Explainable Deep Learning Framework for IIoT Intrusion Detection Using CIC-IIoT 2025

Dr. Sagar Dhanraj Pande[1], Deepak Gupta[2]
[1]Post-Doctoral Researcher, Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia; [2] Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia
[2]Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India
Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia;
Email ID: [1]sagarpande30@gmail.com, [2]myself.deepakgupta@gmail.com

Abstract: The research tries to build a smart system that can detect cyber-attacks in industrial IoT networks. Conventional intrusion detection mechanisms do not cope with traffic of high dimensions and imbalance IIoT. In response to this problem, a deep learning-based framework combined with the hybrid nature-inspired optimization is established with the help of CIC-IIoT 2025 dataset. The optimization approach improves the choice of features and hyperparameter optimization, which boosts the detection and model generalization. Explainable Artificial Intelligence (XAI) methods are implemented to guarantee additional clear and understandable decision-making. The results of the experiment show better detection accuracy, equal precision and recall, and lower false alarm rates. The suggested system offers an optimized, scalable, and explainable cybersecurity system to the contemporary IIoT architectures.
Keywords: IIoT; Intrusion Detection System; Deep Learning; Hybrid Optimization; Explainable AI; DDoS Detection; Cybersecurity.

Introduction

The Industrial Internet of Things revolutionized the contemporary industries through the ability to smarten the manufacturing process, predictive maintenance, and real-time monitoring. Nevertheless, greater interconnection increases the cyber-attack area considerably, and industrial infrastructures become exposed to sophisticated threats. IIoT networks are unlike regular IT systems because of the heterogeneous architectures, specialized protocols, and real-time limitations. Their stratified nature presents several points of attack making it harder and harder to secure the environments. Furthermore, the IIoT traffic is both imbalanced and high-dimensional, and it is difficult to conduct accurate intrusion detection. Deep learning has demonstrated great potential in identifying sophisticated attack patterns. The CIC-IIoT 2025 dataset is useful with the creation of data-driven security models due to realistic industrial traffic. Nevertheless, deep learning models are hyperparameter sensitive and are also not easily interpretable. The challenges encourage the necessity of an optimized and explicable intrusion detection structure. The proposed innovation of this research is a hybrid optimization-based deep learning IDS with XAI, which will enhance the accuracy, robustness, and transparency of IIoT settings.

Related work

The previous works has already covered machine learning, deep learning, reinforcement learning, and software-defined networking in the detection of the IoT intrusion. Various studies enhance the precision of detection and flexibility whereas some are concentrated on lightweight models on constrained devices or real-time detection of DDoS. Some of the novel and efficient pre-existing proposed models are discussed here. Abinaya et al. [1] (2025) concentrated on the increase in the level of network security of IoT sensors by improving intrusion detection protocols. The central focus of their work lies in reinforcing the IDS structures to deal with the changing cyber threats while taking into account the scanty computational power of the IoT devices. The paper presents the best deployment practices to enhance detection performance without adversely affecting the network performance. Ren et al. [2] (2024) introduced a dynamic reward-based deep reinforcement learning technique to detect intrusion of the IoT. Their model responds to evolving patterns of attacks with the reward mechanism which enables them to learn continuously and improve their detection accuracy. The strategy adds flexibility to the very dynamic IoT network settings. Bolat-Akca and Bozkaya [3] (2023) proposed a software-defined intrusion detection model to IoT edge network DDoS attacks. Their system combines Software-Defined Networking (SDN) and IDS to allow centralized monitoring and control of rules to enhance response time and scalability to distributed IoT infrastructures. Singh et al. [4] (2021) created a multi-classifier intrusion detection system based on the deep learning method of IoT cyberattacks. Their strategy uses multiple classifiers to make the system robust and increase detection rates in various types of attacks and their performance is better than that of a single model system. Ariffin et al. [5] (2021) examined local IDS rules configuration on a software-defined IoT testbed.

Research Gap

The current intrusion detection systems are mainly aimed at enhancing the accuracy of detection. Nevertheless, there are not many methods that integrate the hybrid optimization of the feature selection and hyperparameter optimization with explainable AI methods. Also, the current IIoT data is not fully used to develop scalable and generalized frameworks. Hence, a more optimized and understandable IIoT-specific IDS is yet to be obtained.

Key Contributions

The following contributions can be made by this study:

- Suggests a combined optimization-inspired deep learning architecture to IIoT intrusion detection.
- Incorporates nature-inspired optimization in order to optimize feature selection as well as hyperparameter optimisation.
- Uses Explainable AI to give rise to transparent decision-making.
- Analyses the framework based on the latest CIC-IIoT 2025 data to test the framework in realistic industry settings.

Proposed Methodology

The suggested framework combines data preprocessing, feature optimization, deep learning classification, hybrid hyperparameter tuning and explainability analysis. The CIC-IIoT 2025 data is scaled,

normalized, and cleaned to manage a large number of dimensions and imbalance in the number of classes. Hybrid nature-based optimization is used to enhance the optimization of features and parameter settings. The optimised features are imported into a highly trained neural network with the ability to identify various patterns of DDoS attacks. The interpretable AI methods are applied to explain model predictions and the features that the model is impacted by. Accuracy, precision, recall, F1-score are used to evaluate the performance. The framework will be able to provide industrial cybersecurity of high strength, scalability, and energy efficiency. The proposed model framework in detail is presented in the figure 1.

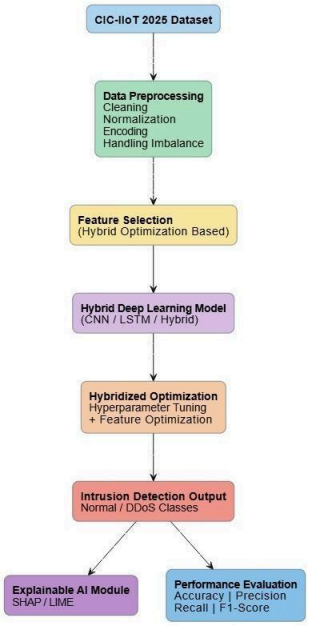

Figure 1: Explainable Deep Learning Framework for IIoT Intrusion Detection

Research Objectives

- Determine gaps in research in IIoT intrusion detection.
- Create a deep learning hybrid model that is highly optimized.
- Carry out comparative analysis with prevailing techniques.
- Bring more transparency with the help of explainable AI.

Results and Discussion

The framework was tested on CIC-IIoT 2025 data of several types of the DDoS attacks. The proposed models were made to be more precise and accurate and had high recall, F1-score, and low false alarm when compared to the baseline techniques. The speed of convergence and the generalization capability was improved through using hybrid optimization. The XAI analysis also aided the interpretation of the model decisions indicating that it was network feature interpretable and meaningful. The results confirm that IIoT intrusion detection performance can be enhanced with the help of the combination of deep learning, hybrid optimization, and explainability.

Conclusion

This work described a simplified and clear intrusion detection framework of IIoT . The hybrid optimization and the novel deep learning model improved the precision of detection and false alarms were reduced

and XAI offered transparency and trust. The given system is a scalable, resilient, and explainable cybersecurity platform that can be utilized in protecting the industrial infrastructures of the Internet of Things presently modern.

References

1. K. Abinaya, T. Lohith and S. J. Kumar, "Enhancing Network Security with Intrusion Detection Systems in IoT Devices," 2025 5th International Conference on Expert Clouds and Applications (ICOECA), Bengaluru, India, 2025, pp. 320-325, doi: 10.1109/ICOECA66273.2025.00062.
2. K. Ren, L. Liu, H. Bai and Y. Wen, "A Dynamic Reward-Based Deep Reinforcement Learning for IoT Intrusion Detection," 2024 2nd International Conference on Intelligent Communication and Networking (ICN), Shenyang, China, 2024, pp. 110-114, doi: 10.1109/ICN64251.2024.10865958.
3. B. Bolat-Akça and E. Bozkaya, "Software-Defined Intrusion Detection System for DDoS Attacks in IoT Edge Networks," 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Abu Dhabi, United Arab Emirates, 2023, pp. 0672-0677, doi: 10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361494.
4. S. Singh, S. V. Fernandes, V. Padmanabha and P. Rubini, "MCIDS-Multi Classifier Intrusion Detection system for IoT Cyber Attack using Deep Learning algorithm," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 354-360, doi: 10.1109/ICICV50876.2021.9388579.
5. S. H. S. Ariffin, C. J. Le and N. H. A. Wahab, "Configuring Local Rule of Intrusion Detection System in Software Defined IoT Testbed," 2021 26th IEEE Asia-Pacific Conference on Communications (APCC), Kuala Lumpur, Malaysia, 2021, pp. 298-303, doi: 10.1109/APCC49754.2021.9609824.
6. L. C. Perry and K. Pious, "Dynamic Synchronization and Adaptive Port Adjustment (DSAPA): A Novel Algorithm for Preventing DDoS Attacks in IoT Networks," 2025 IEEE 11th World Forum on Internet of Things (WF-IoT), Chengdu, China, 2025, pp. 1-3, doi: 10.1109/WF-IoT64238.2025.11270744.
7. K. Garg, K. S. Gill, R. Chauhan, D. Rawat and D. Banerjee, "Distributed Denial of Services (DDoS) Botnet Attack Prevention in Internet of Things (IoT) Devices Using AI," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10442302.
8. B. Pahilajani et al., "Lightweight Intrusion Detection System on IoT Devices Using Machine Learning Techniques," 2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida NCR, India, 2025, pp. 1-5, doi: 10.1109/ICRITO66076.2025.11241861.
9. E. Aydın and Ş. Bahtiyar, "OCIDS: An Online CNN-Based Network Intrusion Detection System for DDoS Attacks with IoT Botnets," 2021 14th International Conference on Security of Information and Networks (SIN), Edinburgh, United Kingdom, 2021, pp. 1-8, doi: 10.1109/SIN54109.2021.9699288.
10. A. Sharma and H. Babbar, "Guarding Against IoT Threats: An Analysis of Intrusion Detection with the Kitsune Attack Dataset," 2024 4th International Conference on Technological Advancements

in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2024, pp. 637-641, doi: 10.1109/ICTACS62700.2024.10840935.