



RESEARCH ARTICLE

OPEN ACCESS

TOWARDS SPATIO-TEMPORAL DEEP LEARNING WITH FEATURE SELECTION FOR ROBUST DDOS ATTACK DETECTION

Mohammed Kamel Benkaddour¹, Mohammed El Aymene Beyat²^{1,2}Department of Computer Science and Information Technology, Laboratory of Artificial Intelligence and Information Technologies (LINATI), Kasdi Merbah University, Ouargla, Algeria.¹<http://orcid.org/0009-0006-2471-3242> , ²<http://orcid.org/0009-0001-5275-4627> E-mail: Benkaddour.kamel@univ-ouargla.dz, beyat.mohammedelaimene@univ-ouargla.dz

ARTICLE INFO

ABSTRACT

Article History

Received: January 30, 2026

Reviewed: February 31, 2026

Accepted: April 01, 2026

Published: May 29, 2026

Keywords:DDoS attacks,
CNN-LSTM,
CICDDoS2019,
PCA,
Cyber security.

Distributed Denial of Service (DDoS) attacks represent a significant challenge to network security, making timely detection critical. In this paper, we present a hybrid deep learning approach that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks with feature selection based on Principal Component Analysis (PCA). We apply this method to the CICDDoS2019 dataset, which includes various DDoS attack scenarios. Our approach aims to enhance detection performance by using CNN for spatial feature extraction and LSTM for temporal sequence learning. Our experiments show that deep learning can effectively identify DDoS attacks with high accuracy when the data is properly preprocessed. The results indicate that our model outperforms traditional methods, achieving high accuracy, precision, and recall.



Copyright ©2026 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

1. INTRODUCTION

Nowadays, networks and connected systems face real threats, whether intentional or accidental. It seems that every day, a new story about cybersecurity challenges is published. Whether it is the hacking of privacy on social networks, credit card fraud, economic espionage, computer system infection, denial of service attacks, and many other cyber threats that represent major problems and challenges for the years to come. These cyber threats of cybersecurity are considered today as one of the main concerns and one of the most active areas of scientific research [1-2]. Distributed Denial of Service (DDoS) attacks have increased in frequency and complexity, posing a major challenge to the security of networks and systems [3]. A DDoS attack floods a target system with an overwhelming amount of traffic, rendering it unavailable to legitimate users. Traditional detection methods based on predefined rules or signature matching have limitations in detecting novel attacks, as they rely on known patterns. The complexity and scale of DDoS attacks have grown rapidly, making traditional detection techniques less effective in dynamic network environments [4]. With the rise of large-scale datasets and machine learning techniques, especially deep learning, there has been a growing interest in automating the detection of these attacks.

Deep learning models, due to their ability to learn complex patterns in data, offer a promising solution to identifying DDoS attacks [5], even those with previously unseen characteristics. Deep learning techniques, particularly Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have shown promise in detecting complex patterns in large-scale datasets [6-7]. CNNs are effective for spatial feature extraction, while LSTMs excel at capturing temporal dependencies in sequential data. By combining both CNN and LSTM, we aim to improve the accuracy of DDoS detection. Furthermore, feature selection using Principal Component Analysis (PCA) helps reduce the dimensionality of the dataset, improving computational efficiency without sacrificing performance [8], [9]. This study proposes DDoS attack detection system combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, integrated with Principal Component Analysis (PCA) for feature selection. CNN is effective in extracting spatial features, while LSTM captures temporal dependencies in network traffic. PCA is employed to reduce feature dimensionality, enhancing model performance. The model is evaluated on the CICDDoS2019 dataset, one of the largest and most realistic DDoS datasets available.

II. RELATED WORK

Previous studies on DDoS detection have employed a wide range of techniques, including statistical methods, rule-based systems, and machine learning models [10]. Traditional approaches, such as traffic analysis based on fixed thresholds or anomaly detection using statistical models, are often unable to cope with the dynamic and evolving nature of DDoS attacks. In recent years, advancements in machine learning (ML) and deep learning (DL) techniques have significantly enhanced the effectiveness of Distributed Denial of Service (DDoS) attack detection systems. These techniques leverage the ability to analyze vast amounts of data, identifying patterns and anomalies that are indicative of DDoS attacks [11], [12]. This section reviews literature focusing on these advancements and their impact on detection systems. Machine learning has been increasingly used in recent years to address these limitations. Techniques such as Support Vector Machines (SVM), Random Forests (RF), and k-Nearest Neighbors (k-NN) have been applied to detect anomalies in network traffic that indicate DDoS attacks. However, these models often require manual feature selection and may not generalize well to new attack patterns. Deep learning, particularly with neural networks, has emerged as a promising approach due to its ability to automatically learn features from raw data.

Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), and Deep Neural Networks (DNN) have shown significant improvements in accuracy over traditional machine learning models for a variety of cybersecurity tasks, including DDoS detection [13], [14], [15]. There are a lot of relevant literature reviews related to DDoS detection employed different techniques, including machine learning and deep learning models. The examination conducted by Hosseini and Azizi [14] employed a hybrid machine learning approach combining Random Forest and Support Vector Machines for DDoS detection. Their model outperformed traditional methods by providing higher accuracy and lower false positive rates, demonstrating the effectiveness of ensemble techniques in handling complex attack patterns. Similarly, Lai et al. in [15] explored the application of Convolutional Neural Networks (CNNs) for detecting DDoS attacks. They used packet-level data and reported that CNNs could automatically extract relevant features from raw data, leading to improved detection rates compared to classical feature engineering methods. In a study by Laghrissi et al. [16], a deep learning architecture known as Long Short-Term Memory (LSTM) networks was utilized to analyze time-series network traffic data.

Their results highlighted LSTM's capability to capture temporal dependencies in traffic patterns, which significantly enhanced the detection of sophisticated attacks. Tekleselassie [17] proposed a multi-layered deep neural network model for DDoS attack detection that incorporated both supervised and unsupervised learning techniques. Their approach effectively distinguished between legitimate and malicious traffic, achieving high detection accuracy and low computational overhead. Salahuddin et al. [18] investigated the use of Autoencoders for anomaly detection in network traffic. Their study showed that Autoencoders could effectively learn the normal behavior of network traffic and identify anomalies that signify potential DDoS attacks, offering an efficient solution for real-time monitoring. The study in Protogerou et al. [19] introduced a novel approach using Graph Neural Networks (GNNs) for DDoS detection. They propose a distributed detection scheme, which aims to monitor efficiently the entire network infrastructure by modelling network traffic as a graph, their method was able to capture complex relationships between different traffic flows and leading to better detection performance. Alghazzawi et al. [20] introduced a hybrid deep learning model that incorporates Principal Component Analysis (PCA) for feature selection to improve the accuracy of DDoS attack detection.

Their approach demonstrates that PCA can effectively reduce the dimensionality of the data, leading to more efficient and accurate detection models. Dash et al. [21] in 2024 applied PCA and convolutional neural networks (CNNs) to DDoS attack detection. Their study highlights how PCA can be used to simplify the data while CNNs provide robust detection capabilities. Shakya et al. in [22] explored the detection of DDoS attacks in IoT networks using PCA and deep learning models. Their research demonstrates the applicability of PCA for feature reduction in resource-constrained environments, and how deep learning can enhance detection capabilities. Overall, these recent advancements underscore the growing importance of sophisticated ML and DL methods in enhancing DDoS attack detection systems. By incorporating diverse approaches and combining multiple techniques, researchers have significantly improved the accuracy, efficiency, and adaptability of detection systems. The rest of this paper is organized as follows: Section 2 gives an overview of related work, Section 3 introduces the details of the proposed system, Section 4 presents the experimental analysis of the proposed system, and Section 5 summarizes this work.

III. MATERIALS AND METHODS

This section details the methodological approach adopted in this work to evaluate the application of deep neural network based intrusion detection system over a network.

III.1 DATASET OVERVIEW

The CICDDoS2019 dataset is widely used for research in DDoS attack detection. It provides realistic network traffic data, including both normal and malicious traffic, with a variety of DDoS attack types [23]. This dataset contains only DDoS attacks and benign traffic. The creators describe it as a realistic cyber defense dataset., it is a joint project of the Canadian Communications Security Establishment (CSE) and The Canadian Institute for Cybersecurity (CIC). CIC-DDoS 2019 is a new, high quality, synthetic dataset, providing both network traffic and log data. CICDDoS2019 provides benign and up-to-date typical DDoS assaults that closely replicate real-world data.

It also includes the results of the network traffic analysis performed using CICFlowMeter-V3, labeled flows based on time stamp, source and destination IPs, source and destination ports, protocols, and attacks (CSV files). In this study, we use the first day of CICDDoS2019 dataset that contain different modern reflective DDoS attacks including PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP. Throughout the training and testing process, data balance is a key component that might have an impact on the final outcomes. Given the dataset's approximately 5 million rows of benign data, the ideal strategy is to extract an appropriate proportion of attack data to match the amount of benign traffic.

However, if the number of assaults is too low, it is appropriate to down-sample innocuous traffic to match the number of attacks. Table 1 shows regenerated dataset details and the number of each assault type utilized for training and testing.

Table 1: CICDDoS2019 dataset classes details.

Dataset	Class	Number of instance for training	Number of instance for testing	Label
CICDDoS2019 (8 classes)	BENIGN	12905	3256	0
	DrDoS_NetBIOS	229153	20569	1
	DrDoS_MSSQL	159367	39948	2
	DrDoS_LDAP	81925	20569	3
	Portmap	73981	18464	4
	Syn	178821	44691	5
	DrDoS_UDP	192146	48525	6
	UDP-lag	74181	18270	7

Source: Authors, (2026).

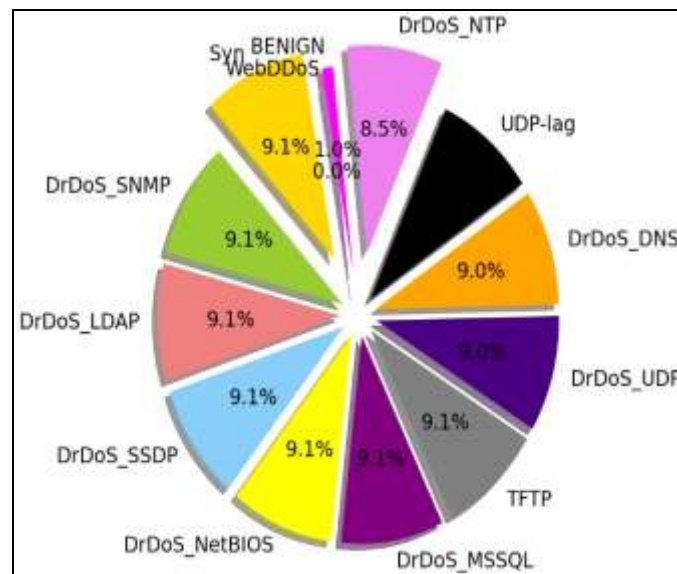


Figure 1: Pie chart of DDoS classes distribution CICDDoS2019
Source: Authors, (2026).

III.2 PREPROCESSING

The CICDDoS2019 dataset is widely used for research in DDoS attack detection. It provides realistic network traffic data, including both normal and malicious traffic, with a variety of DDoS attack types. The dataset contains 80 features, including source and destination IP addresses, packet sizes, protocols, timestamps, and other network traffic attributes.

III.2.1 Data Cleaning

Before feature selection, we applied data cleaning techniques to handle missing values and remove redundant or irrelevant features. For example, IP addresses and ports, which are less informative for DDoS detection, were excluded from the model input.

III.2.2 Normalization

To ensure that features with different scales do not skew the model's performance, we normalized the dataset using Min-Max scaling. This scales all feature values between 0 and 1, which is important for the performance of deep learning models.

III.2.3 Data Balancing

Given the class imbalance, we employed Synthetic Minority Over-sampling Technique (SMOTE) to balance the dataset. This technique generates synthetic instances of the minority class to ensure that the model is not biased towards the majority class during training. The Synthetic Minority Oversampling Technique (SMOTE) is used to address the issue of imbalanced datasets, where the classification categories are not evenly distributed. In network data, most traffic is legitimate, with only a small portion being invalid, leading to an imbalance. This imbalance results in the majority class dominating the data, which can cause classifiers. To improve a classifier's sensitivity to the minority class, two resampling techniques are typically used: under-sampling the majority class and over-sampling the minority class. In this paper, SMOTE is employed as a pre-processing technique to handle the dataset imbalance.

III.2.4 Feature Selection Using PCA

Principal Component Analysis (PCA) was applied to reduce the dimensionality of the dataset, focusing on the most relevant features. After applying PCA, we reduced the dataset's dimensionality from 80 features to 25 principal components, which captured over then 90 % of the variance in the data. This reduction not only improved the computational efficiency but also helped prevent overfitting by eliminating noise and redundancy. The dataset consists of 80 features, many of which may be redundant or irrelevant, leading to high computational costs and overfitting. To address this, Principal Component Analysis was employed for feature selection, reducing the number of features while preserving as much information as possible.

The PCA Steps:

- Covariance Matrix Calculation: The covariance matrix of the features was computed.
- Eigenvalue Decomposition: Eigenvalues and eigenvectors of the covariance matrix were derived to determine the principal components.
- Dimensionality Reduction: Based on the explained variance, the top 25 principal components were selected, reducing the feature set from 80 to 25 features.

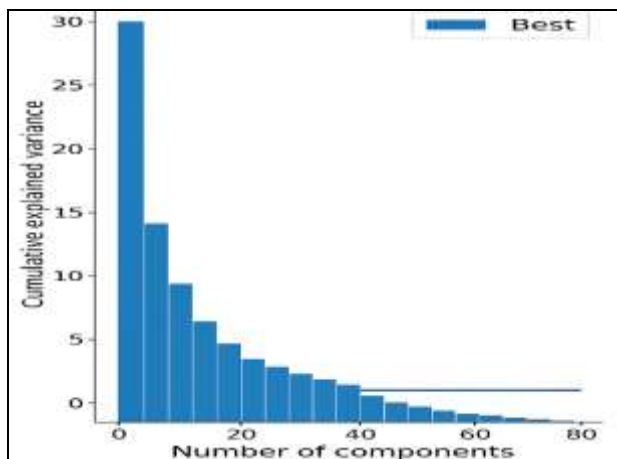
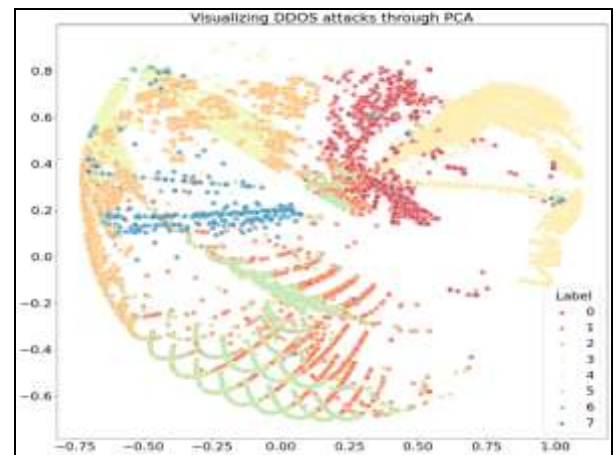


Figure 2: The best Selected Principal Components.

Source: Authors, (2026).



Figures 3: Visualisation of DDOS attack through PCA.

Source: Authors, (2026).

This dimensionality reduction significantly improves the efficiency of the proposed model by minimizing computational complexity while maintaining detection accuracy.

III.3 PERFORMANCE MEASURES

To evaluate the performance of IDS classifiers, three metrics were taken into account: accuracy, precision, and false alert rate. By focusing on these metrics, the ability of IDS classifiers to correctly identify and classify intrusion instances can be assessed while minimizing the occurrence of false positives and false negatives. Equations (1) to (4) provide the mathematical expressions for performance indicators like accuracy, precision, recall and F1-score.

- True Positive (TP): Intrusive traffic is detected as Intrusive.
- False Positive (FP): Normal traffic is detected as Intrusive.
- True Negative(TN): Normal traffic is detected as Normal.
- False Negative (FN): Malicious traffic is detected as Normal.

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

$$\text{F1 - score} = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} \quad (4)$$

III.4 PROPOSED MODEL

The proposed deep learning architecture is a hybrid model that integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to effectively capture both spatial and temporal features from network traffic data. The input to the model consists of 25 features selected through Principal Component Analysis (PCA), which ensures dimensionality reduction while preserving the most informative components.

These features are first processed by a convolutional layer, which extracts local spatial patterns within the data. To further optimize the representation and reduce computational complexity, a max pooling operation is applied to the convolutional outputs. The resulting feature maps are then fed into an LSTM layer, which is designed to learn temporal dependencies and sequential dynamics characteristic of network traffic. Finally, a fully connected layer performs classification to distinguish between normal and different malicious traffic, enabling effective intrusion detection.

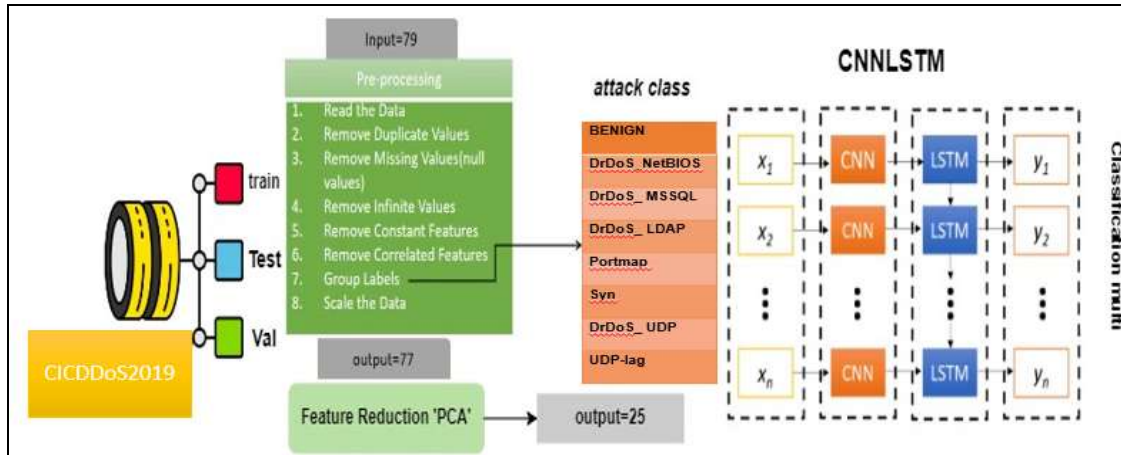


Figure 4: Architectures of the proposed model.

Source: Authors, (2026).

Table 2: Description and parameters of CNN-LSTM model.

Layer Type	Description	Parameters
Input Layer	Input features selected via PCA	PCA output
Convolutional Layer 1	First CNN layer convolution	32 filters, 3x3 kernel size, ReLU activation
Max Pooling Layer	Downsampling layer	2x2 pool size
Convolutional Layer 2	Second CNN layer for deeper feature extraction	64 filters, 3x3 kernel size, ReLU activation
Flatten Layer	Converts 2D feature maps to 1D	Flattened output from CNN layers
LSTM Layer	Sequential pattern learning	100 units
Fully Connected Layer	Dense layer	128 units, ReLU activation
Output Layer	Final output for DDoS detection	Softmax activation

Source: Authors, (2026).

IV. EXPERIMENT AND RESULT

This section presents the experimental setting, including data preparation and assessment methods to measure the framework's performance. The experiment was conducted on CPU Intel(i7) with 2 cores and 16 GB RAM to implement the proposed approach and construct our model. We utilized Google Colaboratory. In this study, it was necessary to carefully select the model to achieve better results. Therefore, we have used different deep learning techniques and other machine learning algorithms were tested, Convolutional neural network (CNN), Deep neural network (DNN), Random Forest (RF), Support vector machine (SVM), k-Nearest Neighbors (kNN) and Long Short-Term Memory (LSTM). The results obtained are shown in Table 3.

Table 3: Performance Comparison of CNN-LSTM vs Traditional Models

Model	Acc	Prec	Recall	F1-Score	AUC
CNN	96.2	95.9	96.0	95.9	95,9
DNN	95.5	94.44	95.74	95.4	95,4
LSTM	93,55	94,13	93,67	93.23	94.0
RF	95.1	94.7	95.0	94.8	95,9
SVM	93.8	93.0	93.5	93.2	0.94
k-NN	90.4	89.8	90.1	89.9	0.91
CNN-LSTM	99.98	98.9	99.20	98.9	0.99

Source: Authors, (2026).

Figure 5 and 6 show the hybrid model combining CNN and LSTM performance metrics such as accuracy and loss.

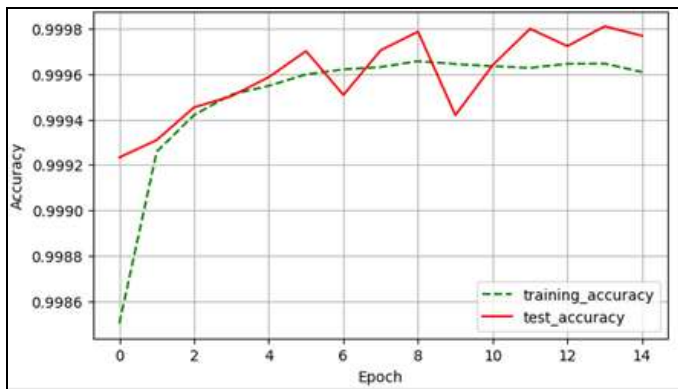


Figure 5: CNN-LSTM accuracy result.

Source: Authors, (2026).

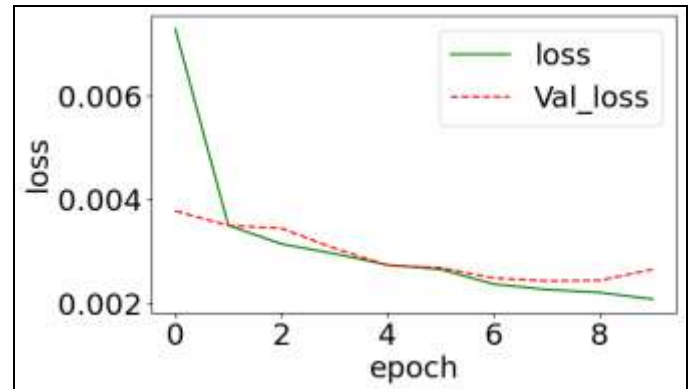


Figure 6: CNN-LSTM Loss result.

Source: Authors, (2026).

The use of oversampling via SMOTE has improved the accuracy of deep learning in a multiclass context, demonstrating the beneficial effect of this method in reducing class imbalance. With SMOTE, the accuracy of the DNN model increased from 0.85 to 0.95, that of the CNN from 0.90 to 0.96, the LSTM model from 0.85 to 0.95 and the proposed CNN-LSTM from 0.93 to 0.99, suggesting that class imbalance can have a significant impact on model performance. By producing synthetic samples for the minority classes, SMOTE helped to make the dataset more balanced, which enhanced the generalization ability of the models.

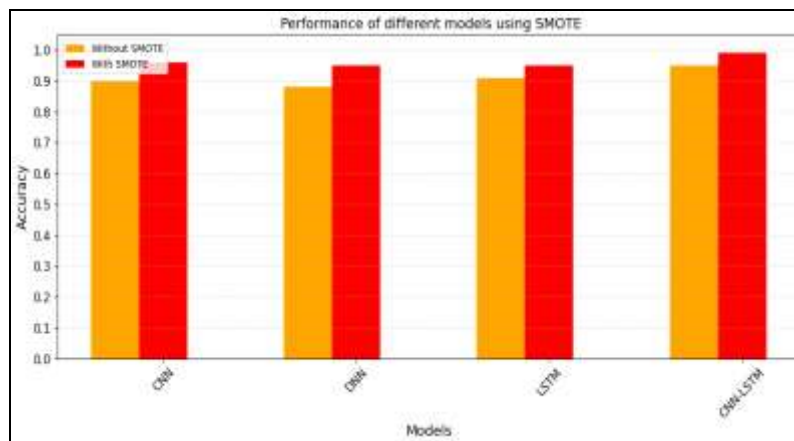


Figure 7. Performance of different models using SMOTE.

Source: Authors, (2026).

The CICIDS2019 dataset is a comprehensive dataset that includes various types of DDoS attacks, making it an ideal benchmark for evaluating the performance of detection models. The hybrid CNN-LSTM model has been tested on this dataset, showing superior performance in classifying different attack types. The integration of CNN and LSTM networks has been shown to outperform traditional detection methods, achieving high accuracy and robustness across different attack scenarios. Principal Component Analysis (PCA) is employed to reduce the dimensionality of the dataset, which helps in focusing on the most informative features. This reduction not only speeds up the training process but also helps in mitigating issues related to overfitting by eliminating noise and redundant data.

The research involved experiments using the CIC DDoS 2019 dataset, which included 8 attack and benign classes, and highlighted the importance of addressing class imbalance and dataset reduction in improving model performance.

Table 4: Classification Report per class of CICDDoS2019

Class	Precision	Rappel	F1-score	Support
BENIGN	1.00	1.00	1.00	40184
LDAP	1.00	1.00	1.00	39994
MSSQL	0.98	0.99	0.98	39944
NetBIOS	0.97	0.96	0.96	39529
Portmap	0.93	0.95	0.94	39997
Syn	1.00	1.00	1.00	39800
UDP	0.99	0.97	0.98	40142
UDPLag	0.98	0.99	0.99	40236

Source: Authors, (2026).

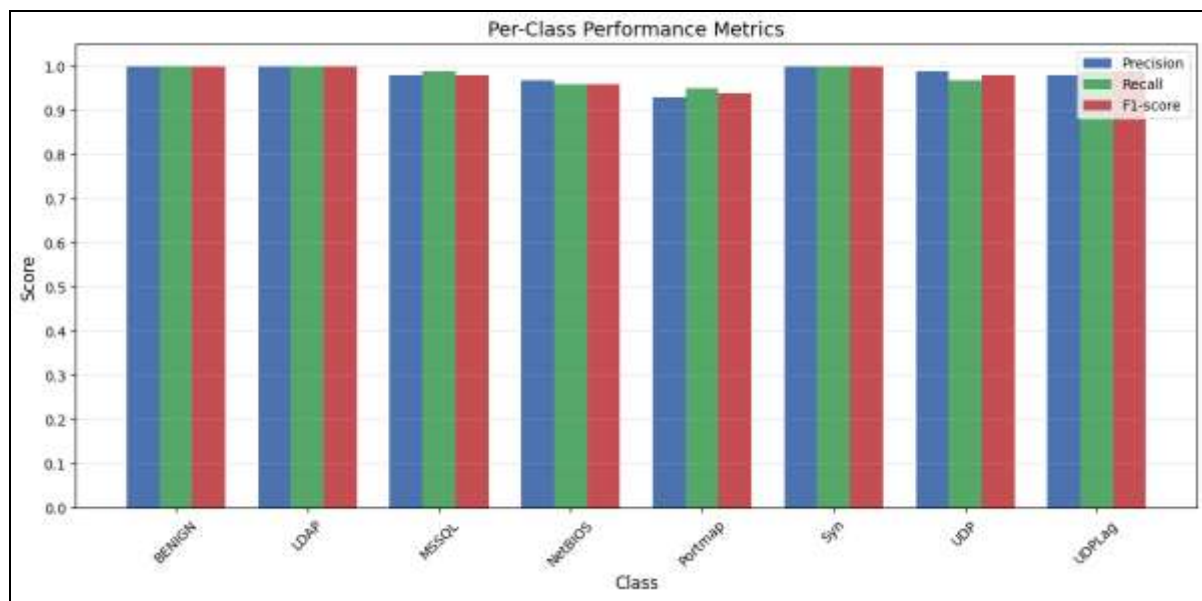


Figure 8: Performance metric multi-class in CICDDoS2019.

Source: Authors, (2026).

The hybrid CNN-LSTM model demonstrated high accuracy in classifying DDoS attacks, showcasing robust performance across various attack scenarios on the CICDDoS2019 dataset, which included multiple versions of DDoS attacks.

V. DISCUSSION

The CICIDS2019 dataset is a comprehensive dataset that includes various types of DDoS attacks, making it an ideal benchmark for evaluating the performance of deep learning models. The dataset's diversity allows for testing the model's generalization capabilities across different attack types. In this study CNNs are utilized to extract spatial features from network traffic data, identifying patterns within individual packets. LSTMs complement this by capturing temporal dependencies, such as the timing and frequency of traffic bursts, which are crucial for identifying DDoS attacks. The proposed CNN-LSTM models have demonstrated high accuracy in detecting DDoS attacks, with some models achieving up to 99.99% accuracy. This is achieved by training on labeled datasets where the model learns to distinguish between normal and malicious traffic.

By reducing the number of features, PCA helps in lowering the computational cost, making the model more efficient and faster without compromising on accuracy. Models utilizing CNNs, LSTMs, and PCA have demonstrated high accuracy and efficiency in classifying DDoS attacks within this dataset, highlighting the effectiveness of these techniques in real-world scenarios. While the integration of CNN, LSTM, and PCA has shown promising results in DDoS attack classification, it is important to consider the challenges and limitations associated with these methods. For instance, the complexity of the model architecture can lead to increased computational requirements, which may not be feasible for all network environments. Additionally, the effectiveness of these models can be influenced by the quality and diversity of the training data, underscoring the need for continuous updates and improvements to the dataset and model architecture.

VI. CONCLUSION

The research presents a deep learning-based detection model that significantly improves the accuracy and generalization of DDoS attack detection, which is crucial for enhancing network security against complex threats. This model's ability to effectively analyze both spatial and temporal features of network traffic data can lead to more reliable and timely responses to DDoS attacks. In this paper, we presented a hybrid CNN-LSTM approach with feature selection based on PCA for detecting DDoS attacks using the CICDDoS2019 dataset. Our experiments demonstrated that this method outperforms traditional machine learning techniques, achieving high accuracy and generalization capability. Our CNN-LSTM model demonstrating superior detection accuracy for DDoS attacks by combining CNN for spatial feature extraction and LSTM for temporal sequence learning, the hybrid model captures both local and long-range dependencies in network traffic data.

Furthermore, feature selection using PCA enhanced the model's efficiency by reducing the dimensionality of the data while maintaining its key characteristics. The integration of these techniques has shown to significantly improve the accuracy and robustness of DDoS attack detection systems. The proposed framework CNN-LSTM model emerged as the most effective for multiclass DDoS attack detection, demonstrating remarkable accuracy, minimal loss, and exceptional precision and recall in identifying DDoS attacks. Future work will focus on novel advanced deep learning model and extending to detect other types of network intrusions on different benchmark, we will also explore the application of other dimensionality reduction techniques and the use of real-time detection frameworks to enhance the model's deployment in production environments.

VII. AUTHOR'S CONTRIBUTION

Conceptualization: Mohammed Kamel Benkaddour and Mohammed El Aymene Beyat.

Methodology: Mohammed Kamel Benkaddour.

Investigation: Mohammed Kamel Benkaddour and Mohammed El Aymene Beyat.

Discussion of results: Mohammed Kamel Benkaddour and Mohammed El Aymene Beyat.

Writing – Original Draft: Mohammed Kamel Benkaddour.

Writing – Review and Editing: Mohammed Kamel Benkaddour and Mohammed El Aymene Beyat.

Resources: Mohammed Kamel Benkaddour.

Supervision: Mohammed Kamel Benkaddour and Mohammed El Aymene Beyat.

Approval of the final text: Mohammed Kamel Benkaddour and Mohammed El Aymene Beyat.

VIII. REFERENCES

- [1] S. P. Dandamudi, J. Sajja, and A. J. Khanna, "Advancing Cybersecurity and Data Networking Through Machine Learning-Driven Prediction Models," *Int. J. of Innovative Research in Computer Science & Technology*, vol. 13, no. 1, pp. 26–33, 2025, doi: 10.55524/ijrcst.2025.13.1.4.
- [2] C.-S. Shieh, T.-T. Nguyen, and M.-F. Horng, "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric," *Mathematics*, vol. 11, no. 9, p. 2145, 2023, doi: 10.3390/math11092145.
- [3] P. Kumar et al., "Investigating the performance of multivariate LSTM models to predict the occurrence of Distributed Denial of Service (DDoS) attack," *PLOS ONE*, vol. 20, no. 1, e0313930, 2025, doi: 10.1371/journal.pone.0313930.
- [4] Z. Xu, "Deep Learning Based DDoS Attack Detection," *ITM Web of Conferences*, vol. 70, p. 03005, Jan. 2025, doi: 10.1051/itmconf/20257003005.
- [5] M. Subramanian, K. Shanmugavadeivel, P. S. Nandhini, and R. Sowmya, "Evaluating the Performance of LSTM and GRU in Detection of Distributed Denial of Service Attacks Using CICDDoS2019 Dataset," in *Proc. Int. Conf.*, pp. 395–406, 2022, doi: 10.1007/978-981-19-2948-9_38.
- [6] T. Dhirta and A. Sharma, "Unveiling the Effectiveness of CNN-based Models for Multiclass DDoS Attack Detection and Classification: A Comparative Analysis," in *Proc. IEEE Conf.*, pp. 1–8, Dec. 2023, doi: 10.1109/icdssai59313.2023.10452429.
- [7] J. Shaikh et al., "Advancing DDoS attack detection with hybrid deep learning: integrating convolutional neural networks, PCA, and vision transformers," *Int. J. on Smart Sensing and Intelligent Systems*, vol. 17, no. 1, Apr. 2024, doi: 10.2478/ijssis-2024-0040.
- [8] L. Bagdadi and B. Messabih, "Distributed denial of service attacks classification system using features selection and ensemble techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 3, pp. 1868–1878, 2024, doi: 10.11591/ijeecs.v34.i3.pp1868-1878.
- [9] D. Tymoshchuk, O. Yasniy, M. Mytnyk, N. Zagorodna, and V. Tymoshchuk, "Detection and classification of DDoS flooding attacks by machine learning method," *arXiv preprint, arXiv:2412.18990*, 2024, doi: 10.48550/arxiv.2412.18990.
- [10] B. Badidová et al., "Federated Learning Approach to Classification of DDoS Attacks by 2D-Convolutional Neural Network," 2024, pp. 1–5, doi: 10.23919/ntsp61680.2024.10726294.
- [11] W. Chen, H. Zhang, X. Zhou, and Y. Weng, "Intrusion Detection for Modern DDoS Attacks Classification Based on Convolutional Neural Networks," in *Lecture Notes in Computer Science*, vol. 45–60, Springer, 2021, doi: 10.1007/978-3-030-79474-3_4.
- [12] A. S. Zaidoun and Z. Lachiri, "Towards deep learning multi-classification of DDoS attacks in software-defined networks," 2024, doi: 10.1109/isivc61350.2024.10577867.
- [13] C. Gao and M. Yin, "DDoS attack detection based on LSTM-GRU in SDN environment," *Proc. SPIE 12800, Int. Conf. on Artificial Intelligence and Optoelectronic Technology*, p. 128001V, 2023, doi: 10.1117/12.3004032.
- [14] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Computer Networks*, vol. 158, pp. 35–45, 2019.

- [15] Y. Lai, J. Zhang, and Z. Liu, "Industrial anomaly detection and attack classification method based on convolutional neural network," *Security and Communication Networks*, vol. 2019, no. 1, p. 8124254, 2019.
- [16] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *Journal of Big Data*, vol. 8, no. 1, p. 65, 2021.
- [17] H. Tekleselassie, "A deep learning approach for DDoS attack detection using supervised learning," in *MATEC Web of Conferences*, vol. 348, p. 01012, 2021.
- [18] M. A. Salahuddin, M. F. Bari, H. A. Alameddine, V. Pourahmadi, and R. Boutaba, "Time-based anomaly detection using autoencoder," in *2020 16th Int. Conf. on Network and Service Management (CNSM)*, pp. 1–9, Nov. 2020.
- [19] A. Protogerou, S. Papadopoulos, A. Drosou, D. Tzovaras, and I. Refanidis, "A graph neural network method for distributed anomaly detection in IoT," *Evolving Systems*, vol. 12, no. 1, pp. 19–36, 2021.
- [20] D. Alghazzawi, O. Bamasag, H. Ullah, and M. Z. Asghar, "Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection," *Applied Sciences*, vol. 11, no. 24, p. 11634, 2021.
- [21] S. K. Dash et al., "Enhancing DDoS attack detection in IoT using PCA," *Egyptian Informatics Journal*, vol. 25, p. 100450, 2024.
- [22] V. Shakya, J. Choudhary, and D. P. Singh, "Principal Component Analysis and Deep Learning-Based Traffic Anomaly Detection in WSN," in *2024 IEEE Int. Students' Conf. on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1–6, Feb. 2024.
- [23] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *IEEE 53rd Int. Carnahan Conf. on Security Technology, Chennai, India, 2019*.