International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 7 Issue 1 PP 180-187, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I1P124

Original Article

AI-Driven Intrusion Detection in Internet of Things Networks Using the Edge-IIoTset Dataset

Sandeep Gupta
SATI, Vidisha.

Received On: 08/01/2025 ***Revised On: 10/02/2026*** ***Accepted On: 15/02/2026*** ***Published On: 18/02/2026***

Abstract *- Network Intrusion Detection System (NIDS) is an essential tool in securing cyberspace from a variety of security risks and unknown cyberattacks. A number of solutions have been implemented for Machine Learning (ML), and Deep Learning (DL) based NIDS. In this paper, a deep learning-based multi-class intrusion detection model is introduced on the Edge-IIoTset dataset that includes realistic IIoT network traffic and attack variants. The dataset was preprocessed through feature refinement, categorical encoding, robust scaling, and imbalance handling to enhance model reliability. Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) were implemented and evaluated in terms of stratified 5-fold cross-validation. Experiments prove that the suggested LSTM model is much more effective than CNN and some traditional machine learning methods, and it has an accuracy of 99.96 with close-to-perfect precision, recall, and F1-score. The analyses of confusion matrix and ROC curve also reinforce the high discriminatory power of the model in all attack classes, such as DDoS, Injection, Malware, and Information Gathering. The results indicate the success of sequential deep learning to model intricate traffic patterns in IIoT systems. The study provides a very dependable and scalable intrusion detection system that can be applicable in IIoT cybersecurity in practice.*

Keywords *- Industrial Internet of Things (IIoT), Cybersecurity, Intrusion Detection System (IDS), IoT devices, Deep Learning.*

1. Introduction

In the ever-evolving field of information technology, the Internet of Things (IoT) has emerged as a groundbreaking innovation, integrating everyday objects into the Internet, making our environment more interactive and automated. n everyday life, IoT devices play a crucial role in people's lives. However, the extensive connectivity of these devices to the internet exposes them to various security risks [1]. For example, IoT devices exchange information over the internet and are susceptible to numerous network attacks, compromising their security [2]. Intrusion detection systems (IDSs) play a crucial role in protecting computer systems by detecting and responding to malicious activities [3][4]. They continuously monitor networks to identify abnormal behaviors or potential attacks, thereby maintaining the integrity, confidentiality, and availability of systems . Traditional IDS methods, designed for standard networks, face major challenges in diverse IoT networks [5][6]. Their lack of flexibility regarding the variety of IoT devices and protocols reduces their effectiveness [7]. Additionally, their inability to process large volumes of data leads to performance and scalability issues. Traditional IDSs also struggle to differentiate legitimate behaviors from malicious ones in varied IoT traffic patterns, thus increasing the risk of errors [8].

In response to these limitations, machine learning has emerged as a promising solution capable of adapting and responding to complex and evolving threats in the IoT environment [9][10]. Machine learning-based IDSs can learn from historical data to detect abnormal behaviors, offering an enhanced ability to identify new and unknown attacks [11][12]. This work is motivated by the need to create a smart and very precise intrusion detection framework that can surmount the shortcomings of conventional IDS methods within complex IoT/IIoT settings. With the dynamism of Internet of Things traffic, high data loads, and the growing variety of cyberattacks, traditional solutions do not allow to ensure high-quality and scalable security. Hence, the proposed study suggests the deep learning-based technique, which is able to memorize the complicated traffic patterns, enhance the performance of multi-class attack detectors, and enhance the overall security system reliability and stability of the IoT networks.

This study makes several significant contributions to the field of IIoT cybersecurity:

- The study ensures fair and robust performance assessment through stratified cross-validation and class imbalance handling, improving detection reliability across all attack categories.
- The framework is designed to support large-scale IIoT environments, making it suitable for deployment in real-world industrial cybersecurity systems.
- A detailed comparative evaluation against NB, DT, existing models demonstrates the clear superiority and robustness of the proposed approach.
- Confusion matrix and multi-class ROC curve analyses confirm the strong discriminative capability and minimal misclassification rate of the proposed model.
- The findings provide empirical evidence that sequential deep learning architectures are highly

effective for capturing complex temporal traffic patterns in IIoT networks, advancing state-of-the-art intrusion detection research.

This study is justified by the fact that the number of cyber threats is increasing in the IoT/IIoT networks. Basic machine learning and traditional IDS is not particularly helpful at detecting multi-class attacks. They also have problem with high dimensional and skewed traffic data. Thus, a deeper and more powerful deep learning solution is needed. The originality of this work is based on the creation of a high-performance LSTM-based multi-class intrusion detection model on the basis of the Edge-IIoTset data set. The suggested model has almost perfect detection performance and it works better than a number of traditional and hybrid models. It is very efficient in tracking the temporal traffic trends and marks a new standard of IIoT intrusion detection precision.

The rest of the paper is organized as follows. Section II briefly reviews IDS solutions for IoT and IIoT environments. Section III describes the research methods used in paper. Section IV present experimental setup, results, and discussions. Finally, Section V concludes work and maps out directions for future work.

2. Literature Review

The literature is vast with studies on data-driven IDSs using different data analytics algorithms. Due to limited space, we briefly review a few of the most relevant studies to provide an insightful overview of the state of the art in this research area.

Chauhan *et al.*, (2026) examines and compares the Graph Attention Networks (GAT) and Transformers architectures to check how well they handle a range of intrusion examples. The dataset for IoT traffic analysis was processed by engineering features, applying normalization and using SMOTE to address uneven classes. Topological relationships between nodes on the network were modeled through the GAT which gave a peak accuracy of 80.25%. The Transformer, using attention mechanisms for sequential data, performed at 60.10%. The study supports cybersecurity by detecting major IoT threats and provides useful suggestions for dealing with infrequent and emerging cyberattacks [13].

Chowdhury *et al.*, (2025) presents a Distributed Intrusion Detection System (DIDS) based on Federated Learning (FL) to enhance security in EoT environments. We use the UNSW-NB15 dataset for network intrusion detection to evaluate FL against Centralized Learning (CL) models. The experimental results show that FL outperforms CL with a test accuracy of 91.67% against 88.17%, confirming its potential towards secure, decentralized, and scalable intrusion detection in EoT networks [14].

Tezcan and Karahan, (2025) focuses on attack detection in Internet of Things (IoT) environments using the CICIoT2023 dataset. Base classifiers included XGBoost (XGB), Random Forest (RF), and LightGBM (LGBM). In hybrid structures, binary integrations such as XGB + RF, RF + LGBM, and LGBM + XGB were created. Among these, the XGB + RF model achieved the highest performance, achieving 96.55% accuracy and a macro F1 score of 0.8828. Furthermore, the effect of extracting highly correlated features on detection accuracy was investigated [15].

Sharma and Babbar, (2024) Utilising characteristics taken from network traffic data, investigate how well-supervised learning algorithms like SVM, Random Forest (RF), LR, and K-Nearest Neighbours (KNN) perform. Each algorithm's detection performance has been assessed using metrics including accuracy, precision, recall, and F1-score. The results show that, at 98.99%, the LR model has the highest accuracy. On the other side, the accuracy rates of the KNN, SVM and RF models are 79.42%, 92.75%, and 97.98%, respectively [16].

Chhetry *et al.*, (2024) presents a novel approach to enhancing reconnaissance detection in IoT by integrating Machine Learning (ML) techniques with heterogeneous data sources. Our ML-based model, trained on this integrated dataset, demonstrates a detection accuracy of 96%, highlighting its potential as a scalable, effective, and real-time intrusion detection solution across diverse IoT environments[17].

Sujatha *et al.*, (2023) employs a deep feed-forward neural network method and reinforcement learning, which is based on Q- learning. In order to detect various sorts of intrusions in the network using an automated trial- and-error method and continually improve its detection skills, the Deep Q-Learning (DQL) model is proposed. The accuracy of the model proposed is 91.4%, while the accuracy of other self-taught learning models is 88.4% and it is a similar case for recall rate and precision as well which are 90.2% and 92.8%[18].

Almutairi and Abdulghani Alshargabi, (2022) an RNN deep learning algorithm is proposed to introduce a model for intrusion detection within the IoT environment. The NSL-KDD dataset is used to train and test the proposed model. The introduced solution achieved a good accuracy of 87%. In future work, we plan to use optimization algorithms to improve the detection accuracy of our model [19].

2.1. Research Gap

According to available literature, there has been positive developments in the IoT intrusion detection application of deep and machine learning models including GAT, Transformer, FL, hybrid ensembles, and reinforcement learning. Nevertheless, there are still a number of gaps. The vast majority of models are based on small datasets, such as CICIoT2023, UNSW-NB15, or NSL-KDD, which decreases extrapolation to actual IoT environments. Cross-domain adaptability and scalability to real-time detection is not mentioned in many works. Little research studies unite space and time or multi-source data. Low-power IoT devices are also under-researched in terms of privacy, model explainability, and energy-efficiency. Therefore, lightweight,

interpretable, and strong frameworks are needed that can be adapted to variable and heterogeneous IoT settings.

3. Methodology

figure 1 provides a description of the end-to-end process in the analysis of the Edge-IIoTset data. It starts with data collection and exploratory analysis then it moves to preprocessing stages like encoding, scaling, and feature selection. This data is then divided into training and test set with ADASYN used to balance it. The proposed models (such as LSTM and CNN) are trained and tested on such customary metrics as accuracy, precision, recall, F1-score, and ROC. Lastly, the models are compared to estimate overall effectiveness to provide a framework of work in intrusion detection research.

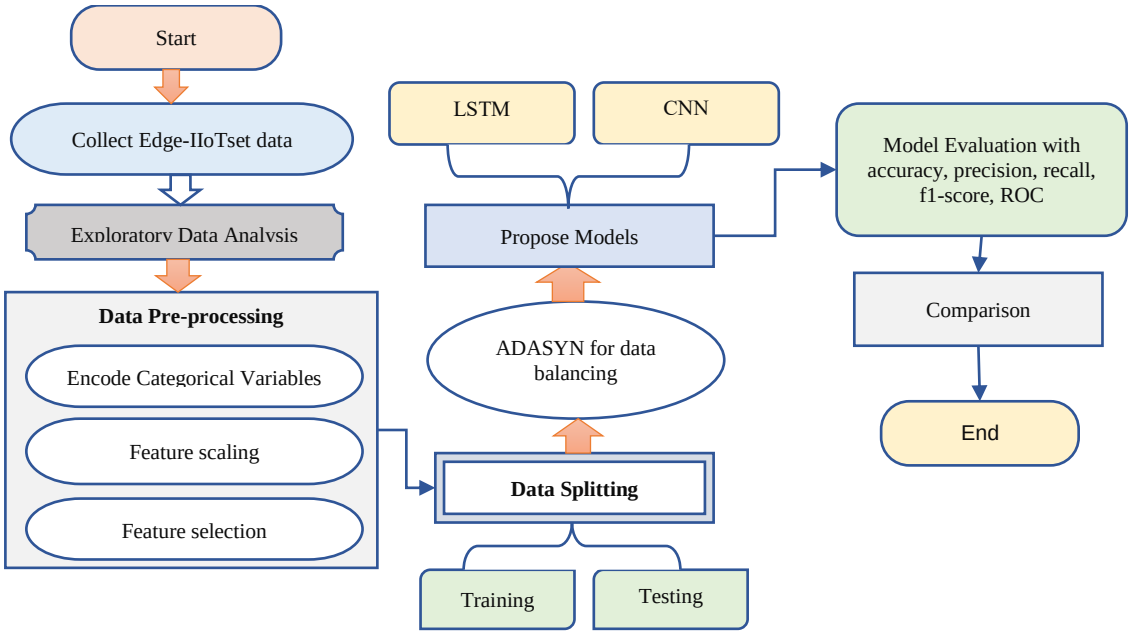

Fig 1: Propose flowchart for Intrusion Detection in Internet of Things Networks

3.1. Data Collection

The Edge-IIoTset Dataset, utilised in this study, was originally developed of realistic IIoT environments. This large-scale dataset captures a wide array of interactions and cyberattacks from November 21, 2021, to January 10, 2022. It was initially comprised of 1176 features, distilled down to 61 high-correlation features to improve manageability and relevance for effective cyberattack detection. The below figure represent the attack category.

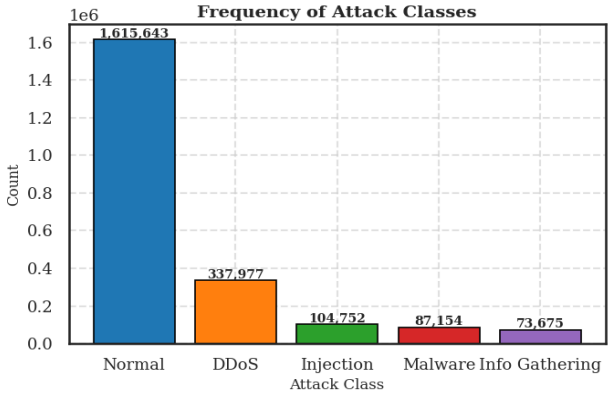

Fig 2: Bar Graph for Attack Class Distribution

Fig. 2 shows the distribution of the instances in five attack types in the dataset. There is a large imbalance of classes with the highest one of 1,615,643 records, which is the Normal class. DDoS attacks are the most common category of attacks with 337,977 cases and then come Injection, Malware and Information Gathering. The graph clearly shows that normal traffic is dominating over the attack classes, and it is important to balance the data properly during model training to provide the accurate and objective classification performance.

Figure 3 illustrates a heatmap of the correlation between the chosen features of the Edge-IIoTset dataset. The cells indicate the direction and the strength of the connection between two features with the blue color denoting a negative connection and red color denoting a positive connection. The visualization is useful to determine the dependence, redundancy and possible feature interactions and aid in more knowledgeable feature choice and enhance the usability of detection patterns in intrusion detection.

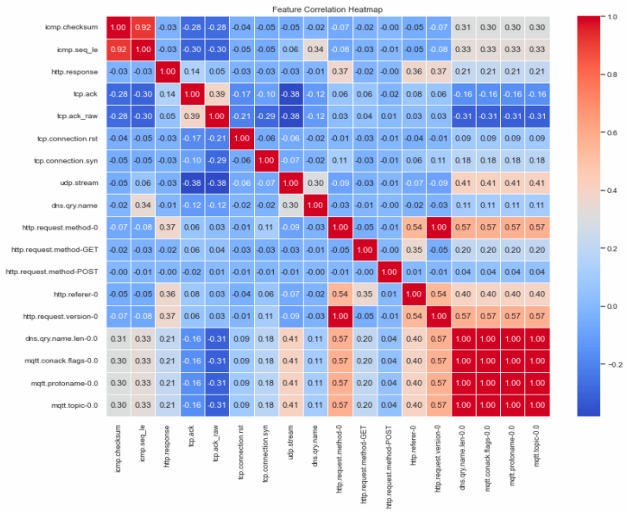

Fig 3: Feature-related correlation Matrix

3.2. Data pre-processing

The dataset is pre-processed prior to using the ML models in an attempt to enhance the accuracy and efficiency of the models. Different types of attacks except DDoS and normal traffic were blocked and the only classes left were normal and DDoS (HTTP, ICMP, TCP, and UDP). Out of the 63 initial features, 15 irrelevant columns have been eliminated. The duplication of records were also filtered out to make clean and memory efficient data to develop the model. The list of other pre-processing steps are given in below:

3.3. One-hot Encoding

The dataset includes categorical variables such as communication protocols (e.g., TCP, UDP), services, and device types. These variables have no inherent ordinal relationship, so we employ one-hot encoding to convert them into binary vectors. Each unique category becomes a separate binary feature, ensuring that no artificial ordering is introduced.

3.4. Feature Scaling

To ensure uniform feature scaling and reduce the impact of outliers, apply the Robust Scaler technique. Unlike standard normalization methods that use mean and standard deviation, the Robust Scaler leverages the interquartile range (IQR), which is more resilient to skewed distributions and extreme values. The transformation is defined as Equation (1):

$$x' = \frac{x - Q_2}{Q_3 - Q_1} \qquad (1)$$

Where Q_1, Q_2, and Q_3 denote the first (25th percentile), second (median), and third (75th percentile) quartiles, respectively. This operation centers the data around the median and scales it according to the IQR, improving the stability of learning algorithms sensitive to feature scales.

3.5. Feature selection

The Random Forest algorithm was employed due to its efficacy in handling high-dimensional data and its robustness against overfitting, which is particularly beneficial in analysing complex datasets with a large number of features. This approach not only helped in determining the most influential features but also in enhancing the overall interpretability of our model's predictions. The selected features significantly improve the predictive accuracy of the models tested, including our proposed algorithm.

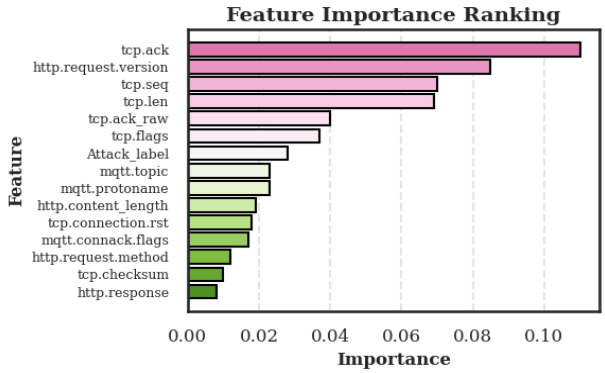

Fig 4: Graph for Feature Importance Score

Figure 4 shows the proportion of the various features in the dataset that contribute to model predictions. Such features as TCP acknowledgments, HTTP request version, attributes of sequence become the most influential, whereas the others, like checksum and response fields, are less affected. The ranking allows identifying the most influential features with the purpose of successful feature selection. The visualization further demonstrates that effective features cut across several protocol layers, which is indicative of the richness of network traffic. In general, it offers a distinctive foundation to prioritise features that improve the intrusion detection performance.

3.6. Data Splitting

A stratified 5-fold cross-validation strategy was applied to each dataset to ensure reliable evaluation, preserving the original class distribution across training and validation splits. This approach provides a measure of generalization, particularly in imbalanced data scenarios typical of IIoT environments.

3.7. ADASYN for Imbalance Handling

ADASYN is an adaptive synthetic oversampling technique based on SMOTE principles. ADASYN focuses on creating synthetic samples for minority class instances that are more difficult to learn. The identification of minority samples that pose challenges for neural network training is of interest to us. Therefore, ADASYN was selected as the method to balance the dataset. After oversampling the minority classes with ADASYN, Figure 5 depicts the updated distribution of the attack categories.

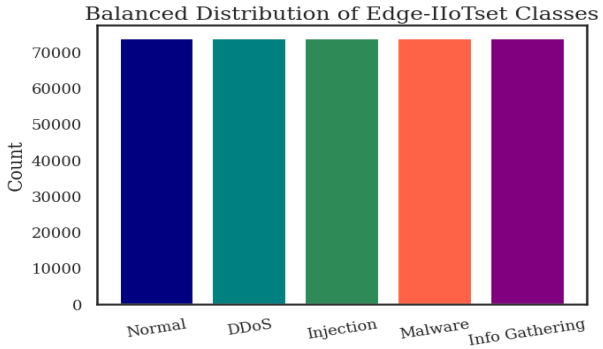

Fig 5: Bar graph for Balance class Distribution

The classes are resampled to obtain an equal representation giving the trainings and evaluation a fair chance. Such a moderate perspective shows that the class adjustment would reduce bias effects of dominant categories and enable more accurate performance evaluation of intrusion detection models.

3.8. Convolutional Neural Network (CNN)

Convolutional Neural Network (CNN) model was created to automatically obtain discriminative variables in IIoT network traffic data and classify multi-class attacks. The architecture is built of convolutional feature extraction layers that are followed with pooling dimensionality and capture dominant pattern layers and fully connected dense layers that are used to make the final classification. ReLU activation functions were employed to add non-linearity and a Softmax layer was utilized in the output layer to predict many classes. The model was trained in 25 epochs with Adam optimizer and a learning rate of 0.01 and Binary Cross-Entropy loss function. The batch size was set to 256 to compromise between computational efficiency and stability of learning. To provide a strong performance evaluation, stratified 5-fold cross-validation was used.

3.9. Deep learning LSTM model

An LSTM network is a type of recurrent neural network that uses LSTM cell blocks instead of traditional neural network layers. The input gate, forget gate, and output gate is three components of these cells. In a neural network, a dense layer is simply a regular layer of neurons. Each neuron in the previous layer receives information from all the neurons in the layer above it, making it tightly linked. A weight matrix W, a bias vector b, and the activations of the previous layer make up this layer. The model has been trained for 25 epochs. Also, the Binary CrossEntropy loss function has been implemented and an Adam optimizer is used to upgrade the weights. The learning rate is selected as 0.01. The batch size is set to 256. Whereas the embedding size is 100. To enhance the accuracy of our model, we have reduced the batch size. The proposed model has 168,769 trainable parameters. The layer of LSTM model are shows in Table 1.

Table 1: LSTM Layered Architecture

Layer (type)	Output size	Param number
Embedding_1 (embedding)	300 x 100	1,000,000
Lstm_1 (LSTM)	300 x 128	117,248
Lstm_2 (LSTM)	64	49,408
Dense_1 (Dense)	32	2080
Dense_2 (Dense)	1	33

3.10. Evaluation Criteria

The proposed classifier repeatedly trained on the training data, and prediction results on the test data have been summarized using several confusion-matrix-based metrics, namely accuracy, precision, recall, F1 score, and false negative rate (FNR). Mathematically, the metrics can be represented by Equations (2)–(5), respectively.

$$ACC = TP + TN/TP + TN + FP + FN \quad (2)$$

$$Pre = TP/TP + FP \quad (3)$$

$$Rec = TP/TP + FN \quad (4)$$

$$F1 = 2 * Precision * Recall/Precision + Recall \quad (5)$$

Where TP, FP, TN, and FN are the number of true positives, the number of false positives, the number of true negatives, and the number of false negatives, respectively. The measure of accuracy assesses the percentage of accurately classified instances. Precision (or positive prediction value) refers to the proportion of correct positive predictions out of all positive predictions made by the model, while recall value (or true positive rate or sensitivity) and FNR pertain to the ability of the trained model to accurately identify all the positive instances. The F1 score combines recall and precision and gives the number of times a correct prediction was made by the model. The AUC score measures the area under the ROC curve and represents the ability of the model to distinguish between classes.

4. Results and Discussion

All experiments were performed on a personal laptop equipped with an Intel(R) 11-th Gen Core(TM) i7–1165G7 processor, rated at 2.80 GHz, with 4 cores, 8 logical processors, 4 GB of RAM, and a 64-bit Windows OS. In this study, the computational analysis is conducted using Google Colab, a cloud-based platform that offers Python 3 backend support. Table II indicates the comparison of the performance of the proposed CNN and LSTM models. CNN model performed reasonably well in classification with a score of 97.15 and F1-score of 96.40 which is a good predictor. Conversely, the LSTM model showed to be stronger than CNN and was able to achieve an accuracy of 99.96 with an almost perfect F1-score. This demonstrates that LSTM is better in its overall performance than CNN on the specified dataset.

Table 2: Experiment Results of Propose Models

Model	Accuracy	Precision	Recall	F1- Score
CNN	97.15	96.23	97.10	96.40
LSTM	99.96	99.96	99.99	99.99

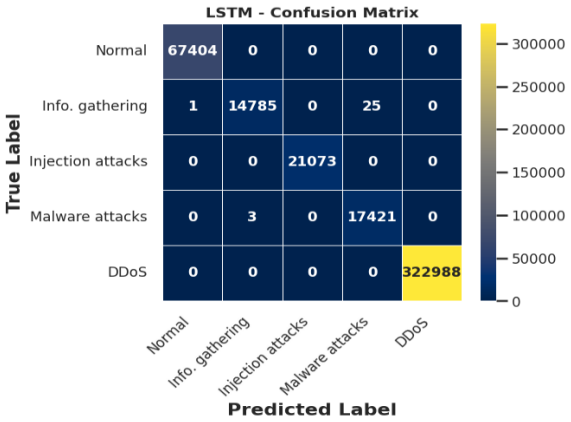

Fig 6: Confusion Matrix of LSTM Models

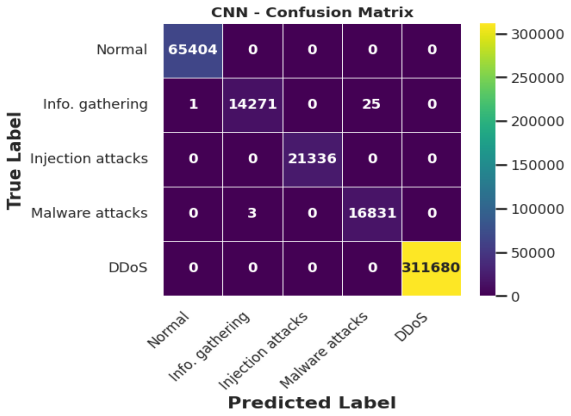

Fig 7: Confusion Matrix Of CNN Models

Figure 6 shows the performance of the LSTM model in classifying the types of attacks. As indicated by the matrix, most of the samples are classified correctly along the diagonal meaning that the model is very accurate. To be more specific, 67,404 Normal, 14,785 Information Gathering, 21,073 Injection Attack, 17,421 Malware Attack, and 322,988 DDoS were all properly predicted. There are not many misclassifications with a small number of Information Gathering samples wrongly predicted as Normal (1) and Malware Attacks (25) and 3 Malware samples misclassified. The DDoS type is notably the most successful where there is no misclassification. The confusion matrix in general demonstrates the strength and good performance of the LSTM model in all categories of attacks, in terms of detection.

Fig. 7 demonstrates the performance in terms of classification of CNN in the five of five classes (Normal, Information Gathering, Injection Attacks, Malware Attacks and DDoS). It is entirely true positive and high true positive numbers (65,404 in case of normal, 21,336 in case of Injection Attacks, 16,831 in case of Malware Attacks, and 311,680 in case of DDoS) would classify most instances correctly. There are only few misclassifications, especially in the Information Gathering class, where very few samples are falsely predicted as Malware. In general, the matrix shows that CNN model results in multi-class attack detection with a high level of accuracy and reliability with a minimum error rate.

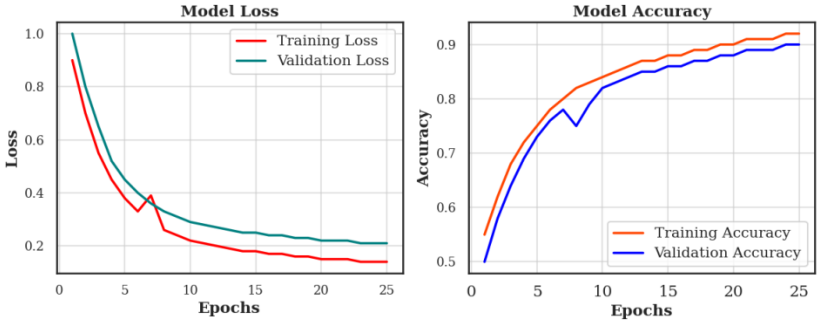

Fig 8: Accuracy and Loss Curve of LSTM Model

Fig. 8 shows training dynamics of the LSTM model in terms of accuracy and loss curves that were generated during 25 epochs. The loss curve indicates a gradual decrease in both training and validation datasets with the training loss always being lower, which is a visualization of successful learning and progressive decrease in the error. At the same time, the accuracy curve shows that there is an evident upward pattern in which the accuracy of training and validation increases with time with a slight difference in that the training accuracy is higher than the validation one. All these plots together show that the model can learn the trends in the data without losing its ability to generalize as the training and validation performance are very close.

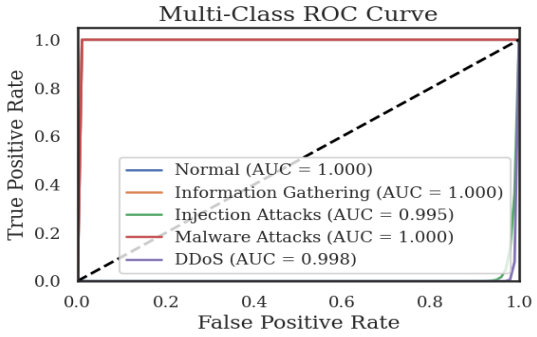

Fig 9: Multi-Class ROC Curve of LSTM Model

Fig. 9 shows a multi-class ROC curve of the LSTM model, which indicates its classification performance on five

categories. All the curves show that the discriminative ability is strong and are close to the top left corner. This is supported by the AUC values, where the values of Normal, Information Gathering, and Malware Attacks stand at the perfect score of 1.000, whereas Injection Attacks and DDoS have almost perfect scores of 0.995 and 0.998 respectively. The diagonal dashed line is the random classifier baseline, with which the better performance of the model is very obvious.

4.1. Comparison and Discussion

Table III shows the comparative analysis of different models of intrusion detection. Conventional models like NB perform poorly with accuracy of 45.0 percent and DT performs moderately with accuracy of 66.57 percent. The ensemble methods such as ETC (95.8% accuracy) and RF (93.78% accuracy) have a higher level of classification. CNN-BiLSTM (92% accuracy) and TCN (93.55% accuracy) models are also capable of offering good performance in terms of deep learning. The results are also enhanced by the proposed CNN model that has an accuracy of 97.15%. Nevertheless, the LSTM model has the most accurate performance of 99.96% which is an obvious success compared to all other methods that are being compared in intrusion detection.

Table 3: Comparative Evaluation for Intrusion Detection

Model	Accuracy	Precision	Recall	F1-Score
CNN-BiLSTM [20]	92	92	92	92
ETC [21]	95.8	96.89	97.87	96.34
NB [22]	45.0	46.7	44.8	41.0
DT [23]	66.57	65.99	79.99	69.23
TCN [24]	93.55	92.95	93.55	92.67
DNN [25]	74.40	55.64	43.53	44.72
RF [26]	93.78	91.26	90.68	90.97
CNN	97.15	96.23	97.10	96.40
LSTM	99.96	99.96	99.99	99.99

The paper presents a substantial contribution to the field of IIoT intrusion detection since it shows that multi-class attack detection with high precision and reliability is possible with the use of the advanced deep learning framework, namely the LSTM model, over the Edge-IIoTset dataset. Its outcomes demonstrate the evident performance improvement when compared to traditional and hybrid models, indicating deep learning efficiency in complex and large-scale IIoT settings. In addition to performance benefits, the study focuses on fairness with the balanced assessment, transparency with the indicators of the performance, and responsible utilization of the publicly available anonymized data. Ethically, the work advocates safe and resistant cybersecurity applications and acknowledges the significance of reducing false alarms and offering reliable real-life implementation of critical IIoT systems.

5. Conclusion and Future Work

The rapid growth of Internet of Things (IoT) devices increases their vulnerability to attacks, necessitating stronger security measures. The machine learning technique is one of the most effective ways to detect anomalies and malicious activity in IoT contexts. This study explored the use of deep learning models in the detection of intrusion in multi-class in Industrial Internet of Things (IIoT) systems. The study has examined different types of cyberattacks using the Edge-IIoTset data. Using extensive experimentation, proposed LSTM model showed excellent performance, having 99.96% accuracy, and precision, 99.99% recall, and 99.99% F1-score, which is better than the CNN model, having 97.15% accuracy and 96.40% F1-score. The findings affirm that sequential learning structures are very effective in learning temporal dependence and intricate traffic pattern within IIoT networks. These results affirm that sequential deep learning structures prove to be quite useful in the process of high complexity traffic patterns in IIoT networks. The research offers a powerful and high-quality intrusion detection system that leads to a considerable increase in the security and reliability of contemporary IIoT systems.

5.1. Limitation

Although the performance of the detection is very high, this study has various limitations. To begin with, the model assessment is performed on a single dataset, Edge-IIoTset. Second, the computational experiments were done on a cloud-based system as opposed to live edge or resource-constrained IIoT devices where latency and memory limit deployment. Also, despite nearly perfect accuracy, deep learning models are vulnerable to adversarial attacks and can produce false positives in the most dynamic network settings.

5.2. Future Work

To continue the work in the future, the cross-dataset validation and real-time implementation in a real IIoT setting should be implemented to test its robustness and scalability. It would be better to develop lightweight or hybrid deep learning models that can run on edge devices. Also, it is possible to improve the interpretability and trust by incorporating explainable AI (XAI) techniques, and evaluate resilience to adversarial attacks by incorporating continual learning, and adaptability to changing cyber threats.

References

[1] K. M. R. Seetharaman and P. Yadav, “A Machine Learning Framework for Detecting and Mitigation of Cyber Threats in IoT Environments,” in *2025 3rd International Conference on Inventive Computing and Informatics (ICICI)*, IEEE, Jun. 2025, pp. 1112–1119. doi: 10.1109/ICICI65870.2025.11069697.

[2] S. K. Chintagunta and S. Amrale, “Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation,” *TIJER – Int. Res. J.*, vol. 9, no. 10, 2022.

[3] S. Singh, “Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation,” in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[4] R. Patel, “Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems)

Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.

[5] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[6] S. Kumara, "AI-Driven Threat Identification and Response: Implications for Secure and Scalable Telecom Infrastructure," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, 2025.

[7] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, 2024.

[8] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[9] S. B. Shah, B. Boddu, N. Prajapati, and S. A. Pahune, "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–7. doi: 10.1109/GINOTECH63460.2025.11076673.

[10] G. Sarraf, "BalanceNet: Addressing Class Imbalance in AI-Powered Intrusion Detection Through Adaptive Sampling," *Asian J. Comput. Sci. Eng.*, vol. 8, no. 4, 2023, doi: https://doi.org/10.22377/ajcse.v8i04.268.

[11] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, 2023, doi: 10.56975/tijer.v10i6.158517.

[12] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[13] R. Chauhan, M. Jena, E. Yafi, M. F. Zuhairi, and A. Mir, "Mitigating IoT Network Threats with a Dual-Model Deep Learning Framework: A Comparative Study of GAT and Transformer Architectures," in *2026 20th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/IMCOM69009.2026.11360928.

[14] A. P. Chowdhury, S. K. Hossain, F. N. Nur, A. H. M. S. Islam, and S. Sultana, "Distributed Intrusion Detection System For Edge of Things To Enhance Security," in *2025 2nd International Conference on Next-Generation Computing, IoT and Machine Learning, NCIM 2025*, 2025. doi: 10.1109/NCIM65934.2025.11160191.

[15] A. Tezcan and O. Karahan, "Addressing Class Imbalance in IoT Intrusion Detection with Hybrid Machine Learning Models," 2025. doi: 10.1109/ismsit67332.2025.11268011.

[16] A. Sharma and H. Babbar, "Guarding Against IoT Threats: An Analysis of Intrusion Detection with the Kitsune Attack Dataset," in *2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS)*, IEEE, Nov. 2024, pp. 637–641. doi: 10.1109/ICTACS62700.2024.10840935.

[17] B. Chhetry, R. K. Dutta, R. Matam, and F. A. Barbhuiya, "Improving Reconnaissance Detection in IoT Environments Using Machine Learning with Heterogeneous Data Integration," in *2024 IEEE Future Networks World Forum (FNWF)*, IEEE, Oct. 2024, pp. 440–445. doi: 10.1109/FNWF63303.2024.11028791.

[18] V. Sujatha, K. L. Prasanna, K. Niharika, V. Charishma, and K. B. Sai, "Network Intrusion Detection using Deep Reinforcement Learning," in *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, IEEE, Feb. 2023, pp. 1146–1150. doi: 10.1109/ICCMC56507.2023.10083673.

[19] A. F. Almutairi and A. Abdulghani Alshargabi, "Using Deep Learning Technique to Protect Internet Network from Intrusion in IoT Environment," in *2022 2nd International Conference on Emerging Smart Technologies and Applications, eSmarTA 2022*, 2022. doi: 10.1109/eSmarTA56775.2022.9935467.

[20] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J. Lee, and D. Kim, "Zero-Trust Marine Cyberdefense for IoT-Based Communications : An Explainable Approach," pp. 1–27, 2024.

[21] A. A. Eshmawi, A. Aldrees, and R. Alharthi, "Smart framework for industrial IoT and cloud computing network intrusion detection using a ConvLSTM-based deep learning model," *Front. Comput. Sci.*, vol. 7, Aug. 2025, doi: 10.3389/fcomp.2025.1622382.

[22] O. Bin Samin, N. A. A. Algeelani, A. Bathich, M. Omar, M. Mansoor, and A. Khan, "Optimizing agricultural data security: harnessing IoT and AI with Latency Aware Accuracy Index (LAAI)," *PeerJ Comput. Sci.*, 2024, doi: 10.7717/PEERJ-CS.2276.

[23] F. Laiq, F. Al-Obeidat, A. Amin, and F. Moreira, "Securing edge-IIoT networks: a comprehensive ensemble-based DDoS detection system," *J. Phys. Complex.*, vol. 6, no. 2, p. 025005, Jun. 2025, doi: 10.1088/2632-072X/ad506b.

[24] W. Gao, M. Wang, Y. Pei, F. Li, and C. Wang, "A Lightweight Multi-Classification Intrusion Detection Model for Edge IoT Networks," Feb. 02, 2026. doi: 10.20944/preprints202601.2418.v1.

[25] I. Izhar, A. Abdullah, M. Zunnurain Hussain, M. Zulkifl Hasan, and C. Author, "ENHANCING IOT/IIOT INTRUSION DETECTION: A COMPARATIVE STUDY OF HYBRID CNN-LSTM AND ADVANCED DNN ML MODEL ON EDGE-IIOTSET," *Spectr. Eng. Sci.* , 2025.

[26] S. Fraihat, Q. Yaseen, Y. Sanjalawe, A. Abu-Errub, S. N. Makhadmeh, and M. A. Al-Betar, "Intrusion detection in industrial internet of things network using feature optimization and hybrid deep learning," *Discov. Internet Things*, Feb. 2026, doi: 10.1007/s43926-026-00284-z.