



Paper Type: Original Article

EdgeGuard: Machine Learning for Proactive Intrusion Detection on Edge Networks

Zakaria Ahmed¹  and Sameh S. Askar^{2,*} 

¹ Department of Computer science, Faculty of Computer and Informatics, Zagazig University, 44519, Egypt; 20912019100575@fci.zu.edu.eg.

² Department of Statistics and Operations Research, College of Science, King Saud University, Riyadh 11451, Saudi Arabia; saskar@ksu.edu.sa.

Received: 01 Mar 2024

Revised: 15 May 2024

Accepted: 11 Jun 2024

Published: 14 Jun 2024

Abstract

Edge computing has emerged as a promising paradigm to address the challenges of latency-sensitive applications and the exponential growth of Internet of Things (IoT) devices. However, the distributed nature of edge networks introduces new security vulnerabilities, necessitating robust intrusion detection mechanisms. In this paper, we propose EdgeGuard, a machine learning-based framework for proactive intrusion detection on edge networks. Leveraging convolutional neural networks (CNNs) arranged in a residual fashion, EdgeGuard effectively captures complex patterns in network traffic data, enhancing the system's ability to detect intrusions with high accuracy. We conduct experiments using the Edge-IoTset Cyber Security Dataset, containing a diverse range of normal and attack traffic samples. The proposed method achieves promising results, as evidenced by the receiver operating characteristic area under the curve (ROCAUC) and confusion matrix analysis. EdgeGuard offers a robust solution to safeguard edge computing environments against cyber threats, contributing to the security and integrity of IoT systems in real-world deployment scenarios.

Keywords: Edge Computing, Intrusion Detection, Machine Learning, Proactive Security, IoT Security, Cybersecurity, Edge Networks, Real-Time Detection, Anomaly Detection.

1 | Introduction

The proliferation of Internet of Things (IoT) devices and the subsequent rise in edge computing have significantly transformed the digital landscape. Edge computing brings computational resources closer to the data source, reducing latency and enhancing real-time data processing capabilities [1-2]. However, this paradigm shift also introduces new security challenges. The decentralized and often resource-constrained nature of edge networks makes them particularly vulnerable to various cyber threats, necessitating robust and proactive intrusion detection mechanisms [3-5].

Intrusion detection systems (IDS) have long been a cornerstone of network security, designed to monitor and analyze network traffic for signs of malicious activity [6]. Traditional IDS solutions, however, are primarily tailored for centralized environments, such as data centers and cloud infrastructures, and may not be suitable for the dynamic and distributed nature of edge networks [7-8]. The unique characteristics of edge computing



Corresponding Author: saskar@ksu.edu.sa



<https://doi.org/10.61356/j.aics.2024.1297>



Licensee **Artificial Intelligence in Cybersecurity**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

demand innovative approaches that can effectively operate within these constraints while providing real-time and accurate threat detection.

In this context, machine learning (ML) emerges as a powerful tool for enhancing intrusion detection capabilities. ML algorithms can learn from vast amounts of data, identifying patterns and anomalies that may indicate security breaches. By leveraging the predictive power of ML, IDS can transition from reactive to proactive, anticipating and mitigating threats before they can cause significant harm [9-11].

This paper presents "EdgeGuard," a machine learning-based framework for proactive intrusion detection on edge networks. EdgeGuard is designed to address the specific challenges of edge computing environments, including limited computational resources, varying network conditions, and the need for real-time processing. The framework integrates advanced ML techniques to create a robust, adaptive, and efficient IDS tailored for edge networks.

2 | Background and Literature

This section provides a comprehensive overview of the foundational concepts essential to this study, including the architecture and operational principles of edge computing [12-15]. Recent advancements in edge computing and the increasing ubiquity of Internet of Things (IoT) devices have catalyzed significant research into securing these environments against various cyber threats. This section reviews key literature that addresses different aspects of intrusion detection systems (IDS) tailored for edge computing. Lin et al. [16] explore the challenge of fair resource allocation in IDS for edge computing, emphasizing the necessity to ensure the security of IoT devices. Their work in "Fair Resource Allocation in an Intrusion-Detection System for Edge Computing" provides a framework that balances security and resource usage, which is crucial given the limited computational capabilities of edge devices. Santhadevi and Janet [17] present EIDIMA, an edge-based intrusion detection system specifically designed to counter IoT malware attacks using decision tree-based boosting algorithms. Their approach, discussed in "EIDIMA: Edge-Based Intrusion Detection of IoT Malware Attacks," showcases the effectiveness of ensemble learning techniques in enhancing detection accuracy and speed in constrained environments.

Wazid et al. [18], in their study "RAD-EI: A Routing Attack Detection Scheme for Edge-Based Internet of Things Environment," introduce a scheme that targets routing attacks in IoT networks. This research highlights the importance of specialized detection mechanisms that can operate efficiently within the limited resources typical of edge-based systems. Mohy-eddine et al. [19] propose an ensemble learning-based approach for intrusion detection in Industrial IoT (IIoT) edge computing environments. Their study, "An Effective Intrusion Detection Approach Based on Ensemble Learning for IIoT Edge Computing," demonstrates significant improvements in detection rates by leveraging multiple learning algorithms to address diverse attack vectors. Kalnoor and Gowrishankar [20] investigate the application of intelligent IDS in IoT-based smart environments. Their work, titled "IoT-Based Smart Environment Using Intelligent Intrusion Detection System," explores how soft computing techniques can enhance the adaptability and robustness of IDS in dynamic IoT ecosystems.

Li et al. [21] present ADRIoT, an edge-assisted anomaly detection framework aimed at mitigating network attacks in IoT settings. In their paper, "ADRIoT: An Edge-Assisted Anomaly Detection Framework Against IoT-Based Network Attacks," they emphasize the critical role of edge computing in providing timely and accurate anomaly detection to safeguard IoT networks. Kumar et al. [22] address the detection of attacks on IP-based IoT deployments using intelligent edge computing techniques. Their research, discussed in "Intelligent Edge Detection of Attacks on IP-Based IoT Deployments," underscores the potential of integrating machine learning models directly on edge devices to enhance security measures. Aldaej et al. [23] explore deep learning-inspired IDS mechanisms for edge computing environments. Their study, "Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments," illustrates the application of deep learning models in identifying complex intrusion patterns, thus improving the resilience of IoT systems against sophisticated attacks.

Sha et al. [24] provide a comprehensive survey of edge computing-based designs for IoT security in their paper "A Survey of Edge Computing-Based Designs for IoT Security." This survey highlights various strategies and frameworks proposed to enhance the security of IoT networks through edge computing solutions. Tekin et al. [25] examine the energy consumption implications of on-device machine learning models for IoT intrusion detection. Their research, "Energy Consumption of On-Device Machine Learning Models for IoT Intrusion Detection," presents critical insights into the trade-offs between security and energy efficiency, which is paramount for battery-operated IoT devices. Lastly, Mohamed and Aydin [26] review various IoT-based intrusion detection systems in their paper "IoT-Based Intrusion Detection Systems: A Review." This review synthesizes current research trends and identifies emerging challenges and opportunities in the field, providing a comprehensive overview of the state-of-the-art in IoT IDS.

3 | Material and Method

In this section, we detail the materials and methodologies employed in the development and evaluation of EdgeGuard, our proposed machine learning-based intrusion detection system for edge networks. Our method leverages convolutional neural networks (CNNs) arranged in a residual fashion to effectively capture and analyze complex patterns in network traffic data, enhancing the system's ability to detect intrusions with high accuracy.

The core of EdgeGuard's intrusion detection capability is a CNN architecture enhanced with residual connections, inspired by ResNet models. Residual connections help mitigate the vanishing gradient problem and allow for deeper network architectures, improving feature extraction and model performance.

Let X represent the input data tensor, and $F(X)$ denote the output of a convolutional layer or a sequence of convolutional layers. In a traditional CNN, the output of each layer l is fed directly to the next layer $l + 1$. In contrast, our residual CNN architecture introduces a shortcut connection that adds the input X directly to the output of $F(X)$.

Mathematically, this can be expressed as:

$$Y = F(X) + X \quad (1)$$

where Y is the output of the residual block. This formulation allows the network to learn an identity mapping more easily, facilitating the training of deeper networks.

Each convolutional layer in our model is defined by a set of filters W and biases b . The operation of a convolutional layer can be expressed as:

$$F(X) = \sigma(W * X + b) \quad (2)$$

where $*$ denotes the convolution operation, and σ is an activation function, typically a Rectified Linear Unit (ReLU). The addition of the input X to the output $F(X)$ forms the residual connection. The residual blocks are repeated to form a deep network capable of capturing intricate patterns in the data. This architecture not only improves the network's ability to detect subtle anomalies indicative of intrusions but also enhances its generalization capabilities.

3.1 | Training and Optimization

The network is trained using a labeled dataset where each sample is categorized as normal or intrusive. The loss function used is the categorical cross-entropy, defined as:

$$L = -\sum y_i \log(\hat{y}_i) \quad (3)$$

where y_i is the true label, and \hat{y}_i is the predicted probability for class i . The model parameters are optimized using the Adam optimizer, which adjusts the learning rate adaptively to converge efficiently.

3.2 | Evaluation Metrics

To assess the performance of EdgeGuard, we employ several evaluation metrics, including accuracy, precision, recall, and F1-score. These metrics provide a comprehensive evaluation of the model's capability to correctly identify intrusions while minimizing false positives and false negatives.

4 | Results and Discussions

Our experiments are conducted using the Edge-IIoTset Cyber Security Dataset, a comprehensive dataset designed to evaluate intrusion detection systems in edge computing environments. The dataset comprises a total of 1,932,201 samples, categorized into both normal and various attack types. The distribution of the data is as follows: 1,615,643 samples are normal traffic, while the remaining 316,558 samples represent different types of attacks. These attacks include DDoS_UDP (121,568 samples), DDoS_ICMP (116,436 samples), SQL injection (51,203 samples), password attacks (50,153 samples), vulnerability scanner (50,110 samples), DDoS_TCP (50,062 samples), DDoS_HTTP (49,911 samples), uploading attacks (37,634 samples), backdoor attacks (24,862 samples), port scanning (22,564 samples), XSS attacks (15,915 samples), ransomware (10,925 samples), MITM attacks (1,214 samples), and fingerprinting (1,001 samples). This diverse dataset enables a thorough evaluation of EdgeGuard's performance across a wide range of cyber threats, ensuring its robustness and efficacy in detecting intrusions in real-world edge computing scenarios.

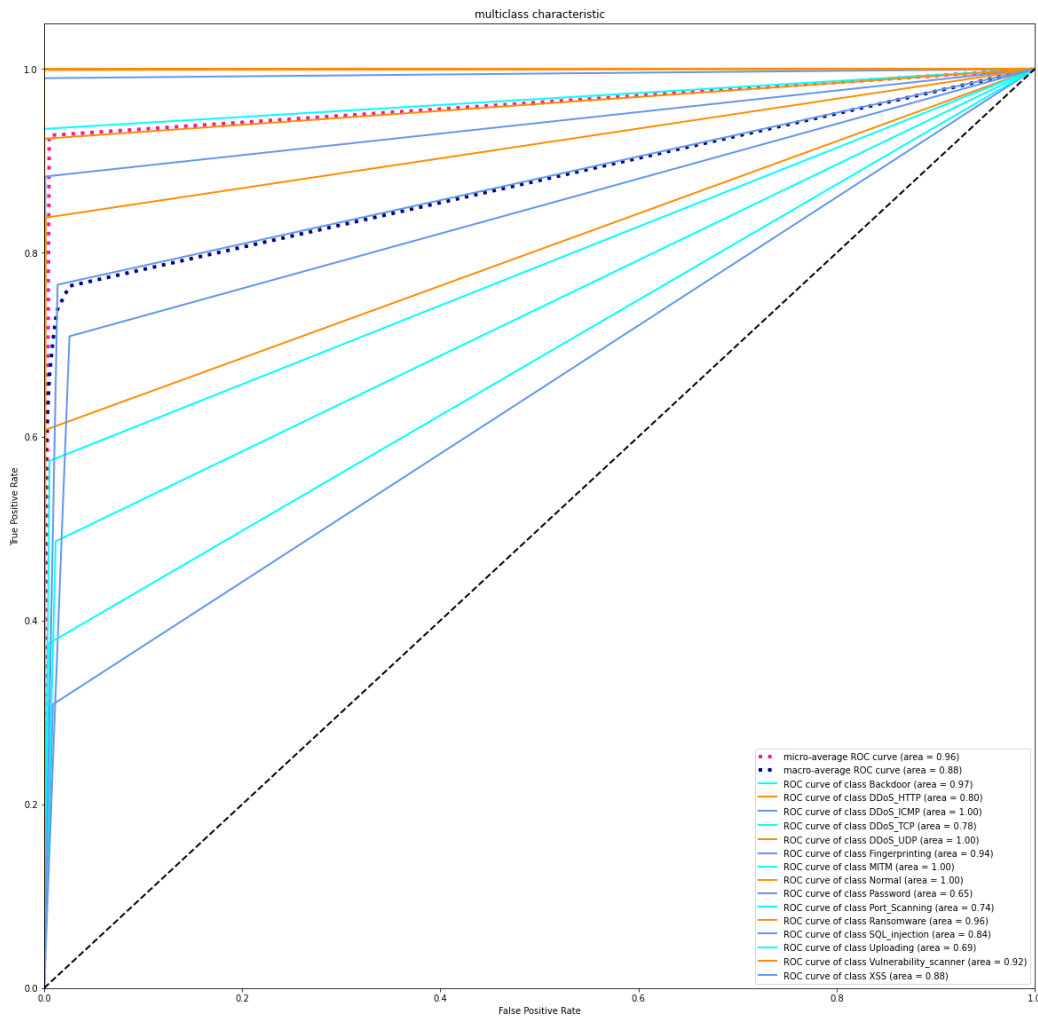


Figure 1. ROC curve of the proposed method.

The receiver operating characteristic area under the curve (ROCAUC) of our proposed method is illustrated in Figure 1. This graphical representation provides a comprehensive overview of the model's performance

across different threshold values, showcasing its ability to balance true positive and false positive rates effectively. A higher ROCAUC value indicates superior discriminative power and better overall performance of the intrusion detection system. By analyzing the ROC curve, we can assess the trade-off between sensitivity and specificity and determine the optimal operating point for the model. The ROCAUC metric serves as a reliable indicator of EdgeGuard's capability to accurately detect intrusions while minimizing false alarms, thus demonstrating its effectiveness in enhancing the security posture of edge computing environments.

The confusion matrix of our proposed method is depicted in Figure 2, providing a detailed breakdown of the model's classification performance across different classes of network traffic. This matrix enables a granular analysis of the true positive, false positive, true negative, and false negative predictions made by the intrusion detection system. By visually inspecting the confusion matrix, we can identify areas where the model excels in correctly classifying instances of normal traffic and various types of attacks, as well as areas where misclassifications occur. This comprehensive evaluation allows us to assess the model's strengths and weaknesses, understand its error patterns, and refine its performance through targeted optimization strategies.

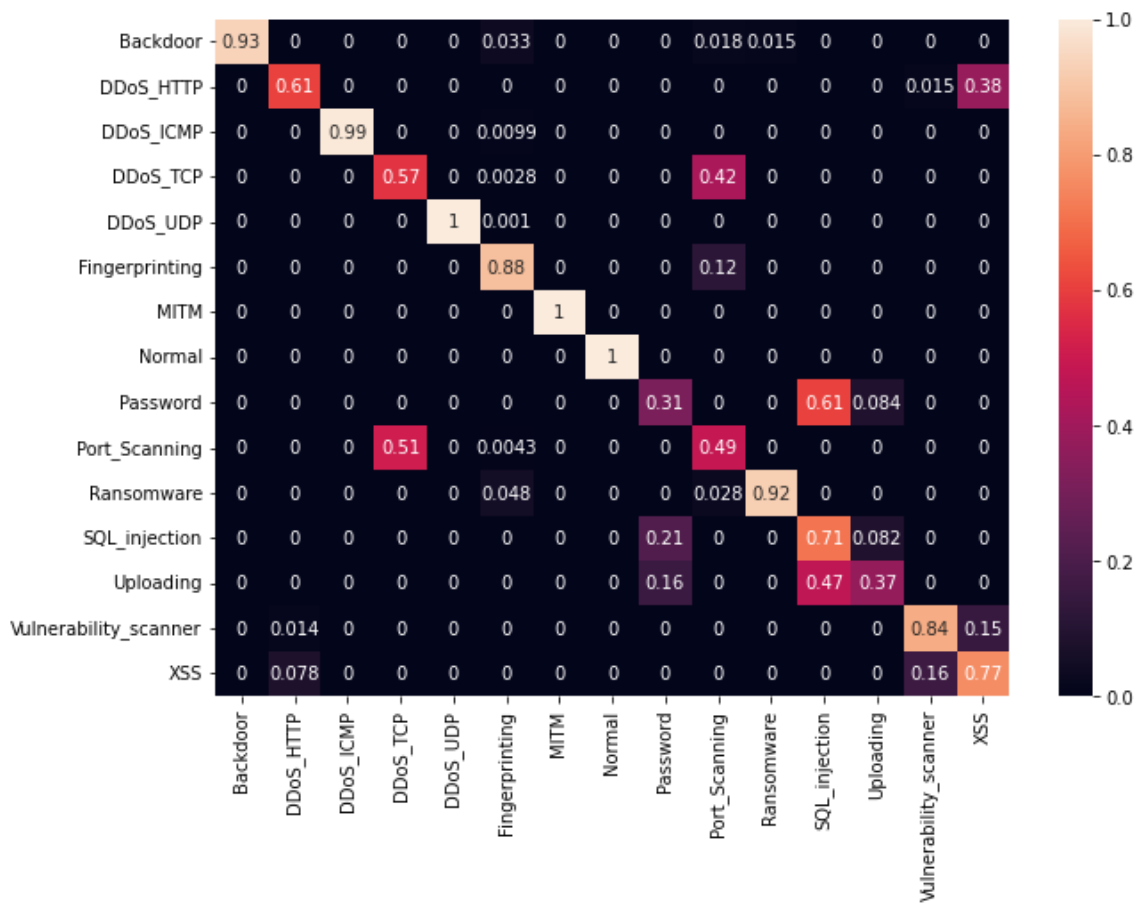


Figure 2. Confusion matrix of the proposed method.

5 | Conclusions

Our study introduces EdgeGuard, a machine learning-based intrusion detection system tailored for edge networks. Leveraging convolutional neural networks with residual connections, EdgeGuard demonstrates robust performance in accurately detecting intrusions amidst diverse network traffic types. Through comprehensive evaluations using the Edge-IIoTset Cyber Security Dataset, we showcase EdgeGuard's effectiveness in enhancing the security posture of edge computing environments. By addressing the unique challenges posed by edge networks and offering proactive threat detection capabilities, EdgeGuard represents a significant step towards safeguarding IoT ecosystems against evolving cyber threats, ultimately contributing to the resilience and integrity of edge computing infrastructures.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contribution

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

- [1] Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey. *Ad Hoc Networks*, 152, 103320. <https://doi.org/10.1016/j.adhoc.2023.103320>
- [2] Mudgerikar, A., Sharma, P., & Bertino, E. (2020). Edge-based intrusion detection for IoT devices. *ACM Transactions on Management Information Systems (TMIS)*, 11(4), 1–21.
- [3] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, 7(8), 6882–6897.
- [4] Aldaej, A., Ullah, I., Ahanger, T. A., & Atiquzzaman, M. (2024). Ensemble technique of intrusion detection for IoT-edge platform. *Scientific Reports*, 14(1), 11703.
- [5] Vimal, S., Suresh, A., Subbulakshmi, P., Pradeepa, S., & Kaliappan, M. (2020). Edge compu-ting-based intrusion detection system for smart cities development using IoT in urban areas. *Internet of Things in Smart Technologies for Sustainable Urban Development*, 219–237.
- [6] Yao, H., Gao, P., Zhang, P., Wang, J., Jiang, C., & Lu, L. (2019). Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection. *IEEE Network*, 33(5), 75–81.
- [7] Singh, A., Chatterjee, K., & Satapathy, S. C. (2022). An edge based hybrid intrusion detection framework for mobile edge computing. *Complex \& Intelligent Systems*, 8(5), 3719–3746.
- [8] Guezzaz, A., Azrou, M., Benkirane, S., Mohy-Eddine, M., Attou, H., & Douiba, M. (2022). A Lightweight Hybrid Intrusion Detection Framework using Machine Learning for Edge-Based IIoT Security. *Int. Arab J. Inf. Technol.*, 19(5), 822–830.
- [9] Shen, S., Cai, C., Li, Z., Shen, Y., Wu, G., & Yu, S. (2024). Deep Q-network-based heuristic intrusion detection against edge-based SIIoT zero-day attacks. *Applied Soft Computing*, 150, 111080.
- [10] Kaura, S., & Bhardwaj, D. (2022). A comprehensive review on intrusion detection in edge-based IoT using machine learning. *Intelligent Communication Technologies and Virtual Mobile Networks: Proceedings of ICICV 2022*, 615–624.
- [11] Hosseininoorbin, S., Layeghy, S., Sarhan, M., Jurdak, R., & Portmann, M. (2023). Exploring edge TPU for network intrusion detection in IoT. *Journal of Parallel and Distributed Computing*, 179, 104712.
- [12] Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J. P. C., & Park, Y. (2020). De-signing efficient sinkhole attack detection mechanism in edge-based IoT deployment. *Sensors*, 20(5), 1300.
- [13] Singh, R., Gehlot, A., & Joshi, A. (2022). Review on Intrusion Detection in Edge Based IOT. *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*, 788–793.

- [14] Mahadevappa, P., Muzammal, S. M., & Murugesan, R. K. (2021). A comparative analysis of machine learning algorithms for intrusion detection in edge-enabled IoT networks. *ArXiv Preprint ArXiv:2111.01383*.
- [15] Bilal, A., Hasany, S. M. N., & Pitafi, A. H. (2022). Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices. *IET Communications*, 16(8), 845–855.
- [16] Lin, F., Zhou, Y., An, X., You, I., & Choo, K.-K. R. (2018). Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of Internet of Things devices. *IEEE Consumer Electronics Magazine*, 7(6), 45–50.
- [17] Santhadevi, D., & Janet, B. (2022). EIDIMA: edge-based intrusion detection of IoT malware attacks using decision tree-based boosting algorithms. In *High Performance Computing and Networking: Select Proceedings of CHSN 2021* (pp. 449–459). Springer.
- [18] Wazid, M., Reshma Dsouza, P., Das, A. K., Bhat K, V., Kumar, N., & Rodrigues, J. J. P. C. (2019). RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment. *International Journal of Communication Systems*, 32(15), e4024.
- [19] Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2023). An effective intrusion detection approach based on ensemble learning for IIoT edge computing. *Journal of Computer Virology and Hacking Techniques*, 19(4), 469–481.
- [20] Kalnoor, G., & Gowrishankar, S. (2021). IoT-based smart environment using intelligent intrusion detection system. *Soft Computing*, 25(17), 11573–11588.
- [21] Li, R., Li, Q., Zhou, J., & Jiang, Y. (2021). ADRIoT: an edge-assisted anomaly detection framework against IoT-based network attacks. *IEEE Internet of Things Journal*, 9(13), 10576–10587.
- [22] Kumar, H., Jadhav, A. R., Sasirekha, G. V. K., Bapat, J., & Das, D. (2021). Intelligent edge detection of attacks on IP-based IoT deployments. *2021 19th OITS International Conference on Information Technology (OCIT)*, 132–137.
- [23] Aldaej, A., Ahanger, T. A., & Ullah, I. (2023). Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments. *Sensors*, 23(24), 9869.
- [24] Sha, K., Yang, T. A., Wei, W., & Davari, S. (2020). A survey of edge computing-based designs for IoT security. *Digital Communications and Networks*, 6(2), 195–202.
- [25] Tekin, N., Acar, A., Aris, A., Uluagac, A. S., & Gungor, V. C. (2023). Energy consumption of on-device machine learning models for IoT intrusion detection. *Internet of Things*, 21, 100670.
- [26] Mohamed, T. S., & Aydin, S. (2022). Iot-based intrusion detection systems: a review. *Smart Science*, 10(4), 265–282.

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.