INTELLITHINGS
Artificial Intelligence | Internet of Things

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

Trends and Challenges in Anomaly Intrusion Detection at the Edge for IoT: A Review

Ata Amrullah[1*], Dicka Yale Kardono[2], Mohammad Mansyur Abidin[3]

[1,2,3]Department of Informatics, Darul Ulum Islamic University, East Java, Indonesia

Received: 2 December 2024
Accepted: 21 January 2025
Published: 24 January 2025

Keywords:
IoT;
Edge Computing;
Anomaly Intrusion Detection;
Network Security;
Cybersecurity.

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

Abstract

The rapid proliferation of Internet of Things (IoT) devices has brought about new security challenges, particularly in the area of intrusion detection. This review article provides a comprehensive analysis of the trends and challenges in anomaly intrusion detection at the edge for IoT. By synthesizing findings from recent literature (2021-2023), we explore various approaches to anomaly detection, including those based on machine learning (ML), deep learning (DL), statistical methods, and rule-based techniques. We also examine network attacks relevant to IoT, such as man-in-the-middle (MitM), replay, and injection attacks. Our findings reveal a growing trend towards the use of ML and DL for anomaly detection, with many studies focusing on hybrid approaches to improve detection accuracy. While edge computing offers advantages in terms of reduced latency and enhanced privacy, significant challenges remain in implementing anomaly detection on resource-constrained edge devices. These include the heterogeneity of devices and protocols, the increasing sophistication of cyberattacks, the limited availability of labeled data, and privacy concerns. This review identifies unresolved research gaps, including the need for more efficient algorithms, more adaptive approaches, methods for generating synthetic anomaly data, and large-scale implementations. Furthermore, this work discusses the practical implications for enhancing IoT security and provides guidance for researchers and practitioners in the field. We conclude that future efforts should emphasize the development of adaptive and efficient methods, particularly for real-time detection, and consider ethical aspects like data privacy in the deployment of anomaly detection at the edge.

1. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has profoundly transformed the technological landscape. Smart devices, ranging from precision sensors in industries to personal wearables in homes, have become an integral part of modern life. However, this rapid expansion has also raised serious security concerns. IoT devices, often characterized by limited computational resources and vulnerable connectivity, have become prime targets for cyberattacks. Therefore, the development of robust security solutions, particularly intrusion anomaly detection, has become a matter of urgency [1].

Intrusion anomaly detection, which focuses on identifying system behavior that deviates from normal patterns, plays a crucial role in maintaining the security of the IoT ecosystem. In the highly diverse context of IoT, anomaly detection becomes increasingly complex due to the wide variety of devices, communication protocols, and operational environments. Traditional approaches that rely on cloud-based data processing have proven to be ineffective for addressing the unique characteristics of IoT,

such as high latency, large bandwidth requirements, and scalability challenges [2].

The concept of edge computing has emerged as an innovative solution to overcome these limitations. By moving data processing and analysis to the edge, closer to the data source (i.e., IoT devices), edge computing can reduce communication latency, conserve bandwidth, and improve energy efficiency. Implementing anomaly detection at the edge provides faster responses to threats, reduces dependence on cloud connectivity, and protects IoT devices from advanced cyberattacks [3].

However, the adoption of anomaly detection at the edge also poses several challenges. Edge devices are often resource-constrained in terms of computational power, memory capacity, and battery life. The heterogeneity of IoT devices and protocols also complicates the development of universal and scalable anomaly detection solutions. Moreover, the evolving threat landscape, which includes attacks such as man-in-the-middle (MitM), replay attacks, and injection attacks, requires the development of more adaptive and intelligent detection approaches [4].

This review article aims to provide an in-depth analysis of trends and challenges in anomaly intrusion detection at the edge for IoT. We will examine various anomaly detection approaches that have been implemented, including those based on machine learning (ML), deep learning (DL), statistical methods, and predefined rules. We will also highlight the main types of cyberattacks of concern in IoT environments, with a specific focus on MitM, replay, and injection attacks.

Furthermore, this review will delve into the main challenges in implementing anomaly detection at the edge for IoT. These challenges include the resource constraints of edge devices, the heterogeneity of IoT ecosystems, the complexity of anomaly detection algorithms, and the need for flexible and scalable solutions. We will also discuss how recent trends in edge computing, such as the utilization of artificial intelligence (AI) and federated learning, have the potential to improve the effectiveness of anomaly detection [5].

The diversity of IoT application environments will also be a key consideration in this review. We will analyze the implementation of anomaly detection at the edge for various scenarios, from industrial applications (such as industrial control systems (ICS), machine monitoring, and process control) to smart home applications (including privacy protection, device security, and user interaction). By examining diverse operational contexts, this review will provide a more comprehensive picture of the specific security needs in each environment [6].

By exploring trends and challenges in anomaly intrusion detection at the edge for IoT, this review hopes to be a valuable source of information for researchers and practitioners in the field. We expect this review to identify existing research gaps, foster innovation, and drive the development of more effective and efficient security solutions for a more secure IoT future [7].

2. RELATED WORK

2.1. Security of the Internet of Things (IoT) and Edge Computing

2.1.1. Security Threats in IoT Devices

The proliferation of Internet of Things (IoT) devices across various sectors has been accompanied by significant security vulnerabilities. Limited computational resources, memory, and battery power often render IoT devices susceptible to cyberattacks. Moreover, the lack of regular security updates and the implementation of weak security protocols exacerbate these risks. Common security threats in IoT include unauthorized access, denial-of-service (DoS) attacks, malware infections, and botnet participation. IoT devices often serve as entry points for attackers to gain access to broader networks and steal sensitive data [8].

2.1.2. Concept and Advantages of Edge Computing

Edge computing emerges as a promising solution to these challenges by moving data processing and analysis closer to the data source, i.e., at the edge of the network. In the context of IoT, this means processing data directly on IoT devices or nearby gateways, rather than in a centralized cloud. Edge computing offers several advantages for IoT security. First, it reduces communication

Table 1. Comparison Based on Literature Review

References	Aspect	Description
[9]	IoT Security Threats	Resource-constrained devices, lack of security updates, and weak protocols make IoT devices vulnerable to attacks like unauthorized access, DoS, malware, and botnets.
[10]	Edge Computing Advantages	Reduces latency, saves bandwidth, enhances data privacy and security by processing data closer to the source (IoT devices).
[11]	Edge Implementation for IoT Security	Enables ML-based anomaly detection, device behavior analysis, and smart firewall implementation at the edge, allowing for faster and more efficient threat response.
[12]	Types of Intrusion Anomalies	Classified into behavior-based, statistical-based, protocol-based, and signature-based anomalies.
[13]	Anomaly Detection Techniques	Utilizes machine learning (ML) with algorithms such as SVM, random forest, k-NN, deep learning (DL) with architectures like autoencoders, LSTM, CNN, statistical methods, and rule-based approaches.
[14]	Man-in-the-Middle (MitM) Attacks	Attackers intercept communication, capturing and manipulating data; difficult to detect as attackers masquerade as legitimate parties.
[15]	Replay Attacks	Attackers record and retransmit valid network traffic for malicious purposes; difficult to detect as data is valid, but usage context is incorrect.
[16]	Injection Attacks	Attackers inject malicious code or data into a system, potentially leading to system disruption, device damage, or data theft.

latency by enabling local data processing, thus eliminating the need for data transfer to the cloud. Second, edge computing saves network bandwidth by only sending relevant data to the cloud. Third, it enhances data privacy and security by preventing sensitive data from being transferred to the cloud [9].

2.1.3. Implementation of Edge Computing in IoT Security

The application of edge computing in IoT security enables the development of more efficient and effective intrusion detection systems. By processing data locally, edge devices can detect anomalies in real-time, providing faster responses to threats. This is particularly vital for time-sensitive IoT applications, such as industrial control systems and autonomous vehicles. Furthermore, edge computing allows for the implementation of more sophisticated data analysis techniques near the data source, thereby enhancing the accuracy of anomaly detection. Examples include machine learning-based attack detection at IoT gateways, monitoring abnormal device behavior at the edge, and implementing smart firewalls at gateways [10].

2.2. Anomaly Intrusion Detection in IoT Networks

2.2.1. Definition and Classification of Intrusion Anomalies

Anomaly intrusion detection is the process of identifying system behavior that deviates from normal patterns. In the context of IoT networks, intrusion anomalies can include unusual network activities, suspicious data

traffic, or abnormal device behavior. Intrusion anomalies can be classified into several types, including: behavior-based anomalies, statistical-based anomalies, protocol-based anomalies, and signature-based anomalies. Behavior-based detection monitors the normal patterns of devices and networks, and detects any deviations from these patterns. Statistical-based anomalies identify data patterns that do not conform to normal statistical models. Protocol-based anomalies monitor for violations of existing network protocols. And signature-based anomalies match network traffic patterns with signatures of known attacks [11].

2.2.2. Techniques for Anomaly Detection in IoT Networks

Various anomaly detection techniques have been implemented in IoT networks. Machine learning (ML) techniques, such as clustering, classification, and regression algorithms, are widely used to learn normal behavior patterns and detect anomalies. Deep learning (DL) methods, with architectures like autoencoders and recurrent neural networks (RNNs), are also gaining popularity due to their ability to learn complex data representations. Statistical-based methods, like time-series analysis and deviation analysis, are employed to detect anomalies based on statistical changes in data. Rule-based approaches, using knowledge bases or expert systems, are used to detect anomalies based on predefined rules [12].

2.3. Relevant Network Attack Types in IoT

2.3.1. Man-in-the-Middle (MitM) Attacks

Man-in-the-middle (MitM) attacks occur when an attacker intercepts the communication between two parties, capturing and manipulating the transmitted data. In the IoT context, MitM attacks can allow attackers to gain unauthorized access to sensitive data, modify control commands, or inject malware. These attacks are often difficult to detect as attackers can act as an invisible intermediary [13].

2.3.2. Replay Attacks

Replay attacks occur when an attacker records valid network traffic and retransmits it to the system for malicious purposes. In the IoT context, replay attacks can be used to reactivate previously executed commands, unlock secured devices, or manipulate sensor data. Replay attacks are challenging to detect as the data used is valid, but the timing and context of its retransmission are incorrect [14].

2.3.3. Injection Attacks

Injection attacks involve injecting malicious code or data into a system. In the context of IoT, these attacks can take the form of code injection into software, command injection into control systems, or data injection into sensor data. Injection attacks can result in system disruption, device damage, or unauthorized collection of sensitive information [15].

In summary, Table 1 comprehensively explains the comparison of eight recent studies as a reference for this article.

3. RESEARCH METHODOLOGY

3.1. Research Approach

This article employs a systematic literature review approach to analyze trends and challenges in anomaly intrusion detection at the edge for the Internet of Things (IoT). This approach is chosen because it allows for a comprehensive and structured analysis of the existing literature, identifies significant patterns and trends, and explores unresolved research gaps. Unlike original research articles that conduct experiments or testing, this review article focuses on synthesizing knowledge from the existing literature to provide a thorough overview of the topic. [16]

The core advantage of a systematic literature review lies in its emphasis on transparency and repeatability, ensuring that the research process is both verifiable and adaptable to future studies. Unlike original research articles, which are often centered on the generation of new experimental results, our primary focus is on the critical evaluation and synthesis of previously published research. We rigorously examine the methodologies employed, the outcomes achieved, and the limitations acknowledged by researchers within the field. This enables us to identify the most promising avenues of investigation, the areas that require more attention, and the challenges that persist despite

advancements in technology and understanding. By aggregating and distilling knowledge from various sources, we are able to provide a cohesive and authoritative perspective on the current state of anomaly intrusion detection at the edge for IoT.

Therefore, the systematic nature of this review allows us to go beyond merely summarizing previous studies; it empowers us to uncover the complexities of this dynamic field, highlight major research gaps, and identify the most pressing concerns faced by both academics and industry professionals. Our approach is intended to serve as a valuable resource, offering guidance to the research community and providing a foundation for future innovation in the development of effective and efficient intrusion detection systems. This approach ensures that the presented analyses are based on carefully selected, high-quality literature, thus providing a reliable assessment of the landscape and directions of research in this critical area.

3.2. Literature Search Strategy

The literature search was conducted systematically using several scientific databases and search engines. The databases used include:

- IEEE Xplore
- ACM Digital Library
- Scopus
- Web of Science
- Google Scholar

The keywords used in the literature search include combinations of:

- "Internet of Things" or "IoT"
- "Edge Computing" or "Fog Computing"
- "Anomaly Detection" or "Intrusion Detection"
- "Network Security" or "Cybersecurity"
- "Man-in-the-Middle Attack" or "MitM"
- "Replay Attack"
- "Injection Attack"
- "Machine Learning" or "Deep Learning"
- "Statistical Analysis"
- "Rule-Based Detection"

The literature search was limited to articles published between 2021 and 2023. We also restricted the search to relevant journal articles, conference proceedings, and review articles.

3.3. Inclusion and Exclusion Criteria

Articles selected for analysis must meet the following inclusion criteria:

- Articles discussing the topic of anomaly intrusion detection at the edge for IoT.
- Articles discussing at least one of the relevant network attacks (MitM, replay, or injection).
- Articles discussing different anomaly detection approaches (ML, DL, statistical, or rule-based).
- Articles published between 2021 and 2023.
- Articles published in English.

Articles that do not meet the above inclusion criteria will be excluded from the analysis (exclusion criteria). Additionally, articles deemed irrelevant or not making significant contributions were also excluded.

3.4. Literature Selection Process

The literature selection process was conducted in several stages:

- Identification: Initial literature search using predefined keywords in the mentioned databases.
- Screening: Abstracts and titles of identified articles were screened to ensure their relevance to the research topic.
- Eligibility: Articles that passed the screening stage were downloaded and read in full to confirm their eligibility based on inclusion and exclusion criteria.
- Inclusion: Articles meeting all inclusion criteria were included in the analysis.

3.5. Literature Analysis

After the literature selection process was completed, the selected articles were analyzed in detail to identify:

- Anomaly detection approaches used
- Types of network attacks discussed

- Application environments (industry, smart homes, or others)
- Evaluation methods
- Research results

- Strengths and weaknesses of the discussed approaches
- Challenges encountered
- Emerging research trends
- Unresolved research gaps

Data extracted from the literature analysis was compiled and synthesized to generate a comprehensive understanding of the trends and challenges in anomaly intrusion detection at the edge for IoT.

4. RESULTS AND DISCUSSIONS

4.1. Overview of Analyzed Literature

Following a systematic selection process, we successfully identified and analyzed a number of articles relevant to the topic of anomaly intrusion detection at the edge for IoT. These articles covered a wide range of anomaly detection approaches, discussed network attack types, application environments, and evaluation methods. Overall, this literature analysis provided a comprehensive overview of recent developments in this field.

4.2. Trends in Anomaly Detection Approaches

The literature analysis revealed several significant trends in anomaly detection approaches at the edge for IoT:

- Increased Use of Machine Learning (ML) and Deep Learning (DL): ML and DL-based approaches are becoming increasingly dominant in anomaly detection research. Algorithms such as Support Vector Machines (SVM), Random Forests, k-Nearest Neighbors (k-NN), autoencoders, Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN) are widely used due to their ability to learn complex data patterns and detect anomalies with high accuracy. Recent research indicates that DL, particularly deep neural network architectures, is gaining more popularity due to its capability to handle data with high dimensions and complexity.
- Hybrid Approach Implementation: Many studies propose hybrid approaches that combine several anomaly detection techniques. For instance, a combination of ML and DL, or the integration of statistical methods with machine learning, aims to leverage the advantages of each approach while overcoming their limitations.
- Focus on Real-Time Detection: Research is increasingly focused on developing anomaly detection methods that can work in real-time or near real-time. This is particularly important for time-sensitive IoT applications, such as industrial control systems or autonomous vehicles. To achieve real-time detection, several studies explore more lightweight detection methods, efficient algorithms, and the use of optimized hardware.

4.3. Challenges in Implementing Anomaly Detection at the Edge for IoT

The literature analysis also revealed various challenges encountered in implementing anomaly detection at the edge for IoT:

- Resource Limitations: Edge devices are often constrained by limited computational resources, memory, and battery power. This poses a challenge in implementing complex and resource-intensive anomaly detection algorithms. Therefore, much research is focused on developing lighter and more efficient algorithms that can perform well on resource-constrained edge devices.
- Heterogeneity of Devices and Protocols: IoT networks consist of various types of devices and communication protocols, making the development of universal and easily scalable anomaly detection solutions difficult. Further research is needed to develop adaptive approaches that can handle the heterogeneity of IoT devices and protocols.

- Evolving Network Attacks: Cyberattacks are continually evolving and becoming more sophisticated. Attacks such as man-in-the-middle (MitM), replay attacks, and injection attacks are increasingly used to target IoT devices. Research needs to focus on developing anomaly detection methods that are capable of detecting these advanced attacks.
- Lack of Labeled Data: The availability of labeled data, which is necessary for training and evaluating machine learning models, remains a challenge. In many cases, anomaly data is difficult to obtain, and methods for generating synthetic data are still in the research phase.
- Privacy Concerns: The implementation of anomaly detection at the edge also raises concerns about data privacy. Some anomaly detection methods require the collection of sensitive data, and data protection issues need to be considered seriously.

4.4. Implications of Findings

The findings from this literature analysis have several important implications for research and implementation of anomaly detection at the edge for IoT:

- Development of Efficient Algorithms: Research should continue to focus on developing lighter, efficient, and adaptive anomaly detection algorithms that can perform well on resource-constrained edge devices.
- Use of Hybrid Approaches: Hybrid approaches that combine several anomaly detection techniques show great potential in improving accuracy and resistance to cyberattacks.
- Focus on Real-Time Security: Research needs to prioritize the development of anomaly detection methods that can work in real-time or near real-time for time-sensitive IoT applications.
- Handling IoT Heterogeneity: Further research is needed to develop anomaly detection approaches that can handle the diversity of devices, communication protocols, and operational environments in IoT.
- Data Privacy Solutions: Research must consider appropriate data privacy solutions when implementing anomaly detection methods.

4.5. Unresolved Research Gaps

This literature analysis also highlighted several research gaps that need further investigation:

- Development of More Intelligent and Adaptive Detection Methods: Research needs to focus on the development of more intelligent and adaptive anomaly detection methods that can handle increasingly sophisticated and complex attacks.
- Development of Methods to Generate Synthetic Anomaly Data: Improved methods for generating synthetic anomaly data are required to address the challenge of labeled data availability.
- Large-Scale Implementation: Research on the implementation of anomaly detection at the edge on a large scale is still limited. Future research needs to address this issue.
- Integration with Emerging Technologies: Research needs to explore the integration of anomaly detection technologies with emerging technologies such as federated learning, blockchain, and generative AI.

5. CONCLUSION

This review article has comprehensively discussed the trends and challenges in anomaly intrusion detection at the edge for the Internet of Things (IoT). We have explored various anomaly detection approaches, ranging from methods based on machine learning (ML) and deep learning (DL) to statistical and rule-based approaches. Furthermore, we have analyzed relevant types of network attacks, including man-in-the-middle (MitM), replay, and injection attacks.

Several key points can be concluded from this review:

- Crucial Role of Edge Computing: Implementing edge computing plays a critical role in enhancing IoT security by reducing latency, saving bandwidth, and enabling faster and more efficient anomaly detection.
- Dominance of ML and DL Approaches: ML and DL-based approaches are increasingly dominant in anomaly detection research due to their ability to learn complex data patterns and detect anomalies with high accuracy.
- Challenges of Edge Implementation: Implementing anomaly detection at the edge faces various challenges, including device resource limitations, the heterogeneity of devices and protocols, increasingly sophisticated attacks, a lack of labeled data, and privacy concerns.
- Need for Hybrid Approaches: Hybrid approaches that combine several anomaly detection techniques show great potential in improving the accuracy and robustness of systems.
- Focus on Real-Time Detection: The development of anomaly detection methods that can work in real-time is vital for time-sensitive IoT applications.
- Practical Implications: Research and development in this field have significant practical implications for enhancing the security of IoT devices across various sectors, including industry and smart homes.

Based on the literature analysis, we have also identified several areas that require further investigation:

- Development of More Efficient Detection Algorithms: Research should continue to focus on developing lighter, efficient, and adaptive anomaly detection algorithms that can perform well on resource-constrained edge devices. This includes exploring techniques for model compression, algorithm optimization, and utilizing optimized hardware.
- Development of Methods to Address IoT Heterogeneity: Further research is required to develop anomaly detection approaches that can handle the heterogeneity of devices, communication protocols, and operational environments within IoT.
- Enhancing Resilience to Advanced Attacks: Research should focus on developing anomaly detection methods capable of detecting increasingly sophisticated and complex attacks, including attacks that employ adversarial techniques.
- Development of Methods for Generating Synthetic Anomaly Data: Improved methods for generating synthetic anomaly data are needed to address the problem of limited labeled data required for training machine learning models.
- Exploration of Federated Learning: Research should explore the potential of federated learning to train anomaly detection models at the edge without the need to gather sensitive data in one central location.
- Large-Scale Implementation: Research into implementing anomaly detection at the edge on a large scale is still limited, and further studies are required to address scalability challenges.
- Integration with Other Security Technologies: Research can explore the integration of anomaly detection with other security technologies such as blockchain and zero trust network access (ZTNA).
- Evaluation with More Realistic Datasets: Future research should evaluate anomaly detection models using more realistic datasets that more closely represent real-world conditions.
- Development of Benchmark Datasets: The development of benchmark datasets specific to anomaly detection at the edge for IoT is crucial for comparing the performance of various approaches and facilitating future research.
- Research on Privacy Aspects: Further research is required to address data

privacy issues arising from the implementation of anomaly detection at the edge.

The findings from this review have several significant practical implications:

- Implementation Guidance: This research can provide guidance to practitioners in choosing the most appropriate anomaly detection approach for their specific environments and needs.
- Development of Security Products: This research can stimulate the development of more effective and efficient security products for IoT devices.
- Enhancement of IoT Security: The implementation of these research findings can enhance the security of the IoT ecosystem as a whole, reducing the risk of cyberattacks and protecting devices and sensitive data.
- Improved Decision-Making: The research findings can assist policymakers in making better decisions related to IoT security.

REFERENCES

[1] A. Amrullah, "A Review and Comparative Analysis of Intrusion Detection Systems for Edge Networks in IoT," *Intellithings J.*, vol. 1, no. 1, pp. 1–10, 2025, [Online]. Available: https://e-jurnal.unisda.ac.id/index.php/intellithings/article/view/8859

[2] R. Singh, A. Gehlot, and A. Joshi, "Review on Intrusion Detection in Edge Based IOT," in *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*, 2022, pp. 788–793. doi: 10.1109/IIHC55949.2022.10060587.

[3] 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.

[4] E. Fazeldehkordi and T.-M. Grønli, "A Survey of Security Architectures for Edge Computing-Based IoT," *IoT*, vol. 3, no. 3, pp. 332–365, 2022, doi: 10.3390/iot3030019.

[5] B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models," *Cyber Secur. Appl.*, vol. 3, p. 100068, 2025, doi: https://doi.org/10.1016/j.csa.2024.100068.

[6] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent Security Trends in Internet of Things: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 113292–113314, 2021, doi: 10.1109/ACCESS.2021.3103725.

[7] K. Dubey, R. Dubey, S. Panedy, and S. Kumar, "A Review of IoT Security: Machine Learning and Deep Learning Perspective," *Procedia Comput. Sci.*, vol. 235, pp. 335–346, 2024, doi: https://doi.org/10.1016/j.procs.2024.04.034.

[8] S. Szymoniak, J. Piątkowski, and M. Kurkowski, "Defense and Security Mechanisms in the Internet of Things: A Review," *Appl. Sci.*, vol. 15, no. 2, 2025, doi: 10.3390/app15020499.

[9] K. Cao, S. Hu, Y. Shi, A. W. Colombo, S. Karnouskos, and X. Li, "A Survey on Edge and Edge-Cloud Computing Assisted Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7806–7819, 2021, doi: 10.1109/TII.2021.3073066.

[10] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: A Review," *Informatics*, vol. 11, no. 4, 2024, doi: 10.3390/informatics11040071.

[11] M. BERHILI, O. CHAIEB, and M. BENABDELLAH, "Intrusion Detection Systems in IoT Based on Machine Learning: A state of the art," *Procedia Comput. Sci.*, vol. 251, pp. 99–107, 2024, doi: https://doi.org/10.1016/j.procs.2024.11.089.

[12] H. Liao *et al.*, "A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things," *IEEE Access*, vol. 12, no. January, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2023.3349287.

[13] E. Ortega, F. Su, R. Chattopadhyay, and K. Chakrabarty, "Discretized-Isolation Forest: Memory- and Compute-Efficient Unsupervised Anomaly Detection for Resource-Constrained Internet of Things Edge Devices," *IEEE Internet Things J.*, vol. 12, no. 2, pp. 1699–1717, 2025, doi: 10.1109/JIOT.2024.3468950.

[14] M. F. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael, "Detecting and classifying man-in-the-middle attacks in the private area network of smart grids," *Sustain. Energy, Grids Networks*, vol. 36, p. 101167, 2023, doi: https://doi.org/10.1016/j.segan.2023.101167.

[15] A. A. Elsaeidy, A. Jamalipour, and K. S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City," *IEEE Access*, vol. 9, pp. 154864–154875, 2021, doi: 10.1109/ACCESS.2021.3128701.

[16] D. Mehta, H. Suhagiya, H. Gandhi, M. Jha, P. Kanani, and A. Kore, "SQLIML: A Comprehensive Analysis for SQL Injection Detection Using Multiple Supervised and Unsupervised Learning Schemes," *SN Comput. Sci.*, vol. 4, no. 3, Mar. 2023, doi: 10.1007/s42979-022-01626-8.