INTELLITHINGS
Artificial Intelligence | Internet of Things

Vol. 1 No. 1, 2025 p-ISSN: xxxx-xxxx e-ISSN: xxxx-xxxx https://doi.org/xxxxxxxxx

A Review and Comparative Analysis of Intrusion Detection Systems for Edge Networks in IoT

Ata Amrullah

Department of Informatics, Darul Ulum Islamic University, East Java, Indonesia

Received: 2 December 2024
Accepted: 17 January 2025
Published: 24 January 2025

Keywords:
IoT;
Edge Network;
IDS;
Machine Learning;
Deep Learning.

Corresponding author:
Ata Amrullah
ata@unisda.ac.id

Abstract

This article presents a comprehensive review and comparative analysis of intrusion detection systems (IDS) designed for edge networks in Internet of Things (IoT) environments. The rapid growth of IoT has heightened security vulnerabilities in edge networks, which are the focus of this study. Various IDS approaches, including signature-based, anomaly-based, and hybrid methods, are explored, with an emphasis on the application of machine learning and deep learning techniques. The review includes an analysis of system architectures, algorithms (LSTM, CNN, Transformer), datasets, performance evaluation metrics, and experimental results from prior research. The literature study indicates that deep learning has significant potential to enhance intrusion detection accuracy; however, its effectiveness depends on dataset quality, appropriate data preprocessing, and handling class imbalances. Optimal feature selection, blockchain integration, and ensemble approaches are also critical. In conclusion, a multi-faceted approach combining advanced algorithms, suitable preprocessing techniques, and a deep understanding of IoT attacks is essential. Future research should focus on developing adaptive, efficient, and robust IDS with realistic datasets and comprehensive evaluation methods. This article provides a valuable resource for researchers and practitioners in the field of IoT edge network security.

1. INTRODUCTION

The Internet of Things (IoT) paradigm has witnessed a massive proliferation of interconnected devices across various sectors, ranging from smart homes and healthcare to industrial automation and transportation [1][2][3]. This rapid expansion, while presenting immense potential for efficiency and convenience, has simultaneously triggered a significant increase in cybersecurity vulnerabilities, particularly within edge networks.

An edge network, within the context of data architecture, refers to a strategic configuration designed to distribute computational resources directly to edge devices within a network. This approach aims to alleviate the processing burden on central servers by offloading a substantial portion of computational tasks to the edge devices themselves [4]. Consequently, edge devices function not merely as terminals that transmit data, but also as active information processing points, thereby resulting in enhanced efficiency and reduced latency. The implementation of this edge network architecture is becoming increasingly relevant in applications requiring real-time data processing and rapid response, such as in Internet of Things (IoT) systems, industrial automation, and autonomous vehicles [5]. In this paradigm, edge devices, such as sensors, actuators, and other embedded devices, leverage local computing power to perform data analysis, machine learning inference, and

decision-making without relying entirely on a central server [6]. This not only reduces the bandwidth required for data transmission but also enhances the overall scalability and resilience of the network [7].

The edge network located at the periphery of network infrastructure as described at Figure 1, often serve as the primary access points for numerous IoT devices, making them critical targets for malicious actors. The inherent resource constraints of many IoT devices, coupled with their often limited security features, further exacerbate the challenges in protecting edge networks from various cyber threats [8].

Intrusion Detection Systems (IDS) have emerged as vital components in the cybersecurity arsenal, offering a proactive approach to identify and mitigate potential security breaches [9]. However, traditional network-based IDS solutions are often ill-suited for the unique characteristics of IoT edge networks, necessitating the development and deployment of specialized IDS solutions tailored to the specific needs and constraints of these environments. These constraints include limited computational resources, low power consumption requirements, diverse communication protocols, and the dynamic nature of IoT deployments.

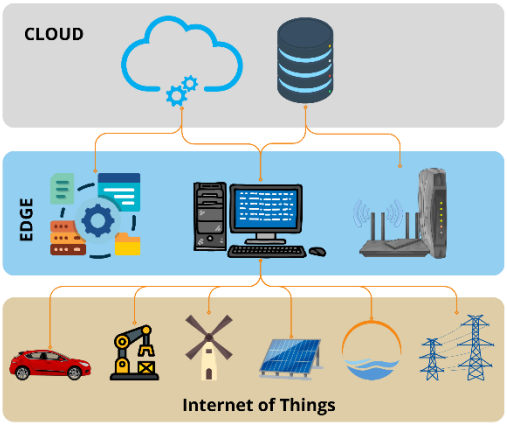

Figure 1. Network infrastructure

This article presents a comprehensive review and comparative analysis of existing intrusion detection systems designed for edge networks in IoT environments. We systematically explore the state-of-the-art in IDS techniques, covering various approaches, including signature-based, anomaly-based, and hybrid methods, while considering their applicability and performance characteristics in the context of resource-constrained edge devices. Additionally, we analyze and compare these systems based on key parameters such as detection accuracy, false alarm rate, computational overhead, and energy efficiency. By providing a rigorous examination of the existing research landscape, this review aims to clarify the current challenges, opportunities, and future directions in securing IoT edge networks against cyber attacks. The primary goal is to provide a valuable resource for researchers and practitioners in identifying the most effective and suitable IDS solutions for specific IoT deployments, contributing to a more secure and resilient IoT ecosystem. This review also highlights research gaps and proposes areas that require further exploration to achieve robust and adaptive intrusion detection for the ever-evolving IoT domain.

2. RELATED WORK

Various previous studies have been conducted to develop intrusion detection systems suitable for IoT environments. Moreover, one of the primary challenges in building intrusion detection systems for IoT is the limited resources of IoT devices, such as computational power, memory, and battery capacity.

a) Evolution of IDS Technology in IoT Edge Networks

The evolution of Intrusion Detection Systems (IDS) within IoT edge networks has been driven by the unique challenges posed by the distributed and resource-constrained nature of these environments. Early IDS deployments in traditional networks, often reliant on signature-based methods, proved ill-suited for the diverse and rapidly evolving threat landscape of IoT. These traditional systems, designed to detect known attack patterns by matching them against a database of signatures, often struggled with the sheer volume and variety of traffic within IoT networks, leading to high rates of false alarms and missed intrusions. Furthermore, the resource-intensive nature of signature matching made them impractical for deployment directly on many IoT edge devices with limited processing power and battery life [10]. This inadequacy prompted

a shift towards anomaly-based detection techniques which aim to identify deviations from normal behavior, allowing the detection of previously unseen attacks. However, these approaches also presented challenges, including the need for accurate profiling of normal network behavior, which is difficult to establish in dynamically changing IoT environments, and the potential for generating false positives due to unforeseen legitimate activities [11].

b) The Role of Datasets in IDS Development for IoT

Datasets play a pivotal role in the development and evaluation of Intrusion Detection Systems (IDS) for IoT environments, serving as the foundation for training and testing machine learning models. The effectiveness of any ML-based IDS is heavily contingent on the quality, size, and representativeness of the dataset used. Ideal datasets should accurately reflect the diverse range of network traffic patterns, device behaviors, and attack vectors that characterize real-world IoT deployments. However, obtaining such datasets presents numerous challenges. IoT networks are heterogeneous and rapidly evolving, making it difficult to create datasets that are both comprehensive and up-to-date [12]. Furthermore, the sensitive nature of data collected from IoT devices, often involving personal or proprietary information, raises privacy and ethical concerns that must be carefully addressed [13]. Thus, the creation and use of high-quality, representative datasets are critical to driving progress in the field of IoT security.

c) IDS Integration with Other Technologies

Beyond standalone implementations, the integration of Intrusion Detection Systems (IDS) with other technologies is emerging as a promising direction for enhancing security in IoT environments. One notable area is the convergence of IDS with Software-Defined Networking (SDN), enabling dynamic and adaptable security responses. In this context, SDN can be leveraged to reroute traffic and implement mitigation strategies based on real-time alerts generated by the IDS, thus providing a more efficient and effective means of containing and neutralizing detected threats [14]. Another significant trend involves the integration of IDS with blockchain technologies. This integration not only ensures the integrity and provenance of security logs generated by IDS, but also allows for decentralized threat intelligence sharing and consensus-based decision-making among IoT devices, thereby enhancing the resilience of the overall security framework. Such integrations provide not only enhanced security capabilities but also increase trust and transparency in the increasingly complex IoT ecosystem [15]

d) The Impact of IDS on IoT Data Privacy

While Intrusion Detection Systems (IDS) are crucial for securing IoT networks, their implementation and operation can also have a significant impact on data privacy. The very act of monitoring network traffic to detect anomalies or intrusions inherently involves the collection and analysis of data, which may include sensitive or personal information transmitted by IoT devices. This raises concerns about the potential for privacy breaches, as IDS themselves can become targets for malicious actors seeking to intercept or misuse the collected data [16]. The deployment of IDS within IoT environments, therefore, necessitates the careful consideration of data protection mechanisms and the implementation of privacy-enhancing technologies to mitigate the associated risks. This includes techniques such as data anonymization, encryption, and access control measures to limit exposure to sensitive data.

Furthermore, the effectiveness of an IDS is often dependent on its ability to understand network traffic, which may require the use of machine learning models trained on data containing user behavior patterns. If not properly anonymized or managed, these training datasets can pose a risk to the privacy of the users whose data they contain, potentially leading to inferential privacy breaches where sensitive information can be derived indirectly. Therefore, it is crucial to develop and implement privacy-preserving machine learning techniques that can learn from data without compromising the privacy of individuals [17]. These techniques may include federated learning, differential privacy, and other secure multi-party computation approaches that allow for the training of models

Table 1. Related Survey Papers

Survey Paper	Year	Dataset	Contributions	Methodology
[18]	2025	CICIoMT2024 for binary and multi-class classification	Emphasize the model's balance between accuracy and computational demands, making it suitable for resource-constrained IoMT devices.	using a deep learning model with two LSTM layers followed by two dense layers (L2D2)
[19]	2024	UNSW-NB 15, UNSW-2018-IoTBotnet, and Edge-IIoT	proposing an anomaly-based intrusion detection system using machine learning and deep learning algorithms to detect and mitigate DDoS attacks in IoT environments.	using a combination of machine learning algorithms and a metaheuristic optimization approach
[20]	2024	NF-UNSW-NB15-v2 and CICIDS2017	developing a hybrid Transformer-CNN deep learning model for intrusion detection that addresses class imbalance issues.	involving a hybrid deep learning model combining a Transformer and a Convolutional Neural Network
[21]	2024	TON_IoT and Edge_IIoT datasets	proposing a cybersecurity anomaly detection system for the Internet of Healthcare Things that integrates AI models with Ethereum blockchain and IPFS	involving a two-stage process. First, they train various AI models. Second, they validate the AI models' findings using a blockchain technology component.
[22]	2024	Edge-IIoT dataset	a semi-automated intrusion detection system for detecting and classifying multi-layer attacks in IoT infrastructure	centering around a Semi-Automated Intrusion Detection System designed for multilayer attack detection in IoT
[23]	2024	KDD99, NSL-KDD, UNSW-NB15	offering a comprehensive survey of machine learning-based intrusion detection systems for IoT security, focusing on real-time responsiveness, detection accuracy, and algorithm efficiency	employing a systematic literature review methodology to analyze machine learning-based intrusion detection systems for IoT security
[24]	2023	DS2OS dataset	proposing a novel intrusion detection model specifically designed for IoT-enabled smart homes	proposing a multi-phase methodology for intrusion detection in IoT-enabled smart homes

on decentralized data without directly revealing the underlying sensitive information.

Addressing the tension between security and privacy is paramount when implementing IDS within IoT networks. The design and operation of IDS must prioritize not only the detection of security threats but also the safeguarding of sensitive user data. This requires a holistic approach that combines robust security measures with privacy-enhancing technologies, and it also necessitates the adoption of ethical frameworks that govern the collection, processing, and storage of data within the IoT ecosystem.

Several researchers have proposed novel approaches, such as placing intrusion detection systems at the network edge, to address these challenges. Furthermore, machine learning approaches have been widely used to improve the performance of intrusion detection systems, utilizing classification algorithms trained on realistic IoT attack data.

Research [18] proposes an LSTM-based L2D2 model for multi-class intrusion detection in IoMT environments. This model was trained and evaluated using the CICIoT2024 dataset and compared against several baseline models.

Studied from [19] compares the performance of various machine learning and deep learning algorithms in detecting DDoS attacks in IoT environments. The use of entropy-based window time is also proposed to enhance detection efficiency.

Research [20] proposes a hybrid deep learning model combining Transformer and CNN, combined with class imbalance handling techniques and improved data preprocessing, to build a more effective intrusion detection system.

Research [21] integrates AI models and blockchain technology to detect cybersecurity anomalies and provide secure and tamper-proof data management in IoHT. The methodology used involves data collection, AI model selection and training, IPFS and blockchain integration, performance evaluation, and an IoHT case study.

Research [22] employs a machine learning-based approach to detect multilayer attacks in IoT environments. The methodology involves feature selection, classification using various machine learning algorithms, and model performance evaluation using several metrics.

Research [23] also utilizes several machine learning algorithms to detect intrusions in IoT networks. The algorithms considered include both supervised and unsupervised learning algorithms.

Research [24] proposes an ensemble-based intrusion detection model for IoT-connected smart homes. This model was trained and tested using the DS2OS dataset and evaluated based on several performance metrics. The objective is to detect various types of attacks and normal behavior in smart home environments.

Various studies have indicated that developing intrusion detection systems (IDS) for the Internet of Things (IoT) environment faces significant challenges, particularly concerning the limited resources of IoT devices. To address this, recent research has focused on edge-based approaches and the utilization of machine learning to improve the efficiency and performance of IDS. These studies cover various models, ranging from LSTM, CNN, and Transformer-based deep learning to integration with blockchain technology and the use of ensemble techniques. Additionally, realistic datasets, data preprocessing techniques, and handling class imbalances are critical focuses for improving detection accuracy. Overall, these studies are contributing to the development of more adaptive, efficient, and effective IDS solutions for protecting the IoT ecosystem from various cyber security threats. To facilitate a clearer understanding, the systematic explanation of the discussed topics is structured and presented in Table 1, enabling a more accessible and organized overview.

3. RESEARCH METHODOLOGY

To achieve the objectives of this research, a comprehensive and systematic literature study was conducted to understand and analyze in-depth the landscape of machine learning-based intrusion detection systems (IDS) applied to the Internet of Things (IoT) environment. This process involved a thorough search and rigorous selection of relevant scientific publications from various leading databases. The databases focused on include, but are not limited to, IEEE Xplore, ACM Digital Library, ScienceDirect, and Springer Link. The selection of these databases was based on their reputation for publishing high-quality research in the fields

of computer science, electrical engineering, and cybersecurity.

The search strategy was carefully designed using a combination of relevant and specific keywords. The primary keywords used were "Intrusion Detection System," "IoT," "Machine Learning," "Deep Learning," and "Security." This combination of keywords aimed to encompass articles that discussed the research topic comprehensively and from various perspectives. Time constraints were also applied during the search process to ensure that only relatively recent publications, i.e., within the last five years (from the date of writing), were included in the study. This time limitation criterion aimed to capture the latest trends and recent developments in the field of machine learning-based IoT intrusion detection systems.

After the search phase, a phased publication selection process was conducted. The selected publications had to explicitly focus on the application of machine learning and deep learning techniques for the development of intrusion detection systems on IoT devices and networks. Furthermore, the publications that passed the initial selection were analyzed in-depth to identify key aspects that included system architectures, machine learning algorithms used (e.g., classification, clustering, and deep neural networks), datasets used to train and test the systems, performance evaluation metrics (e.g., accuracy, precision, recall, F1-score, and AUC), and reported experimental results.

This initial phase of the literature review focused on breadth, aiming to capture the wide array of methodologies and approaches being utilized within the field. The keywords used in the search were purposefully broad, intended to identify both established research and more novel explorations of the topic. The subsequent phases involved a refinement of the focus, homing in on specific areas where the literature demonstrated a high degree of activity or a potential for future advancements. This iterative process allowed for a thorough overview of existing work while also emphasizing the most pertinent and groundbreaking contributions to the field.

The in-depth analysis of selected publications included a critical evaluation of the methodologies employed, the robustness of the validation processes, and the practical relevance of the proposed solutions. Special attention was paid to the justifications for the use of particular algorithms, the rationale behind dataset selection, and the thoroughness of the performance assessment. This step involved a qualitative assessment of the research design, ensuring that each included study adhered to rigorous scientific practices. This included evaluating the clarity of the stated problem, the appropriateness of the proposed methodology, and the validity of the conclusions drawn.

Furthermore, the identified datasets used in the studies were examined in terms of their characteristics, representativeness, and availability. This assessment aimed to understand the limitations of the current datasets and identify areas where the creation of more realistic and comprehensive data resources is needed. The evaluation of performance metrics considered the potential biases inherent in different evaluation approaches and sought to identify how effectively each metric captured the specific challenges of intrusion detection within IoT environments. The rationale behind the selection of metrics was also scrutinized to ensure the chosen metrics were appropriate for the specific task.

The synthesis of information from various publications involved a careful comparative analysis, wherein different methodologies were juxtaposed to identify common themes, conflicting results, and gaps in the current understanding. This process aimed to uncover both the strengths and weaknesses of existing approaches and to develop a coherent narrative of the field's progress to date. The identification of trends and recurring themes was used to highlight the most promising avenues for future research and development.

Based on the systematic analysis and careful interpretation, key conclusions were drawn, and constructive recommendations for the future direction of research in the field of machine learning-based intrusion detection systems for IoT environments were formulated. learning-based intrusion detection systems for IoT environments were formulated. These recommendations aim to provide guidance for researchers and practitioners interested in contributing to the development of more effective and efficient cybersecurity solutions for the IoT ecosystem.

Vol. 1 No. 1, 2025 p-ISSN: xxxx-xxxx e-ISSN: xxxx-xxxx https://doi.org/xxxxxxxxx

Table 2. The Presented Studied Analysis

Survey Paper	Year	Research Problem	Limitation	Recommendation
[18]	2025	the need for an accurate and efficient multi-class intrusion detection system capable of identifying various attack types in real-time	Computationally expensive approaches like Graph Neural Networks.	Exploring alternative deep learning models and optimization techniques to further enhance performance and reduce computational overhead.
[19]	2024	the vulnerability of cloud-based IoT infrastructures to Distributed Denial of Service attacks, which pose significant threats to network security and operational integrity	The reliance on specific datasets (UNSW-NB 15, UNSW-2018 IoT Botnet, and Edge IIoT) might limit the generalizability of the findings to other IoT environments or attack scenarios	developing more adaptive and real-time detection mechanisms for DDoS attacks in IoT environments.
[20]	2024	detecting intrusions in network systems, particularly focusing on the limitations of existing methods in handling class imbalance	Potential limitations related to computational complexity	exploring further optimization strategies to reduce the computational complexity of the model, enabling its deployment in resource-constrained environments.
[21]	2024	the critical issue of cybersecurity anomalies within the Internet of Healthcare Things, focusing on the need for secure and tamper-proof data management	the computational overhead of blockchain transactions and the scalability challenges	Exploring alternative blockchain platforms, Investigating the use of more advanced AI models and techniques.
[22]	2024	the challenge of optimizing feature selection for machine learning models designed to detect multilayer attacks	the effectiveness of the proposed feature selection method might vary depending on the specific machine learning algorithm	Investigating other feature selection methods, Evaluating the proposed method on a wider range of attacks and datasets.
[23]	2024	addresses the growing concern of security threats targeting Internet of Things devices and networks	the heterogeneity of IoT devices and networks poses a challenge for developing universally applicable solutions.	Developing more sophisticated machine learning models, Creating more robust and adaptable systems
[24]	2023	the expanding attack surface introduced by the interconnected nature of smart home devices and the limitations of traditional security solutions	potential limitations related to the computational complexity of the ensemble approach and the reliance on a specific dataset	Developing more adaptive and dynamic intrusion detection systems, Integrating the proposed model with other security mechanisms

4. RESULTS AND DISCUSSIONS

The results of this literature study indicate the existence of diverse approaches and solutions that have been developed to enhance the security of IoT networks through machine learning-based intrusion detection systems (IDS). One prominent finding is the use of deep learning in research [18], where an LSTM-based L2D2 model was proposed for multi-class intrusion detection in the Internet of Medical Things (IoMT) environment. This model, evaluated using the CICIoT2024 dataset, demonstrated promising performance compared to the baseline models used. This research highlights the capability of LSTM in handling complex data sequences and the importance of selecting relevant datasets to train and evaluate IDS models. On the other hand, research [19] focused on detecting Distributed Denial of Service (DDoS) attacks using various machine learning algorithms. This study shows a performance comparison of several algorithms in detecting DDoS attacks in IoT environments and proposes the use of entropy-based window time to improve detection efficiency. This underscores the importance of considering specific attack characteristics in the selection of IDS algorithms.

Furthermore, research [20] proposes a hybrid deep learning model combining Transformer and Convolutional Neural Network (CNN) to build a more effective intrusion detection system. This model not only focuses on improving detection performance

but also on handling class imbalances through resampling techniques. This indicates that in addition to sophisticated algorithms, proper data preprocessing and handling techniques are crucial in building a robust IDS. Research [21] takes a different approach by integrating artificial intelligence (AI) models and blockchain technology to detect cybersecurity anomalies and provide secure data management in the Internet of Healthcare Things (IoHT) environment. This integration aims not only to enhance security but also to ensure data integrity, demonstrating the trend of using decentralized technologies in IoT security.

Research [22] highlights the importance of feature selection in the development of machine learning-based IDS, showing that optimal feature selection can improve model performance in detecting multilayer attacks in IoT environments. In addition, research [23] also explores various machine learning algorithms, both supervised and unsupervised, for intrusion detection in IoT networks. This study emphasizes the flexibility of machine learning approaches in addressing various types of attacks and IoT environments. Finally, research [24] proposes an ensemble-based intrusion detection model specifically designed for IoT-connected smart home environments. This model was tested using the DS2OS dataset and evaluated based on several performance metrics, demonstrating that ensemble approaches can enhance the accuracy and reliability of IDS in complex IoT environments.

Building upon these findings, it is evident that the selection of appropriate machine learning techniques is highly context-dependent. For instance, models like LSTM excel in handling time-series data, making them particularly suitable for detecting anomalies in network traffic patterns, as demonstrated in [18]. On the other hand, studies focusing on DDoS detection, such as [19], often rely on simpler algorithms combined with clever feature engineering, emphasizing the need for a tailored approach. Moreover, the issue of data quality and class imbalance, addressed in [20], cannot be overlooked. Techniques like resampling are essential, but the choice of such techniques should be based on a deep understanding of the dataset's characteristics and the specific problem at hand. Furthermore,

the increasing adoption of blockchain technologies, as shown in [21], demonstrates a significant shift toward distributed and more secure data handling methods in IoT security. This integration not only enhances data integrity but also offers new opportunities for decentralized anomaly detection mechanisms.

The research also highlights the increasing importance of explainable AI (XAI) in intrusion detection. While deep learning models often achieve superior performance, they can be difficult to interpret, limiting their practical application in critical security systems. Therefore, recent studies have started exploring methods to improve the transparency and interpretability of machine learning models, especially in the context of anomaly detection, where understanding the reasons behind an alert

is paramount. Such efforts may include the use of attention mechanisms, which highlight the specific features of data that triggered an alert, or the integration of more interpretable models with deep learning techniques. The development of such transparent models is crucial for enhancing trust and user adoption in IoT security solutions.

In summary, the ongoing research landscape showcases a trend toward more sophisticated and adaptive IDS approaches for IoT edge networks. The continuous evolution of attack vectors requires equally dynamic security solutions, which can learn from new attacks and adapt to changing environments. Future research directions should consider the development of lightweight yet effective IDS models suitable for the resource-constrained nature of many IoT devices, with particular attention paid to both accuracy and computational efficiency. Furthermore, the investigation of novel techniques for data augmentation, federated learning, and adversarial training are critical for the evolution of robust and versatile IDS systems. To provide a more detailed and structured overview of the concepts discussed and their interrelationships, Table 2 presents a comprehensive and systematic exposition, serving as a key reference for further analysis.

5. CONCLUSION

This literature study highlights that the development of machine learning-based intrusion detection systems (IDS) for the Internet of Things (IoT) is an active and complex area of research. Various approaches, particularly those utilizing deep learning such as LSTM, Transformer, and CNN, show great potential in improving intrusion detection accuracy. However, the effectiveness of these models is highly dependent on the quality of the datasets, data preprocessing techniques, and proper handling of class imbalances. Furthermore, research also indicates the importance of optimal feature selection, the integration of technologies such as blockchain, and ensemble approaches to enhance the security and integrity of data in heterogeneous and vulnerable IoT environments.

Overall, this study affirms that there is no single solution to address the security challenges in IoT. A multi-faceted approach is needed, combining advanced machine learning algorithms, appropriate data preprocessing techniques, the integration of relevant technologies, and a deep understanding of the characteristics of attacks and the IoT environment. Future research should focus on developing more adaptive, efficient, and robust IDS, as well as building more realistic datasets and developing comprehensive evaluation methods. Collaboration between researchers, industry, and government is also crucial to achieving a secure and trustworthy IoT ecosystem.

REFERENCES

[1] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1–2, pp. 81–98, Sep. 2018, doi: 10.1016/J.IOT.2018.08.009.

[2] A. Amrullah, M. U. H. Al Rasyid, and I. Winarno, "Implementasi dan Analisis Protokol Komunikasi IoT untuk Crowdsensing pada Bidang Kesehatan," *INOVTEK Polbeng - Seri Inform.*, vol. 7, no. 1, p. 122, 2022, doi: 10.35314/isi.v7i1.2365.

[3] S. Bayer, H. Gimpel, and D. Rau, "IoT-commerce - opportunities for customers through an affordance lens," *Electron. Mark.*, vol. 31, no. 1, pp. 27–50, 2021, doi: 10.1007/s12525-020-00405-8.

[4] M. Satyanarayanan, "The Emergence of Edge Computing," *Computer (Long. Beach. Calif).*, vol. 50, no. 1, pp. 30–39, 2017, doi: 10.1109/MC.2017.9.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, 2016, doi: 10.1109/JIOT.2016.2579198.

[6] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 219–235, 2019, doi: https://doi.org/10.1016/j.future.2019.02.050.

[7] L. M. Vaquero and L. Rodero-Merino, "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014, doi: 10.1145/2677046.2677052.

[8] P. Spadaccino and F. Cuomo, "Intrusion Detection Systems for Iot : Opportunities and Tem Taxonomy Sys-," 2020, [Online]. Available: https://arxiv.org/abs/2012.01174

[9] Z. Lin, Y. Shi, and Z. Xue, "IDSGAN: Generative Adversarial Networks for Attack Generation Against Intrusion Detection," in *Advances in Knowledge Discovery and Data Mining*, J. Gama, T. Li, Y. Yu, E. Chen, Y. Zheng, and F. Teng, Eds., Cham: Springer International Publishing, 2022, pp. 79–91.

[10] M. M. Rahman, S. Al Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Secur. Appl.*, vol. 3, p. 100082, 2025, doi: https://doi.org/10.1016/j.csa.2024.100082.

[11] Y. Liu, Z. Pang, M. Karlsson, and S. Gong, "Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control," *Build. Environ.*, vol. 183, p. 107212, 2020, doi: https://doi.org/10.1016/j.buildenv.2020.107212.

[12] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, "A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms," *Comput. Secur.*, vol. 132, p. 103283, 2023, doi: https://doi.org/10.1016/j.cose.2023.103283.

[13] B. Kaur *et al.*, "Internet of Things (IoT) security dataset evolution: Challenges and future directions," *Internet of Things*, vol. 22, p. 100780, 2023, doi: https://doi.org/10.1016/j.iot.2023.100780.

[14] N. Mazhar, R. Salleh, M. A. Hossain, and M. Zeeshan, "Paper_83-SDN_based_Intrusion_Detection_and_Prevention.pdf," vol. 11, no. 12, 2020.

[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 618–623. doi: 10.1109/PERCOMW.2017.7917634.

[16] P. Sun, Y. Wan, Z. Wu, Z. Fang, and Q. Li, "A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions," *Comput. Secur.*, vol. 148, p. 104097, 2025, doi: https://doi.org/10.1016/j.cose.2024.104097.

[17] S. El-Gendy, M. S. Elsayed, A. Jurcut, and M. A. Azer, "Privacy Preservation Using Machine Learning in the Internet of Things," *Mathematics*, vol. 11, no. 16, 2023, doi: 10.3390/math11163477.

[18] G. Akar, S. Sahmoud, and M. O. Member, "L2D2 : A Novel LSTM Model for Multi-class Intrusion Detection Systems in The Era of IoMT," vol. 11, pp. 1–12, 2025, doi: 10.1109/ACCESS.2025.3526883.

[19] M. E. Manaa, S. M. Hussain, S. A. Alasadi, and H. A.a.al-Khamees, "DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments," *Intel. Artif.*, vol. 27, no. 74, pp. 152–165, 2024, doi: 10.4114/intartif.vol27iss74pp152-165.

[20] H. Kamal, "Advanced Hybrid Transformer-CNN Deep Learning Model for Effective Intrusion Detection Systems with Class Imbalance Mitigation Using Resampling Techniques," *Futur. Internet*, vol. 16, no. 12, 2024, doi: 10.3390/fi16120481.

[21] O. P. Olawale and S. Ebadinezhad, "Cybersecurity Anomaly Detection: AI and Ethereum Blockchain for a Secure and Tamperproof IoHT Data Management," *IEEE Access*, vol. 12, no. August, pp. 131605–131620, 2024, doi: 10.1109/ACCESS.2024.3460428.

[22] B. Al Sukhni, S. K. Manna, J. M. Dave, and L. Zhang, "Extracting Optimal Number of Features for Machine Learning Models in Multilayer IoT Attacks," *Sensors*, vol. 24, no. 24, 2024, doi: 10.3390/s24248121.

[23] M. Esmaeili, M. Rahimi, H. Pishdast, D. Farahmandazad, and M. Khajavi, "Machine Learning-Assisted Intrusion Detection for Enhancing Internet of Things Security," pp. 1–34, 2024.

[24] D. Rani, N. S. Gill, P. Gulia, F. Arena, and G. Pau, "Design of an Intrusion Detection Model for IoT-Enabled Smart Home," *IEEE Access*, vol. 11, no. April, pp. 52509–52526, 2023, doi: 10.1109/ACCESS.2023.3276863.