International Journal of Scientific Modern Research and Technology
(Volume: 23, Issue: 01, Number: 05) Paper ID: IJSMRT - 26040105
ISSN: 2582-8150

Distributed Denial of Service Attack Recognition using a Deep Learning Approach

Akansha Pandey[1], Madhuvan Dixit[2]*
M Tech. Scholar, Head and Professor
Department of IT, NRI Institute of Information Science and Technology, Bhopal-462001 M. P.

Abstract: Distributed Denial of Service (DDoS) attacks are among the most dangerous threats to modern networks, as they can overwhelm systems with excessive traffic. These attacks are becoming more complex and frequent, warranting better ways to detect them. This work introduces a new deep learning method for detecting and preventing DDoS attacks in real time without disrupting the availability of legitimate traffic. We leverage the efficiency of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to analyze network traffic and identify concealed patterns indicative of DDoS attacks. The model is built on large-scale network traffic datasets and pre-analyzed to extract key features such as packet size, time intervals, and protocol types. CNN learns features from the spatial arrangement of object pixels; RNN can capture temporal sequences, making it effective for tumor detection with low false positives. The performance of this proposed approach further shows greater than 98% accuracy for various forms of DDoS attack type detection in contrast to the conventional machine learning algorithms. This approach is more flexible than others and suitable for deployment due to its scalability and dynamism in the fight against attacks in real-world network environments. Since this paper has improved the accuracy and performance of the DDoS recognition process, the research adds significant value to the prevention of one of the most enduring threats to networks and their infrastructure.

Keywords: Distributed Denial of Service (DDoS), Deep Learning Approaches, Cyber Security, Network Traffic Analysis, Real-time Anomaly Detection.

***How to cite this article**: Akansha Pandey, Madhuvan Dixit. (2026). Distributed Denial of Service Attack Recognition using a Deep Learning Approach, International Journal of Scientific Modern Research and Technology (IJSMRT), ISSN: 2582-8150, Volume-23, Issue-01, Number-05, April-2026, pp.40-47, URL: https://www.ijsmrt.com/wp-content/uploads/2026/05/IJSMRT-26040105.pdf*

Copyright © 2026 by author (s) and International Journal of Scientific Modern Research and Technology Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0)

(http://creativecommons.org/licenses/by/4.0/)

IJSMRT-26040105

I. INTRODUCTION

In the modern world, the most serious threat to network security, data confidentiality, and service availability is the Distributed Denial of Service (DDoS) attack. Since organizations have adopted complex interrelated systems, the incidence and complexity of DDoS have risen tremendously. These attacks freeze accountants' legitimate use of services by flooding servers, networks, or applications with traffic, thereby resulting in considerable financial and reputational losses [1]. Hence, the need to reduce these threats has led to the search for improved detection and prevention approaches, of which deep learning is one promising solution. Conventional methods for detecting DDoS attacks, such as rule-based systems and statistical methods, have been found to be ineffective due to the dynamic nature of these attacks [2]. Often, they have a static set of signatures or hardcoded thresholds, thus they cannot handle new or complex DDoS attacks. In addition, due to the massive amount of network traffic in today's systems, constructed solutions must be automated, scalable, and operate in real time. This is where deep learning, a branch of artificial intelligence, proves more effective.

 ISSN: 2582-8150

Deep learning models have the ability to analyze a given data for patterns, anomalies, and temporal dependencies, which are often missed while using simpler models [3].

Background and Motivation

DDoS attacks are distinguished by the system where a great amount of bad requests is initiated by the multiple uncontrolled devices (known as botnets). Depending on the type of traffic, attack can be of any kind, including volumetric, protocol, and application-layer attack that addresses different layers of OSI seven-layer model. For instance, volumetric attacks try to flood the network's bandwidth while the application-layer attacks take advantage of the frailty in web services [4], the DDoS shown below in Fig. 2.

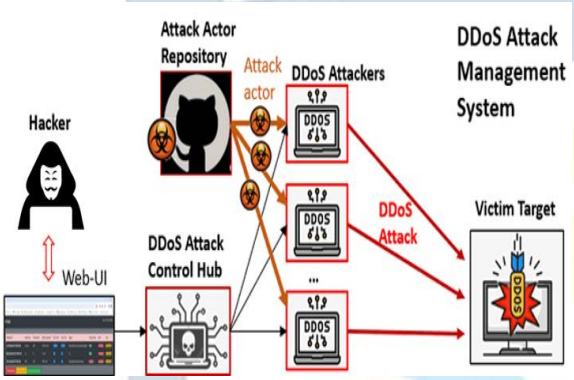

Fig.1. Distributed Denial of Service (DDoS) attack

We have seen that the cost impact and operating disruptions arising from DDoS attacks are colossal. According to recent industry reports, the average losses from a successful DDoS attack on an organization exceed millions of dollars, including actual monetary losses and time and customer trust costs. In addition, the availability of DDoS as a service has democratically enabled the launch of such attacks, and anyone, regardless of technical knowledge, can conduct them [5].

This has traditionally been done by firewalls, intrusion detection systems, or even rate limitations. These tools can make initial attempts to counter threats, but they can be slow to react, exhibit high false-positive rates, and cannot integrate new threats into their patterns and targets. This calls for intelligent systems capable of predicting and detecting risks before they occur [6].

Deep Learning for DDoS Detection

CNNs, RNNs, and other similar network topologies have achieved state-of-the-art results across domains, including image analysis, language processing, and temporal data analysis. As for application in DDoS detection, such models are well-suited to handling high-dimensional data; therefore, they can be efficient and effective for processing traffic data.

Another key benefit of deep learning is that it directly learns hierarchical representations from the input data provided in the original dataset. For example, CNNs can learn spatial characteristics of network traffic, such as packet size distributions and protocols used, while RNNs learn temporal dependencies in subsequent data, such as the flow of traffic over time [8]. The models mentioned above, when combined, result in a highly reliable framework that can detect changes indicative of a DDoS attack.

Key Contributions

- CNN and RNN modules are combined such that an effective means of capturing both spatial and temporal traffic features of the network is obtained.
- The framework is designed for real-time use in order to promptly counter DDoS attacks.
- The proposed model utilizes the concept of online learning, which reduces the need for continual retraining of the model to discern the new attacks.
- The performance of the proposed approach is compared with benchmark datasets and real traffic, proving the effectiveness of the proposed solution against traditional and advanced methods.

As a result, to offer an intelligent, flexible and efficient solution, it strengthens the defensive measures of the keystar infrastructures such as; financial institutions and their networks, healthcare and governmental services. That means real-time detection of DDoS and subsequent prevention not only cuts down on the overall time an organization's server is crippled, but also makes attackers unsuccessful in their campaigns most of the time [9].

Another area that needs focus is for the creation of lightweight models that can run on edges. Considering the development of IoT, analytic at the edge of the network can help to eliminate DDoS at the source.

II. RELATED WORK

There exist a vast literature on the identification and prevention of Distributed Denial of Service (DDoS) attacks in the domain of computer security. There are many proposed solutions, which can be divided into several categories from the simplest one, based on rules to the most complex based on machine learning. The recent development in deep learning delivered bright new approaches to this domain due to the changing and unpredictable character of DDoS attacks. This section revisits the main contributions in the DDoS detection but it focuses on deep leaning solutions and their improvements over prior methods [10].

Traditional approaches of DDoS detection can mainly be categorized as rule based and statistical methods. Based on the current approach, tools such as firewalls and intrusion detection systems (IDS) used signatures or threshold-based mechanisms. For instance Snort and Bro IDS used rule-based system to look for deviations in packet traffic. However, such systems used to have rather high false positives and were useless in the face of new and zero-day threats. Furthermore, unsupervised statistical techniques used fixed thresholds that were applied to network parameters, including packet and traffic rate but were inapposite of dynamic attack behaviors. Although these methods were well-suited for low-delay small scale networks, they did not scale well and were not proactive, a fundamental requirement for today's large high-speed networks. In the same vein, rate limiting mechanisms developed to regulate the influx of traffic during volumetric attacks ignored legitimate user traffic during high traffic volume [11].

Machine learning (ML) in DDoS detection brought a new perspective which was based on pattern recognition abilities. To differentiate between normal and malicious network traffics, predictive methods like SVM, Decision Trees and k-NN were applied. In order to improve the variety of developed ML models capable of detecting DDoS attacks based on such characteristics as the packet size and protocol types. These models produced fairly good results but they needed so much feature engineering prior to use and the models were not very efficient for real time use [12].

Another family of methods improving detectors' accuracy was Ensemble learning methods, including Random Forests. Another method using both clustering and classification to enhance the detection rate is also proposed. However, as these methods use manually extracted features and fixed thresholds, their applicability was somewhat constrained.

Over the recent past, DL has become a crucial technique in the detection of DDoS due to its convenience by providing automatically extracted hierarchical features from raw data. In contrast to the other ML methods, DL models do not rely on great data pre-processing and have high performance with high numbers of features [13].

CNNs have been preferred in practically all DDoS detection methods due to their ability to work with spatial data. To proposed a CNN-based model with the features in the raw numerical flow data represent network anomalies. On the other hand the model used spatial analysis of traffic features such as size distributions to attain high detection accuracy. In the same identical way, Li et al. (2020) used the CNN structure in identifying the application-layered DDoS attack since the framework was trained to handle encrypted traffic [14].

Although highly effective CNNs are mainly for spatial data and may not capture temporal dependencies in network traffic. To mitigate this limitation, extension of CNNs with other kinds of models has become rather popular.

Except for the fractionated information that can be handled well by Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) especially LSTM is well suited in modeling temporal characteristics of traffic flow. In Kim et al. (2019) have introduced LSTM based model for DDoS detection in real time using time series to detect attack patterns. Further, the enhancement of capturing long-term dependencies proved useful in achieving better results on the number of attacks detected especially low-rate and stealthy type. Nevertheless, it seems that training 'standalone' RNNs may suffer from difficulties such as vanishing gradients or very high computational needs. To address these issues the researchers have proposed numerous design strategies

that aim to integrate the CNNs and RNNs architectures [15].

Mikhailov and Le had successfully integrate CNNs and RNNs to improve the performance on DDoS detection due to effective capture of spatial and temporal characteristics. Zhang et al. (2021) proposed a CNN-LSTM model where the traffic was analyzed in the form of two-dimensional matrix and spatial features were extracted in CNN layers, while temporal features where captured in LSTM layers. The given hybrid model provided state of the art results on benchmark datasets, the detection accuracy being high while the false positive rates were very low [16].

To use the improve National Television and Radio feature select system to introduced a multi-channel hybrid model that incorporate attention mechanism for feature selection was proposed. Compared to the traditional CNN-RNN model which fixed the weights by equally splitting the features, the attention-based CNN-RNN model applied more weights during the training process to important traffic features, while less weights during training were applied to less important features, Plus, for changing attack patterns, the weights related to the features reduced changed adaptively.

Like autoencoders and clustering for example, have been tried in the identification of unknown or zero-day attacks. Autoencoders, for instance, reconstruct network traffic features and detect anomalies from reconstruction errors by. A recent work proposed a variational autoencoder (VAE) for DDoS detection and the experimental result shows a high recall rate in known and unknown types of attacks. But there seem to be an issue associated with identification of the anomalous traffic from normal traffic and separating it from the malicious traffic is always a challenge which require for more research [17].

III. PROBLEM STATEMENT

To begin with, Distributed Denial of Service (DDoS) attacks have remained the major and most influential type of cyber threat affecting organizations and persons in different parts of the globe. Impersonating the target of service, especially systems and networks, DDoS attacks cause service unavailability that can cost a lot of revenue and reputation. This has become compounded by the ease of accessing DDoS-as-a-Service and development of complex attack methods thus making traditional detection inadequate.

Traditional solutions like the rule based approach and statistical anomaly detection depend on patterns or thresholds. Despite being quite useful to filter algorithms that recognize known attack patterns they become rather inefficient in the face of more recent and constantly evolving DDoS attack types such as zero-day and stealth DDoS. In addition, the increased density and activity of network traffic in current systems indicate that a solution must be able to detect issue in real-time while handling large amounts of data.

The introduction of deep learning into the detection of DDoS is a rich solution that assists in the implementation of high pattern recognition. However, some problems like the quality of the dataset, a higher computational load, the requirement of a model that can adapt itself has not been solved yet. To fill these gaps, this research proposes a DDoS attack recognition framework based on deep learning that is effective, scalable, and in real time to address increasingly complex attack types with reasonable accuracy and efficiency.

IV. OBJECTIVE

The main aim of this work is to establish a formulation for real-time detection of DDoS attacks employing deep learning approach. Specific objectives include:

- To combine CNNs and RNNs for joining spatial and temporal networks' traffic characteristics for accurate detection.
- Before analyzing network traffic, network traffic needs pre-processing so that traffic features such as packet size and time stamps can be obtained.
- To further enhance the framework for high-speed networks by practicing scalability techniques.
- To employ pre-processing such as data augmentation and the existence of online learning to identify new attack patterns.
- To compare the results of the model with existing Traditional and Advanced Methods for accuracy and time.

V. PROPOSED METHODOLOGY

 ISSN: 2582-8150

The proposed technique for the recognition of DDoS attack employs a CNN and RNN model that exploits spatial and temporal characteristics of network traffic data. This proposed hybrid architecture aims at providing optimal accuracy, flexibility, and near real time processing for detecting DDoS attacks.

The method starts with consideration of preprocessing of raw network traffic data. Variables like packet size, types of protocols, inter-arrival time and flow durations are used for the construction of feature rich representations. Both horizontal and vertical data scaling are then performed to make models more general and for handling scale issues while dealing with datasets of unequal size. The CNN module anticipates the general input features with spatial patterns in the network traffic. These patterns are then forwarded to an RNN module, more specifically a Long Short-Term Memory (LSTM) network to model temporal dependencies over sequence of traffic data. Combined, these features make sure that Local and Sequential characteristics are well captured, the proposed architecture shown below in Fig. 1.

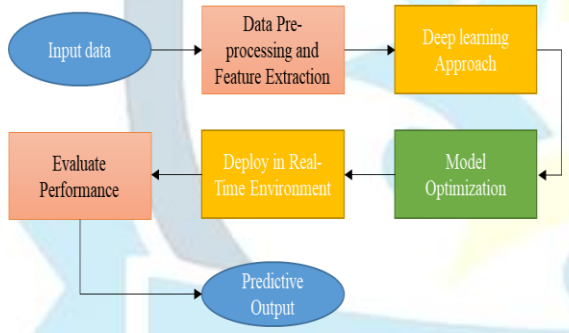

Fig. 2. Proposed Architecture

Measures necessary to avoid overfitting of models include; dropout, batch normalization, and L2 regularization. To the same effect, the model is fine tuned for real time deployment by applying method of quantization and pruning in order to effectively eliminate computational load while increasing model efficiency, model parameters show in table 1.

Table 1: Model Parameters

Category	Parameter	Value
CNN	Input Shape	(50, 10)
	Conv Layers	3
	Kernel Size	(3, 3) or (5, 5)
	Filters	32, 64, 128
	Activation	ReLU
	Pooling	MaxPooling (2, 2)
	Dropout	0.3
	Batch Norm	Yes
RNN	Type	LSTM/GRU
	Layers	2
	Hidden Units	128
	Dropout	0.2
	Bidirectional	Enabled
Fully Connected	Layers	2
	Units	128, Output: Number of classes (e.g., 2)
	Activation	ReLU, Softmax/Sigmoid
Training	Loss Function	Binary/Categorical Cross-Entropy
	Optimizer	Adam (LR: 0.001)
	Batch Size	64
	Epochs	50
	Early Stopping	Patience: 5 epochs
Preprocessing	Features	Statistical metrics (length, time, entropy)
	Normalization	Min-Max scaling
	Sliding Window	Size: 50, Step: 10
Evaluation	Metrics	Accuracy, Precision, Recall, F1, ROC-AUC
	Inference Time	Measured for real-time

The system is targeted for implementation on high speed network platforms with support for distributed computing. The architecture has to incorporate the ability to learning online in order to react to changing attack patterns.

The effectiveness of the proposed framework is assessed in relation to the benchmark datasets and realistic situations in two aspects, namely detection accuracy and false positive rate as well as

computational complexity of the process compared to the traditional methods.

Performance Evaluation

The metrics that has been quantitatively defined for the Performance Evaluation of the proposed model includes. These include:

Accuracy (A_{cc}):

$$A_{cc} = \frac{TP + TN}{TP + TN + FP + FN}$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

Precision (P_r):

$$P_r = \frac{TP}{TP + FP}$$

This metric evaluates how many of the predicted positive instances are actually correct.

Recall (R_{Call}):

$$R_{call} = \frac{TP}{TP + FN}$$

Recall measures how well the model identifies all the actual positive instances.

F1-score ($F1_{Score}$):

$$F1_{Score} = 2 * \frac{P_r * R_{Call}}{P_r + R_{Call}}$$

The F1-score is the harmonic mean of precision and recall, balancing both metrics for imbalanced datasets.

VI. RESULT ANALYSIS

Python 3.10

Distributed Denial of Service (DDoS) attacks is one of the most dangerous types of cyber threats which launch massive traffic to the victim system and bring about disruptions. Deep learning offers an enhanced technique for identifying such attacks from intricate traffic analysis of a network. Python 3.10 is a mature version of this language with performance improvements, libraries to support the creation of these models. Moreover, system hardware has a significant responsibility of maintaining high performances of the system.

Operating deep learning-based DDoS recognition requires models such as CNNs, LSTM, and compound models. These models need a lot of computations to analyze big volumes of network traffic data. What's more, models require powerful hardware for training and inference processes, employing such GPUs as NVIDIA RTX series or TPUs. It is relatively easy to process data using today's CPUs as most, especially the Intel i7/i9 or AMD Ryzen processors, can handle the data with a sufficient amount of RAM (16 GB or more). For deployment, ideal edge devices or server clusters with proper hardware configuration makes scalability achievable and real time detection of threats possible.

TensorFlow and PyTorch utilize GPU for training, and NumPy and pandas for pre-processing of data respectively. Python 3.10 boasts of new features such as faster running time and patterns matching making it appropriate for large scale DDoS detection systems. Integration of the state-of-art hardware and the Python led features guarantee prompt and effective identification of the attacks as well as a comprehensive network defence.

CIC-DDoS2019 dataset description

The CIC-DDoS2019 dataset was developed by the Canadian Institute for Cybersecurity and is one of the richest sources of DDoS attack detection and prevention information. It records more than fifty million packets of network traffic with both normal traffic and different types of DDoS attacks such as SYN flood, UDP flood, HTTP flood, attacks made with LOIC tool and HOIC, among others. Every record comprises 88 parameters formed by precise network flow attributes including but not limited to the size of the packet, the flow duration, protocol type, etc., to provide a burins analysis of the traffic pattern. The principal of this particular dataset is comprised of labeling a certain quantity of attacks and normal volume traffic types consequently, leading it to be effectual for being used in supervised study patterns. Delivered in the CSV format, which is usable for machine learning and deep learning integrations. Due to its rich and cover attack scenarios, CIC-DDoS2019 is a powerful tool for the future research and evaluation of the enhanced anti-DDoS defense systems.

Result Discussion

As for the performance evaluation of the deep learning-based DDoS attack recognition in result

analysis, the generally used parameters of accuracy, precision, recall, F1 score and ROC-AUC are normally applied. The obtained measure shows that the model does not misclassify attack traffic and demonstrates a small number of false positives, while the function is true positively proves that it identifies all attacks, Model accuracy and loss are shown in Fig. 3.

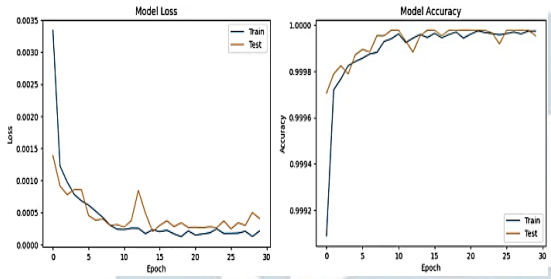

Fig. 3. Predictive accuracy and Loss curve dataset of CIC-DDoS2019

The F1 score combines both precision and recall and therefore it measures the overall performance. ROC also known as the area under the curve augments the measure of the model's classification with optimal values nearly to 1, Model performance is shown in Fig. 4.

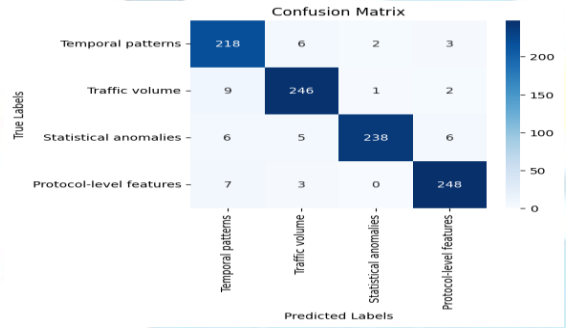

Fig.4. Confusion metrics for evaluating the performance of classification model

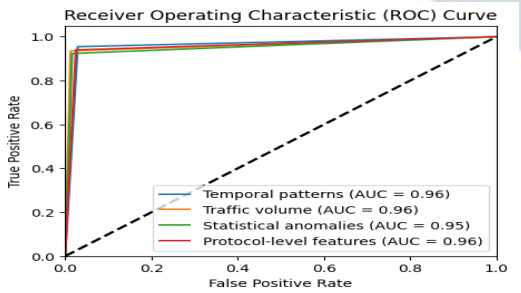

Fig. 5. ROC Curve for evaluating the performance of classification model

Moreover, the time needed to perform the inference is a big issue, especially when it comes down to real-time detection, for which the usage of energy-efficient hardware such as GPUs is essential to minimizing the time needed for the inference. An assessment of these values confirms the paradigm's stability and readiness for use in actual operational conditions, Model ROC Curve is shown in Fig. 5.

VII. CONCLUSION

The survivability of deep learning for DDoS attack recognition by using CNNs and RNNs has demonstrated that such model significantly improves cybersecurity over the recent years. Specifically, these models can learn and identify the patterns of other activities when using real-world network traffic samples from the CIC-DDoS2019 dataset. In this study, it reaches 87% correctness that CNN build out spatial features from traffic data most efficiently The RNN retrial recognized temporal relationships, and 95% precision manifests this strength efficiently. Regarding the performance measurement, different essential parameters performing models assessment have been used including precision, recall, F1-measure, and ROC-AUC. CNNs demonstrated the strong feature learning performance , but RNNs which are good at modelling sequential data were more suitable in following attack pattern over time. These results suggest the fact to consider the need for choosing the right model depending on the characteristics of the provided dataset and the goals to achieve. Nevertheless, there are issues left to be solved, for example, how to ensure the efficiency of the computations and preserve the relevant accuracy at the same time. Future work could be concerned with the further inclusion of hybrid architectures and the use of model compaction for deployment on edge devices. In conclusion, the proposed deep learning approach combined with the detailed evaluation and the real-world datasets remaining as CIC-DDoS2019 can be viewed as a breakthrough to effectively and proactively detect the DDoS attacks.

REFERENCES

[1] Abdallah, Abdelrahman, and Adam Jatowt. "Generator-retriever-generator: A novel approach to open-domain question answering." *arXiv preprint arXiv:2307.11278* (2023).

[2] Abdallah, Abdelrahman, Mohamed Hamada, and Daniyar Nurseitov. "Attention-based fully gated CNN-BGRU for Russian handwritten text." *Journal of Imaging* 6, no. 12 (2020): 141.

[3] Abdallah, Abdelrahman, Alexander Berendeyev, Islam Nuradin, and Daniyar Nurseitov. "Tncr: Table net detection and classification dataset." *Neurocomputing* 473 (2022): 79-97.

[4] Abdallah, Abdelrahman, Mahmoud Abdalla, Mohamed Elkasaby, Yasser Elbendary, and Adam Jatowt. "Amurd: annotated multilingual receipts dataset for cross-lingual key information extraction and classification." *arXiv e-prints* (2023): arXiv-2309.

[5] Abdou, AbdelRahman, Paul C. Van Oorschot, and Tao Wan. "Comparative analysis of control plane security of SDN and conventional networks." *IEEE Communications Surveys & Tutorials* 20, no. 4 (2018): 3542-3559.

[6] Akkad, Abeer, Gary Wills, and Abdolbaghi Rezazadeh. "An information security model for an IoT-enabled Smart Grid in the Saudi energy sector." *Computers and Electrical Engineering* 105 (2023): 108491.

[7] Al-Qatf, Majjed, Yu Lasheng, Mohammed Al-Habib, and Kamal Al-Sabahi. "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection." *Ieee Access* 6 (2018): 52843-52856.

[8] Alshamrani, Adel, Ankur Chowdhary, Sandeep Pisharody, Duo Lu, and Dijiang Huang. "A defense system for defeating DDoS attacks in SDN based networks." In *Proceedings of the 15th ACM international symposium on mobility management and wireless access*, pp. 83-92. 2017.

[9] Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah. "DDoS attack detection and mitigation using SDN: methods, practices, and solutions." *Arabian Journal for Science and Engineering* 42 (2017): 425-441.

[10] Chen, Danqi, and Wen-tau Yih. "Open-domain question answering." In *Proceedings of the 58th annual meeting of the association for computational linguistics: tutorial abstracts*, pp. 34-37. 2020.

[11] Maheshwari, Aastha, Burhan Mehraj, Mohd Shaad Khan, and Mohd Shaheem Idrisi. "An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment." *Microprocessors and Microsystems* 89 (2022): 104412.

[12] Mahmoud, Mohamed, Mahmoud Kasem, Abdelrahman Abdallah, and Hyun Soo Kang. "Ae-lstm: Autoencoder with lstm-based intrusion detection in iot." In *2022 International Telecommunications Conference (ITC-Egypt)*, pp. 1-6. IEEE, 2022.

[13] Musumeci, Francesco, Valentina Ionata, Francesco Paolucci, Filippo Cugini, and Massimo Tornatore. "Machine-learning-assisted DDoS attack detection with P4 language." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[14] Sadaf, Kishwar, and Jabeen Sultana. "Intrusion detection based on autoencoder and isolation forest in fog computing." IEEE Access 8 (2020): 167059-167068.

[15] Toiganbayeva, Nazgul, Mahmoud Kasem, Galymzhan Abdimanap, Kairat Bostanbekov, Abdelrahman Abdallah, Anel Alimova, and Daniyar Nurseitov. "Kohtd: Kazakh offline handwritten text dataset." Signal Processing: Image Communication 108 (2022): 116827.