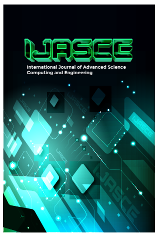
International Journal of
Advanced Science Computing and Engineering

Journal Homepage www.ijasce.org/index.php/ijasce



# Distributed Denial-of-Service Attack Detection Using One-Dimensional Convolutional Neural Network in Airline Reservation Systems (ARS)

Dhurgham Kareem Gharkan [a,*], Bahaa Kareem Mohammed [a], Hussein Ali Salah [b], Mariana Mocanu [c]

*[a] Department of Medical Instruments Techniques, Middle Technical University, Technical Institute Kut, Baghdad, Iraq*
*[b] Department of Computer Systems, Middle Technical University, Technical Institute- Suwaira, Baghdad, Iraq*
*[c] Computer Science Department, National University for Science and Technology Politehnica, Bucharest, Romania*

*Corresponding author: [*]dhurgham-kareem@mtu.edu.iq*

***Abstract*— A prevalent and perilous in the contemporary are Distributed Denial of Service (DDoS) attacks. in which attackers attempted to prevent authorized users from accessing internet services by deploying many attack workstations. This research presents a detection approach based on One Dimension Convolutional Neural Networks, which has created an innovative approach for detecting DDoS attacks that addresses the limitations of conventional methods. The primary objective of this study was to analyze and detect DDoS attacks through the examination of a dataset about the booking of airline tickets. The present investigation utilized the APA-DDoS dataset, comprising two discrete categories: benign traffic and DDoS traffic. Wireshark was utilized to simulate airline data as well. Utilized as one-dimension convolutional neural network (1D CNN) technology, the model achieved an accuracy rating of 99.5%. The experimental outcomes demonstrated that the proposed model effectively and consistently identified DDoS attacks. Solid ability to differentiate between legitimate and malicious traffic has been exhibited by the system, thereby ensuring network security.**

***Keywords*— APA-DDoS-Dataset; distributed denial of service; DDoS; 1D CNN; ARS.**

*Manuscript received 5 Jul. 2024; revised 17 Jul. 2024; accepted 2 Nov. 2024. Date of publication 31 Dec. 2024.*

## I. Introduction

In the contemporary era, the reliance of individuals on the internet was ubiquitous. It has facilitated advancements in various domains such as interaction, learning, business, and retail [1]. Despite society's heavy reliance on the internet, there has been a significant increase in criminal activities such as the dissemination of false information, hacking, and cyber-attacks. Envisage the consequences of the unavailability of desired services. This form of assault is commonly referred to as a Denial of Service assault [2]. A single-demand-of-service assault refers to an attack that is executed using only one system. In contrast, a widespread Denial of Service (DDoS) attack refers to an attack that is carried out by infecting multiple machines. DDoS assaults result in financial losses, network performance degradation, and the unavailability of vital services [3]. For prevention purposes, it is necessary to develop a technique for identifying Distributed Denial of Service (DDoS) attacks. Distributed Denial of Service (DDoS) assaults have been prevalent during the past twenty years [4]. A Distributed Denial of Service (DDoS) attack caused the inactivity of computer systems [5].

On the other hand, a DDoS assault overwhelms the intended service by utilizing many computers and Internet connections[6]. A Distributed Denial of Service (DDoS) assault can be carried out by a vast array of computers, commonly referred to as malware networks or hordes of computers that have been compromised by the attacker, sometimes known as the boaster [7]. Each of these compromised computers would immediately flood the target server with a high volume of packets [8]. This phenomenon unduly consumes the entirety of the server's available bandwidth, rendering the server unusable for any additional requests or causing it to crash entirely. DDoS attacks pose significant challenges in terms of detection and defense due to their wide range and complexity [9].

Some reports indicate a consistent rise in the number of DDoS attacks over the past decade. In all airports worldwide, a ticket reservation system is available for booking travel dates for passengers. These official websites may be exposed to threats through a distributed denial-of-service attack, and the website becomes unavailable and unable to provide reservations to travelers. It will not perform its function and will not send and receive official requests to travelers [10].

One of the most dangerous attacks targeting these sites at present is the DDoS attack, which directly affects servers and the Internet in general by consuming network resources with fraudulent requests and stopping legitimate users. The resources most vulnerable to attack are routers and server CPUs, as well as specific protocol applications, such as SYN-attack, which bypasses the TCP packet of the operating system [11]. These packets are sent to the attacker, which leads to a decrease in network bandwidth. Also, in the DNS protocol, some vulnerabilities lead to a significant increase in traffic for attackers. Classifying and detecting DDoS attacks is very difficult. The main point of knowing a DDoS attack is to track and detect drifts in the structure of Internet networks [12]. Detecting DDoS attacks is a significant challenge for network and system administrators.

Therefore, it is necessary to take necessary actions and measures to avoid the device being part of a malicious botnet, for example, by not installing unknown software, using effective antivirus software, and fixing devices with security updates [13], [14]. In addition, the use of deep learning techniques, which is a type of machine learning, significantly influences the processing of images and data by extracting practical features from live data using layers. This data may consist of text, images, or network traffic [15]. At present, deep learning is regarded as the cutting-edge technology for constructing precise data classification models [16]. The three primary layers of a deep neural network are the input layer, the hidden layers, and the output layer. As an example of deep neural networks, the Convolutional Neural Network (CNN) is utilized in the majority of prevalent techniques [17]. To ensure accessibility and facilitate further research, the APA-DDoS dataset is readily available to all researchers on the Kaggle website [18].

Our primary goal is twofold: first, to provide a comprehensive description of a newly developed dataset called APA-DDoS-Dataset, which includes a total of 151,201 samples and includes twenty-three distinct features, as well as simulation data via Wireshark. Secondly, we aimed to conduct an in-depth analysis of the dataset to detect attacks accurately. This work aims to overcome the constraints of current IDS designs, which frequently have difficulties in identifying unfamiliar traffic during DDoS attacks. It proposes an innovative IDS framework that utilizes deep learning techniques. Our methodology integrates deep learning algorithms and architectural measures to optimize accuracy and boost the identification of unidentified traffic. In addition, the system's gradual learning feature enables it to adjust to new techniques of attack by integrating newly labeled specimens supplied by telecommunication technicians, consistently enhancing its protective effectiveness.

In this study, a binary dataset was used, focusing on the attack type "DDoS-PSH-ACK", while legitimate usage was classified as "benign". To improve the dataset and enhance the accuracy of our model. The subsequent sections of this work are structured as follows: Section 2 provides a comprehensive summary of pertinent literature. Section 3 describes the approaches used for detecting Distributed Denial of Service (DDoS) attacks, which are based on deep learning techniques. Section 4 outlines the empirical results, while Section 5 wraps up the study and explores prospective directions for further research.

## II. Materials and Method

In this section, we discuss some of the most important methodologies for detecting DDoS attacks. Shaaban et al. in [11] used Convolutional neural network (CNN) technology to distinguish between benign and malevolent DDoS traffic with an accuracy of 99% across two distinct data sets. The first is extracted from a Wireshark simulation of the My Client Center (MCC) network, and the second is an open-source dataset that was predefined. In comparison to alternative classification algorithms, including support vector machines (SVM), neural networks (NN), decision trees (D-Tree), and K-Nearest Neighbors (K-NN), the findings are presented.

Chaudhari et al. [12] identify a possible different type of DDOS attack, including TCP, SYN VLOOT, Ping, UDP, VLOOD, Plans Attack, and Attack Smurf. Researchers have implemented a variety of defense mechanisms to detect DDoS attacks, and a multitude of data mining algorithms are utilized to compile detection strategies. Regression, classification, neural networks, clustering, and classification algorithms yield accurate and timely outcomes as a result of research analysis and examination. false detection, true negative, true positive, positive-negative, and detection rate. Assembling the algorithm, combined with the classification algorithm, yields high accuracy.

A study by [13] found that comparing and analyzing these detection strategies is important to find an efficient strategy for detecting a DDoS attack in the behavior of the cloud. The data mining technique is one of the most efficient and effective strategies that can be used to detect DDoS. This review paper examines how powerful data mining algorithms can track and detect DDoS attacks. Decision Tree=95.6, SVM=96.4, KNN= 96.6, K-Means= 96.7, Naive Bayesian= 97.2, Fuzzy C Means= 98.7. Hou et al. [14] sets out a scheme for identifying and tracking DDoS traffic in conjunction with NetFlow feature identification and machine learning. First, they extract both flow-based and pattern-based features from real-time NetFlow data samples. They then built a detector based on Random Forest. They evaluated it by tracking the research lab's network, which contains DDoS traffic and various types of benign traffic, using popular DDoS tools. The results showed that this method achieves a false positive of less than 0.5% and an average accuracy of more than 99%. Besides, this experiment is valid for DDOS means such as stealth DDoS attacks.

In a study by [15], the pandemic modelling tools and resources of IoT networks consisting of WSNs were used. The researchers constructed a proposed framework for detecting abnormal defensive activities. Given the influence of IoT-specific characteristics—such as power constraints, inadequate processing capabilities, and node density—on the formation of the botnet, several formidable obstacles have been identified. Standard datasets for two widely recognized active attacks, including Miraa, were employed. A range of data mining and machine learning algorithms was implemented, including neural networks, LSVMs, and decision trees, to identify and classify anomalous activities, including DDoS features.

Based on the empirical findings, it was determined that the integration of the random forest and the decision tree yielded a notable degree of precision in the identification of attacks. A study by [16] has proposed a novel approach called GA-DT, which combines a genetic algorithm (GA) with a decision tree (DT) to address the problem of detecting various types of DDoS attacks. The implementation of this approach utilizes Mininet as the default SDN emulator for experimentation. To evaluate the effectiveness of GA-DT, the authors employed real traces of four modern DDoS attack types: UDP Flooding, TCP SYN Flood, TCPKill, and ICMP Flooding. These traces were captured using Wireshark. In comparison to existing methods such as DT, Neural Network (NN), Logistic Regression (LR), Self-Organizing Map (SOM), Support Vector Machine (SVM), Nearest Neighbors (KNN), and Random Forests (RF), the proposed hybrid classification method was evaluated. The results obtained demonstrate that GA-DT exhibits a significantly higher accuracy compared to the other methods. It achieved an accuracy rate of over 96%, which was comparable to that of Random Forests. LR had the lowest accuracy rate at 69.85%. MLP, IBK, SOM, J48, and SVM followed, with accuracy rates ranging from 82% to 93%. These findings highlight the efficiency and effectiveness of GA-DT in detecting DDoS attacks, making it a promising approach for improving the accuracy and performance of intrusion detection systems.

The study conducted by [17] provides a comprehensive analysis of the structure and features of DDoS attacks, aiding in the comprehension of their complete operational process. Data mining methods were employed to identify Distributed Denial of Service (DDoS) attacks [19]. The analysis utilized a recently acquired dataset containing 25 distinct attributes and 6 categories. The Multilinear Perceptron (MLP) classifier outperformed the Random Forest (RF) and Naïve Bayes algorithms in accurately identifying DDoS attack types, achieving the greatest accuracy rate. The study described in reference [20] developed a smart device that utilizes four methods of machine learning to identify and categorize any abnormal internet traffic patterns. The outcome demonstrated that the multilayered perceptron classification likewise attained the best level of reliability.

A study by [21] proved that CNNs are effective in detecting DDoS attacks. The study authors developed a customizable CNN detection approach to address the issues of a high rate of false alarms and low accuracy in identifying assaults. They achieved this by changing the Network Security Laboratories (NSL) dataset into input photos that the CNN algorithm may accept. The researchers in [22] introduced a platform for the development of intrusion detection systems (IDS) called IDS-CNN. This system utilizes a Convolutional Neural Network (CNN) method to detect Denial of Service (DoS) attacks. The detection process is carried out using the KDD Cup-99 dataset [23], which is a widely used dataset in the field of Knowledge Acquisition and Data Mining Tools Challenge. The investigators employed Convolutional Neural Networks (CNN), which are represented as a matrix of pixels, to address the problems associated with Denial of Service (DoS). Furthermore, a comparative experiment was carried out to assess the efficacy of the CNN model concerning various machine learning methodologies, including K-Nearest Neighbor, Support Vector Machines, and Naïve Bayes.

The experimental findings demonstrated that the system outperformed alternative machine learning methods, exhibiting superior accuracy and a rapid identification rate. The research primarily addresses DoS assaults and does not explicitly include DDoS attacks, which involve a single computer and a web connection. Hence, this study concentrates explicitly on detecting Distributed Denial of Service (DDoS) attacks by utilizing the Convolutional Neural Network (CNN) deep learning technique.

Moreover, the settings of the algorithm used by CNN will be fine-tuned to attain superior outcomes. In their study, the scientists introduced a novel method for detecting DDoS attacks called Deep Protection Deep Learning. They employed various deep learning techniques, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) such as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), as well as fully connected layers. Deep learning techniques autonomously extract characteristics. Their technique exhibits superior performance in comparison to conventional machine learning algorithms.

The researchers in [24] employed deep learning approaches, such as Stacked Restricted Habsburg Machine (RBM), to develop a network intrusion detector based on finding anomalies. By utilizing the KDDCup99 dataset, they demonstrated that their method can effectively identify and categorize intrusions into five distinct groups with a high level of accuracy. In a previous study, researchers introduced an innovative method that utilizes Deep Neural Networks (DNNs) and Pyramid Systems to identify botnet activity in TCP/UDP/IP traffic flows.

### A. Proposed Framework

The framework proposed in this study aims to detect abnormal behavior in data movement by analyzing the data flow between the sender and the receiver. That is, the servers of the ticket reservation system in airline companies must be completely secured from any threats, especially DDoS. Figure 1 below illustrates the overall framework of this assault.

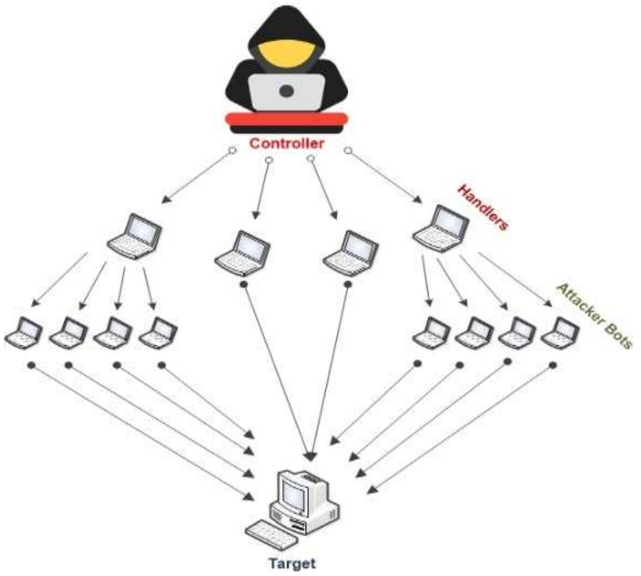


Fig. 1 General structure of DDoS attacks

At a specific time, the target server remotely simulated a DDoS attack. The assault commenced with pre-installed software on network devices that intended to render the target server inaccessible to authorized clients. The target server simulated the ticketing system's telemetry, which was transmitted to all devices via a network-installed application. These assumptions align with the specifications of HTTP and TCP. A Flood DDoS assault was initiated at a specific moment. The assault commenced with pre-installed software on network devices that aimed to disable legitimate clients from accessing the target server. It is time to apply the 1D Convolutional Neural Networks algorithm independently for DDoS detection and classification, as it was utilized in this paper, as shown in Fig. 1.

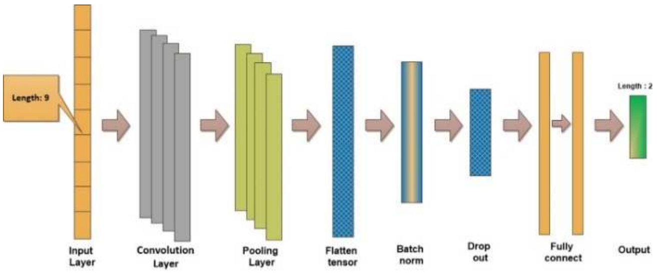


Fig. 2 1D CNN architecture

Two datasets were utilized in training the classifiers: one was obtained from the pre-simulation network, and the other was downloaded offline. The phases of the classification procedure are delineated in the subsequent paragraph.

### B. Data Collection

As stated previously, the models were trained using two distinct collections of data: A- A dataset that was captured and monitored throughout the DDoS assault; it was exported to an Excel file and assigned the identifier data1. B- The dataset was downloaded from the Kaggle website - A P A Dataset - and is usually called the DDoS attack dataset [18]. The datasets contain classification models. In addition, the one-dimensional CNN algorithm was used.

### C. Data Modeling

The dataset underwent training and modeling using the Convolutional Neural Network (CNN) technique. The neural network comprises two convolutional layers, two pooling layers, and three fully connected layers. The Rectified Linear Unit (ReLU) activation algorithm was employed in every layer. The technique was optimized using the dynamic amplitude estimating (Adam) approach, with the number of periods set at 80. The framework operates by performing a convolution operation on the supplied data using a collection of n cores.

### D. Feature Extraction

Through the filters of each layer, these features are embedded within the convolution layers; in this manner, the backpropagation procedure is utilized to learn and optimize the parameters of each filter.

### E. Comparison Stage

The Comparison Stage compares the results of other classifications with those from the 1D CNN, which consists of an input layer, a hidden layer (convolutional, function activation, pooling, fully connected), and an output layer. As shown in Fig. 3, activation and convolutional function layers were extracted from the input layer data using filters that depend on an activation function. The pooling layer, responsible for reducing the size of the matrix, uses one of the following methods: average pooling or maximum pooling, to prevent the problem of overfitting and to increase the speed of the learning process. Data from the final pooling layer is transferred to the fully connected layer. Following their arrangement into a one-dimensional vector, a one-dimensional array representing the categories (DDoS attack, normal) is generated. In brief, the CNN algorithm consists of four phases. The initial phase comprises the input layer, followed by three convolutional layers. The pooling layer receives the outputs from these convolutional layers. The input layer is absent from the second stage, which comprises the input layer. The output layer and an entirely connected network comprise the third stage.

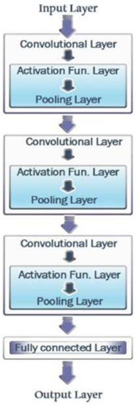


Fig. 3 Proposed 1D CNN layers

### F. 1D CNN Classifier

The current study utilized a One-Dimensional Convolutional Neural Network (1D CNN) as the foundation of the design because of its ability to recognize patterns in data. 1D CNNs are capable of extracting complex characteristics from raw input, making them well-suited for detecting unusual patterns in Distributed Denial of Service (DDoS) assaults. The output consists of two prediction levels, which correlate to the categories of Benign and Assault. The presented classifier algorithm utilizes a CNN-based structure of many convolutional layers, which are further accompanied by continuous normalization, abandonment, and fully interconnected layers. The quantity of filtration and the measurement of the screens are gradually decreased, leading to a reduction in the map of features. This allows the model to better detect intricate patterns in the network flow data. Batch normalizing and layer dropouts mitigate excessive fitting and enhance model resolution throughout learning. The program demonstrated significant efficacy in precisely detecting various forms of traditional DDoS attacks.

## III. Results and Discussion

Two categories of data are present in each dataset: malicious and normal. Dataset-A comprises 10,000 simulation-generated samples, whereas Dataset-B comprises 151,201 samples. Before this mention, Wireshark sniffer data from Dataset-A was acquired and exported. Pcap format, and subsequently converted to .CSV format. In CSV format, Dataset-B was downloaded from the Internet. The 1D CNN model and all other classifiers were supplied with data through exported CSV files. The 1D CNN model distinguished between training and assessment data from the input samples. The activation function employed for the convolutional and fully connected layers was the ReLU function, while the output layer utilized the softmax function. Twenty epochs after training the model with the initial dataset. The outcomes of the 1D CNN model, which achieved an accuracy of 99.5%, are illustrated in Figs. 4 and 5. Additionally, the outcomes for dataset-A are presented in Figs. 6 and 7, and those for dataset-B are presented in Figs. 8 and 9. Table 1 provides a comprehensive explanation of the outputs derived from each layer utilized in the model.

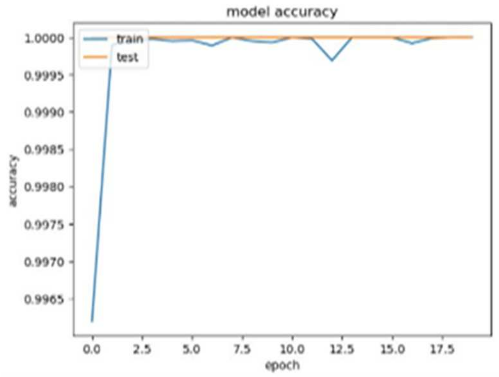


Fig. 4 Accuracy for Dataset-A

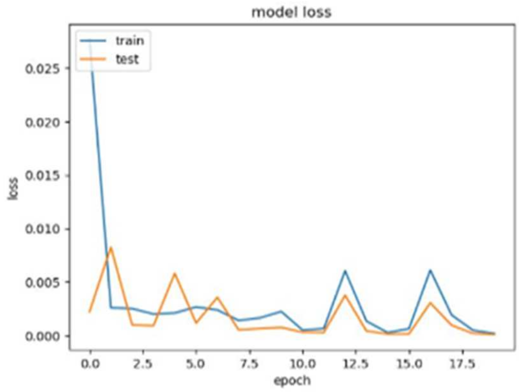


Fig. 5 Loss for Dataset-A

TABLE I
1D CNN SUMMARY

| Layer (type) | Output Shape | Param # |
|---|---|---|
| conv1d_1 (Conv1D) | (None, 21, 64) | 256 |
| max_pooling1d_1 (MaxPooling 1D) | (None, 10, 64) | 0 |
| conv1d_2 (Conv1D) | (None, 8, 128) | 24704 |
| max_pooling1d_2 (MaxPooling 1D) | (None, 4, 128) | 0 |
| conv1d_3 (Conv1D) | (None, 2, 256) | 98560 |
| flatten_1 (Flatten) | (None, 512) | 0 |
| dense_1 (Dense) | (None, 256) | 131328 |
| dropout (Dropout) | (None, 256) | 0 |
| dense_2 (Dense) | (None, 128) | 32896 |
| dropout_1 (Dropout) | (None, 128) | 0 |
| dense_3 (Dense) | (None, 64) | 8256 |
| dropout_2 (Dropout) | (None, 64) | 0 |
| dense_4 (Dense) | (None, 1) | 65 |

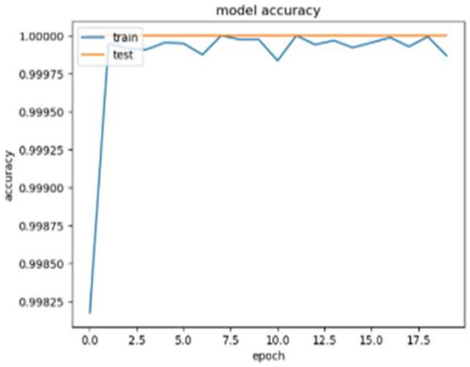


Fig. 6 Accuracy for Dataset-B

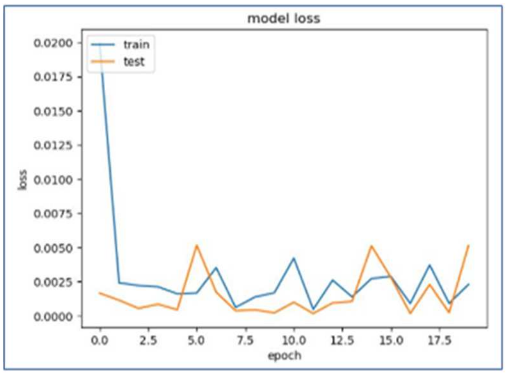


Fig. 7 Loss for Dataset-B

The results were compared between the proposed 1D CNN model and other models, such as KNN and ANN. As shown in Table 2, the 1D CNN algorithm has a high ability to classify and detect DDoS attacks with accuracy and better performance than other classifications. The above classification algorithms are applied to a device with 8GB RAM with a Windows 10 64-bit operating system. To evaluate the accuracy of different DL techniques, the Python-based Keras tool was used.

TABLE II
COMPARISON BETWEEN OUR MODEL AND OTHERS

| Technique | Dataset-A | Dataset-B |
|---|---|---|
| ANN | 95.8% | 97.2% |
| KNN | 93.7% | 96.4% |
| 1D CNN | 99.5% | 99.7% |

## IV. CONCLUSION

This study primarily aims at providing an approach to detection. This proposal introduces a model that utilizes a one-dimensional convolutional neural network to identify and forecast Distributed Denial of Service (DDoS) threats in ARS. The performance demonstrates enhancement compared to the currently employed conventional machine learning methods. The proposed model is suitable for administrators of networks, consumers of information, website developers, business groups, and cloud professionals. Nevertheless, the research also provides an opportunity to evaluate the generated algorithm on a more authentic data set to assess its effectiveness further. This research was centered on Distributed Denial of Service attacks, one of the most perilous hazards today, that targets servers directly. This paper presents and implements three distinct classification algorithms to identify DDoS attacks. Each model is developed and trained utilizing an individual pair of datasets. Using a convolutional neural network (1D CNN), routine traffic was distinguished from DDoS attack traffic. Based on the findings and analysis, 1D CNN exhibits superior performance compared to alternative classifiers, achieving an accuracy rate exceeding 99.5%. Concerning future work, we intend to construct a novel DDoS attack prevention model by integrating Long Short-Term Memory (LSTM) and CNN technologies.

## Acknowledgment

We thank the Department of Medical Instruments Techniques, Middle Technical University, Technical Institute Kut, Baghdad, Iraq, the Middle Technical University, Technical Institute-Suwaira, the Department of Computer Systems, and the Computer Science Department, National University for Science and Technology Politehnica Bucharest, Romania, for the support given during this work.

## References

[1] J. Bhajo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Eng. Appl. Artif. Intell.*, vol. 123, p. 106432, 2023, doi:10.1016/j.engappai.2023.106432.

[2] R. F. Fouladi, O. Ermiş, and E. Anarim, "A novel approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-defined network," *Comput. Secur.*, vol. 112, p. 102524, 2022, doi:10.1016/j.cose.2021.102524.

[3] D. K. Gharkan and A. A. Abdulrahman, "Construct an efficient distributed denial of service attack detection system based on data mining techniques," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 29, no. 1, pp. 591–597, 2023, doi: 10.11591/ijeecs.v29.i1.pp591-597.

[4] O. Belej and L. Halkiv, "Using hybrid neural networks to detect DDOS attacks," in *Proc. 2020 IEEE 3rd Int. Conf. Data Stream Mining Process. (DSMP)*, 2020, pp. 61–66, doi:10.1109/DSMP47368.2020.9204166.

[5] B. M. Rahal, A. Santos, and M. Nogueira, "A distributed architecture for DDoS prediction and bot detection," *IEEE Access*, vol. 8, pp. 159756–159772, 2020, doi: 10.1109/ACCESS.2020.3020507.

[6] J. Bhajo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, "A time-efficient approach toward DDoS attack detection in IoT network using SDN," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3612–3630, Mar. 2021, doi: 10.1109/JIOT.2021.3098029.

[7] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, p. 103096, 2023, doi: 10.1016/j.cose.2023.103096.

[8] A. Mathew, P. Amudha, and S. Sivakumari, "Deep learning techniques: an overview," in *Adv. Mach. Learn. Technol. Appl. Proc. AMLTA 2020*, 2021, pp. 599–608, doi: 10.1007/978-981-15-3383-9_54.

[9] A. R. Shaaban, E. Abdelwaness, and M. Hussein, "TCP and HTTP flood DDoS attack analysis and detection for space ground network," in *Proc. 2019 IEEE Int. Conf. Vehicular Electron. Saf. (ICVES)*, 2019, pp. 1–6, doi: 10.1109/ICVES.2019.8906302.

[10] B. Bala and S. Behal, "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges," *Comput. Sci. Rev.*, vol. 52, p. 100631, 2024, doi:10.1016/j.cosrev.2024.100631.

[11] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via convolutional neural network (CNN)," in *Proc. 2019 IEEE 9th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, 2019, pp. 233–238, doi: 10.1109/ICICIS46948.2019.9014826.

[12] R. S. Chaudhari and G. R. Talmale, "A review on detection approaches for distributed denial of service attacks," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, 2019, pp. 323–327, doi:10.1109/ISS1.2019.8908125.

[13] S. Sumathi and N. Karthikeyan, "Search for effective data mining algorithm for network based intrusion detection (NIDS)-DDOS attacks," in *Proc. IEEE Int. Conf. Intell. Comput. Commun. Smart World, I2C2SW*, 2018, pp. 41–45, doi:10.1109/I2C2SW45816.2018.8997522.

[14] A. Saber, M. Abbas, and B. Fergani, "A DDoS attack detection system: Applying a hybrid genetic algorithm to optimal feature subset selection," in *Proc. 4th Int. Symp. Informatics Appl. (ISIA)*, 2020, pp. 1–6, doi: 10.1109/ISIA51297.2020.9416558.

[15] A. Bhati *et al.*, "Evaluation of classification algorithms for distributed denial of service attack detection," in *Proc. 2020 IEEE 3rd Int. Conf. Artif. Intell. Knowl. Eng. (AIKE)*, 2020, pp. 138–141, doi:10.1109/aike48582.2020.00030.

[16] P. Preamthaisong *et al.*, "Enhanced DDoS detection using hybrid genetic algorithm and decision tree for SDN," in *Proc. 16th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, 2019, pp. 152–157, doi:10.1109/jcsse.2019.8864216.

[17] A. K. A. Al-Mashadani and M. Ilyas, "Distributed denial of service attack alleviated and detected by using mininet and software defined network," *Webology*, vol. 19, no. 1, pp. 4129–4144, 2022, doi:10.14704/web/v19i1/web19272.

[18] Yashwanth, K. A. P. "APA-DDOS Dataset," *Kaggle*, 2024. [Online]. Available: https://www.kaggle.com/datasets/yashwanthkumbam/APADDoS-dataset (accessed May 26, 2024).

[19] A. E. Abdallah *et al.*, "Detection of management-frames-based denial-of-service attack in wireless LAN network using artificial neural network," *Sensors*, vol. 23, no. 5, p. 2663, 2023, doi:10.3390/s23052663.

[20] A. Fathima, G. S. Devi, and M. Faizaanuddin, "Improving distributed denial of service attack detection using supervised machine learning," *Meas. Sensors*, vol. 30, p. 100911, 2023, doi:10.1016/j.measen.2023.100911.

[21] M. A. Aladaileh *et al.*, "Detection techniques of distributed denial of service attacks on software-defined networking controller—A review," *IEEE Access*, vol. 8, pp. 143985–143995, 2020, doi:10.1109/access.2020.3013998.

[22] N. Nishanth and A. Mujeeb, "Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference," *IEEE Syst. J.*, vol. 15, no. 1, pp. 17–26, 2021, doi: 10.1109/JSYST.2020.2984797.

[23] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, p. 100229, 2022, doi: 10.1016/j.array.2022.100229.

[24] I. Ahmad, Z. Wan, and A. Ahmad, "A big data analytics for DDOS attack detection using optimized ensemble framework in Internet of Things," *Internet Things*, vol. 23, p. 100825, 2023, doi:10.1016/j.iot.2023.100825.