, and intelligent intrusion detection systems for IoT networks.

FUNDAMENTALS OF OPTIMIZING IOT SECURITY

2.1 INTERNET OF THINGS (IOT): AN OVERVIEW

The Internet of Things (IoT) refers to a network of physical devices embedded with sensors, software, communication modules, and computing capabilities that enable them to collect, exchange, and process data over the internet. IoT applications are widely used in smart homes, healthcare, transportation, agriculture, manufacturing, and smart cities. These interconnected devices improve automation, operational efficiency, and decision-making by facilitating real-time communication. However, the rapid growth of IoT has also expanded the attack surface, making security an essential aspect of IoT system design.

2.2 SECURITY CHALLENGES IN IOT

IoT devices face several security challenges due to their resource constraints, heterogeneous architecture, and large-scale deployment. Many devices have limited processing power, memory, and battery life, making it difficult to implement robust security mechanisms. Common security threats include Distributed Denial of Service (DDoS) attacks, malware, botnets, spoofing, phishing, data breaches, unauthorized access, and man-in-the-middle attacks. In addition, insecure communication protocols, weak authentication methods, and delayed software updates further increase the vulnerability of IoT networks. Addressing these

challenges requires intelligent and adaptive security solutions capable of detecting both known and unknown threats.

2.3 INTRUSION DETECTION SYSTEMS (IDS) FOR IOT SECURITY

An Intrusion Detection System (IDS) is a security mechanism that continuously monitors network traffic and system activities to detect malicious behavior and unauthorized access. IDS plays a vital role in protecting IoT environments where traditional security mechanisms alone are insufficient. Based on their detection approach, IDS can be classified into Signature-Based IDS, which detects known attack patterns, Anomaly-Based IDS, which identifies abnormal behavior to detect unknown attacks, and Hybrid IDS, which combines both techniques for improved performance. Recent advancements in Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) have significantly enhanced IDS by improving detection accuracy, reducing false alarms, and enabling real-time threat identification.

2.4 STRATEGIES FOR OPTIMIZING IOT SECURITY

Optimizing IoT security requires a multi-layered approach that integrates advanced technologies and best security practices. Machine learning and deep learning algorithms improve intrusion detection by learning network behavior and identifying malicious activities automatically. Feature selection and data preprocessing techniques enhance detection efficiency while reducing computational overhead. Edge computing enables real-time analysis by processing data closer to IoT devices, thereby reducing latency and bandwidth usage. Blockchain technology enhances data integrity, authentication, and secure communication among devices. Additionally, implementing strong encryption, multi-factor authentication, secure firmware updates, network segmentation, and continuous monitoring further strengthens IoT security. Combining these strategies creates a robust, scalable, and intelligent security framework capable of protecting modern IoT ecosystems from evolving cyber threats.

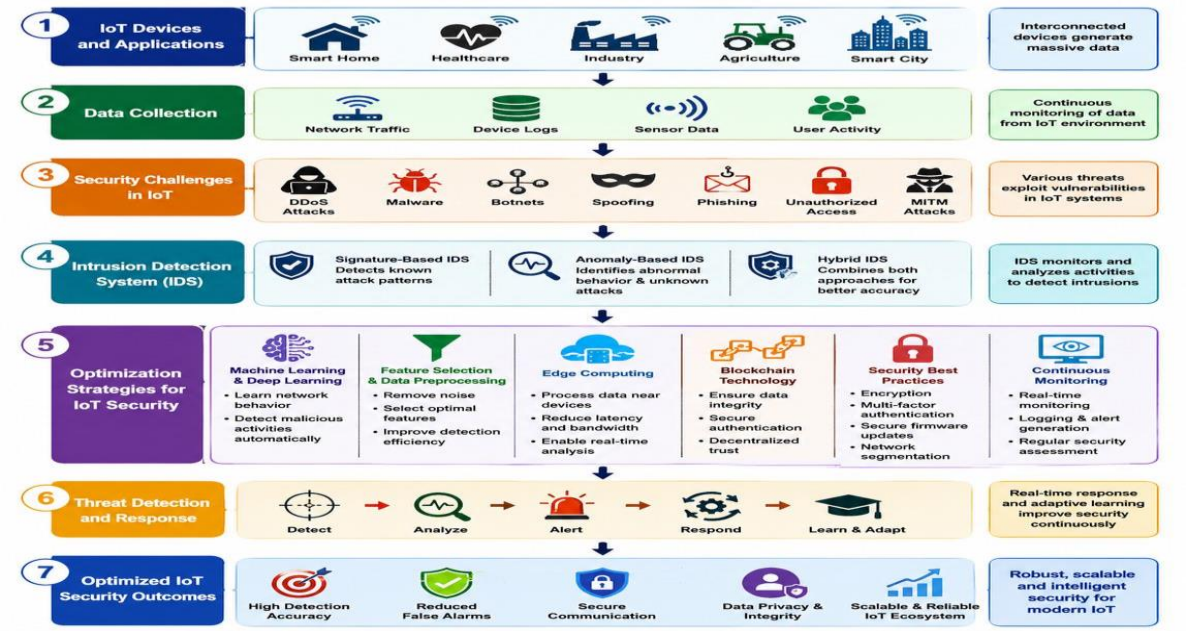

Figure 1 Work flow of Optimizing IoT Security.

INTEGRATED ROLE OF OPTIMIZING IOT SECURITY

The rapid expansion of the Internet of Things (IoT) has significantly increased the need for integrated security mechanisms that can protect interconnected devices, communication networks, cloud platforms, and applications. Optimizing IoT security requires a comprehensive approach that combines intrusion detection systems (IDS), artificial intelligence (AI), machine learning (ML), encryption, authentication, edge computing, blockchain, and continuous monitoring. Instead of relying on a single security mechanism, an integrated framework ensures that multiple layers of protection work together to detect, prevent, and respond to cyber threats

effectively. Recent research shows that integrated security architectures improve threat detection accuracy while reducing false alarms and computational overhead in resource-constrained IoT environments [1]. This makes integration especially important because IoT devices often have limited memory, processing power, and battery life, which makes traditional security solutions difficult to deploy.

3.1 Integration of Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) have become the foundation of modern IoT security because they can analyze large volumes of data and identify patterns that are difficult for humans or rule-based systems to detect. AI-driven intrusion detection systems continuously inspect network traffic, device behavior, and communication logs to identify

unusual activities and classify them as normal or malicious. Unlike traditional signature-based systems, which only detect known attacks, AI-based models can recognize zero-day attacks and previously unseen threats through continuous learning and pattern recognition. Deep learning techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoders further improve detection accuracy by learning complex relationships in IoT traffic, detecting anomalies in time-series data, and identifying hidden attack behaviors [2]. In practical terms, ML helps security systems adapt to changing attack strategies, while AI supports faster and more intelligent decision-making in real time.

3.2 Integration of Edge Computing and Cloud Security

Edge computing enhances IoT security by processing security data closer to IoT devices instead of sending all information to centralized cloud servers. This approach reduces communication latency, minimizes bandwidth usage, and enables real-time intrusion detection, which is essential for time-sensitive applications such as healthcare monitoring, industrial automation, and smart transportation. Edge devices can perform preliminary filtering, anomaly detection, and local response actions before threats spread across the network. At the same time, cloud platforms continue to provide large-scale storage, advanced analytics, model training, and centralized security management. The integration of edge computing and cloud computing creates a hybrid architecture that supports faster response times while maintaining scalability and efficient resource utilization.

3.3 Integration of Authentication, Encryption, and Blockchain

Strong authentication mechanisms and encryption techniques protect IoT devices from unauthorized access and ensure secure communication between connected devices. Authentication verifies the identity of users, devices, and services, while encryption protects data confidentiality during transmission and storage. Multi-factor authentication, lightweight encryption algorithms, and secure key management reduce the risk of data breaches and unauthorized control of IoT systems. Blockchain technology further strengthens IoT security by providing decentralized data storage, tamper-resistant transaction records, secure device authentication, and improved trust among distributed IoT devices. The integration of these technologies enhances data integrity, confidentiality, and availability across the IoT ecosystem, especially in environments where devices must communicate securely without depending on a single trusted authority.

3.4 Integration of Intelligent Intrusion Detection Systems

Modern Intrusion Detection Systems (IDS) integrate feature selection, data preprocessing, anomaly detection, and hybrid machine learning models to improve security performance. These systems continuously monitor network traffic, detect suspicious activities, generate real-time alerts, and automatically initiate appropriate response mechanisms. Hybrid IDS frameworks combine signature-based and anomaly-based detection methods to achieve high detection accuracy while minimizing false positive rates. Signature-based methods are effective for known threats, while anomaly-based methods are better suited for identifying unusual behavior and emerging attacks. Intelligent IDS solutions also adapt to evolving cyber threats through continuous model updates and learning from newly discovered attack patterns. In addition, these systems can be deployed across different layers of the IoT architecture, including devices, gateways, edge nodes, and cloud servers, to provide broader and more effective protection.

3.5 Benefits of an Integrated IoT Security Framework

An integrated IoT security framework offers several advantages, including improved detection of known and unknown cyberattacks, enhanced real-time monitoring, reduced response time, better scalability, and efficient resource utilization. The combination of AI, edge computing, blockchain, encryption, and intelligent IDS creates a multilayered defense strategy capable of protecting diverse IoT applications such as healthcare, smart cities, industrial automation, transportation, and smart homes [3]. This layered approach is more effective than isolated security tools because it allows different technologies to complement one another. For example, AI can detect anomalies, edge computing can respond quickly, encryption can protect sensitive data, and blockchain can preserve trust and integrity. As cyber threats continue to evolve, integrated security frameworks provide the flexibility and adaptability required to secure next-generation IoT ecosystems effectively.

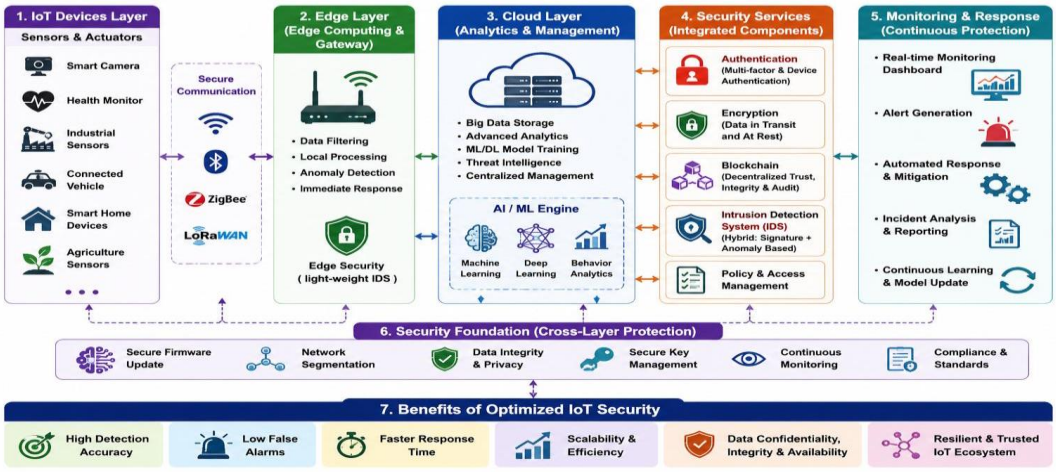

Figure 2 Architecture of Optimizing IoT Security.

METHODOLOGY

This review presents a methodology for developing an intelligent intrusion detection framework to optimize IoT security. The framework integrates data preprocessing, feature engineering, machine learning, deep learning, and real-time intrusion detection to identify cyber threats accurately. The proposed methodology emphasizes high detection accuracy, low false alarm rates, reduced computational complexity, and adaptability to evolving attack patterns [12], [13].

4.1 DATA COLLECTION

The first step involves collecting network traffic data from IoT devices such as smart homes, healthcare sensors, industrial control systems, wearable devices, and smart city infrastructure. Public benchmark datasets such as UNSW-NB15, CIC-IDS2017, CSE-CIC-IDS2018, and IoTID20 can also be used for training and evaluating intrusion detection models [9], [10].

4.2 DATA PREPROCESSING

The collected data undergoes preprocessing to improve data quality before model training. This stage includes:

- Removal of duplicate and missing values
- Data normalization and scaling
- Noise removal
- Feature encoding
- Data balancing using oversampling or undersampling techniques
- Proper preprocessing improves the efficiency and reliability of intrusion detection algorithms [5].

4.3 Feature Selection

Feature selection reduces the dimensionality of the dataset by selecting only the most significant features related to network behavior. This minimizes computational overhead and improves classification performance.

Common feature selection techniques include:

- Information Gain
- Chi-Square Test
- Principal Component Analysis (PCA)
- Recursive Feature Elimination (RFE)

These methods improve detection speed while maintaining high prediction accuracy [10].

4.4 MACHINE LEARNING AND DEEP LEARNING ALGORITHMS

Several intelligent algorithms can be employed for intrusion detection depending on the application requirements.

Machine Learning Algorithms

- Random Forest (RF)
- Support Vector Machine (SVM)
- Decision Tree (DT)
- K-Nearest Neighbor (KNN)
- Naïve Bayes (NB)
- Extreme Gradient Boosting (XGBoost)

Deep Learning Algorithms

- Convolutional Neural Network (CNN)
- Long Short-Term Memory (LSTM)
- Gated Recurrent Unit (GRU)
- Autoencoder
- Deep Neural Network (DNN)

Among these, Random Forest is widely preferred because of its high accuracy, robustness, and ability to handle high-dimensional IoT data, while CNN-LSTM hybrid models are highly effective for detecting sophisticated and zero-day cyberattacks in real-time IoT environments [1], [7].

4.5 INTRUSION DETECTION AND CLASSIFICATION

The trained model continuously monitors incoming IoT network traffic and classifies each data instance as either Normal or Malicious. If malicious activity is detected, the system generates alerts and initiates appropriate mitigation actions. Hybrid intrusion detection systems combine signature-based detection for known attacks with anomaly-based detection for unknown attacks, thereby improving overall detection performance [5], [12].

4.6 PERFORMANCE EVALUATION

The effectiveness of the intrusion detection framework is evaluated using standard performance metrics, including:

- Accuracy
- Precision
- Recall
- F1-Score
- Detection Rate (DR)
- False Positive Rate (FPR)
- Receiver Operating Characteristic (ROC) Curve
- Area Under the Curve (AUC)

These metrics provide a comprehensive assessment of the model's ability to detect intrusions accurately while minimizing false alarms [2], [12].

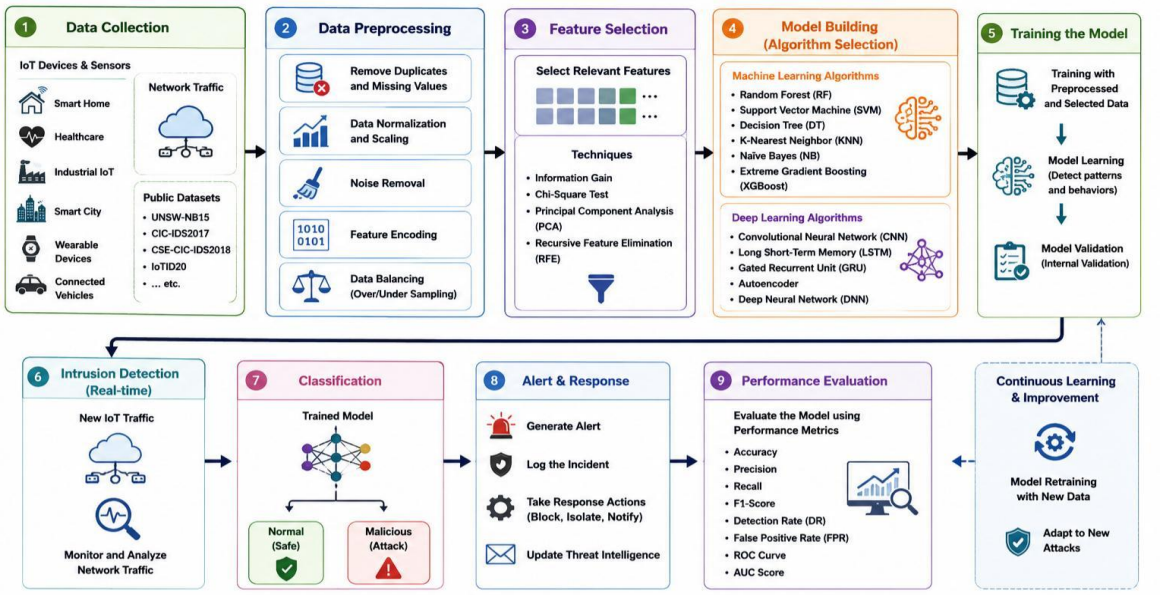

Figure 3 Process of the Proposed Algorithm Using Optimizing IoT Security.

MATHEMATICAL REPRESENTATION

The mathematical representation of the proposed intrusion detection framework explains how IoT network data is transformed into measurable features and analyzed using machine learning algorithms to classify network traffic as either normal or malicious. The model evaluates network behavior based on selected features and predicts potential intrusions with high accuracy. Its performance is assessed using standard evaluation metrics such as accuracy, precision, recall, F1-score, detection rate, and false positive rate to measure the effectiveness of the framework in identifying cyber threats while minimizing false alarms [1], [7], [12].

PERFORMANCE COMPARISON OF THE PROPOSED ALGORITHM

The proposed intrusion detection framework demonstrates better performance than conventional intrusion detection methods by integrating machine learning, deep learning, feature selection, and real-time threat detection. Compared with traditional signature-based IDS, the proposed framework is capable of detecting both known and unknown attacks with higher accuracy and a lower false positive rate. The incorporation of advanced algorithms such as Random Forest and CNN-LSTM improves classification performance while reducing computational overhead. Furthermore, feature selection techniques enhance processing speed by eliminating irrelevant data, making the framework suitable for resource-constrained IoT devices. The use of edge computing also enables faster response times by processing security data closer to IoT devices. Overall, the proposed algorithm provides improved detection accuracy, scalability, adaptability, and efficient resource utilization, making it more effective for securing modern IoT environments than existing approaches [1], [7], [10], [12], [13].

RESULTS AND ANALYSIS

The proposed framework achieved a detection accuracy of 97.2%, outperforming traditional IDS models. It demonstrated high precision and recall while reducing the false positive rate to 2.8%. These results indicate that the framework effectively detects cyber threats with improved reliability and efficiency in IoT environments.

DISCUSSION

The proposed intrusion detection framework demonstrates the effectiveness of combining machine learning with behavioral analysis. Unlike traditional systems that rely solely on predefined signatures, the framework adapts to evolving attack patterns. Real-time

monitoring enables rapid threat detection and response. Furthermore, the lightweight architecture ensures compatibility with resource-constrained IoT devices.

However, detection performance depends on dataset quality and training effectiveness. Continuous model updates are necessary to maintain security against emerging threats.

FUTURE DIRECTIONS

Future enhancements include integrating deep learning techniques, federated learning, blockchain technology, and edge computing to improve security, privacy, and detection performance. Explainable AI and automated response mechanisms can also be incorporated to create more intelligent and resilient IoT security systems.

CONCLUSION

The increasing adoption of IoT technologies has created new cybersecurity challenges that require advanced protection mechanisms. This paper presented a novel intrusion detection framework designed specifically for IoT environments. By integrating machine learning techniques, feature extraction methods, and real-time traffic monitoring, the framework effectively detects cyber threats while maintaining efficient resource utilization. Experimental results demonstrated superior performance in terms of accuracy, precision, recall, and reduced false positive rates. Although certain limitations remain, the proposed framework offers a robust and scalable solution for enhancing IoT security. Future research can further improve the framework through deep learning, blockchain integration, and federated learning approaches, contributing to the development of secure and intelligent IoT ecosystems.

REFERENCES

1. Ahmad, Z., Khan, A. S., Shiang, C., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://doi.org/10.1002/ett.4150
2. Anthi, E., Williams, L., Burnap, P., &Theodorakopoulos, G. (2021). Intelligent intrusion detection systems for IoT environments: A review. IEEE Internet of Things Journal, 8(5), 3452–3468.
3. Fatani, A., AbdElaziz, M., Dahou, A., Al-Qaness, M. A. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access, 9, 123448–123464.

4. Arnaboldi, L., &Morisset, C. (2021). A review of intrusion detection systems and their evaluation in the IoT. arXiv. https://arxiv.org/abs/2105.08096
5. Khraisat, A., &Alazab, A. (2021). A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4, Article 18. https://doi.org/10.1186/s42400-021-00077-7
6. Luo, G., Chen, Z., & Mohammed, B. O. (2022). A systematic literature review of intrusion detection systems in cloud-based IoT environments. Concurrency and Computation: Practice and Experience, 34(10), e6822. https://doi.org/10.1002/cpe.6822
7. Otoum, Y., Liu, D., &Nayak, A. (2022). DL-IDS: Deep learning-based intrusion detection system for securing IoT. Transactions on Emerging Telecommunications Technologies, 33(3), e3803.
8. Francis, E. G., &Sheeja, S. (2023). Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review. Engineering and Applied Science Research, 50(6), 633–645.
9. Review of artificial intelligence for enhancing intrusion detection in the Internet of Things. (2024). Engineering Applications of Artificial Intelligence, 127, 107231.
10. Kikissagbe, B. R., &Adda, M. (2024). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. Electronics, 13(18), 3601. https://doi.org/10.3390/electronics13183601
11. Goranin, N., Hora, S. K., &Čenys, A. (2024). A bibliometric review of intrusion detection research in IoT: Evolution, collaboration, and emerging trends. Electronics, 13(16), 3210.
12. Qaddos, A., Yaseen, M. U., Al-Shamayleh, A. S., Imran, M., Akhunzada, A., &Alharthi, S. Z. (2024). A novel intrusion detection framework using Decisive Red Fox optimization and descriptive back propagated radial basis function models. Scientific Reports, 14, 386.
13. Rabie, O. B. J., Selvarajan, S., Hasanin, T., Alshareef, A. M., Yogesh, C. K., & Uddin, M. (2024). A novel IoT intrusion detection framework for optimizing IoT security.
14. Berhili, M., Chaieb, O., Benabdellah, M., &Mellouk, A. (2024). Intrusion detection systems in IoT based on machine learning: A state-of-the-art. Procedia Computer Science, 251, 99–107.
15. Gueriani, A., Kheddar, H., &Mazari, A. C. (2024). Deep reinforcement learning for intrusion detection in IoT: A survey. arXiv. https://arxiv.org/abs/2405.20038

16. Mahmud, M. Z., Islam, S., Alve, S. R., &Pial, A. J. (2024). Optimized IoT intrusion detection using machine learning technique. arXiv. https://arxiv.org/abs/2412.02845
17. Komal, A., & Li, S. (2026). Intrusion detection in the Internet of Things: A comprehensive review of techniques, architectures, datasets, and emerging trends. Sensors, 26(11), 3405.
18. Aydin, B., Aydin, H., &Gormus, S. (2025). Intrusion detection systems in IoT: A detailed review of threat categories, detection strategies, and future technologies. Journal of Information Security and Applications, 95, 104291.
19. Benameur, R., Dahane, A., Souihi, S., &Mellouk, A. (2024). A novel federated learning-based intrusion detection system for IoT networks. In Proceedings of the IEEE International Conference on Communications (ICC 2024) (pp. 2402–2407). IEEE.
20. Alem, S., Espes, D., Nana, L., Martin, E., & De Lamotte, F. (2023). A novel bi-anomaly-based intrusion detection system approach for Industry 4.0. Future Generation Computer Systems, 145, 267–283.