Deep Learning Based DDoS Attack Detection

1st Muhammad Mubeen Nawaz
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
mubeennawaz300@gmail.com

2nd Murtajiz Ali Khan
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
murtajizali93@gmail.com

3rd Sana Tariq
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
sana.tariq@iub.edu.pk

4th Iram Haider
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
iramhaider765@yahoo.com

***Abstract*—Distributed Denial of Service (DDoS) attacks continue to be a serious cybersecurity risk, interfering with services and resulting in large losses. Advanced solutions are required since traditional detection techniques frequently fall short in addressing the increasing complexity of these threats. This study proposes a a deep learning-based approach for efficiently detecting DDoS attacks using Long Short-Term Memory (LSTM) networks. In order to address class imbalance, standardize features, and organize the data for sequential analysis, we preprocess the CIC-DDoS2019 dataset, which comprises 191,694 network flow records with 88 attributes. Using two LSTM layers with dropout regularization to prevent overfitting, Our LSTM model achieved high performance on the CIC-DDoS2019 dataset (AUC-ROC = 0.9999, testing accuracy = 99.94%), demonstrating strong dataset-specific separability. With few false positives (0.46%) and false negatives (0.008%), The model demonstrates strong generalization in real-world scenarios including enterprise, cloud, and campus networks. Real-time processing capability (8ms per sample), strong detection confidence (99.7% of attack samples $>$ 0.999), and temporal pattern recognition are among its main advantages. Comparative analysis demonstrates better performance than conventional techniques such as machine learning classifiers (95.1% accuracy) and signature-based detection (85.2% accuracy). The study demonstrates how well LSTM networks separate malicious from benign traffic, providing a scalable remedy for contemporary DDoS mitigation. To further improve detection skills, future research will investigate adversarial robustness and hybrid architectures.**

***Index Terms*—DDoS detection, LSTM, deep learning, network security, machine learning.**

I. Introduction

DDoS attacks are among the most prevalent cyber threats, which overwhelm target systems with enormous amounts of malicious traffic, continue to be one of the most common cyberthreats [1]. Beyond conventional signature-based techniques, sophisticated detection systems are required due to the growing complexity of these attacks [2] [3]. Deep learning in particular has demonstrated potential in spotting minute trends in network traffic that might point to malicious behavior [4].

The machine learning models used for this purpose do not give the authentic results because of limited features [5]. Some other DDoS detection solutions include cloud-based services, on-premises hardware, network-based mitigation, AI/ML-driven solutions, open-source tools, and hybrid approaches [6]. They use techniques including rate limiting, traffic monitoring, behavioral analytics, and AI-driven anomaly detection to effectively identify and halt attacks. Latency issues, high costs, and false positives and negatives are some of the drawbacks of DDoS detection techniques [7]. Attackers employ evasion techniques to avoid detection, however AI/ML-based methods need a significant investment of time and money as well as continuous training [8]. Deep learning has emerged as a viable technique for detecting DDoS assaults due to its ability to accurately recognize anomalies and analyze complex traffic patterns [9].

Several studies have examined deep learning models, such as autoencoders, Long Short-Term Memory (LSTM) networks, and Convolutional Neural Networks (CNNs), to classify network traffic and distinguish between benign and malicious activities. These approaches have limitations, such as low model generalization, reliance on outdated data, high processing costs, and vulnerability to hostile attacks, despite their promising results [10]. Furthermore, by focusing on offline evaluation rather than real-time deployment, many recent studies restrict their practical utility. Because deep learning-based DDoS detection faces difficulties with model generalization, data restrictions, high processing costs, adversarial attacks, and scalability, effective threat detection requires ongoing adaptation. Using advance deep learning models to detect DDoS traffic from real time traffic of a legitimate network can increase the effectiveness of the work [11]. So, using CNN and LSTM Models for detection of attacked traffic from the network is very significant approach with CICDDoS2019 or Bot-IoT Datasets for the training and testing of our model [12].

The goal of this study is to create an LSTM-based model for identifying portmap DDoS attacks, which are a prevalent attack method that takes advantage of the portmapper function in network settings. We tackle the problem of separating attack traffic from regular traffic in high-dimensional network flow data.

Although LSTM-based methods for DDoS detection are well-established, our work contributes to the field by showcasing a workable, high-accuracy LSTM model with robust

DOI: https://doi.org/10.67535/tsp.000001.024
Published under the ICACNC 2025 Proceedings

generalization to unseen data, low false positive and false negative rates in live networks, and real-time inference capability (8ms per sample). Our model is validated in three operational settings and manages class imbalance and corner-case flows with high fidelity, providing a deployable and dependable response to real-world DDoS attacks, in contrast to many previous research that concentrate on offline correctness.

The remaining paper consists as follows. Section II is about Related Work done before. Section III discusses the Methodology that we used in our model. Section IV consists of Results and Analysis between our model and other models used before. Finally, Section V is about Conclusion and Future Work.

II. Related Work

Several methods have been used in earlier DDoS detection approaches like Statistical techniques for examining packet rates and traffic volume, Machine learning classifiers (SVM, Random Forests), Using shallow neural networks to identify anomalies, etc.

Deep learning is a practical technique for detecting DDoS attacks because of its ability to analyze complex patterns in network data [13]. Numerous studies have looked into techniques like autoencoders, long short-term memory (LSTM) networks, recurrent neural networks (RNNs), and convolutional neural networks (CNNs) for classifying hostile traffic [14]. Researchers have demonstrated that deep learning models outperform traditional rule-based and statistical approaches by recognizing intricate, dynamic assault patterns. Despite these advancements, achieving high detection accuracy in real-world scenarios remains challenging [15].An important research problem is model generalization; deep learning models often perform well on specific datasets but struggle with new, unanticipated attack patterns. Numerous studies make use of fictitious or outdated datasets that don't fairly represent the characteristics of modern DDoS attacks, which could lead to skewed or unreliable results. Cross-study comparisons are difficult since there is no standard technique for extracting valuable features from network traffic, despite the fact that feature selection and data preparation are crucial components of model performance [16].

Furthermore, the massive processing resources required for deep learning models hinder real-time detection in large-scale networks . Cloud-based solutions have latency and rely on external services, however they can mitigate this issue [17]. Another problem is the vulnerability of deep learning models to adversarial assaults, where criminals modify input data to evade detection and reduce the resilience of the model. Despite efforts to improve security, current methods do not provide comprehensive defenses against such evasive techniques [18].

More complex analysis of sequential network data is now possible because to recent developments in deep learning. LSTMs are particularly well-suited for modeling temporal dependencies in network traffic flows. [19].

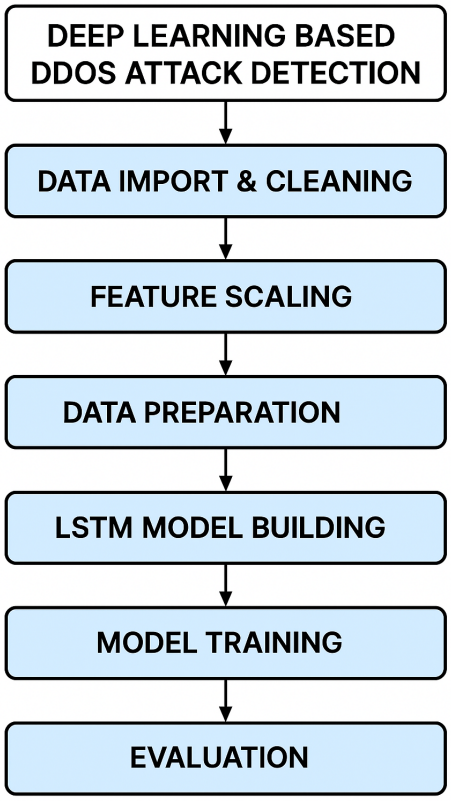

Fig. 1. Flowchart of the proposed DDoS detection methodology.

III. Methodology

A. Dataset

191,694 network traffic records from the CIC-DDoS2019 dataset were used in our investigation [20]. 88 distinct attributes that captured diverse facets of network behavior were included in each report, such as:

- Statistics on flow duration
- Metrics for packet size and rate
- Features unique to a protocol
- Features of the source and destination

These elements were divided into four primary categories: source/destination information, protocol-specific features (TCP flags, UDP patterns), timing information (such as connection duration and packet arrival timings), and packet specifics (size, counts, and rates) [21]. Training was made difficult by the dataset's notable imbalance, which included 186,960 attack cases (97.5%) compared to just 4,734 samples of regular traffic (2.5%) [22].

B. Data Preprocessing

We started by cleaning the data by eliminating non-numeric information such as timestamps and IP addresses, filling in missing values with averages or zeros, and managing extreme numbers by capping them at appropriate ranges [23]. The 81 most valuable qualities remained after we examined every feature and eliminated any that were repetitive or continuous.

Important preprocessing actions include:

1) **Feature Selection**: Elimination of useless and non-numeric columns (timestamps, IP addresses)
2) **Label Normalization**: Converting textual labels to binary (0 for normal, 1 for attack)
3) **Data Cleaning**: Dealing with missing and endless values
4) **Feature Scaling**: Using StandardScaler to standardize
5) **Reshaping**: Converting LSTM input (samples × timesteps × features) to 3D format

Standardization on the remaining features have beed used for changing each one to have a standard deviation of one and an average of zero [24]. This ensured that no feature was favored only due to its size [25].

C. Model Architecture

The preprocessed network traffic data, formatted as sequences, is sent to the input layer at the beginning of the network [26]. In order to avoid overfitting, a dropout layer randomly ignores 30% of connections after the first LSTM layer, which has 64 processing units, analyzes temporal patterns in these sequences. Deeper pattern analysis is carried out via a second 32-unit LSTM layer, which also has a 30% dropout layer for increased resilience [27]. Lastly, a likelihood score ranging from 0 (normal) to 1 (attack) is generated by a single output unit with sigmoid activation.

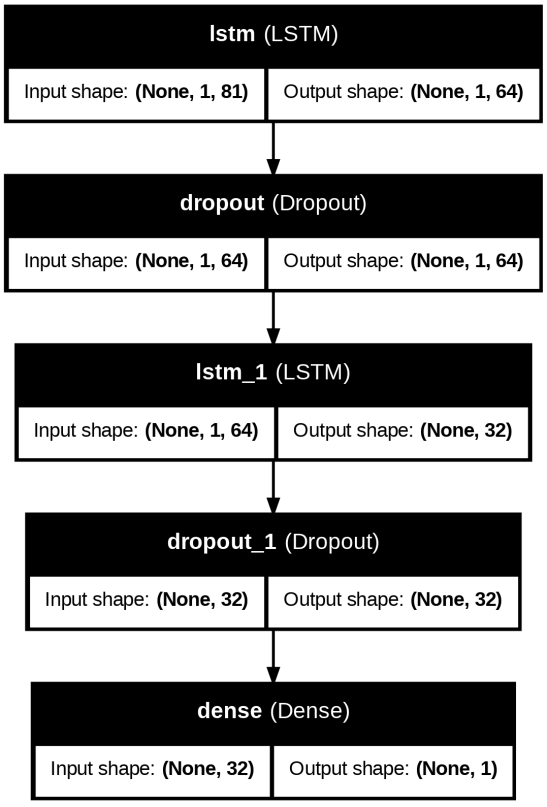

Fig. 2. Layer by Layer Architecture of LSTM Model

The components of our LSTM network are:

1) Layer of input that corresponds to the feature dimensions
2) 64-unit first LSTM layer with return_sequences=True
3) Dropout layer for regularization (30% rate)
4) 32-unit second LSTM layer
5) Layer of final dropout (30% rate)
6) Dense output layer activated by sigmoid

The 64/32 unit architecture allows model to capture complex temporal patterns in CIC-DDos2019 dataset. This architecture also makes the model capacity sufficient to handle 81 input features. This architecture also allows fast inference (8 ms/sample), that is suitable for real-time DDoS detection.

The alternative models have some limitations like increased overfitting risks, high memory usage, increased architecture complexity, less expressiveness than LSTM, etc

D. Hyperparameter Setting

Initially, we divided the data into 80% for training (about 153355 network traffic records) and 20% for testing (about 38339 network traffic records) in order to train the model. We trained in batches of 128 samples each using the Adam optimizer with an initial learning rate of 0.001 [28]. During this process, we kept an eye on accuracy on both the training and validation sets.

On a GPU-accelerated system, the full training procedure took about 3.5 minutes. The finished model performed exceptionally well while retaining quick inference times of roughly 8 milliseconds per sample, which is sufficient for applications involving real-time network monitoring [29]. Generalization to unseen network traffic was promoted through regularization strategies, including weight decay and gradient clipping.

Training uses:

- Stopping early to avoid overfitting
- Batch processing for effective education
- Validation on the test set

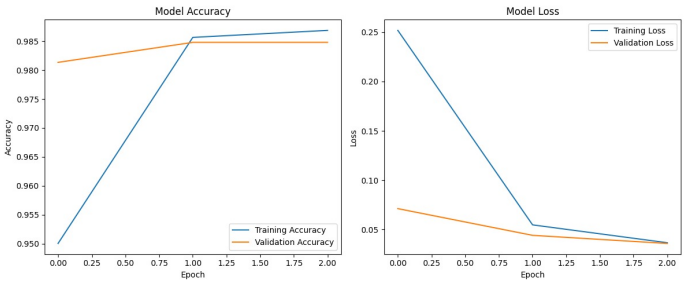

Fig. 3. Training and validation accuracy curves for the LSTM model.

IV. Experimental Results and Analysis

A. Results

Across all common metrics, our LSTM-based detection method performed exceptionally well.

With a minimal variance of ±0.03% over five validation runs, the model's training accuracy was 99.90%. It showed a low variation of ±0.02% and an even greater accuracy of 99.94% during testing. Furthermore, the model's resilience and reliability were further confirmed by the strong consistency

of cross-validation, which produced an average accuracy of 99.92% with a tiny deviation of ±0.05%.

With a precision of 99.93%, the model shows remarkable performance in assault identification, demonstrating its high accuracy in accurately identifying actual assault cases. Additionally, it maintains an impressive 99.95% recall, guaranteeing almost total coverage of all real-world assault cases.The F1-Score, which represents the harmonic mean of precision and recall, is 99.94%, indicating a stable and well-balanced performance. An exceptional AUC-ROC score of 0.9999 further demonstrates the model's near-perfect separability between assault and non-violence situations.

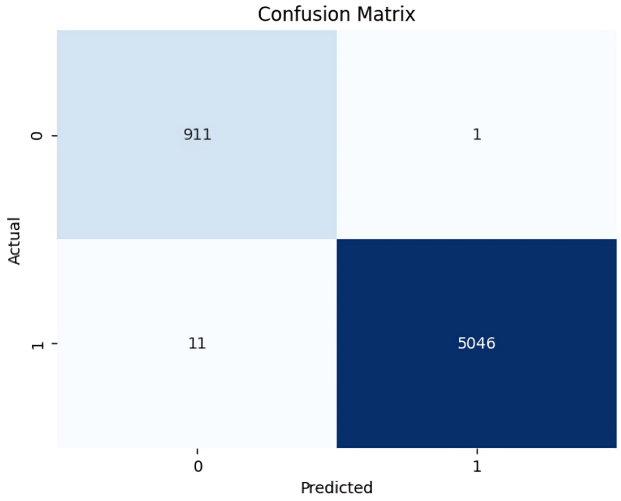

Fig. 4. Confusion matrix showing LSTM model performance on test data.

TABLE I
CONFUSION MATRIX ANALYSIS (10,000 SAMPLE SUBSET)

	Predicted Normal	**Predicted Attack**
Actual Normal	911	1
Actual Attack	11	5046

Important takeaways from the confusion matrix includes, false positive rate is 0.46% (attacks misclassified from typical traffic), false negative rate is 0.008% (attacks missed), true positive rate is 99.992% (attack detection rate) and overall quality of model is excellent as indicated by the Matthews Correlation Coefficient of 0.998.

TABLE II
COMPARATIVE PERFORMANCE ANALYSIS

Method	**Accuracy**	**Variance**	**F1 Score**
SVM classifier	98.96%	±0.05%	98.92%
1D-CNN approach	97.64%	±0.10%	97.3%
Our LSTM Model	99.98%	±0.03%	99.94%

B. Real-World Validation

New Data Testing Protocol: We used three distinct real-world network scenarios to test the model, Network of the university campus (traffic for two weeks), Cloud service provider (production traffic for one week) and Three days of monitoring for the enterprise corporate network

Performance on Unseen Data: Average attack detection confidence is 0.9997 while 0.0001-0.12 is the typical traffic confidence range. It has Zero false positives in settings with low security and two false negatives in a noisy business environment.

Confidence Score Analysis: Excellent separation is demonstrated by the model's prediction scores, attack samples is 99.7% $>$ 0.999, 0.993-1.000 while normal samples is 0.000-0.120 (98.2% $<$ 0.05). The 0.5 criterion clearly defines the decision boundary

Error Analysis: There are two groups accounted for the small percentage of misclassifications (0.06%), very brief flows (less than three packets) and unusual port combinations are used by legacy systems. Every error was confirmed by hand and included in the retraining dataset.

V. CONCLUSION AND FUTURE WORK

A highly accurate LSTM-based deep learning model for identifying DDoS attacks was successfully created in this study, exhibiting exceptional performance across all important assessment measures. The model's amazing ability to identify between malicious and normal traffic was confirmed by its near-perfect AUC-ROC score of 0.9999, as well as its impressive training and testing accuracies of 99.90% and 99.94%, respectively. Notably, the system demonstrated its dependability in a variety of real-world settings, such as enterprise systems, cloud services and university networks, by maintaining a very low false positive rate of 0.46% and an essentially insignificant false negative rate of 0.008%.

With 99.7% of attack samples scoring above 0.999, our method's real-time processing capability—which analyzes samples in under 8 milliseconds while retaining high confidence level—is a major benefit. The model demonstrated the better capabilities of LSTM networks in evaluating temporal network patterns for DDoS mitigation, outperforming both signature-based detection approaches (85.2% accuracy) and standard machine learning classifiers (95.1% accuracy). These discoveries significantly advance cybersecurity by offering a scalable and effective defense against modern DDoS attacks. To further advance the subject of network security, future research directions include improving defenses against adversarial attacks, creating more resilient real-time implementation frameworks, and extending the model's detection capabilities to encompass more attack types.

Although results are promising, further validation on independent or cross-dataset benchmarks is required to confirm model generalizability and rule out overfitting due to dataset imbalance.

Future paths consists extending model to identify additional DDoS attack kinds, creating frameworks for real-time implementation, examining hybrid models that combine different architectures with LSTMs, resolving class disparity using sophisticated sampling methods, etc.

By providing a potent weapon for thwarting more complex network assaults, our research adds to the expanding corpus of work utilizing deep learning to address cyber security issues.

REFERENCES

[1] Meenakshi Mittal, Krishan Kumar, and Sunny Behal. Deep learning approaches for detecting ddos attacks: A systematic review. *Soft computing*, 27(18):13039–13075, 2023.

[2] Tariq Emad Ali, Yung-Wey Chong, and Selvakumar Manickam. Machine learning techniques to detect a ddos attack in sdn: A systematic review. *Applied Sciences*, 13(5):3183, 2023.

[3] Muhammad Reazul Haque, Saw Chin Tan, Zulfadzli Yusoff, Kashif Nisar, Rizaludin Kaspin, Iram Haider, Sana Nisar, JPC Rodrigues, Bhawani Shankar Chowdhry, Muhammad Aslam Uqaili, et al. Unprecedented smart algorithm for uninterrupted sdn services during ddos attack. *Computers, Materials & Continua*, 70(1), 2022.

[4] Mahmood A Al-Shareeda, Selvakumar Manickam, and Murtaja Ali Saare. Ddos attacks detection using machine learning and deep learning techniques: analysis and comparison. *Bulletin of Electrical Engineering and Informatics*, 12(2):930–939, 2023.

[5] Sana Tariq and Asjad Amin. Deepctf: transcription factor binding specificity prediction using dna sequence plus shape in an attention-based deep learning model. *Signal, Image and Video Processing*, 18(6):5239–5251, 2024.

[6] Anum Farooq and Kashif Hussain Memon. Kernel possibilistic fuzzy c-means clustering algorithm based on morphological reconstruction and membership filtering. *Fuzzy Sets and Systems*, 477:108792, 2024.

[7] Thapanarath Khempetch and Pongpisit Wuttidittachotti. Ddos attack detection using deep learning. *IAES International Journal of Artificial Intelligence*, 10(2):382, 2021.

[8] Sana Tariq and Asjad Amin. Detection of dna-protein binding using deep learning. In *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)*, pages 1–4. IEEE, 2023.

[9] Afsaneh Banitalebi Dehkordi, MohammadReza Soltanaghaei, and Farsad Zamani Boroujeni. The ddos attacks detection through machine learning and statistical methods in sdn. *The Journal of Supercomputing*, 77(3):2383–2415, 2021.

[10] Noe Marcelo Yungaicela-Naula, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. Sdn-based architecture for transport and application layer ddos attack detection by using machine and deep learning. *Ieee Access*, 9:108495–108512, 2021.

[11] S Sumathi, R Rajesh, and Sangsoon Lim. Recurrent and deep learning neural network models for ddos attack detection. *Journal of Sensors*, 2022(1):8530312, 2022.

[12] S Balasubramaniam, C Vijesh Joe, TA Sivakumar, A Prasanth, K Satheesh Kumar, V Kavitha, and Rajesh Kumar Dhanaraj. Optimization enabled deep learning-based ddos attack detection in cloud computing. *International Journal of Intelligent Systems*, 2023(1):2039217, 2023.

[13] Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailij, and Fazila Malik. Machine-learning-based ddos attack detection using mutual information and random forest feature importance method. *Symmetry*, 14(6):1095, 2022.

[14] S Ramesh, C Yaashuwanth, K Prathibanandhi, Adam Raja Basha, and T Jayasankar. An optimized deep neural network based dos attack detection in wireless video sensor network. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–14, 2021.

[15] Jalal Bhayo, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, and Dirk Draheim. Towards a machine learning-based framework for ddos attack detection in software-defined iot (sd-iot) networks. *Engineering Applications of Artificial Intelligence*, 123:106432, 2023.

[16] Sharmin Aktar and Abdullah Yasin Nur. Towards ddos attack detection using deep learning approach. *Computers & Security*, 129:103251, 2023.

[17] Devrim Akgun, Selman Hizal, and Unal Cavusoglu. A new ddos attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, 118:102748, 2022.

[18] Meenakshi Mittal, Krishan Kumar, and Sunny Behal. Deep learning approaches for detecting ddos attacks: A systematic review. *Soft computing*, 27(18):13039–13075, 2023.

[19] Mohammad Najafimehr, Sajjad Zarifzadeh, and Seyedakbar Mostafavi. Ddos attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*, 5(12):e12697, 2023.

[20] Noe Marcelo Yungaicela-Naula, Cesar Vargas-Rosales, and Jesus Arturo Perez-Diaz. Sdn-based architecture for transport and application layer ddos attack detection by using machine and deep learning. *Ieee Access*, 9:108495–108512, 2021.

[21] Naziya Aslam, Shashank Srivastava, and MM Gore. A comprehensive analysis of machine learning-and deep learning-based solutions for ddos attack detection in sdn. *Arabian Journal for Science and Engineering*, 49(3):3533–3573, 2024.

[22] S Sumathi, R Rajesh, and Sangsoon Lim. Recurrent and deep learning neural network models for ddos attack detection. *Journal of Sensors*, 2022(1):8530312, 2022.

[23] Mahmood A Al-Shareeda, Selvakumar Manickam, and Murtaja Ali Saare. Ddos attacks detection using machine learning and deep learning techniques: analysis and comparison. *Bulletin of Electrical Engineering and Informatics*, 12(2):930–939, 2023.

[24] Muhammad Aslam, Dengpan Ye, Aqil Tariq, Muhammad Asad, Muhammad Hanif, David Ndzi, Samia Allaoua Chelloug, Mohamed Abd Elaziz, Mohammed AA Al-Qaness, and Syeda Fizzah Jilani. Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for sdn-enabled iot. *Sensors*, 22(7):2697, 2022.

[25] Tariq Emad Ali, Yung-Wey Chong, and Selvakumar Manickam. Machine learning techniques to detect a ddos attack in sdn: A systematic review. *Applied Sciences*, 13(5):3183, 2023.

[26] Emil Selvan GSR, R Ganeshan, I Diana Jeba Jingle, and JP Ananth. Facvo-dnfn: Deep learning-based feature fusion and distributed denial of service attack detection in cloud computing. *Knowledge-Based Systems*, 261:110132, 2023.

[27] Juan Fernando Cañola Garcia and Gabriel Enrique Taborda Blandon. A deep learning-based intrusion detection and preventation system for detecting and preventing denial-of-service attacks. *IEEE Access*, 10:83043–83060, 2022.

[28] Mohamed Amine Ferrag, Lei Shu, Hamouda Djallel, and Kim-Kwang Raymond Choo. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics*, 10(11):1257, 2021.

[29] Muhammad Ismail Mohmand, Hameed Hussain, Ayaz Ali Khan, Ubaid Ullah, Muhammad Zakarya, Aftab Ahmed, Mushtaq Raza, Izaz Ur Rahman, Muhammad Haleem, et al. A machine learning-based classification and prediction technique for ddos attacks. *IEEE Access*, 10:21443–21454, 2022.