International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

An Efficient DDoS Attack Detection Approach in IoT using a Recurrent Neural Network

Dr. S. Anitha

Assistant Professor, Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tamil Nadu, India
Email: *selvianitha1974[at]gmail.com*

Abstract: ***The rapid growth of the Internet of Things (IoT) has increased the susceptibility of interconnected devices to Distributed Denial-of-Service (DDoS) attacks, necessitating efficient and reliable intrusion detection mechanisms. This study presents a comparative evaluation of three recurrent deep learning (DL) models- Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU)- for DDoS attack detection using the CICIoT2023 benchmark dataset. To address class imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) was applied during data preprocessing. Experimental results demonstrate that all three models achieved high detection performance, with the GRU consistently outperforming the RNN and LSTM. The GRU attained 99.22% accuracy, 99.16% precision, 99.28% recall, 99.22% F1-score, and an AUC of 0.9984, indicating excellent discrimination between benign and malicious IoT traffic with a low false alarm rate. Its simplified gating mechanism efficiently captured temporal dependencies while requiring lower computational complexity. These findings demonstrate that the GRU model is an effective and computationally efficient solution for real-time DDoS attack detection in IoT environments.***

Keywords: Long Short-Term Memory; Gated Recurrent Neural Network; DDoS Attack Detection; Internet of Things (IoT)

1. Introduction

With the rapid development of IoT, many application fields such as smart homes, healthcare, industrial automation, intelligent transportation, and smart cities have been revolutionized. Billions of IoT devices are connected to heterogeneous communication networks and continuously exchange massive data to provide intelligent and automated services. However, the wide deployment of IoT devices has increased the attack surface against cyberattacks due to the limited computing power, poor authentication mechanisms, and bad security configurations of such devices. Hence, IoT networks have become attractive targets for cybercriminals, especially for DDoS attacks. A DDoS attack is an attempt to make the network service unavailable by flooding the target system with massive amounts of malicious traffic generated by multiple compromised systems. Such large-scale botnets of vulnerable IoT devices can be used to launch sophisticated DDoS attacks quickly, causing significant service disruption, financial loss, and network performance degradation [1]. As the occurrence and complexity of DDoS attacks increase, the development of effective and accurate detection techniques for DDoS attacks has become a major research challenge in modern IoT settings [2].

Traditional machine learning-based DDoS detection approaches heavily rely on manually designed feature engineering and often cannot capture the complex temporal dependencies of network traffic. DL techniques have been promising alternatives since they can automatically learn discriminative representations from sequential traffic data without much manual feature extraction. Of these techniques, RNN, LSTM networks, and GRU have demonstrated great potential in analyzing temporal patterns in network traffic and detecting malicious activities. However, the effectiveness of these models depends greatly on the quality and distribution of the training data. Class imbalance in IoT security datasets is one of the main challenges, where attack and benign samples are not equally distributed. Such imbalance can cause the learning algorithms to be biased toward the majority classes and thus perform poorly in detecting the minority classes. The solution to this problem is the use of SMOTE to generate synthetic samples for minority classes, giving a more balanced dataset and improving the generalization ability of DL models. The CICIoT2023 dataset is one of the newest benchmark datasets for IoT security research and also one of the biggest datasets. It includes real network traffic generated by a huge number of IoT devices in normal conditions and with the presence of different cyber-attack scenarios, including different classes of DDoS attacks. The dataset is heterogeneous and large; thus, it is very suitable for evaluating the effectiveness of DL models for DDoS attack detection.

In this work, the performance of three recurrent DL architectures i.e., RNN, LSTM, and GRU, is evaluated for DDoS attack detection using the CICIoT2023 dataset. In an effort to reduce the effect of class imbalance, the dataset is balanced with SMOTE before training the model. The models are evaluated by commonly accepted performance indicators such as Accuracy, Precision, Recall, F-score, and AUC. The experimental results show that the detection performance of the GRU model is better than the RNN and LSTM models. The accuracy is 99.22%, and the AUC is 0.9984. The results show that GRU can learn the temporal dependencies of IoT network traffic and achieve high detection accuracy and a low false alarm rate, which is a promising solution for real-time DDoS attack detection in IoT networks. The main contributions of this work are summarized below:

- The CICIoT2023 dataset is resampled to address the class imbalance problem using SMOTE and pre-processed.
- Comparative evaluation of three recurrent DL models, RNN, LSTM, and GRU, for DDoS attack detection.
- The model performance is well tested with Accuracy, Precision, Recall, F-score, AUC, and ROC curve analysis.
- The simulation results demonstrate that the detection performance of the GRU model overall is the best, with an accuracy of 99.22% and an AUC of 0.9984. It shows the effectiveness of the model for intelligent DDoS attack detection in the IoT environment.

The rest of this paper is ordered as follows. Section 2 gives the related work on DDoS attack detection methods in IoT. The research methodology for the RNN, LSTM, and GRU models is described in Section 3. Section 4 describes the experimental and comparative analysis. Section 5 finally concludes the paper and discusses future research.

2. Literature Survey

Various DL techniques, including RNN, LSTM, GRU, CNN-LSTM, Transformer, and federated learning models, have demonstrated promising detection performance in the related work on DDoS attack detection in IoT. However, most of the existing works mainly focus on improving classification accuracy with little attention paid to computational efficiency, model complexity, and performance comparison of recurrent neural networks on the latest CICIoT2023 dataset. Moreover, the effect of dealing with class imbalance using SMOTE has not been extensively evaluated among RNN, LSTM, and GRU models. Therefore, the systematic comparison of these recurrent architectures is needed to find the most optimal and computationally efficient model for real-time IoT-based DDoS attack detection.

For example, A. I. Jony et al. (2024) [3] proposed an LSTM-based model, which surpasses other models in detecting known and evolving cyber-attack patterns with high accuracy in extensive experimental evaluations using the large-scale CIC-IoT2023 dataset, which contains a broad spectrum of IoT network traffic scenarios. S. Abbas et al. (2024) [4] investigate detecting cyberattacks on different network traffic streams. The proposed approach is evaluated on the dataset of CIC-IoT2023. They propose a method based on preprocessing of data, robust scalar and label encoding of categorical variables, and prediction using DL models. The experimental results indicate that the RNN model has the highest accuracy, which is 96.56%. P. Vidhya et al. (2026) [5] have proposed an ERNN-based DL approach for IDS to detect anomalies in network traffic. Feature selection was performed using BBOA. The model was tested in two experimental settings: (i) binary classification (benign vs attack) and (ii) multiclass classification where the same ERNN architecture is employed to classify different attack categories. The CIC-IoT-2023 dataset also provided good performance with an accuracy of 98.87%, detection rate of 98.72%, precision of 98.41%, F1-score of 98.56%, and specificity of 98.94%. The study of S. Abbas et al. (2023) [6] presented a novel approach for the detection of large-scale attacks on IoT devices by using federated learning and the new CIC_IoT 2023 dataset. The technique used a federated DNN for precise classification. Proposed Method the proposed method includes feature normalization, data balancing, and federated learning-based data prediction. The experimental results indicated that the proposed approach achieved an excellent accuracy of 99.00%, thus recommending it for attack detection.

B. Fathimamary et al. (2026) [7] proposed the LSTM model optimized by IBSO, where the COBL is added to the Brain Storm Optimization algorithm to increase the diversity of the population, enhance global exploration, and avoid early convergence. The training and validation are done on the CIC-IoT-2023 dataset, which contains real IoT traffic and various scenarios of DDoS attacks. The proposed IBSO+LSTM model has a high detection rate of 98.92 which is better than a few other state-of-the-art models. A. Gueriani et al. (2024) [8] proposed the IDS model, which is a grouping of CNN and LSTM models. The fusion permits the classification of IoT via the utilization of the spatial feature extraction capability of CNN and the sequential memory capability of LSTM for recognizing complex time dependencies to achieve enhanced accuracy and efficiency. For the training and final testing, the recently developed CICIoT2023 dataset was used by the authors to evaluate the performance of the proposed model. The authors also verified the performance of the model by final testing. The suggested model achieves an accuracy of 98.42% with a minimum loss value of 0.0275. FPR is equally important, and getting 9.17%, with an F1-score of 98.57%. B. Susilo et al. (2025) [9] approach helped in a multistage feature extraction process where AEs were first used to extract robust features from unstructured data on the left side of the model architecture. The LSTM analyzes features to distinguish temporal patterns. The extracted features are temporally refined and then fed into the CNN for the final classification. This framework is designed to handle different attacks like DoS and Mirai attacks, which are very harmful to IoT systems. The proposed method was evaluated with the CICIOT 23 dataset for efficiency and robustness, and 99.15% accuracy was achieved.

Z. S. Mahdi et al. (2025) [10] proposed a hybrid DL and ML approach to detect DDoS and spoofing attacks, reduce false alarms, and take the required defensive measures. The proposed hybrid methodology includes three stages. The first stage proposes a hybrid method of feature selection based on techniques. The second stage is to present a hybrid model by combining DL neural networks with a machine learning classifier, and the third stage is to enhance network defense mechanisms and block ports after detection of threats and maintenance of network integrity. The proposed methodology was trained and evaluated with three datasets, and these data were also balanced to get effective results. We obtained accuracies of 99.91 %, 99.88%, and 99.77 %. The detection model by Z. Mahdi et al. (2024) [11] is based on two stages: feature selection and detection model construction, using the K-neighbors algorithm with two classifiers, LR and SGD. The

two classifiers are combined by ensemble, and the parameters are optimized by Grid Search-CV to improve the accuracy of the system. The performance evaluation showed the potential of our model for robust intrusion detection in IoT networks.
S.-M. Tseng et al. (2024) [12] proposed an effective intrusion detection method in 2024. Develop 7 DL models, including a Transformer, to analyze the network traffic characteristics to identify abnormal behavior and potential intrusions using binary and multivariate classifications. The Transformer model used in binary classification is less accurate than the DNN and CNN+LSTM hybrid models. But it is better in multi-class classification. The model improves by 0.74% in accuracy over other papers applying Transformer on TON-IOT for binary classification. The best-performing model combination is Transformer with an accuracy of 99.40%. Its accuracy is 3.8% higher than 95.60%, 0.65% higher than 98.75%, and 0.29% higher than 99.11% reported in papers using the same dataset, respectively.

M. M. Khan et al. (2024) [13] worked on modelling ML techniques for efficient anomalous network traffic detection using the openly available CICIOT 23 dataset. The dataset has 33 types of IoT attacks in 7 major categories. In this paper, we pre-process the dataset and use a balanced representation of classes to generate non-biased supervised RF, Adaptive Boosting, LR, MLP, and DNN models. These models are further analyzed by removing highly correlated features, performing dimensionality reduction, reducing overfitting, and reducing training times. The Random Forest demonstrated the best performance in binary and multiclass classification of IoT Attacks, achieving an accuracy of around 99.55% in both the reduced and full feature spaces. S. Yaras et al. (2024) [14] conducted a study to analyze the attained traffic dataset to detect attacks using a DL algorithm. The datasets 'CICIoT2023' and 'TON_IoT' are used for training and testing the model. The correlation method reduces the features of the datasets and ensures the presence of significant features in the tests. A hybrid algorithm is developed with the help of a one-dimensional CNN and LSTM. The accuracy rate of 99.995% and 99.96% for binary and multiclass classification on the 'CICIoT2023' dataset after the study. The experimental results on the 'TON_IoT' dataset demonstrate that the binary classification accuracy is 98.75%. K. Jakotiya et al. (2025) [15] proposed several ML models. This paper used the CICIoT 2023 Dataset and proposed a two-step process of Intrusion detection. The best accuracy of the neural network-based federated learning model after fine-tuning was 99.84%. The present research aims to propose hybrid or optimized complex models, rather than comparing basic recurrent architectures under the same experimental conditions. There has not been a comprehensive study on the effect of SMOTE on recurrent neural networks for DDoS detection. Most of the works consider accuracy as the most important metric, neglecting the computational complexity and real-time deployment requirements. There is a lack of systematic comparison among RNN, LSTM, and GRU with the same preprocessing and evaluation metrics on the latest CICIoT2023 dataset.

3. Research Methods

The following subsection discusses the research methods in detail.

3.1 LSTM

LSTM [16] is a complex recurrent neural network, designed to address the gradient vanishing and exploding problems of standard RNNs. It makes use of a memory cell and three gates, the forget gate, input gate, and output gate, to learn long-term dependencies in sequential data. The forget gate learns to decide what to keep or throw away from the previous cell state. h_{t-1} is the previous hidden state info and x_t is the current input. f_t is the output of the forget gate and can be calculated as in the equation below.

$$f_t = \sigma(W_f \times [h_{t-1}, x_t] + b_f) \quad (1)$$

Here, W_f are the forget gate weights, and b_f is the forget gate bias. For LSTM, the memory is the cell state, and the input gate is used to update the cell state. The current input and the hidden state information are first fed into a sigmoid function to transform them into the range of $0\ to\ 1$. The cell keeps it at a production level of 1. i_t is the output of the sigmoid and $\tilde{C}_t$ is the output of the tanh activation. They can be calculated with the following equations.

$$i_t = \sigma(W_i \times [h_{t-1}, x_t] + b_i) \quad (2)$$
$$\tilde{C}_t = \tanh(W_c \times [h_{t-1}, x_t] + b_c) \quad (3)$$

When multiplied by zero, values would decrease during point-wise multiplication. If C_{t-1} is previous state information and C_t is present state information, then C_t can be determined by using the equation.

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \quad (4)$$

Let o_t be the sigmoid output of this gate and h_t be the output of this gate; they can be obtained with the help of the following equation.

$$o_t = \sigma(W_o \times [h_{t-1}, x_t] + b_o) \quad (5)$$
$$h_t = o_t \times \tanh(C_t) \quad (6)$$

Here, W_o is the weight of the output gate and b_o is the bias of the output gate. At the beginning of the process, the current and the hidden state information are combined with the input and are called combine. The hidden layer receives the input of the combine, and it selects the necessary information. The candidate layer generates this information that will be added to the cell state. The input gate takes the combine as input and picks out the data that would be inserted in the new cell state as part of the candidate. Then the output of the forget and input gates is used to update the cell state and give the new hidden state. The next state determines what information will be included. The output is taken into account. Hence, LSTM produces output considering the past states.

3.2 GRU

Similar to the LSTM, the GRU method also uses gates that are different neural networks that decide what information should be forgotten or kept. GRU has two gates, Update and Reset, that govern its operation. The first one is responsible for determining which information regarding a new entry will be forgotten and which new information will be added. The second, however, tells you how much past data will be forgotten. Both gates employ a sigmoidal activation function, which is used for simplification purposes as it normalizes its output to values between 0 and 1. When multiplied by 0, any value is lost. When multiplied by 1, the values are preserved. To calculate the value of h_t the cell concatenates h_{t-1} and x_t and then feeds the resulting vector into the Reset and Update gates, getting their output r_t and u_t via the following equations.

$$r_t = \sigma(W_r.[h_{t-1}, x_t] + b_r) \quad (7)$$
$$u_t = \sigma(W_u.[h_{t-1}, x_t] + b_u) \quad (8)$$

u_t and W_u are the neural networks' weight matrices, and b_r and b_u are the neural networks' bias vectors. The output $\check{h}_t$ of this neural network is computed by the equation below.

$$\check{h}_t = tanh\ (W_o.[r_t * h_{t-1}, x_t] + b_o) \quad (9)$$

Two outputs are added pointwise to give the hidden state h_t, the output of the GRU cell. This is expressed by the following equation.

$$h_t = (1 - u_t) * h_{t-1} + u_t * \check{h}_t \quad (10)$$

3.3 RNN

RNNs are neural network models for sequential data; hence, they are appropriate for DDoS attack detection, where the network traffic changes over time. Here, the model is trained to classify normal and malicious traffic based on a sequence of flow-based features such as packet rate, duration, byte count, and inter-arrival time, using the previous hidden context to improve the classification. RNNs are popular in research for intrusion detection because they are able to learn temporal dependencies that static machine learning algorithms cannot learn. The hidden state in an RNN is updated recursively as

$$h_t = \Phi(W_x x_t + W_h h_{t-1} + b_h) \quad (11)$$

x_t is the current input vector, h_{t-1} is the previous hidden state, W_x and W_h are the weight matrices, b_h is the bias term, and Φ is a nonlinear activation function. The detection of a DDoS attack is calculated as the output probability as follows:

$$\hat{y}_t = softmax\left(W_y h_t + b_y\right) \quad (12)$$

$\hat{y}_t$ is the predicted class distribution for benign or attack traffic. For training the model, the loss can be defined with cross-entropy as

$$L = \sum_{i=1}^{C} y_i \log \hat{y}_i \quad (13)$$

where y_i is the true label and $\hat{y}_t$ is the predicted probability of class i. The parameter update can be written as

$$\theta_{k+1} = \theta_k - \eta \nabla_\theta L \quad (14)$$

Where, θ is the model parameters, and η is the learning rate. This optimization enables the network to learn the patterns that differentiate the attack traffic from the legitimate traffic step by step. Another important relationship in recurrent learning is the accumulation of information over time, which can be written as

$$H_t = \sum_{j=1}^{t} \alpha_j x_j \quad (15)$$

Where, H_t is the learned temporal representation and α_j is the contribution of earlier traffic observations. This is useful for DDoS detection, because the attack behavior is usually reflected as repeated bursts or continued abnormal requests over many time windows. Standard RNNs may have vanishing gradient problems on long sequences, so LSTM variants are generally preferred in research for better memory retention and higher detection accuracy.

4. Experimental results and discussion

In this section, we present the experimental evaluation of the proposed DDoS attack detection framework using the dataset CICIoT2023. All experiments were conducted using MATLAB R2022a with the DL Toolbox, on a Windows-based computing platform. The comparative results indicate the effectiveness of each recurrent architecture and the most suitable model for real-time IoT-based DDoS attack detection. We trained RNN, LSTM, and GRU models with the same hyperparameter settings for fair and unbiased comparison. All models were trained using the Adam optimizer, a learning rate of 0.001, 128 hidden units, a batch size of 64, and 100 training epochs. The models were trained using the cross-entropy loss function with a softmax output layer for binary classification on the dataset CICIoT2023.

4.1 Dataset

In 2023, the "Canadian Institute for Cybersecurity" (CIC) [17] released a new and practical dataset, CICIoT2023, which is a collection of IoT attacks. All attacks recorded in this dataset were carried out by malicious IoT devices, targeting other IoT devices. The CICIoT2023 dataset contains 232,885 connections with 47 features. The CICIoT2023 dataset consists of 33 sub-attacks and belongs to seven different attack classifications.

4.2 Data preprocessing

The CICIoT2023 dataset requires careful preprocessing before it can be used for DDoS detection, because raw network traffic usually contains noise, missing values, duplicate records, inconsistent entries, and highly imbalanced class distributions. The first step is to inspect and clean the dataset by removing corrupted or irrelevant samples and ensuring that all feature

values are valid and consistent. Since the dataset contains both numerical and categorical attributes, each type must be handled properly so that the final data is in a uniform format suitable for analysis.

Categorical values such as protocol-related fields or connection labels are converted into numerical form, while numerical traffic features are retained for further processing. After cleaning and encoding, the next step is feature scaling to bring all attributes into a common range and reduce the effect of large-magnitude values on learning. This helps improve numerical stability and ensures that no single feature dominates the others during model training. In addition, redundant or less informative attributes may be reduced to simplify the dataset and improve efficiency. Because DDoS classes in CICIoT2023 are often imbalanced, balancing the data is also important so that the model can learn both normal and malicious traffic effectively.

To handle this imbalance, SMOTE can be applied to generate synthetic samples for minority attack classes. This technique creates new examples by interpolating between existing minority instances, which improves the representation of rare attack categories without simply duplicating records. Finally, the processed data is divided into training and testing sets, with validation data used when needed, to support fair evaluation and reliable DDoS detection performance.

4.3 Performance Metrics

In this work, the detection algorithm was assessed using the following performance measures as [18].

- Accuracy is the sum of the percentage of IoT network traffic correctly labeled as either a DDoS attack or normal traffic.:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100\% \quad (16)$$

- Recall is the measure of the proportion of actual DDoS attacks correctly identified by the model. Higher recall means fewer missed attacks.

$$Recall = \frac{TP}{TP+FN} \times 100\% \quad (17)$$

- Precision is the proportion of traffic predicted as DDoS attacks that were actually attacks. High precision helps to reduce false alarms in the IoT network.

$$Pr\,e\,cision = \frac{TP}{TP+FP} \times 100\% \quad (18)$$

- F1-score: F1 score is a measure of detection performance, which is a harmonic mean of precision and recall and is balanced, especially for imbalanced IoT traffic datasets,

$$F-score = 2 * \frac{Pr\,ecision.Re\,call}{Pr\,ecision+Re\,call} \times 100\% \quad (19)$$

Where, TP = correctly detected DDoS attacks, TN = correctly identified normal traffic, FP = normal traffic incorrectly classified as DDoS attacks, FN = DDoS attacks incorrectly classified as normal traffic.

4.4 Result analysis

Table 1: Performance comparison results

Methods	Accuracy	Precision	Recall	F-Score	AUC
RNN	97.12	97.04	97.08	97.06	0.9878
LSTM	98.31	98.27	98.24	98.25	0.9942
GRU	99.22	99.16	99.28	99.22	0.9964

The experimental results show that the choice of the architecture of a recurrent neural network has a significant impact on the efficiency of DDoS attack detection in the IoT environment. Table 1 and Figure 1 show the performance results analysis. The evaluation of RNN, LSTM, and GRU models on the SMOTE-balanced CICIoT2023 dataset demonstrates that all three methods can detect malicious network traffic with high accuracy. Significant differences were observed in their ability to learn temporal patterns and to discriminate between benign and attack traffic. The traditional RNN model obtained an accuracy of 97.12% and an AUC of 0.9878, demonstrating its effectiveness in detecting DDoS attacks. However, the performance is relatively lower compared to LSTM and GRU. This can be attributed to its limited ability to retain long-term sequential information due to the vanishing gradient problem. The network traffic of IoT often has complex time characteristics, and the standard RNN cannot retain important historical information, which affects its detection performance.

The LSTM model enhanced the detection capability by utilizing the memory cells and gating mechanisms, enabling the network to selectively retain the relevant information and remove the irrelevant features. Thus, the LSTM produced 98.31% accuracy and 0.9942 AUC, outperforming the traditional RNN model in all evaluation metrics. This improvement validates the importance of long-term dependency learning for modeling the dynamic IoT traffic patterns and reducing the classification errors. The best overall performance was achieved by GRU with an accuracy of 99.22%, precision of 99.16%, recall of 99.28%, F1-score of 99.22%, and AUC of 0.9964 among the models evaluated. The superior performance of GRU is mainly due to its simpler gating structure consisting of update and reset gates and is able to capture temporal dependencies efficiently with fewer parameters than LSTM. This simplified architecture leads to faster learning, better generalization, and lower computational requirements, making GRU more suitable for resource-constrained IoT environments. The high value of recall indicates that the model can detect a large proportion of DDoS attack occurrences, and the high value of precision means that the false alarm rate is low, which is very important for practical intrusion detection systems.

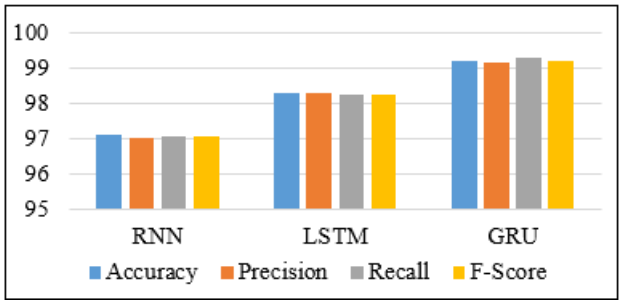

Figure 1: Performance comparison results of DDoS attack detection methods

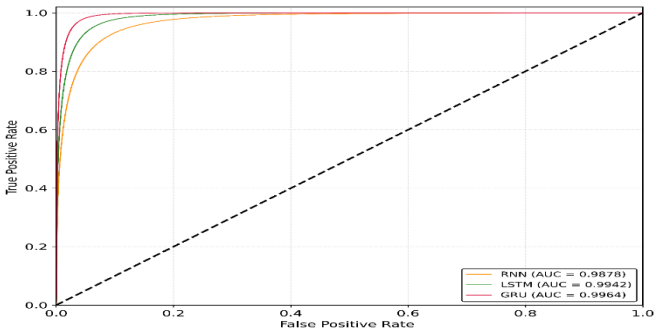

Figure 2: AUC-ROC comparison

Furthermore, the ROC curve analysis (Figure 2) supports the effectiveness of the proposed models. The models obtained high AUC values, which means they have a strong classification ability, but the GRU model had the largest area under the curve, which means it has better discrimination between normal and malicious traffic. Moreover, the convergence analysis shows that the GRU converges to stable performance faster than RNN and LSTM, which validates the learning efficiency of GRU and its suitability for real-time applications in attack detection.

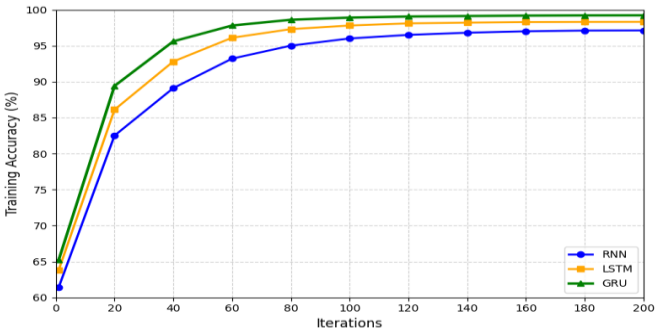

Figure 3: Convergence analysis

5. Conclusions and future works

In this paper, the performance of RNN, LSTM, and GRU models for DDoS attack detection was compared using the CICIoT2023 dataset. In an effort to manage the class imbalance, SMOTE was used in the data preprocessing phase. Detection performance of all models was good, but the GRU model was better than RNN and LSTM consistently. It achieved an accuracy of 99.22%, precision 99.16%, recall 99.28%, F1-score 99.22%, and AUC 0.9984, showing great discrimination between benign and malicious IoT traffic. The simple gating mechanism enabled it to successfully learn temporal dependencies with lower computational complexity as compared to LSTM. The performance was relatively lower for the RNN as it had a limited ability to capture long-term dependencies. The results, in general, show that GRU is an accurate and computationally efficient solution for IoT DDoS detection. Future work integrating attention or Transformer-based architectures, optimizing features and hyperparameters, and validating the model in real-time IoT environments.

References

[1] P. Deepika and S. Nathiya, "A Hybrid Phishing Website Detection Framework Using URL Feature Analysis and Visual Intelligence," *Advances in Computer Engineering and Science,* vol. 1, no. 1, pp. 26-29, 2026.

[2] B. Fathimamary, N. Subbareddy Ramireddy, and K. Vijayakumari, "Anomaly-Based Detection of Distributed Denial of Service Attacks in Internet of Things Using Deep Autoencoder," *Advances in Computer Engineering and Science,* vol. 1, no. 3, pp. 92-98, 2026.

[3] A. I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset," *Journal of edge computing,* vol. 3, no. 1, pp. 28-42, 2024.

[4] S. Abbas *et al.*, "Evaluating DL variants for cyber-attacks detection and multi-class classification in IoT networks," *PeerJ Computer Science,* vol. 10, p. e1793, 2024.

[5] P. Vidhya *et al.*, "A cyber-attack detection model for IoT-IDS utilizing an Elman Recurrent Neural Network," *Discover Internet of Things,* 2026.

[6] S. Abbas *et al.*, "A novel federated edge learning approach for detecting cyberattacks in IoT infrastructures," *IEEE Access,* vol. 11, pp. 112189-112198, 2023.

[7] B. Fathimamary, M. Nasreen, and K. Velusamy, "An Efficient DDoS Attack Detection Using Optimized Long Short-Term Optimization Based on Improved Brainstorm Optimization," *Indian Journal of Science and Technology,* vol. 19, no. 5, pp. 298-312, 2026.

[8] A. Gueriani, H. Kheddar, and A. C. Mazari, "Enhancing IoT security with CNN and LSTM-based intrusion detection systems," in *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, 2024: IEEE, pp. 1-7.

[9] B. Susilo, A. Muis, and R. F. Sari, "Intelligent intrusion detection system against various attacks based on a hybrid DL algorithm," *Sensors,* vol. 25, no. 2, p. 580, 2025.

[10] Z. S. Mahdi, R. M. Zaki, and L. Alzubaidi, "Advanced hybrid techniques for cyberattack detection and defense in IoT networks," *Security and Privacy,* vol. 8, no. 2, p. e471, 2025.

[11] Z. Mahdi, N. Abdalhussien, N. Mahmood, and R. Zaki, "Detection of real-time distributed denial-of-service (DDoS) attacks on internet of things (IoT) Networks

using machine learning algorithms," *Computers, Materials, & Continua,* vol. 80, no. 2, p. 2139, 2024.

[12] S.-M. Tseng, Y.-Q. Wang, and Y.-C. Wang, "Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset," *Future Internet,* vol. 16, no. 8, p. 284, 2024.

[13] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," *Scientific reports,* vol. 14, no. 1, p. 5872, 2024.

[14] S. Yaras and M. Dener, "IoT-based intrusion detection system using new hybrid DL algorithm," *Electronics,* vol. 13, no. 6, p. 1053, 2024.

[15] K. Jakotiya, V. Shirsath, and S. Inamdar, "INTRUSION DETECTION WITH MACHINE LEARNING: A TWO-STEP FEDERATED APPROACH USING THE CIC IoT 2023 DATASET," *Computer Science,* vol. 26, no. 2, 2025.

[16] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: hybrid deep neural network for network intrusion detection system," *IEEE Access,* vol. 10, pp. 99837-99849, 2022.

[17] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors,* vol. 23, no. 13, p. 5941, 2023.

[18] J. C. Obi, "A comparative study of several classification metrics and their performances on data," *World Journal of Advanced Engineering Technology and Sciences,* vol. 8, no. 1, pp. 308-314, 2023.