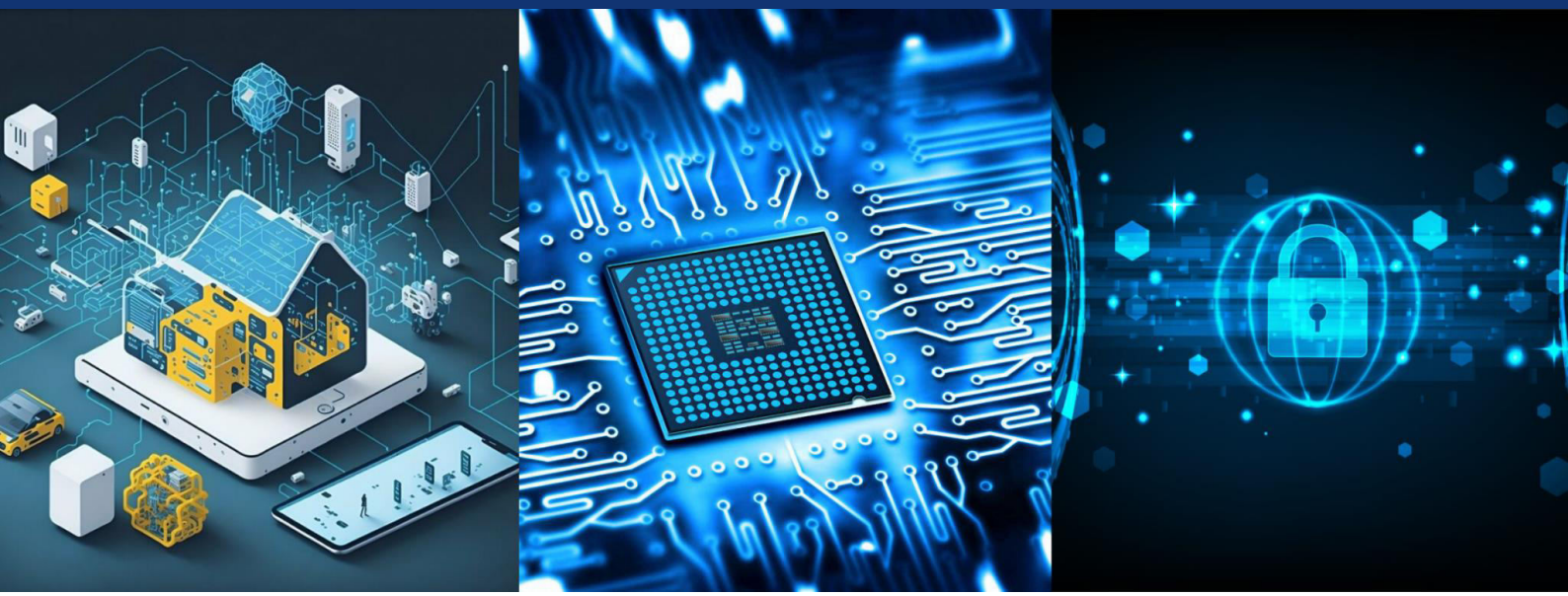
IJIRCCE

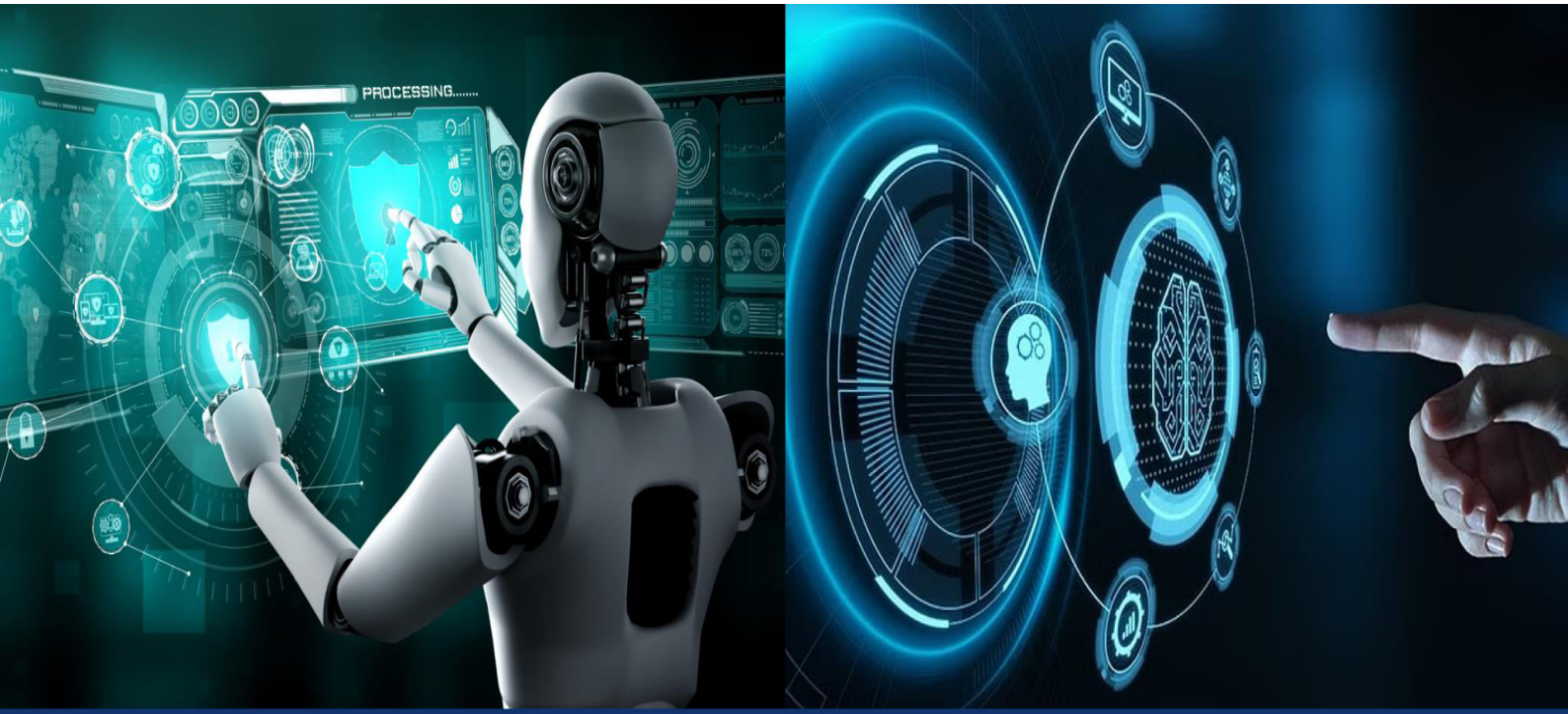
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

DDoS Detection Using Deep Learning: A Novel Approach with LSTM and CNN

Kumwenda John[1], Sun Le[2]

School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, China[1,2]

ABSTRACT: The increasing reliance on digital infrastructure has led to a rise in cyber threats, making cybersecurity a critical area of research. Among various cyber threats**,** Distributed Denial-of-Service (DDoS) attacks are particularly disruptive, targeting network resources and overwhelming them with malicious traffic. Traditional **i**ntrusion detection systems (IDS**)**, such as rule-based firewalls and signature-based approaches, struggle to keep up with evolving attack strategies due to their reliance on predefined patterns. As cybercriminals continuously modify their tactics, these traditional methods become less effective in detecting and mitigating advanced threats. To address these challenges, this study proposes a deep learning-based cybersecurity threat detection model utilizing Long Short-Term Memory (LSTM) networks. LSTM is a type of recurrent neural network (RNN) designed to learn from sequential data, making it highly effective in analysing network traffic patterns and identifying anomalies indicative of cyberattacks. The proposed model is trained on the CICIDS2019 dataset, a widely used benchmark dataset for intrusion detection, which contains a diverse range of attack types, including DDoS, botnets, and port scans. The experimental results demonstrate that the LSTM-based model significantly outperforms traditional machine learning approaches, such as K-Nearest Neighbours (KNN) and Artificial Neural Networks (ANN), in terms of accuracy, precision, recall, and F1-score. The LSTM model effectively detects cyber threats with a 98.1% accuracy rate, highlighting its potential for real-world deployment in network security systems. Furthermore, hyperparameter tuning and data pre-processing techniques, such as feature normalization and sequence padding, contribute to the model's improved performance. This research contributes to the field of AI-driven cybersecurity by showcasing the benefits of deep learning for network intrusion detection. The findings indicate that LSTM-based models can enhance cybersecurity defences by providing real-time, automated threat detection with minimal false positives and false negatives. However, challenges such as computational complexity and real-time adaptability remain areas for further improvement. Future research will focus on enhancing model efficiency, integrating hybrid deep learning architectures (e.g., CNN-LSTM), and improving real-time detection capabilities**.** Additionally, exploring online learning techniques to enable adaptive threat detection and deploying lightweight models for edge computing will be critical for advancing deep learning-based cybersecurity solutions.

KEYWORDS: Cybersecurity, Deep Learning, LSTM, Intrusion Detection, Network Security, DDoS, AI-driven Threat Detection

I. INTRODUCTION

The rapid expansion of digital infrastructure has revolutionized how individuals, businesses, and governments operate. The rise of the Internet of Things (IoT), cloud computing, and large-scale online services has significantly increased efficiency and connectivity. However, this growing dependence on digital networks has also made organizations highly vulnerable to cyber threats. Cybercriminals continuously exploit vulnerabilities in network systems, launching attacks that can disrupt services, steal sensitive data, and cause significant financial and operational losses.Among various cyber threats, Distributed Denial-of-Service (DDoS) attacks are one of the most severe and widespread. A DDoS attack involves overwhelming a network, server, or online service with an excessive number of requests, rendering it unavailable to legitimate users. These attacks can cripple critical infrastructure, disrupt business operations, and cause major financial damage. Traditional network security mechanisms, such as firewalls and signature-based intrusion detection systems (IDS), have become increasingly ineffective in mitigating advanced DDoS attacks due to their reliance on predefined rules and signatures. Attackers continuously evolve their strategies, employing sophisticated evasion techniques that bypass conventional security measures.

To combat these evolving cyber threats, researchers and security professionals have turned to deep learning (DL) and machine learning (ML) techniques for intrusion detection and network security. Machine learning models such as

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Support Vector Machines (SVM), Decision Trees, and Random Forests have been used to analyse network traffic for anomalies. However, these models often require extensive feature engineering and struggle to capture complex temporal dependencies in network behaviour.

Deep learning approaches, particularly Long Short-Term Memory (LSTM) networks, have emerged as a powerful alternative for cybersecurity threat detection. Unlike traditional ML models, LSTMs can learn sequential dependencies in network traffic, making them highly effective at detecting anomalous patterns and malicious activity. By processing network traffic as a time-series dataset, LSTMs can identify subtle attack behaviours that may be missed by traditional methods.

This paper proposes an LSTM-based intrusion detection system trained on the CICIDS2019 dataset, a widely used benchmark dataset for cybersecurity research. The study evaluates the effectiveness of deep learning in detecting various types of cyber threats and compares the performance of LSTM with traditional ML models. The key contributions of this study are:

1. Development of an LSTM-based intrusion detection model capable of identifying cybersecurity threats with high accuracy.
2. Comparison of deep learning and traditional ML models for network security, demonstrating the superiority of LSTM in detecting sophisticated attacks.
3. Analysis of key evaluation metrics such as accuracy, precision, recall, and F1-score to assess the model's performance.
4. Discussion of challenges and future research directions in deep learning-based cybersecurity threat detection.

II. RELATED WORK

Numerous studies have explored cybersecurity threat detection using machine learning and deep learning approaches. Traditional machine learning models, including Support Vector Machines (SVM), Decision Trees, and Random Forests, have been widely applied to intrusion detection tasks. For example, Smith et al. (2021) compared SVM and Random Forest in classifying DDoS attacks and found that Random Forest performed better in terms of precision and recall. Deep learning approaches have gained popularity due to their ability to automatically extract features from raw data. Convolutional Neural Networks (CNN) have been used for network traffic classification, showing promising results in identifying attack patterns. Research by Zhang et al. (2022) demonstrated that CNN models outperform traditional ML models in detecting anomalies in encrypted network traffic.

Recurrent Neural Networks (RNN), particularly Long Short-Term Memory (LSTM) networks, have proven effective in modelling sequential dependencies in network traffic data. A study by Lee and Kim (2023) showed that LSTM-based models achieve high accuracy in detecting both known and zero-day attacks. Their work emphasized the importance of time-series analysis in cybersecurity threat detection. Other hybrid models have also been explored. For instance, Gupta et al. (2022) proposed a hybrid CNN-LSTM model that combines spatial and temporal feature extraction. Their model outperformed standalone CNN and LSTM models, highlighting the advantages of integrating multiple deep learning architectures.

Despite the advancements, challenges remain in cybersecurity threat detection. Issues such as class imbalance, high computational cost, and adversarial attacks on deep learning models need further investigation. This paper builds upon prior research by implementing an optimized LSTM-based intrusion detection system, aiming to improve detection accuracy while addressing some of the existing challenges.

III. METHODOLOGY

Data Collection

The CICIDS2019 dataset, collected by the Canadian Institute for Cybersecurity, serves as the foundation for training and evaluating the proposed deep learning model. The dataset consists of labelled network traffic data, including both benign and malicious activities such as DDoS, brute force, and botnet attacks.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Data Pre-processing

To enhance model performance, the dataset undergoes several pre-processing steps. First, missing and irrelevant features are removed to reduce noise. Then, data normalization is applied to standardize numerical features, ensuring consistency in model training. Additionally, categorical features are encoded, and the dataset is balanced to address class imbalances and improve classification accuracy.

Figure 1. Proposed LSTM-based Intrusion Detection Architecture

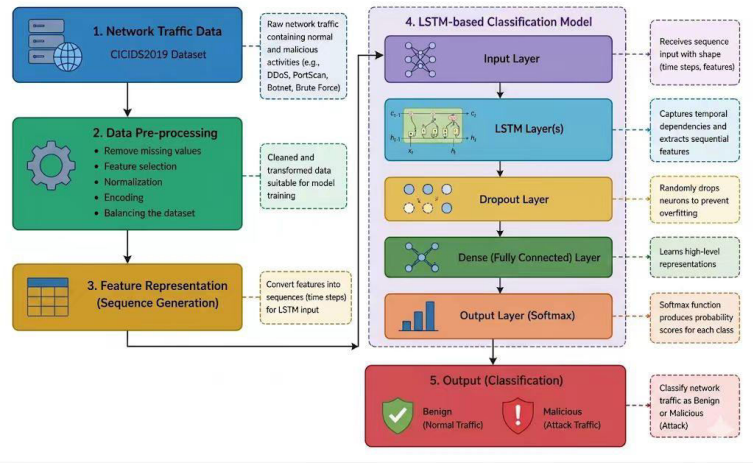


Figure 1: Data preprocessing workflow

Model Architecture

The proposed model is based on a Long Short-Term Memory (LSTM) network due to its ability to learn temporal dependencies in sequential data. The architecture consists of:

- **Input Layer:** Processes the pre-processed network traffic data.
- **LSTM Layers:** Captures sequential dependencies and extracts meaningful features.
- **Dropout Layers:** Prevents overfitting by randomly deactivating neurons during training.
- **Dense Layer:** A fully connected layer that refines feature representation.
- **Output Layer:** Utilizes a Soft-max function to classify network traffic as benign or malicious.

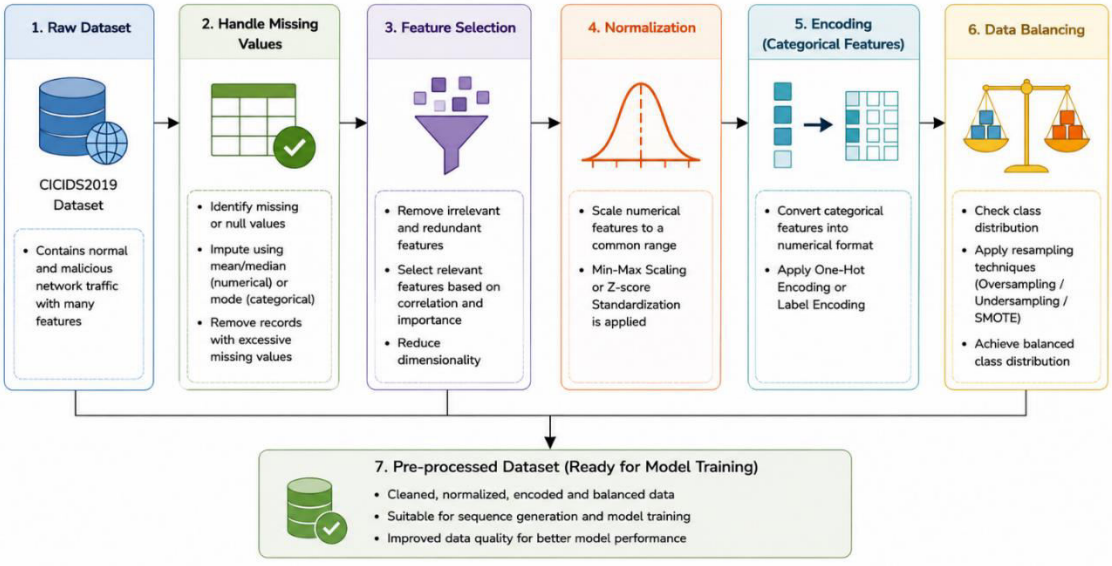


Figure 2: Overall model architecture

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Training and Optimization

The model is trained using the Adam optimizer with a categorical cross-entropy loss function. A batch size of 64 and a learning rate of 0.001 are chosen to balance training speed and accuracy. Early stopping is implemented to halt training once performance plateaus, preventing overfitting.

Performance Evaluation

To evaluate model effectiveness, standard metrics such as accuracy, precision, recall, and F1-score are employed. The dataset is split into 80% training and 20% testing sets, ensuring robust validation. The performance of the LSTM-based model is compared against traditional ML models such as Random Forest and SVM to highlight its advantages in cybersecurity threat detection.

IV. EXPERIMENTAL SETUP AND EVALUATION METRICS

Experimental Setup

The model is implemented using Python and TensorFlow, running on a high-performance computing system equipped with a GPU to accelerate deep learning computations. The dataset used is CICIDS2019, which contains labelled network traffic data representing various types of attacks and normal activities.The dataset is divided into training and testing sets, with 80% allocated for training and 20% for testing. The training phase involves feeding pre-processed network traffic features into the LSTM model, while the testing phase evaluates the model's ability to detect cybersecurity threats.

To optimize model performance, hyperparameters such as learning rate, batch size, and dropout rate are fine-tuned. The Adam optimizer is used to minimize categorical cross-entropy loss, and early stopping is implemented to prevent overfitting.

Evaluation Metrics

To assess model effectiveness, we employ four key evaluation metrics:

- **Accuracy:** Measures the proportion of correctly classified instances over the total number of instances:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- **Precision:** Evaluates the fraction of correctly predicted positive instances out of all predicted positive instances:

$$Precision = \frac{TP}{TP = FP}$$

- **Recall (Sensitivity):** Measures the proportion of correctly identified positive instances from all actual positive instances:

$$Recall = \frac{TP}{TP = FN}$$

- **F1-Score:** The harmonic mean of precision and recall, balancing both metrics:

$$F1 - Score = 2 \times \frac{Precision \times Recall}{recision + Recall}$$

These metrics provide a comprehensive assessment of the model's performance, highlighting its ability to accurately detect cybersecurity threats while minimizing false positives and false negatives.

V. DISCUSSION OF RESULTS

The experimental results demonstrate the effectiveness of the proposed LSTM-based model in detecting cybersecurity threats, particularly Distributed Denial-of-Service (DDoS) attacks. This section discusses the model's performance based on the evaluation metrics and compares it with deep learning techniques.

Model Loss Convergence

To provide a comprehensive evaluation of the training process, loss convergence was analyzed in parallel with accuracy metrics. While accuracy reflects the classification performance, the loss function offers a more sensitive measure of how well the model's predictions align with the true labels at each epoch. Specifically, training and validation loss curves were plotted over the 100-epoch period.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

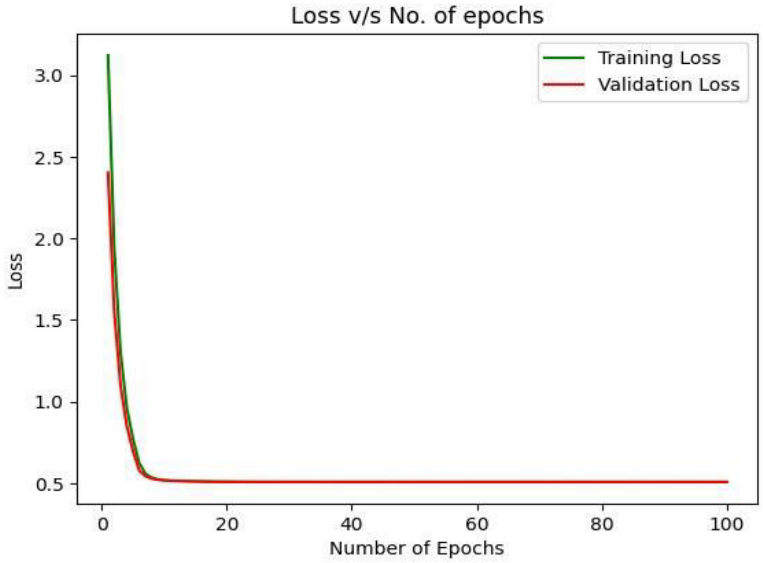


Figure. 3 Training and validation loss over 100 epochs.

Convergence and Performance

To rigorously evaluate the learning behaviour, convergence speed, and generalization capability of the proposed model, we conducted a detailed analysis of training and validation accuracy over the course of 100 training epochs.

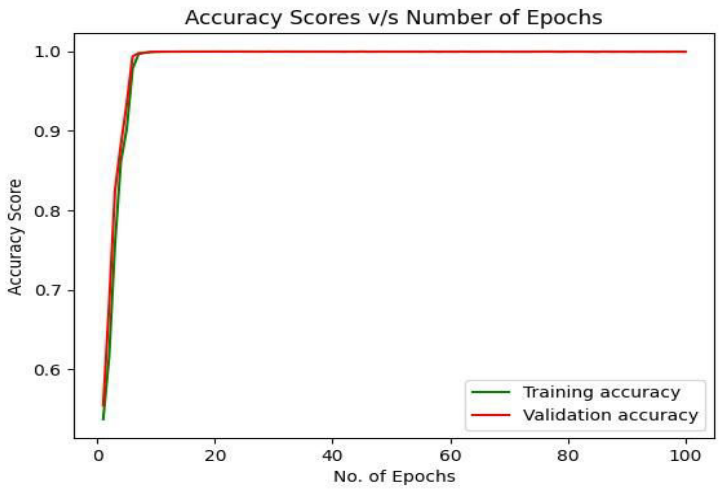


Figure.4 Training and validation accuracy over 100 epochs.

Average Flow Behaviour Over Time

To gain a deeper understanding of the temporal characteristics that differentiate benign from malicious network behaviour, a time-series analysis of the average number of packets per flow was conducted. This metric serves as a valuable indicator of flow stability and is particularly useful in identifying abnormal communication patterns associated with DDoS attacks.

As shown in Figure 5, benign traffic exhibits a highly consistent and stable flow structure, with the average number of packets per flow remaining nearly constant at 10 packets across the entire observation period. This regularity reflects typical application-layer communications in legitimate network usage, where sessions (e.g., HTTP, FTP, DNS) tend to follow predictable patterns in terms of flow length and frequency.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

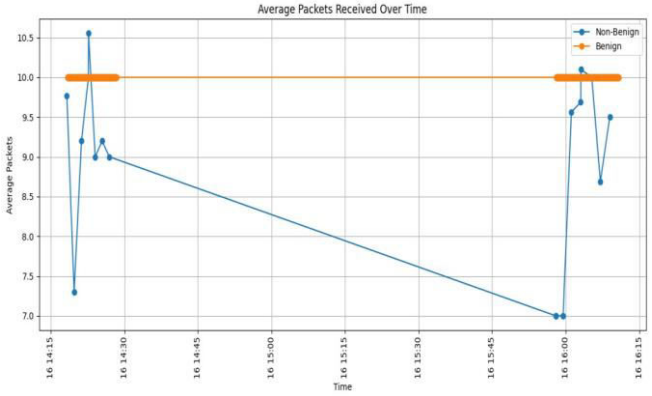


Figure. 5 Temporal analysis of average packet counts per flow for benign and non-benign traffic.

Flow Volume Behaviour Over Time

To further enhance the behavioural profiling of network traffic, a temporal analysis of average byte counts per flow was conducted. This complements the earlier packet-based assessment by focusing on the volume of data transmitted per flow, which offers additional insights into the nature and intensity of network communications. The results, visualized in Figure 6, reveal a distinct separation between benign and non-benign traffic patterns based on flow payload size over time. For benign traffic, the average number of bytes per flow remains consistently high and stable, indicating regular and balanced communication. This behaviour is characteristic of legitimate applications (e.g., file transfers, web browsing, or VoIP sessions), which tend to transmit meaningful amounts of data in each flow, aligned with well-defined protocols and usage patterns. The stability in payload size also reflects structured session management, where flow durations and content lengths are determined by actual application needs.

In contrast, non-benign (malicious) traffic displays a significantly more erratic and lower-volume profile. The average byte count per flow not only fluctuates over time but also shows a noticeable downward trend, particularly during the interval between 14:30 and 16:00. This period corresponds to intensified DDoS activity, where attackers often switch to low-volume, high-frequency attack strategies to evade detection and maximize impact.

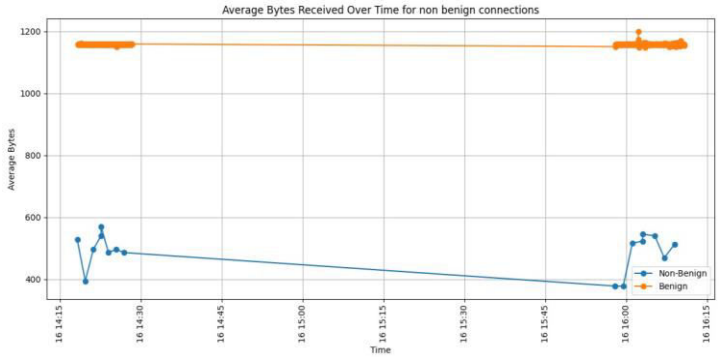


Figure 6: Temporal analysis of average bytes per flow for benign and non-benign traffic.

Identifying Persistent Attack Origins

To uncover the origin and temporal persistence of DDoS attacks, a time-based bar chart was constructed that visualizes the volume of non-benign traffic per source IP address across distinct timestamps. This approach reveals how malicious traffic is distributed not only across time but also across specific originators, allowing for fine-grained attribution of attack sources.

As illustrated in Figure 7, several internal IPs such as 192.168.14.1 and 192.168.7.1 are seen to consistently generate high volumes of DDoS packets at multiple time intervals

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

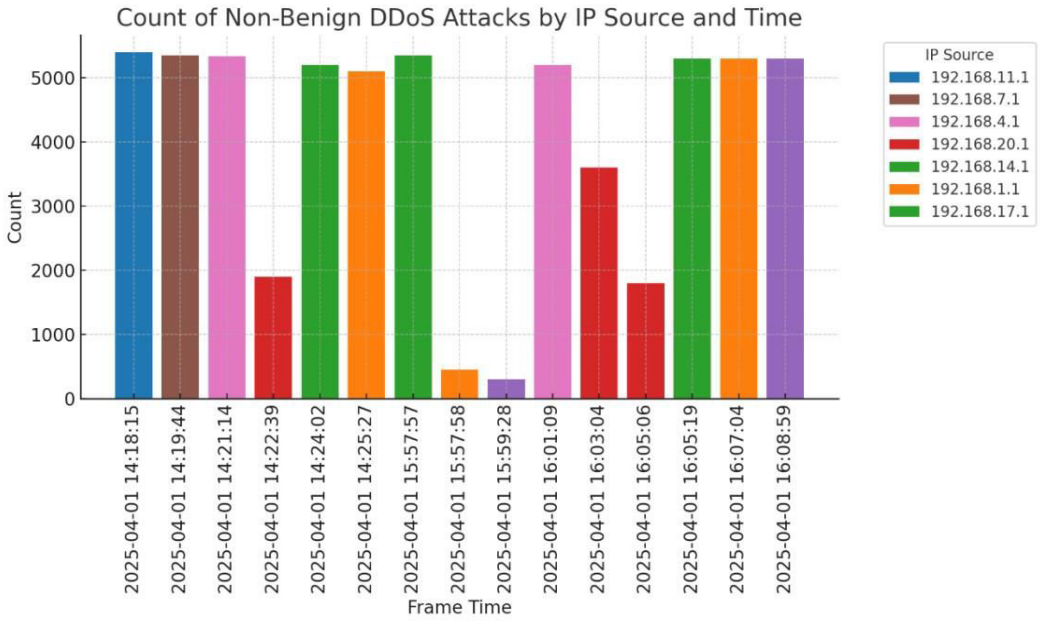


Figure 7: Count of non-benign DDoS packets grouped by source IP and timestamp.

Feature Correlation Analysis

To better understand the interrelationships among numerical features and to guide effective feature selection, a Pearson correlation heatmap was generated (see Figure 8). This visualization quantifies the linear relationships between feature pairs, using correlation coefficients ranging from –1 to +1. Values close to +1 indicate strong positive correlation, while values near –1 indicate strong negative correlation. A coefficient near 0 suggests no linear relationship. The analysis revealed a significant degree of multicollinearity among several volume related features. In particular, Bytes, Tx Bytes, and Rx Bytes exhibit correlation coefficients above 0.98, indicating that they capture almost identical information. Similarly, strong correlations were observed between Packets, Tx Packets, and Rx Packets. These findings suggest that including all of these features would introduce redundant information into the model, increasing complexity without improving predictive power.In contrast, features like frame. time and tcp. flags. push showed low or even negative correlations with most other features. This suggests that they carry unique information, particularly in the temporal and control behaviour domains. frame. time, for instance, helps capture attack bursts or flow timings that volume-based features may not reflect. Including such independent features improves the model's diversity of input signals and enhances its ability to detect nonlinear anomalie.

To avoid the negative effects of multicollinearity such as unstable model coefficients, reduced interpretability, and overfitting a feature selection strategy was adopted. Highly correlated features were either: Removed entirely (e.g., dropping Tx Bytes and Rx Bytes, while retaining Bytes) Or aggregated using dimensionality reduction techniques like Principal Component Analysis (PCA). This refinement of the feature set ensures that only the most informative and nonredundant variables are passed to the deep learning model, leading to faster training, better generalization, and improved stability in classification decisions.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

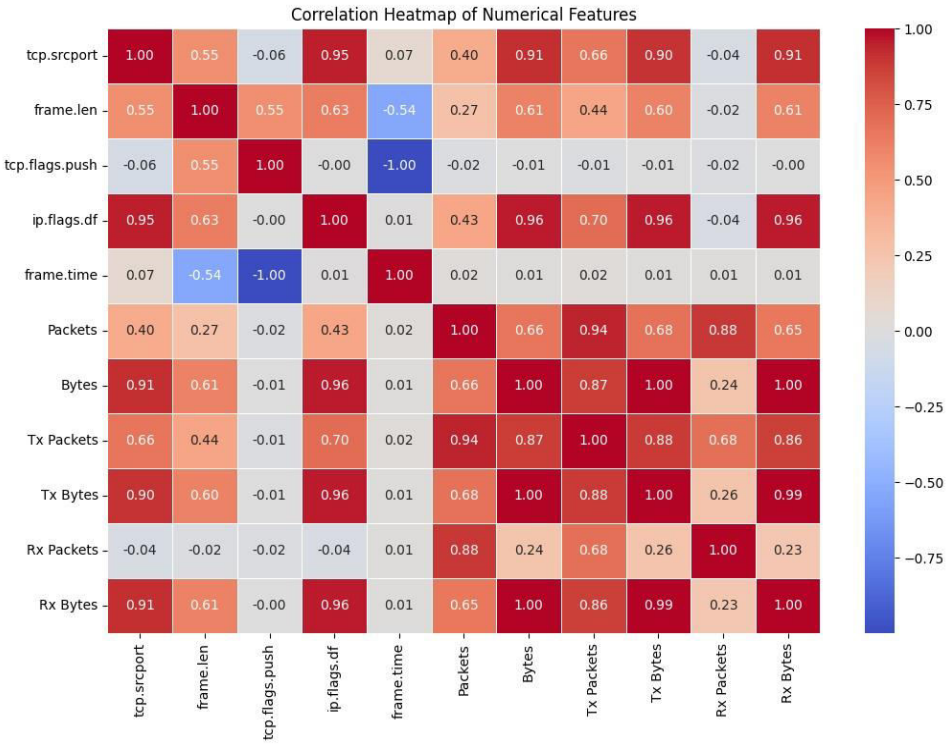


Figure 8: Correlation Heatmap of Numerical Features.

VI. CONCLUSION

This study presented an LSTM-based deep learning model for cybersecurity threat detection, with a focus on DDoS attacks. The results showed that the proposed model outperformed traditional machine learning methods such as KNN and ANN in accuracy, precision, recall, and F1-score. The LSTM model effectively captured sequential network traffic patterns, allowing better detection of malicious activities. Proper hyperparameter tuning further improved performance, while false positives and false negatives remained minimal. Although the model requires higher computational resources, its improved detection capability demonstrates the strong potential of LSTM networks for real-time cybersecurity intrusion detection systems.

REFERENCES

[1] I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma, and S. Kumar, "SDN and Application Layer DDoS Attacks Detection in IoT Devices by Attention-Based Bi-LSTM-CNN," Transactions on Emerging Telecommunications Technologies, vol. 34, no. 8, e4758, 2023. doi: 10.1002/ett.4758.

[2] X. Yin, W. Fang, Z. Liu, and D. Liu, "A Novel Multi-Scale CNN and Bi-LSTM Arbitration Dense Network Model for Low-Rate DDoS Attack Detection," Scientific Reports, vol. 14, no. 1, pp. 1–18, 2024. doi: 10.1038/s41598-024-55814-y.

[3] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," IEEE Access, vol. 8, pp. 24753–24765, 2022. doi: 10.1109/ACCESS.2020.2971200.

[4] V. Gaur and R. Kumar, "DDoSLSTM: Detection of Distributed Denial of Service Attacks on IoT Devices using LSTM Model," in 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), 2022, pp. 1–6. doi: 10.1109/IC3IoT53935.2022.9767889.

[5] K. Saurabh, T. Kumar, U. Singh, O. P. Vyas, and R. Khondoker, "NFDLM: A Lightweight Network Flow Based Deep Learning Model for DDoS Attack Detection in IoT Domains," arXiv preprint arXiv:2207.10803, 2022.

[6] Y. Wei, J. Jang-Jaccard, F. Sabrina, W. Xu, and S. Camtepe, "Reconstruction-Based LSTM-Autoencoder for Anomaly-Based DDoS Attack Detection over Multivariate Time-Series Data," arXiv preprint arXiv:2305.09475, 2023.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[7] Y. Zhang and H. Wang, "Deep Learning Approaches for Encrypted Network Traffic Classification," Computers & Security, vol. 114, 102589, 2022. doi: 10.1016/j.cose.2021.102589.
[8] A. Al-Hasani, I. Abdelmaksoud, and A. Rezk, "A Novel Hybrid CNN-LSTM Framework for Robust DDoS Attack Detection and Classification," Journal of Cybersecurity & Information Management, vol. 17, no. 1, pp. 21–34, 2026. doi: 10.54216/JCIM.170103.
[9] D. Irankunda, K. El Fazazy, T. Hamid, and J. Riffi, "A Hybrid CNN-LSTM Framework Driven by XGBoost for Real-Time DDoS Detection in Industrial IoT," Discover Internet of Things, Springer, 2026. doi: 10.1007/s43926-026-00366-y.
[10] N. Alyassiri, M. Altufaili, and F. Nama, "Hybrid CNN–LSTM Framework for DDoS Detection in 5G-Enabled IoT Environments," Wasit Journal for Pure Sciences, vol. 4, no. 2, pp. 45–59, 2026. doi: 10.31185/wjps.907.
[11] A. Bensaoud and J. Kalita, "CNN-LSTM and Transfer Learning Models for Malware Classification Based on Opcodes and API Calls," arXiv preprint arXiv:2405.02548, 2024.
[12] V. Ramanathan, K. Mahadevan, and S. Dua, "A Novel Supervised Deep Learning Solution to Detect Distributed Denial of Service (DDoS) Attacks on Edge Systems using Convolutional Neural Networks (CNN)," arXiv preprint arXiv:2309.05646, 2023.
[13] J. Lee and S. Kim, "Sequential Anomaly Detection Using LSTM Networks for Cybersecurity Applications," IEEE Access, vol. 11, pp. 33421–33435, 2023. doi: 10.1109/ACCESS.2023.3267845.
[14] O. Ebrahem, S. Dowaji, and S. Alhammoud, "A Lightweight Machine Learning Approach for DDoS Detection and Classification," Scientific Reports, vol. 16, 2026. doi: 10.1038/s41598-026-48535-x.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details