International Journal of Informatics Engineering and Computing (IJIMATIC)
Vol. 2, No. 2, 2025
E-ISSN: 3090-9112 DOI: 10.70687/ijimatic

Detection of DDoS Attacks Using Hybrid LSTM and SVM Algorithm

Ivansius Nahak[1], M. Hizbul Wathan[2]

Abstract

Distributed Denial of Service (DDoS) attacks pose serious threats to network infrastructures by disrupting services through massive malicious traffic. This study proposes a hybrid detection model that integrates Long Short-Term Memory (LSTM) with a Support Vector Machine (SVM) classifier to improve the accuracy of DDoS detection in network traffic. The LSTM model captures temporal patterns within sequential traffic data, while the SVM performs the final classification to distinguish between normal and anomalous traffic. The experiment uses a dataset containing 104,345 records with 23 features that undergo preprocessing, encoding, scaling, and class balancing before model training. Experimental results demonstrate that the proposed hybrid model achieves stable learning performance with training accuracy reaching approximately 93% and validation accuracy around 94%. The loss curves show consistent decreases across 50 training epochs, indicating effective convergence and minimal overfitting. Confusion matrix analysis shows that the model correctly classifies the majority of normal and anomalous traffic samples, with relatively low false positive and false negative rates. Overall evaluation results show that the hybrid LSTM–SVM model achieves 95% accuracy with balanced classification performance. The model records strong precision, recall, and F1-score values for both normal and anomalous traffic classes.

Keywords:
Detection, DDoS Attacks, LSTM, SVM

1. Introduction

The rapid growth of the Internet and cloud-based services significantly increases the volume and complexity of network traffic. While this development enables efficient communication and digital services, it also exposes networks to various cybersecurity threats. Among these threats, Distributed Denial of Service (DDoS) attacks remain one of the most disruptive forms of cyberattacks. A DDoS attack attempts to overwhelm a target system, network, or service with a massive volume of traffic generated from multiple distributed sources. This flood of malicious traffic exhausts system resources and prevents legitimate users from accessing services. As modern networks become more interconnected through cloud computing, Internet of Things (IoT), and software-defined networking (SDN), the scale and sophistication of DDoS attacks continue to increase. Consequently, detecting such attacks in real time becomes a critical challenge

[1] Ivansius Nahak, Universitas Respati Yogyakarta, Indonesia (Email: 21220029@respati.ac.id)
[2] M. Hizbul Wathan, Politeknik Manufaktur Negeri Bangka Belitung, Indonesia

for network security systems, especially when traditional rule-based security mechanisms fail to adapt to evolving attack patterns [1], [6].

Traditional intrusion detection systems (IDS) rely heavily on signature-based or rule-based approaches to identify malicious activities. These systems compare network traffic patterns with known attack signatures stored in predefined databases. Although this approach works effectively for detecting previously identified threats, it struggles to recognize new or evolving attack strategies. DDoS attackers frequently modify their attack patterns, making signature-based detection less reliable. In addition, conventional statistical and machine learning techniques often rely on manually engineered features that may not fully capture the complex relationships present in large-scale network traffic data. As network infrastructures become more dynamic, the limitations of traditional detection methods highlight the need for more intelligent and adaptive approaches capable of identifying anomalies within highly complex traffic environments [2], [5].

Machine learning techniques have recently gained attention as potential solutions for network intrusion detection because they can automatically identify patterns and anomalies from large datasets. Algorithms such as Support Vector Machines (SVM), Random Forests, and logistic regression have been widely applied for detecting DDoS attacks. Among these approaches, SVM has proven effective in classification tasks involving high-dimensional data and nonlinear decision boundaries. SVM models can separate malicious traffic from legitimate traffic by constructing optimal hyperplanes within feature spaces. Several studies demonstrate that SVM-based detection systems achieve promising accuracy in identifying network intrusions, particularly when appropriate feature selection techniques are applied. However, conventional machine learning models still rely heavily on handcrafted features and often struggle to capture temporal relationships within sequential network traffic data [3], [13].

Deep learning methods offer a more advanced solution for analyzing complex network traffic patterns because they can automatically learn hierarchical representations from raw data. Unlike traditional machine learning approaches, deep learning models perform feature extraction and classification simultaneously. Neural network architectures such as Convolutional Neural Networks (CNN), Deep Neural Networks (DNN), and Recurrent Neural Networks (RNN) have been increasingly applied to intrusion detection systems. These models can process large volumes of network traffic and identify hidden patterns that may indicate malicious behavior. Empirical studies show that deep learning-based intrusion detection systems achieve higher detection accuracy and improved adaptability compared to classical approaches. Nevertheless, selecting an appropriate architecture remains challenging due to the diverse characteristics of network traffic data [4], [7].

Among deep learning architectures, Recurrent Neural Networks (RNN) are particularly suitable for analyzing sequential data such as network traffic flows. Network traffic exhibits strong temporal characteristics, where patterns evolve over time as packets are transmitted through communication channels. Long Short-Term Memory (LSTM), a specialized form of RNN, addresses the limitations of traditional RNN models by introducing memory cells and gating mechanisms that enable the network to retain relevant information across longer time intervals. LSTM models can effectively capture temporal dependencies in sequential data, making them well suited for detecting anomalous behavior in network traffic. Previous studies demonstrate that LSTM-based detection systems significantly improve the identification of DDoS attack patterns by learning temporal correlations among traffic features [8], [10].

Despite the advantages of deep learning approaches, relying solely on a single neural network architecture may not fully capture the complexity of network traffic patterns. Deep learning models often require large datasets, extensive training time, and

careful parameter tuning to achieve optimal performance. Moreover, neural networks may suffer from overfitting or reduced interpretability when dealing with high-dimensional network traffic data. These challenges motivate researchers to explore hybrid approaches that combine deep learning models with traditional machine learning techniques. Hybrid models aim to leverage the strengths of multiple algorithms while minimizing their individual limitations, thereby improving detection accuracy and system robustness [9], [14].

Several recent studies propose hybrid intrusion detection frameworks that integrate deep learning feature extraction with machine learning classification methods. In these frameworks, deep neural networks such as LSTM or CNN act as feature extractors that learn complex patterns from raw network traffic, while machine learning classifiers perform the final decision-making process. For example, combining LSTM with SVM allows the system to benefit from LSTM's ability to model temporal dependencies and SVM's strong capability for classification in high-dimensional feature spaces. Research findings indicate that hybrid models can significantly improve detection performance, reduce false positives, and enhance generalization across different attack scenarios. However, many existing studies focus on specific datasets or limited attack categories, which restricts the generalizability of their results [11], [15].

Therefore, further investigation is required to develop more robust hybrid models capable of accurately detecting DDoS attacks in dynamic network environments. A hybrid LSTM–SVM framework provides a promising solution by integrating sequential pattern learning with effective classification mechanisms. This study explores the effectiveness of such a hybrid approach for detecting DDoS attacks in network traffic data. By leveraging LSTM for temporal feature learning and SVM for classification, the proposed model aims to improve detection accuracy while maintaining computational efficiency. The findings of this research contribute to the development of more reliable and intelligent intrusion detection systems capable of protecting modern network infrastructures from increasingly sophisticated DDoS threats [1], [12].

2. Related Works

Several studies investigated the application of traditional machine learning techniques for detecting Distributed Denial of Service (DDoS) attacks in network traffic. Researchers widely adopted algorithms such as Support Vector Machines (SVM), Decision Trees, and Random Forests to classify malicious and legitimate traffic patterns. For instance, previous work applied SVM to network intrusion datasets and demonstrated that the algorithm effectively separated attack traffic from normal traffic using hyperplane-based classification. The study reported high detection accuracy due to SVM's capability to handle high-dimensional feature spaces. However, the model relied heavily on manually engineered features and statistical attributes extracted from traffic flows. As a result, the performance depended strongly on feature quality and dataset characteristics, which limited its adaptability to evolving DDoS attack patterns [3], [13].

Other researchers focused on anomaly-based intrusion detection systems that utilized statistical learning approaches to identify abnormal traffic behavior. These studies analyzed traffic distribution patterns such as packet rate, flow duration, and protocol usage to detect potential attacks. Experimental results showed that anomaly detection methods could identify unknown attack types that were not present in predefined signature databases. Despite this advantage, the approaches suffered from relatively high false-positive rates because legitimate traffic sometimes exhibited patterns similar to abnormal behavior. Furthermore, statistical models often struggled to

capture complex nonlinear relationships within large-scale network datasets, which reduced their effectiveness in modern high-speed network environments [2], [5].

Recent research explored deep learning methods to improve the performance of intrusion detection systems. Several studies implemented deep neural networks to automatically learn complex representations from network traffic data. For example, researchers applied Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN) to detect malicious traffic patterns. Their experiments showed that deep learning models achieved higher detection accuracy than traditional machine learning algorithms because they automatically extracted relevant features from raw network data. CNN-based models particularly demonstrated strong capability in identifying spatial correlations among traffic attributes. However, these models mainly captured static patterns and did not fully exploit the sequential nature of network traffic flows [4], [7].

To address the temporal characteristics of network traffic, several studies implemented Recurrent Neural Networks (RNN) for intrusion detection. Researchers applied Long Short-Term Memory (LSTM) networks to analyze sequential packet flows and identify temporal anomalies associated with DDoS attacks. Experimental results showed that LSTM-based models effectively captured long-term dependencies in traffic sequences and improved detection accuracy compared with conventional neural networks. The memory gating mechanism of LSTM allowed the model to retain relevant information from earlier time steps. Nevertheless, these models often required large training datasets and significant computational resources, which limited their deployment in real-time network monitoring systems [8], [10].

Some studies investigated hybrid deep learning architectures to combine the strengths of different neural network models. For example, researchers integrated CNN and LSTM layers within a unified framework to extract spatial and temporal features from network traffic data simultaneously. The CNN layers performed feature extraction by identifying local traffic patterns, while the LSTM layers modeled temporal relationships between traffic flows. Experimental evaluations demonstrated that hybrid CNN–LSTM models improved DDoS detection accuracy and reduced false alarm rates compared with standalone models. However, the increased architectural complexity introduced higher training costs and parameter tuning challenges, which required careful model optimization [9], [11].

In addition to hybrid deep learning approaches, several researchers explored the integration of deep learning with classical machine learning classifiers. In these frameworks, deep neural networks performed feature extraction, while algorithms such as SVM or Random Forests conducted the final classification process. These hybrid approaches leveraged the feature learning capability of deep learning and the strong classification performance of traditional machine learning models. Experimental results showed that such combinations improved detection accuracy and model generalization across multiple intrusion detection datasets. Despite these advantages, many studies evaluated their models using limited datasets, which restricted the reliability of the results in real-world network environments [12], [14].

Recent research also emphasized the importance of dataset diversity and real-time detection capability in DDoS defense systems. Some studies evaluated detection models using modern intrusion detection datasets such as CICIDS2017 and CSE-CIC-IDS2018. These datasets contained realistic network traffic scenarios and various attack types, which enabled more comprehensive evaluation of detection models. Researchers reported that deep learning models trained on these datasets achieved promising performance in detecting complex attack patterns. However, several studies indicated that many detection systems still struggled with generalization when applied to unseen network environments or new attack variants [1], [6].

Although existing research demonstrated significant progress in DDoS detection using machine learning and deep learning techniques, several limitations remained. Many previous studies focused on single-model architectures that either emphasized temporal learning or classification capability but did not effectively combine both aspects. In addition, the trade-off between detection accuracy, computational efficiency, and model generalization remained a major challenge. Therefore, integrating sequential learning models such as LSTM with robust classifiers such as SVM could provide a more balanced solution for DDoS detection. This study built upon previous work by proposing a hybrid LSTM–SVM framework that aims to improve detection performance while maintaining computational efficiency for practical network security applications.

3. Proposed Method

This study proposes a hybrid approach combining LSTM networks to analyze temporal traffic patterns and SVM for attack classification. LSTM captures long term dependencies in sequential network data, while SVM provides robust binary classification. This integration aims to improve detection accuracy and generalization across diverse network environments by harness the power of deep learning and traditional machine learning techniques. In this paper, we utilize LSTM represents advanced level variant of RNN specifically engineered in capture long- range temporal dependencies in sequential data. Through its unique architecture featuring memory cells and specialized gating mechanisms, LSTM effectively regulates information flow, overcoming the vanishing gradient limitation inherent in conventional RNNs.

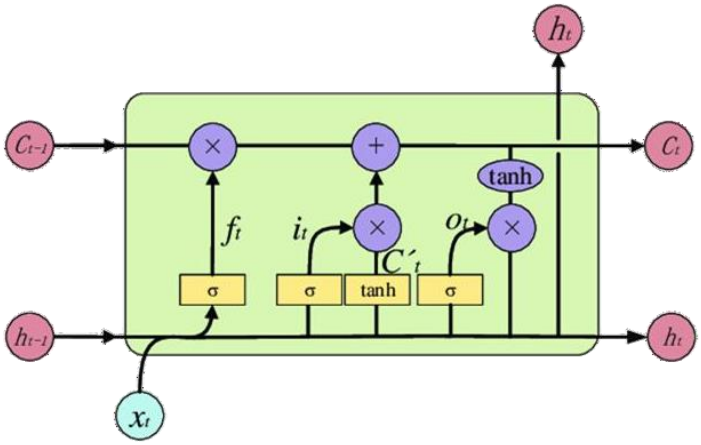

Fig. 1 LSTM Model Architecture

1. Forget Gate (f_t)

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

Table 1. Forgotten Gate description

Notation	Description
f_t	: Forget gate value
W_f	: Weights connecting the forget gate to input
b_f	: Bias of forget gate
σ	: Sigmoid activation function maps values between 0 and 1

2. Input Gate (i_t)

$$i_t = \sigma(W_i \,.\, [h_{t-1}, x_t] + b_i \quad (2)$$

Table 2. Notation of input Gate (input layer)

Notation	Description
W_i	: Weights of the input gate
h_{t-1}	: Hidden state
x_t	: Input current
b_i	: Bias input gate
σ	: This activation function outputs values between 0 and 1.

$$C_t = \tan\,(W_{c.}\ [h_{t-1}, x_t] + b_c \quad (3)$$

Table 3. Notation of input Gate (soil layer)

Notation	Description
W_c	: Weight cell state
h_{t-1}	: Hidden state
x_t	: Current input
b_c	: Bias of the cell state
tanh	: It scales inputs to a range between -1 and 1

3. Output Gate (o_t)

$$o_t = \sigma(W_o \,.\, [h_{t-1}, x_t] + b_o \quad (4)$$

Table 4. The Mathematical Notation of output Gate (gate output value)

Notation	Description
O_t	: Output gate
W_o	: Weights connecting the output gate to the input
b_o	: Bias of the output gate
σ	: Sigmoid activation that maps values between 0 and 1
h_t	: Hidden state
C_t	: Cell state

$$h_t = o_t * tanh\,(C_t) \quad (5)$$

Table 5. The Mathematical Notation of output Gate (hidden state)

Notation	Description
h_t	: *Hidden state*
O_t	: *Output gate*
C_t	: *Cell state*

SVM is a robust supervised learning method mainly used for classification and regression tasks. The algorithm functions by determining an ideal decision boundary (hyperplane) that enhances the separation margin among various classes within the feature space. This maximum-margin method boosts the model's ability to generalize and increases classification precision.

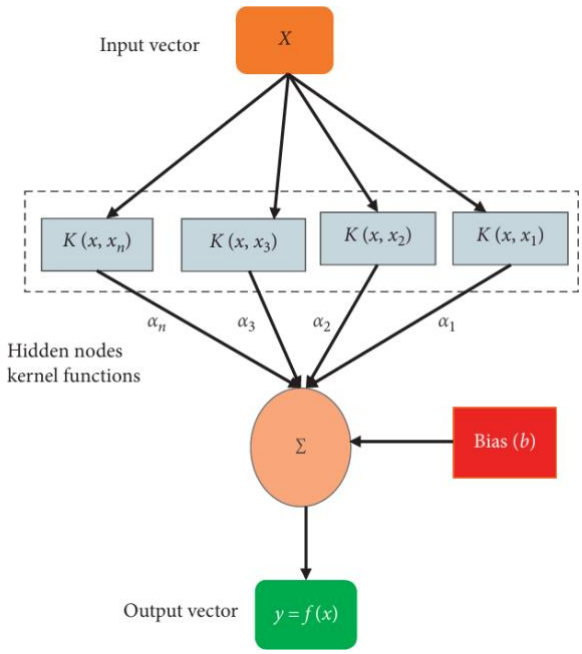

Fig. 2 SVM Model Architecture

Fig. 2 illustrates the workflow of the Support Vector Machine (SVM) classification process. The input layer receives feature vectors x that represent the network traffic data and forwards them to the hidden layer. In the hidden layer, a kernel function $K(x, x_i)$ such as Linear, Polynomial, or Radial Basis Function (RBF) is applied to measure the similarity between the input vector and the support vectors in a higher-dimensional feature space. This transformation enables the model to handle complex and non-linear data patterns. Finally, the output layer produces the classification result by computing the weighted sum of the kernel outputs and adding a bias term, which determines whether the input data is classified as normal traffic or anomalous traffic.

$$y = f(x) = \sum_{i=1}^{n} \alpha_i . K(x, x_i) + b \quad (6)$$

$f(x) > 0$, classified as a class +1.
$f(x) < 0$, classified as a class -1.

Table 5. Mathematical Notation of output SVM

Notation	Description
α_i	: Lagrange coefficient for each support vector
y	: Class label
K	: Kernel between input data x *and support vector* x_i
b	: Bias that determines the position of the margin

4. Experimental Setup

This study prepares a quantitative experimental framework that combines deep learning and machine learning techniques to detect Distributed Denial of Service (DDoS) attacks in network traffic. We propose a hybrid LSTM–SVM model that integrates sequential pattern learning with robust classification capability. The study utilizes the "dataset_sdn.csv" dataset obtained from Kaggle, which contains 104,345 records with 23 network traffic features labeled as either Normal or Anomaly. The experimental process begins with exploratory data analysis and preprocessing steps to improve data quality and consistency. These steps include data cleaning, label encoding, feature scaling, and feature selection. The dataset is then divided into training and testing sets using an 80%–20% ratio. To address potential class imbalance, the study applies one-hot encoding and Synthetic Minority Over-sampling Technique (SMOTE). Finally, the prepared data is reshaped into a three-dimensional structure suitable for LSTM input representation.

This study then performs model training and evaluation using the proposed hybrid architecture. The LSTM component is designed to capture temporal relationships within network traffic sequences and is trained for 50 epochs with a batch size of 32. During the training process, performance metrics such as loss and accuracy are monitored to ensure stable learning and to prevent overfitting or underfitting. After the LSTM model learns the sequential patterns of the data, the extracted feature representations from the LSTM output are used as input to a Support Vector Machine (SVM) classifier for the final classification stage. The SVM model performs the decision-making process to distinguish between normal traffic and DDoS attack traffic. The overall performance of the hybrid model is evaluated using several standard classification metrics, including accuracy, precision, recall, and F1-score, to ensure reliable and comprehensive detection performance.

5. Result and Analysis

The results show that the hybrid LSTM-SVM model performs optimally in detecting DDoS attacks, as evidenced by the following performance metrics:

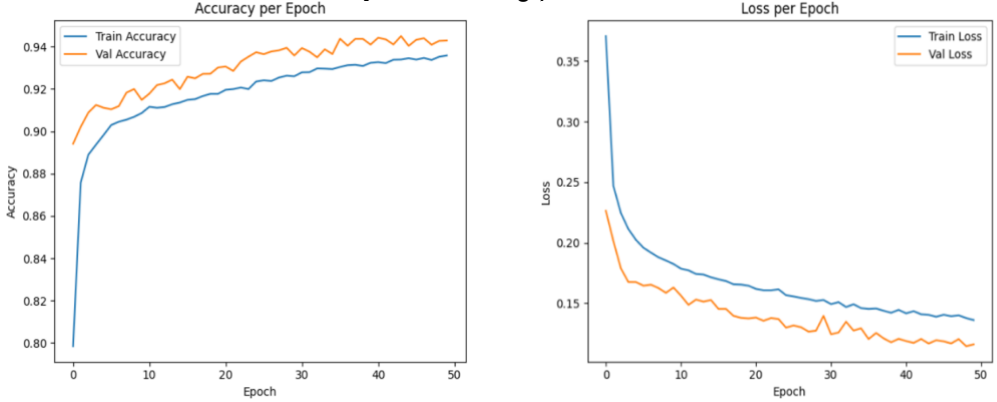

Fig. 3 Accuracy and Loss of hybrid LSTM-SVM model

Fig. 3 illustrates the training performance of the proposed hybrid LSTM–SVM model during the learning process. The left graph presents the accuracy progression over 50 training epochs for both training and validation datasets. The results indicate a steady improvement in model performance throughout the training phase. The training accuracy increases from approximately 80% in the initial epochs to around 93% by the end of the training process. Similarly, the validation accuracy gradually rises and stabilizes at approximately 94%. The close alignment between the training and validation accuracy curves indicates that the model learns the underlying traffic patterns effectively while maintaining stable generalization capability.

The right graph in Fig. 3 presents the loss values recorded during the training and validation phases. Both curves show a consistent downward trend across the 50 epochs, indicating that the model progressively minimizes prediction errors during learning. The training loss decreases rapidly in the early epochs and continues to decline gradually as training progresses. The validation loss follows a similar pattern and remains slightly lower than the training loss. Importantly, no significant divergence appears between the two curves, which suggests that the model does not experience overfitting. These results demonstrate that the hybrid LSTM–SVM framework achieves stable convergence and effectively captures the temporal patterns within the network traffic data for accurate DDoS attack detection.

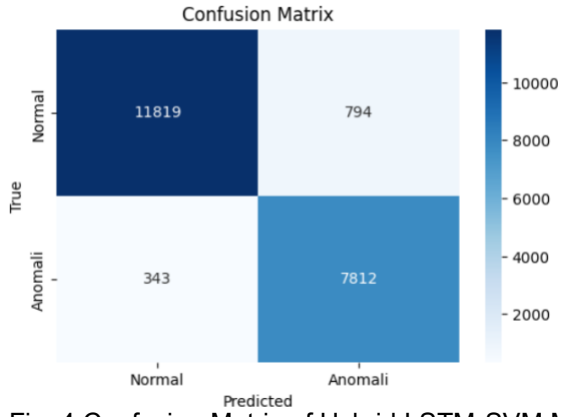

Fig. 4 Confusion Matrix of Hybrid LSTM-SVM Model

The classification results indicate that the proposed model performs effectively in distinguishing between normal and anomalous network traffic. The model correctly identifies 11,819 instances of normal traffic as Normal, representing the true negative cases, while 7,812 instances of anomalous traffic are correctly classified as Anomaly, representing the true positive detections. However, the model produces 794 false positive cases, where normal traffic is incorrectly classified as anomalous, resulting in false alarms within the detection system. In addition, 343 anomalous instances are misclassified as normal, representing false negatives where certain DDoS attack activities remain undetected. Overall, the confusion matrix results demonstrate that the model achieves strong detection capability while maintaining relatively low misclassification rates in identifying network traffic anomalies.

	precision	recall	f1-score	support
0	0.97	0.94	0.95	12613
1	0.91	0.96	0.93	8155
accuracy			0.95	20768
macro avg	0.94	0.95	0.94	20768
weighted avg	0.95	0.95	0.95	20768

The classification report demonstrates the model's strong detection capabilities, achieving 95% overall accuracy on 20,768 test samples. For normal traffic (Class 0), it shows exceptional performance with 97% precision and 94% recall, while anomaly detection (Class 1) maintains robust results at 91% precision and 96% recall. The balanced F1-scores of 0.95 for normal and 0.93 for anomalous traffic indicate consistent classification performance across both categories. The following is the calculation.

6. Conclusion

This study proposes and applies a hybrid LSTM–SVM model to detect Distributed Denial of Service (DDoS) attacks in network traffic data. We explore the capability of combining temporal pattern learning from Long Short-Term Memory networks with the strong classification ability of Support Vector Machines. The experimental results demonstrate that the proposed model learns network traffic behavior effectively during the training process. The training accuracy increases steadily from approximately 80% in the early epochs to about 93% at the end of the learning process, while the validation accuracy reaches around 94%. At the same time, the loss curves for both training and validation decrease consistently across the 50 epochs, indicating that the model successfully minimizes prediction errors. The close alignment between the training and validation curves confirms that the model converges well and maintains stable generalization without experiencing significant overfitting.

Furthermore, we evaluate the detection capability of the proposed model using confusion matrix analysis. The results show that the model correctly classifies 11,819 instances of normal traffic as Normal and successfully detects 7,812 anomalous traffic samples as Anomaly. Although the model produces 794 false positive cases and 343 false negative cases, the overall misclassification rate remains relatively low compared with the total number of observations. These results indicate that the hybrid approach effectively distinguishes between legitimate network activity and malicious traffic patterns. The integration of LSTM allows the system to capture temporal dependencies in network traffic sequences, while the SVM classifier strengthens the final decision boundary for anomaly detection.

Finally, we assess the overall classification performance using standard evaluation metrics. The classification report shows that the model achieves an overall accuracy of 95% on 20,768 test samples. For normal traffic detection, the model obtains 97% precision and 94% recall, while anomaly detection achieves 91% precision and 96% recall. The balanced F1-scores of 0.95 for normal traffic and 0.93 for anomalous traffic demonstrate consistent predictive performance across both classes. In addition, the

Receiver Operating Characteristic analysis shows an Area Under the Curve value of 0.99, indicating excellent discriminative capability between normal and malicious traffic. These findings confirm that the proposed hybrid LSTM–SVM framework provides a reliable and highly effective approach for DDoS attack detection in network environments.

References

[1] R. Efendi, T. Wahyono, and I. R. Widiasari, "DBSCAN SMOTE LSTM: Effective strategies for distributed denial of service detection in imbalanced network environments," *Big Data and Cognitive Computing*, vol. 8, no. 9, p. 118, 2024, doi: 10.3390/bdcc8090118.

[2] Alshamrani, A. Anwar, and M. Alsubhi, "An investigation into the application of deep learning in the detection and mitigation of DDoS attack on SDN controllers," *Technologies*, vol. 9, no. 1, p. 14, 2021, doi: 10.3390/technologies9010014.

[3] M. Revathi and M. Malathi, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, p. 1095, 2022, doi: 10.3390/sym14061095.

[4] Raza et al., "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection," *Applied Sciences*, vol. 11, no. 24, p. 11634, 2021, doi: 10.3390/app112411634.

[5] H. Alkahtani et al., "Security analysis of DDoS attacks using machine learning algorithms in network traffic," *Electronics*, vol. 10, no. 23, p. 2919, 2021, doi: 10.3390/electronics10232919.

[6] M. R. H. Siddiqui et al., "A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking," *Sensors*, vol. 23, no. 9, p. 4441, 2023, doi: 10.3390/s23094441.

[7] M. A. Al-Adib et al., "Performance evaluation of CNN, LSTM, and DNN for feature flow-based DDoS attack detection on CSE-CIC-IDS2018 dataset," *Jurnal Komputer Teknologi Informasi Sistem Informasi*, vol. 4, no. 3, pp. 1639–1649, 2025.

[8] S. Saini and S. Jang-Jaccard, "An adversarial DBN-LSTM method for detecting and defending against DDoS attacks in SDN environments," *Algorithms*, vol. 16, no. 4, p. 197, 2023, doi: 10.3390/a16040197.

[9] H. Liu and P. Patras, "NetSentry: A deep learning approach to detecting incipient large-scale network attacks," *IEEE/ACM Transactions on Networking*, 2022.

[10] Y. Wei et al., "Reconstruction-based LSTM-autoencoder for anomaly-based DDoS attack detection over multivariate time-series data," *Future Generation Computer Systems*, 2023.

[11] M. Revathi and M. Malathi, "Detection of unknown DDoS attacks with deep learning and Gaussian mixture model," *Applied Sciences*, vol. 11, no. 11, p. 5213, 2021, doi: 10.3390/app11115213.

[12] R. Efendi et al., "Real-time DDoS detection in high-speed networks: A deep learning approach with multivariate time series," *Electronics*, vol. 14, no. 13, p. 2673, 2024.

[13] M. A. Ullah et al., "Detecting distributed denial of service attacks using logistic regression and support vector machine methods," *Journal of Network and Computer Applications*, 2024.

[14] Churcher et al., "An experimental analysis of attack classification using machine learning in IoT networks," *Future Internet*, vol. 13, no. 1, 2021.

[15] Hekmati et al., "Correlation-aware neural networks for DDoS attack detection in IoT systems," *IEEE Internet of Things Journal*, 2023.

[16] Sharma et al., "Attention meets UAVs: A comprehensive evaluation of DDoS detection in low-cost UAVs," *IEEE Access*, 2024.

[17] S. Kanthimathi et al., "A self-attention-enabled weighted ensemble-based convolutional neural network framework for distributed denial of service attack classification," *Computer Networks*, 2024.

[18] Alasmari et al., "CNN-LSTM based deep learning approach for DDoS attack detection in IoT networks," *Frontiers in Artificial Intelligence*, 2023.

[19] M. A. Al-Qatf et al., “Deep learning approach combining CNN and LSTM for network intrusion detection,” *Springer International Journal of Computational Intelligence Systems*, 2025.
[20] K. Singh and S. Jang-Jaccard, “Hybrid deep learning model for detecting distributed denial of service attacks in software-defined networks,” *Journal of Network and Systems Management*, Springer, 2024.