International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0540
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3415-3417

AI-Enhanced Intrusion Detection System for IoT Edge Networks

Dr. Anuradha Patil[1], Arti Hilli[2], Bhagyashree Allagi[3], Mahadevi[4], Bhagyashree Hayyal[5]
[1]Associate Professor, Electronics and Communication Engineering, Sharanbasava University, Kalburgi, Karnataka, India.
[2,3,4,5]UG, Electronics and Communication Engineering, Sharanbasava University, Kalburgi, Karnataka
Emails: *anuradha.keshul@gmail.com[1], artikhilli027@gmail.com[2], bhagyacallagi@gmail.com[3], Somashekaranikeri@gmail.com[4], bhagyashreehayyal9447@gmail.com[5]*

Abstract
The Internet of Things (IoT) connects billions of smart devices, creating a highly dynamic environment that demands efficient and secure data communication. However, IoT edge networks are highly vulnerable to cyberattacks due to limited resources and diverse communication protocols. To address these challenges, this paper presents an AI-Enhanced Intrusion Detection System (IDS) for IoT edge networks that integrates artificial intelligence with edge computing to achieve real-time threat detection and response. The proposed system employs machine learning and deep learning algorithms to analyze network traffic, detect anomalies, and accurately predict potential intrusions while minimizing false positives. By processing data at the edge, the system ensures low latency, scalability, and energy efficiency, overcoming the limitations of traditional cloud-based IDS solutions. Experimental evaluations demonstrate that the AI-based IDS improves detection accuracy, adapts to evolving attack patterns, and enhances the overall security, reliability, and resilience of IoT infrastructures. This study emphasizes the transformative potential of AI in developing intelligent, adaptive, and future-ready cybersecurity frameworks for next-generation IoT ecosystems.

Keywords: *Internet of Things (IoT), Edge Computing, Intrusion Detection System (IDS), Artificial Intelligence (AI), Machine Learning, Cybersecurity, Anomaly Detection.*

1. Introduction
AI-enhanced intrusion detection system (IDS) for IoT edge networks uses machine learning to monitor network traffic, identify malicious activity, and adapt to new threats more effectively than traditional, rule-based systems. The "AI-enhanced" aspect means it uses techniques like deep learning to analyze large datasets, making it more accurate and able to handle complex, zero-day attacks without needing constant manual updates. The "IoT edge networks" focus is because this approach is crucial for securing the distributed, resource-constrained environment of the IoT at the network's edge, where processing data locally can reduce latency and bandwidth usage, shown in Table 1 [1-3].

2. Methodology
- **Dataset & Pre-processing:** Collect instruction-level IoT traffic $D = \{x_i, y_i\}$, remove duplicates/outliers: $D' = D -$ noise.
- **Data Cleaning:** Handle missing values using mean/median: $x_{ij} = \frac{\Sigma x_{ij}}{n}$ if $x_{ij} =$ null.
- **Categorical Encoding:** Convert categorical fields using One-Hot: $O_{ik} = 1$ if category $k$present else 0.
- **Feature Scaling & Selection:** Normalize using Min-Max: $x' = \frac{x - \min(x)}{\max(x) - \min(x)}$; select features with variance threshold $V(x) > t$.
- **Data Splitting & Model:** Split dataset into train/test: $D_{train}, D_{test} = D' \times (0.8, 0.2)$; train

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0540
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3415-3417

model $\hat{y} = f(x')$for edge-level instruction detection [4-7].

Table 1 Training Part of Data Set

Characteristics	Training part of data set	Testing part of dataset
Total records	1795575	575643
Normal records	1633190	530785
Attack records	162385	162385
Number of classes	10	15 (seven classes are different to training classes)

3. Results and Discussions

3.1 Result

This section provides a clear explanation of the suggested hybrid deep learning (DL) models for identification, along with specific details. The implementation and assessment of this method took place using the Jupyter Notebook program, which is an interactive integrated development environment (IDE) based on Python and included in the Anaconda package. The research utilized Keras, a deep learning framework built on Python. The hardware used consists of a Core i5 processor with 16 GB of RAM. For data analysis, it relies on the open-source library Pandas and the Python version 3.10.4 programming language. It also uses batch size, learning rate, and optimizer type to reduce the loss function effectively. With optimization techniques, it becomes easier to decrease the cost function while using minimal resources. After considering various options, this study selected the ADAM optimizer because it effectively maximizes categorical cross-entropy loss across multiple classes. For training purposes, 80% of the data is used, while the remaining 20% is reserved for testing [8-13].

3.2 Discussions

Superiority of AI/ML Models: The project results confirm that AI and machine learning techniques, especially deep learning models like CNN and LSTM, are more effective than traditional methods at detecting sophisticated and previously unknown (zero-day) attacks, due to their ability to learn and adapt to new patterns.

Benefits of Edge Deployment: Processing data locally at the edge enhances privacy and security by keeping sensitive data on-device and reduces bandwidth usage and transmission latency to the cloud.

Addressing Challenges: The report would discuss how specific methodologies addressed common changes. For instance, using contemporary data sets like CICIoT2023 was vital for training the models on relevant, real-word attack data [14-15].

Conclusion and Future Work

AI-powered Intrusion Detection Systems greatly boost the safety and dependability of IoT edge networks by offering smart, real-time threat detection near where the data is generated. These systems use machine learning, deep learning, and local computing to lower delays, increase detection precision, and adjust more effectively to changing cyber threats compared to standard IDS solutions. By processing data right at the edge, they reduce bandwidth consumption and improve privacy, while ongoing learning enables the system to identify new attack methods. In summary, AI-driven IDS provides a flexible, adaptable, and forward-thinking security approach that is crucial for safeguarding today's IoT environments.

Acknowledgements

I want to sincerely thank everyone who helped me finish my project called "AI-Enhanced Intrusion Detection System for IoT Edge Networks." I am very grateful to my guide for their helpful advice, positive feedback, and ongoing support, which

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0540
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3415-3417

made it easier for me to grasp the ideas and successfully complete this work. I also appreciate the department and institution for giving me the resources, facilities, and a supportive environment to learn. I extend my heartfelt thanks to my friends and classmates for their teamwork and encouragement during this project. Lastly, I want to thank my family for their unwavering support, understanding, and motivation, which inspired me to dedicate myself to completing this project.

References

[1]. 1.Saravanan, V. et al. IoT-based blockchain intrusion detection using optimized recurrent neural net-work. Multimedia Tools and Applications. 83(11), 31505–31526 (2024).

[2]. 2.Santhosh Kumar, S. V. N., Selvi, M. & Kannan, A. A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. Comput. Intell. Neurosci. 1, 8981988 (2023).

[3]. Ullah; Imtiaz; Qusay H. Mahmoud. An anomaly detection model for IoT networks based on flow and flag features using a feed-forward neural network. In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2022. 363–368.

[4]. Xue; Yu; Yiling Tong; Ferrante Neri. An ensemble of differential evolution and Adam for training feed-forward neural networks. Inf. Sci. 608, 453–471 (2022).

[5]. Jamal, B. et al. Machine learning-enabled internet of things (iot): Data, applications, and industry perspective. Electronics 11(17), 2676 (2022).

[6]. Khalid, A. et al. IoT intrusion detection using machine learning with a novel high performing feature selection method. Appl. Scie. 12(10), 5015 (2022).

[7]. Jie, Y. et al. Internet of things intrusion detection system based on convolutional neural network. Comput. Mater Contin. 75, 2119–2135 (2023)

[8]. Stefanos, T., Lagkas, T. & Rantos, K. Deep learning in IoT intrusion detection. J. Network Syst. Manag. 30(1), 8 (2022).

[9]. Muhammad, S. et al. Enhancing intrusion detection: a hybrid machine and deep learning approach. J. Cloud Comput. 13(1), 123 (2024).

[10]. Maghrabi; Louai, A. Automated Network Intrusion Detection for Internet of Things Security Enhancements. IEEE Access 2024.

[11]. Priyanka, S. et al. Feed-forward deep neural network (FFDNN)-based deep features for static malware detection. Int. J. Intell. Syst. 1, 9544481 (2023).

[12]. Almotairi, A., Atawneh, S. & Osama, A. Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. Syst. Sci. Control Eng. 12(1), 2321381 (2024).

[13]. Jing, Li. et al. Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning. J. Big Data 11(1), 36 (2024).

[14]. Asgharzadeh; Hossein; Ali Ghafiari; Mohammad Masdari; Farhad Soleimanian Gharehchopogh. An Intrusion Detection System on the Internet of things Using Deep Learning and Multi-objective Enhanced Gorilla Troops Optimizer. Journal of Bionic Engineering 2024, 1–27.

[15]. Campos; Alejandro Domínguez; Felipe Lemus-Prieto; José-Luis González-Sánchez; Andrés Caro Lindo. Intrusion detection on IoT environments through side-channel and Machine Learning techniques**.** IEEE Access 2024