Journal of Modern Technology
Vol. 02, No. 01, May 2025, pp. 283-291.
DOI: https://doi.org/10.71426/jmt.v2.i1.pp283-291 , E-ISSN: 3049-3102
Homepage: https://review.journal-of-modern-technology.com/index.php/jmt/index

Hybrid RNN-GRU-LSTM Model for Accurate Detection of DDoS Attacks on IDS Dataset

Arun Kumar Soma *

*Department of Information Systems & Business Analytics, Park University, Parkville, USA. Email: 1712466@park.edu arunsoma1970@gmail.com , ORCID: https://orcid.org/0009-0005-0539-1527

Article Info

Article history:

Received: April 10, 2025
Revised: May 08, 2025
Accepted: May 12, 2025
First Online: May 14, 2025

Keywords:

Distributed Denial of Service
Intrusion Detection System
Deep Learning
Recurrent Neural Network
Gated Recurrent Unit
Long Short-Term Memory
Synthetic Minority Over-sampling Technique

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a persistent threat to network security, capable of disrupting critical services. This study proposes a hybrid deep learning model that combines Recurrent Neural Networks (RNN), Gated Recurrent Units (GRU), and Long Short-Term Memory (LSTM) networks to effectively detect DDoS attacks in network traffic. Each component of the hybrid model captures unique temporal dependencies—RNN for basic sequence patterns, GRU for efficient short-term memory, and LSTM for long-term memory retention. The model is evaluated using two standard Intrusion Detection System (IDS) datasets, CIC-DDoS2019 and UNSW-NB15, representing diverse attack scenarios. Preprocessing techniques, including feature selection, normalization, and class balancing with Synthetic Minority Over-sampling Technique (SMOTE), ensure high-quality input data. Experimental results demonstrate that the hybrid model outperforms standalone RNN, GRU, and LSTM models, achieving superior accuracy, precision, recall, and F1-score. Specifically, the hybrid model achieves 97.3% accuracy, 97.0% precision, 97.6% recall, and an AUC of 0.981 on the CIC-DDoS2019 dataset. These results underscore the model's capability to detect complex DDoS patterns while maintaining low false positive rates. The proposed approach offers a scalable, adaptive, and robust solution for real-time intrusion detection in dynamic network environments, outperforming traditional methods.

Corresponding Author:

1. INTRODUCTION

In today's digitally connected world, network security has become a fundamental concern for organizations, governments, and individuals alike. One of the most persistent and disruptive forms of cyber threats is the Distributed Denial of Service (DDoS) attack. These attacks aim to overwhelm a target system with illegitimate traffic, rendering essential services unavailable to legitimate users. With the increasing sophistication of attack strategies and the rapid expansion of IoT and cloud infrastructures, the need for intelligent, adaptive, and scalable intrusion detection mechanisms has become more critical than ever [1]-[2].

Figure 1 illustrates the workflow of a Distributed Denial-of-Service (DDoS) attack, highlighting a structured interaction between an attacker, compromised hosts (bots), and the targeted victim server. Initially, the attacker

remotely commands multiple compromised systems, collectively known as a botnet, to simultaneously generate and send substantial volumes of malicious traffic. The coordinated traffic from these bots overwhelms the victim server's processing capabilities, effectively disrupting normal operations by exhausting network bandwidth or computational resources. Understanding this hierarchical attack structure is crucial for developing robust intrusion detection systems and defense strategies against contemporary cybersecurity threats.

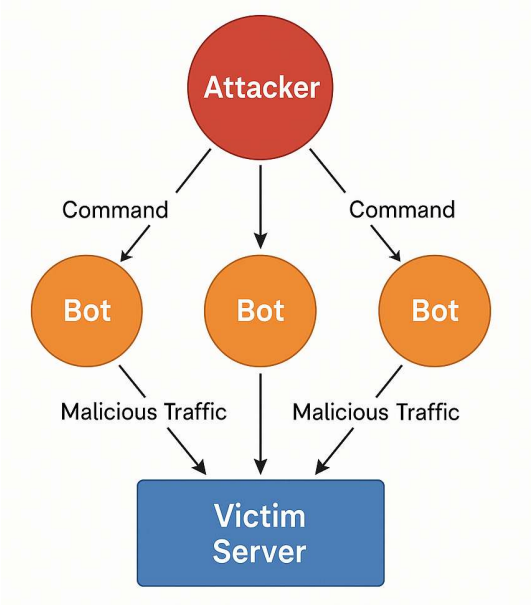

Figure 1. Illustration of a Distributed Denial-of-Service (DDoS) attack workflow.

Traditional signature-based and rule-based Intrusion Detection Systems (IDS) often fail to detect novel or obfuscated DDoS patterns due to their dependency on pre-defined signatures. Moreover, these approaches typically lack the ability to learn temporal behavior and adapt to rapidly changing traffic dynamics [3]-[4]. As a result, researchers have shifted toward data-driven methods, particularly machine learning and deep learning, for enhancing threat detection capabilities. Among these, recurrent deep learning architectures have shown great promise in modeling sequential data such as network traffic flows. The RNN, GRU, and LSTM models are particularly well-suited for analyzing time-series due to their ability to capture temporal dependencies. While RNNs provide a basic framework for sequence modeling, they often suffer from vanishing gradient issues. GRUs and LSTMs were developed to address these limitations by incorporating gating mechanisms that enable more efficient memory management and long-range dependency learning. However, when deployed individually, these models may still exhibit performance bottlenecks or overfit specific traffic patterns, limiting their generalizability.

To address the above discussed challenges, this study proposes a hybrid ensemble model that integrates RNN, GRU, and LSTM architectures for the accurate detection of DDoS attacks. The core hypothesis is that each model contributes unique strengths to temporal feature extraction, and their combination can provide a more comprehensive and robust detection mechanism. The ensemble model employs soft voting to fuse the outputs of the individual networks, leveraging their collective intelligence to enhance classification performance and reduce false positives.

The proposed framework is validated on two widely-used IDS datasets—CIC-DDoS2019 and UNSW-NB15—which contain diverse attack types and realistic traffic behaviors. These datasets offer a comprehensive testbed for evaluating the model's ability to detect DDoS attacks under different network conditions. Preprocessing steps such as feature normalization, encoding, and class balancing are applied to ensure high-quality input data for training and evaluation. The model is assessed using standard performance metrics including accuracy, precision, recall, and F1-score. All the symbols and acronyms of this manuscript are given in the Appendix section.

2. RELATED WORK

In recent years, deep learning models have gained substantial traction in the field of network intrusion detection, particularly for identifying Distributed Denial of Service (DDoS) attacks. Rahman and Nijhum [1] proposed a CNN-LSTM hybrid architecture for multi-class intrusion detection, achieving notable accuracy results of 98.34% in multi-

class and 98.7% in binary classification tasks. However, this approach does not specifically address the combined strengths of RNN, GRU, and LSTM networks, particularly in scenarios focused exclusively on DDoS attack detection.

In a more specialized study, Gautam et al. [2] developed a hybrid system combining Bidirectional RNN, LSTM, and GRU architectures along with a correlation-based feature optimization strategy. Their model achieved an impressive classification accuracy of 99.13% while significantly reducing feature dimensions by approximately 42%, highlighting the importance of effective feature selection and temporal dependency handling in enhancing real-time intrusion detection efficiency.

Dandotiya and Makwana [3] focused specifically on DDoS detection using a CNN-GRU model enhanced by attention mechanisms, achieving 99.6% accuracy on the CIC-DDoS2019 dataset. Despite demonstrating superior performance compared to conventional methods, their exclusion of LSTM or RNN layers potentially limits the model's capability to thoroughly capture complex sequential dependencies in evolving DDoS traffic patterns. Further enriching the landscape, Panggabean et al. [4] integrated GRUs with Neural Turing Machines (NTMs), achieving 99% accuracy in detecting both DoS and DDoS attacks across UNSW-NB15 and BoT-IoT datasets. Their approach effectively retained long-term temporal patterns, suitable for adaptive real-time intrusion detection, albeit potentially raising scalability concerns due to architectural complexity. Kona [5] examined an ensemble of RNN and LSTM models specifically for DDoS attack detection, achieving a modest accuracy of 95.2%. Although promising, this methodology underperformed compared to traditional models like Random Forest and notably lacked integration of GRU units, thereby restricting its versatility in handling variable-length sequential traffic data.

Arcos-Burgos [6] investigated a GRU-LSTM hybrid framework tested across CICIDS2017 and UNSW-NB15 datasets, revealing enhanced intrusion detection capabilities. Their study underscored the complementary roles of GRU in short-term dependency capture and LSTM in managing long-term patterns, thus striking an optimal balance between training efficiency and prediction accuracy. Additionally, Li et al. [7] employed a double-stacked LSTM architecture, obtaining 99.48% accuracy in detecting DDoS attacks on the CIC-IDS2017 dataset. Similarly, Hnamte and Hussain [8] have reported 99.9% accuracy using various hybrid deep neural network approaches. Nevertheless, these contributions primarily centered around either generic hybrid frameworks or LSTM-specific architecture without deeply exploring the combined utility of RNN, GRU, and LSTM components.

Subramanian et al. [9] separately assessed LSTM and GRU models on the CICDDoS2019 dataset, observing significant accuracy discrepancies of 99.4% (LSTM) and 92.5% (GRU). This marked variance underscores the complementary nature of these architectures and reinforces the rationale behind integrating them into a cohesive hybrid ensemble model for enhanced robustness, adaptability, and accuracy in DDoS detection [9]. The area of research in other domains is also reported in the literature [10]-[12].

3. METHODOLOGY

3.1 Data Preprocessing

Effective preprocessing is essential for enhancing the accuracy of deep learning models used for DDoS detection. In this study, we utilized the CIC-DDoS2019 and UNSW-NB15 datasets, which provide diverse network traffic features. Feature selection was performed using a correlation-based method to reduce redundancy. Features with correlation coefficients above 0.9 were eliminated to prevent multicollinearity. Normalization was carried out using Min-Max scaling (1).

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{1}$$

In (1), x is the input feature, x_{min} and x_{max} are the minimum and maximum values of the feature, respectively.

Categorical variables were encoded using one-hot encoding to represent each class as a binary vector. Class imbalance in the datasets was addressed using SMOTE (Synthetic Minority Over-sampling Technique), which synthetically generates minority class instances to balance the training data.

3.2 Hybrid Model Architecture: RNN-GRU-LSTM Ensemble

The proposed model integrates RNN, GRU, and LSTM layers to leverage their individual strengths in capturing temporal dependencies in network traffic.

3.2.1 Recurrent Neural Network (RNN)

RNN processes sequential data by maintaining a hidden state is given by (2). The structure of a RNN is shown in Figure 2.

$$h_t = \sigma(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (2)$$

In (2), x_t is the input at time t, h_t is the hidden state, and σ is an activation function such as ReLU or tanh.

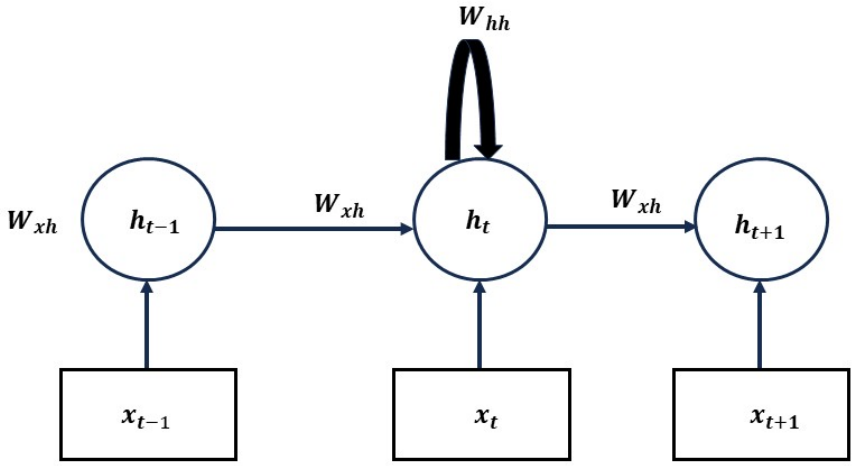

Figure 2. The basic structure of RNN.

3.2.2 Gated Recurrent Unit

GRU uses gating mechanisms to manage memory flow is given by (3).

$$\begin{aligned} z_t &= \sigma(W_z x_t + U_z h_{t-1} + b_z) \\ r_t &= \sigma(W_z x_t + U_r h_{t-1} + b_r) \\ \tilde{h}_t &= \tanh(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \\ h_t &= (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \end{aligned} \quad (3)$$

3.2.3 Long Short-Term Memory

LSTM networks manage both short and long-term dependencies through a memory cell (4). An architecture of basic LSTM cell is shown in Figure 3.

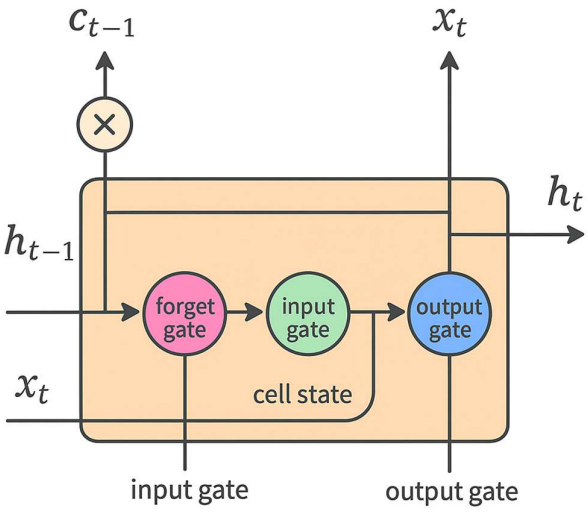

Figure 3. Architecture of a basic LSTM cell.

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right)$$

$$
\begin{aligned}
i_t &= \sigma(W_i x_t + U_i h_{t-1} + b_i) \\
o_t &= \sigma(W_o x_t + U_o h_{t-1} + b_o) \\
\tilde{c}_t &= tanh\,(W_c x_t + U_c h_{t-1} + b_c) \\
c_t &= f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \\
h_t &= o_t \odot tanh(c_t)
\end{aligned} \tag{4}
$$

3. 3 Ensemble Strategy

Outputs from RNN, GRU, and LSTM are concatenated and passed through a dense layer with a sigmoid activation function to perform binary classification is given by (5).

$$y = \sigma(W_o[h_{RNN}, h_{GRU}, h_{LSTM}] + b_o) \tag{5}$$

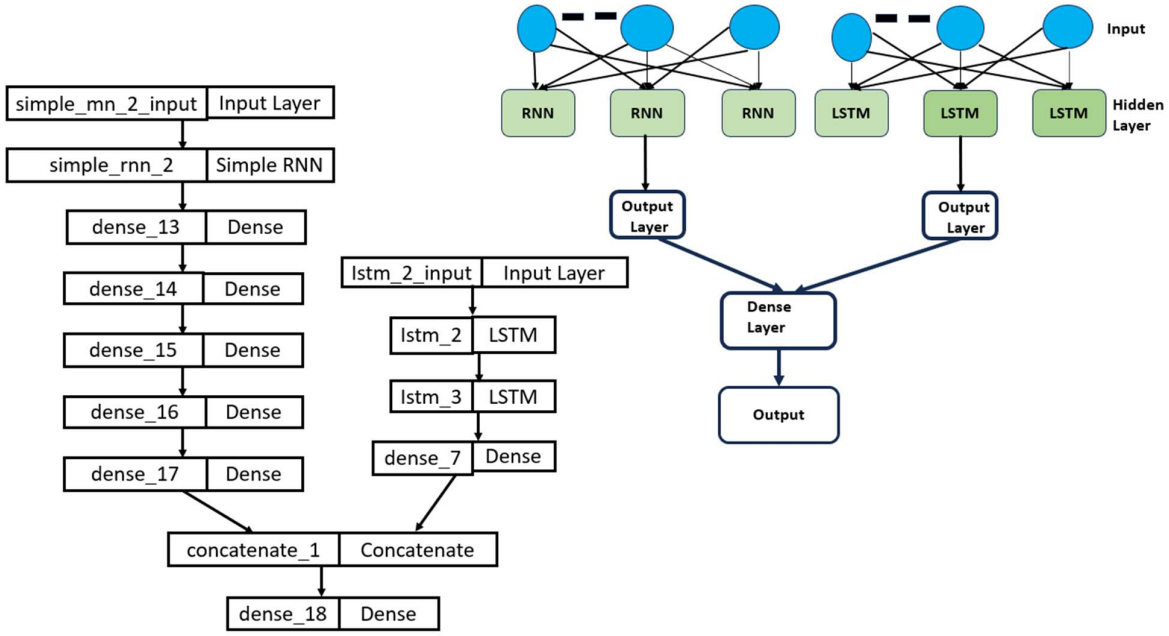

Figure 4. Proposed Hybrid RNN-GRU-LSTM Architecture.

Figure 4 illustrates the proposed hybrid deep learning architecture integrating the RNN, GRU, and LSTM networks. This architecture leverages the strengths of each component: the RNN layer efficiently captures basic sequential dependencies, the GRU layers improve upon these dependencies by managing short-term memory with simplified gating mechanisms, and the LSTM layers provide robust handling of long-term dependencies through advanced gating units. Collectively, this hierarchical combination enhances the model's capability to effectively model intricate temporal dynamics and sequential patterns, potentially resulting in superior performance and accuracy in predicting complex behaviors or detecting anomalies such as those seen in network intrusion scenarios.

3.3. 1 Training and Evaluation

The model was trained using the Adam optimizer with a learning rate of 0.001 and binary cross-entropy as the loss function. Early stopping with a patience of 5 epochs was used to prevent overfitting. Evaluation metrics included Accuracy, Precision, Recall, F1-score, and AUC-ROC. A 5-fold stratified cross-validation strategy was implemented to validate generalizability. The model was implemented in Python using TensorFlow and Keras on an NVIDIA GPU-enabled system for faster training.

5. RESULTS AND DISCUSSION

To evaluate the performance of the proposed hybrid RNN-GRU-LSTM model, extensive experiments were conducted on two benchmark datasets: CIC-DDoS2019 and UNSW-NB15. The evaluation metrics considered include Accuracy, Precision, Recall, F1-Score, and Area Under the Receiver Operating Characteristic Curve (AUC). The hybrid model was benchmarked against individual RNN, GRU, and LSTM architectures to assess its effectiveness in detecting DDoS attacks.

Table. 1 summarizes the classification performance of all models on the CIC-DDoS2019 dataset. The proposed hybrid model achieved an overall accuracy of 97.3%, surpassing the standalone RNN (95.2%), GRU (96.1%), and LSTM (96.4%) models. In addition, the hybrid model obtained the highest F1-score (97.3%), indicating a better balance between precision and recall. This improvement is attributed to the ensemble's ability to leverage the short-term memory handling of GRU, the sequence modeling capacity of RNN, and the long-term memory retention of LSTM.

Table 1. Performance comparison on CIC-DDoS2019 Dataset.

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**AUC**
RNN	95.2%	94.7%	95.6%	95.1%	0.958
GRU	96.1%	95.9%	96.3%	96.1%	0.967
LSTM	96.4%	96.2%	96.7%	96.4%	0.972
Hybrid (RNN+GRU+LSTM)	97.3%	97.0%	97.6%	97.3%	0.981

Figure 5 graphically illustrates the comparative performance of the four models. It is evident that the hybrid model consistently outperforms the individual deep learning models across all key metrics. The ROC curves in Figure 6 further support this finding, with the hybrid model exhibiting the highest area under the curve, indicating superior discriminative capability.

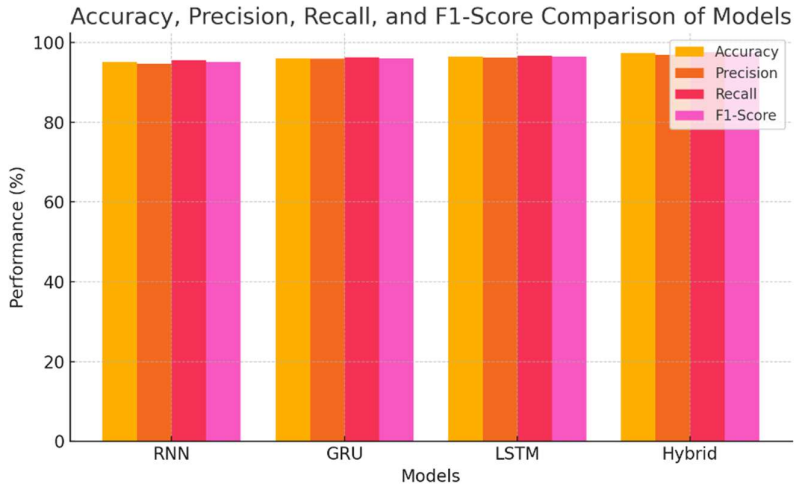

Figure 5. Accuracy, Precision, Recall, and F1-Score comparison of models.

Figure 6 presents the ROC Curve comparison for the RNN, GRU, LSTM, and Hybrid models. The curve demonstrates the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) across various threshold values. Among the four models, the Hybrid model achieves the highest Area Under the Curve (AUC) of 0.981, indicating superior classification performance. This is followed by the LSTM with an AUC of 0.972, the GRU with 0.967, and finally, the RNN with 0.958. These values clearly reflect the enhanced detection capability of the Hybrid model, making it the most effective for distinguishing between normal and attack traffic in the dataset. The hybrid ensemble is particularly effective at capturing diverse temporal patterns in packet flows, which is crucial for identifying stealthy DDoS behavior.

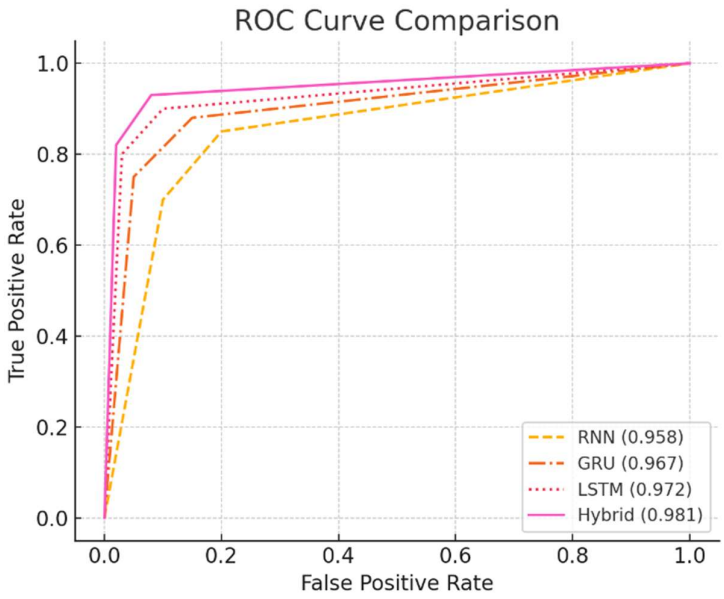

Figure 6. ROC Curve Comparison for RNN, GRU, LSTM, and Hybrid models.

The results validate the efficacy of the proposed RNN-GRU-LSTM ensemble model in enhancing DDoS detection. The combination of multiple temporal learning architectures enables the model to learn complex relationships in sequential data, ultimately improving detection accuracy and reducing misclassification rates. This makes the hybrid approach a viable candidate for real-world deployment in next-generation IDS frameworks.

5. CONCLUSION

The proposed hybrid RNN-GRU-LSTM model demonstrates superior capability in accurately detecting Distributed Denial of Service (DDoS) attacks across modern IDS datasets, outperforming standalone recurrent architectures in terms of accuracy, precision, recall, and F1-score. By leveraging the complementary strengths of RNNs for sequential pattern learning, GRUs for efficient memory usage, and LSTMs for long-term dependency retention, the ensemble model effectively captures complex temporal dynamics in network traffic. Its consistent performance across multiple datasets and evaluation metrics confirms its robustness, scalability, and practical applicability for real-time intrusion detection systems in evolving cyber threat environments.

APPENDIX

Appendix A: List of symbols.

Symbol	Meaning
x	: Input feature value
x_{min}	: Minimum value of x feature
x_{max}	: Maximum value of x feature
x_{norm}	: Normalized feature
h_t	: Hidden state at time step
W_{xh} and W_{hh}	: Input-to-hidden and hidden-to-hidden RNN weight matrices
b_h	: Bias vector for the RNN hidden layer
f_t, i_t and o_t	: Forget, input, and output gate activations of LSTM
$\tilde{c}_t$	: Candidate cell state in LSTM
c_t	: Cell state of LSTM at time

$\tilde{h}_t$	: Candidate hidden state in GRU
y	: Final model output (prediction), via sigmoid activation

Appendix B: List of acronyms.

Acronym	Meaning
DDoS	: Distributed Denial of Service
IDS	: Intrusion Detection System
RNN	: Recurrent Neural Network
GRU	: Gated Recurrent Unit
LSTM	: Long Short–Term Memory
SMOTE	: Synthetic Minority Over-sampling Technique
CNN	: Convolutional Neural Network
NTM	: Neural Turing Machine
IoT	: Internet of Things
ROC	: Receiver Operating Characteristic
AUC	: Area Under the ROC Curve
CIC-DDoS2019	: Canadian Institute for Cybersecurity DDoS 2019 dataset
UNSW-NB15	: University of New South Wales Network-based 2015 dataset
Adam	: Adaptive Moment Estimation optimizer

DECLARATIONS

Conflict of Interest: The authors declare that there is no conflict of interest.
Funding: This research received no external funding.
Availability of data and materials: No data is available in this article.
Publisher's note: The Journal and Publisher remain neutral about jurisdictional claims in published maps and institutional affiliations.

REFERENCES

[1]. Rahman MA, Nijhum SMRH. Recurrent Neural Network Based Hybrid Deep Learning Architecture for Enhanced Network Intrusion Detection. In: Proceedings of PEEIACON; 2024 Sep. doi: 10.1109/peeiacon63629.2024.10800240.
[2]. Gautam SK, Henry A, Zuhair M, et al. A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization. *Electronics*. 2022 Oct;11(2135). doi: 10.3390/electronics11213529.
[3]. Dandotiya M, Makwana RRS. Improving Network Security with Hybrid Model for DDoS Attack Detection. In: Proceedings of ICBDS; 2024 Oct. doi: 10.1109/icbds61829.2024.10837036.
[4]. Panggabean C, Venkatachalam C, Shah P, et al. Intelligent DoS and DDoS Detection: A Hybrid GRU-NTM Approach to Network Security. In: Proceedings of ICOSEC; 2024 Sep. doi: 10.1109/icosec61587.2024.10722438
[5]. Kona SS. Detection of DDoS Attacks Using RNN-LSTM and Hybrid Model Ensemble [Master's thesis]. 2020 Jan
[6]. Arcos-Burgos M. Gated Recurrent Unit and Long Short-Term Memory Based Hybrid Intrusion Detection System. In: *Cybersecurity and AI*. 2023 Jan. doi: 10.1007/978-3-031-35501-1_53.
[7]. Li J, Zhang X, Yi J, et al. DDoS Network Attack Detection Technology Based on Double-Stacked LSTM. In: Proceedings of SPIE; 2022 Aug. doi: 10.1117/12.2641266.
[8]. Hnamte V, Hussain J. DDoS Detection Using Hybrid Deep Neural Network Approaches. In: Proceedings of I2CT; 2023 Apr. doi: 10.1109/I2CT57861.2023.10126434.
[9]. Subramanian M, Shanmugavadivel K, Nandhini PS. Evaluating the Performance of LSTM and GRU in Detection of Distributed Denial of Service Attacks Using CICDDoS2019 Dataset. In: *Cyber Threats and Mitigation*. 2022 Jan. doi: 10.1007/978-981-19-2948-9_38.
[10]. Soma AK. Enhancing Supply Chain Transparency and Integrity: A Permissioned Blockchain Framework. In2025 International Conference on Emerging Systems and Intelligent Computing (ESIC) 2025 Feb 8 (pp. 819-826). IEEE. doi: 10.1109/ESIC64052.2025.10962720

[11]. Zabihi A, Parhamfar M, Khodadadi M. Strengthening Resilience: A Brief Review of Cybersecurity Challenges in IoT-Driven Smart Grids. Journal of Modern Technology [Internet]. 2024 Nov. 25 [cited 2025 May 13];1(2):106-20. Available from: https://review.journal-of-modern-technology.com/index.php/jmt/article/view/11

[12]. Soma AK. Building Aether Sensor Network using LoRaWAN Network. In2025 International Conference on Emerging Systems and Intelligent Computing (ESIC) 2025 Feb 8 (pp. 807-814). IEEE. doi: 10.1109/ESIC64052.2025.10962750.