Nigerian Journal of Technology (NIJOTECH)
Vol. 41, No. 6, November, 2022, pp.1017 - 1024
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
http://dx.doi.org/10.4314/njt.v41i6.12

DETECTION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS USING CONVOLUTIONAL NEURAL NETWORKS

A. O. Akinwumi[1,*], A. O. Akingbesote[2], O. O. Ajayi[3], and F. O. Aranuwa[4]

[1,2,3,4]Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria

*corresponding author (Phone Number: +234-816-245-3834. Email: ayodeji.akinwumi@aaua.edu.ng)

Article history: Received 14 February, 2022. Revised 22 March, 2022. Accepted 27 April, 2022

Abstract
The rapid evolution of the Internet has brought tremendous benefits to the world at large. To effectively leverage on the importance of the internet, there is the need for a secured and reliable network. But currently, there are lots of network attacks against network infrastructures. One of such attack is the Distributed Denial of Service (DDoS) attacks which is an attempt by hackers to deny authorized users access internet service availability using many attack machines. In this paper, a Convolutional Neural Network based detection model is proposed to proffer solution to the challenges of DDoS attacks. The dataset for the modelling was sourced from the KDD Cup-99 Dataset. The evaluation of the experiment conducted was based on three standard metrics of accuracy, sensitivity and specificity. The experimental results showed that the developed model had an accuracy of 99.72%, specificity of 99.69% and sensitivity of 99.71%. Furthermore, the performance of the model was compared with other existing traditional learning models, the results indicated that the model presented in this work performed significantly better.

Keywords: Distributed Denial of Service, Convolutional Neural Networks, Network Traffic, Network Security, Machine Learning, Cybercrime.

1.0 INTRODUCTION

The increasing growth rate of the internet has resulted to lots of activities being conducted online. More opportunities for work and business have emerged as a result of the development of the internet [1]. According to a survey, the internet accounts for more than 60% of total commercial transactions [2]. There is no doubt, the advent of internet has brought about immense social changes and improved the way we live and do things. Therefore, to effectively leverage on the importance of the internet, there is a need for a secured and reliable network. However, there are a lot of network attacks or malicious activities against network infrastructures [3]. The rise in technological innovation and the internet has resulted in the emergence of a new variety of computer-related criminal activities, in addition to a significant increase in the incidence of criminal activities [1]. Hacking and cyber warfare are becoming more widespread these days, and new attack routes are constantly emerging [4]. The Denial of Service (DoS) attack is one of these several types of attacks. DoS attack is a type of cybercrime in which an attacker explores available resources to attack a network, application, or service in order to deny authorized users access to their network service.

A Distributed Denial of Service (DDoS) attack is a more complex type of DoS attack that happens on a much bigger scale. While a DoS attack normally employs one computer and one Internet connection to flood a specified system or resource, a DDoS attack floods the targeted resource using multiple computers and Internet connections. A DDoS intrusion can be executed from a large number of computers (also known as botnets or zombies) that have been hijacked by the attacker (also known as botmaster), each of which will simultaneously send a large number of packets to the target server [5]. This excessively absorbs all the server's bandwidth and, as a result, renders the server unresponsive to further requests or causes it to crash completely [6]. Due to the diversity and multiplicity of DDoS attacks, they are among the hardest network security problems to detect and

defend against [6], and according to available reports, DDoS attacks have been steadily increasing in recent years [7].

These attacks are now a major cause of concern to the current internet community and have become a weapon of choice for various categories of internet violators, including hackers, cyber extortionists, and cyber terrorists [8]. The major aim of DDoS attacks is not to steal data from the victims but to deny services for as long as possible [9]. This is done to compromise the availability of internet resources that fall within the triad of information security; (CIA - confidentiality, integrity and availability). DDoS attacks have caused network service abnormalities, resulting in devastating consequences [10] for their victims, which include private organizations, government agencies, healthcare, education, and financial institutions, as well as the telecommunications industry [6]. The work of [11] attempts to calculate the direct cost of a DDoS attack on Internet of Things (IoT) device users whose machines were affected. According to the report, the authors observed that it cost device owners about $323,973.75. Apart from this, a lot of organizations have suffered reputational damage, lost their ability to trade and business opportunities have been lost as a result of DDoS attacks [12].

A lot of work has been done by researchers to mitigate the menace of DDoS attacks. Some of these methods include Ingress Filtering [13], Client Puzzles [14], Intrusion Detection Mechanisms [15], Honey Pots [16], among others. While these have proved to be effective, especially in the area of detecting attackers, issues of accuracy, specificity, sensitivity, among other issues, still require more attention. To solve these issues, researchers have been investigating how machine learning tools can be applied in the area of intrusion detection. Machine learning is a branch of computer science that groups and extracts behaviors and entities from data using pattern recognition [3]. These previously known patterns and relationships, trained by machine learning algorithms, will then be used to do prediction tasks on new sets of data. As reported by [17], deep learning algorithms have also recently emerged as a result of various advancements and evolutions in machine learning. One classification of such deep learning algorithms is the convolutional neural network.

Convolutional Neural Network (CNN) have been widely utilized in the area of computer vision such as classification of images [18], speech recognition [19], vehicle recognition [20], detection of objects [21], recognition of facial expressions [22] among many others. While the performance of CNN in terms of accuracy and efficiency in the aforementioned areas have achieved great success, however, in the area of Network Security, particularly the detection of anomaly traffic, this performance has not been fully exploited [23]. Therefore, this research aims at making a contribution in this area, which is to apply the use of CNN for the detection of DDoS attacks.

1.1 LITERATURE REVIEW

The work of [24] discussed in detail the anatomy and characteristics of DDoS attacks, which is helpful to understand the full mode of operation of DDoS attacks. [25] used data mining techniques as a way of detecting DDoS attacks. A Newly collected dataset with twenty-seven (27) characteristics and five (5) classes was used. Out of the three machines learning algorithms (Multilinear Perceptron (MLP), Random Forest, and Naïve Bayes) that were applied to identify the DDoS attack types, MLP classifier achieved the highest accuracy rate. The research presented in [9] designed an intelligent system to detect and classify any anomalous behavior of the network traffic using four machine learning algorithms. The result showed that the multilayer perceptron classifier also achieved the highest accuracy rate.

The work of [26] demonstrated that CNN could be used for the detection of DDoS attacks. The researchers were able to design a flexible CNN detection based system to prevent high false alarm rates and low detection accuracy against attacks by transforming the obtained dataset, which is the Network Security Laboratory (NSL) dataset, to be accepted as input pictures by the CNN algorithm. The researchers in [27] proposed an intrusion detection system (IDS) platform based on CNN technique called the IDS-CNN to detect DoS attack using Knowledge Discovery and Data Mining Tools Competition commonly referred to as the KDD Cup-99 dataset [28].

The researchers used CNN, which is represented as a pixel matrix, to combat issues of DoS. An experiment was also conducted to compare the performance of the CNN model with other machine learning techniques such as K-Nearest Neighbour, Support Vector Machines, and Naïve Bayes. The result of the experiment showed that the system performed better than the other machine learning techniques, with higher accuracy and with an early detection rate. The

area of attention in this research is that the authors only focused on solving DoS attacks and not on DDoS attacks, i.e., attacks related to one computer and one internet connection. Therefore, in this paper, the researchers focus on the detection on DDoS using the CNN deep learning algorithm. Furthermore, the parameters of the CNN algorithm will be optimized to achieve better results.

1.1.1 Convolutional Neural Network

CNN is an end-to-end deep learning technique that takes a raw image as an input and produces a prediction based on distinguishing features extracted from intermediate layers [29]. It is also commonly referred to as ConvNet. It is a class of deep learning algorithms that are commonly used to solve complex problems, and they have considerably high efficiency and accuracy [30]. A standard CNN model consists of three key layers, which are the convolution layer, the pooling layer, and the fully connected layer [26].

In the first layer, which is the convolution layer, an image to be classified is supplied into the input layer, and the output is the predicted class label derived using extracted features from the image [29]. Then, in the next layer, an individual neuron is connected to some neurons in the preceding layer; this association is known as the receptive field [30]. The Receptive field is used to extract local features from the input image. A weight vector is formed by the receptive field of a neuron in the previous layer associated with a particular region, which remains constant at all points on the plane, in which the plane refers to the neurons in the next layer. The pooling layer reduces the number of parameters that can be trained and introduces translation invariance. To accomplish the pooling action, a window is chosen, and the input items in that window are passed through a pooling function. [31]. Afterwards, the output of the first phase is fed into the fully connected layer (including the repetitive convolution and pooling), and the dot product of the weight vector and input vector is produced for the final output. [32]

2.0 METHODOLOGY

The architecture of the model presented in this work is depicted in Figure 1. The architecture consists of four layers: The first layer is the Data Collection layer, the second is the data pre-processing layer, the third layer is the training layer, and the fourth layer is the developed DDoS Detection layer. A Performance evaluation based on standard metrics of accuracy, sensitivity, and specificity is performed to determine the efficiency of the model.

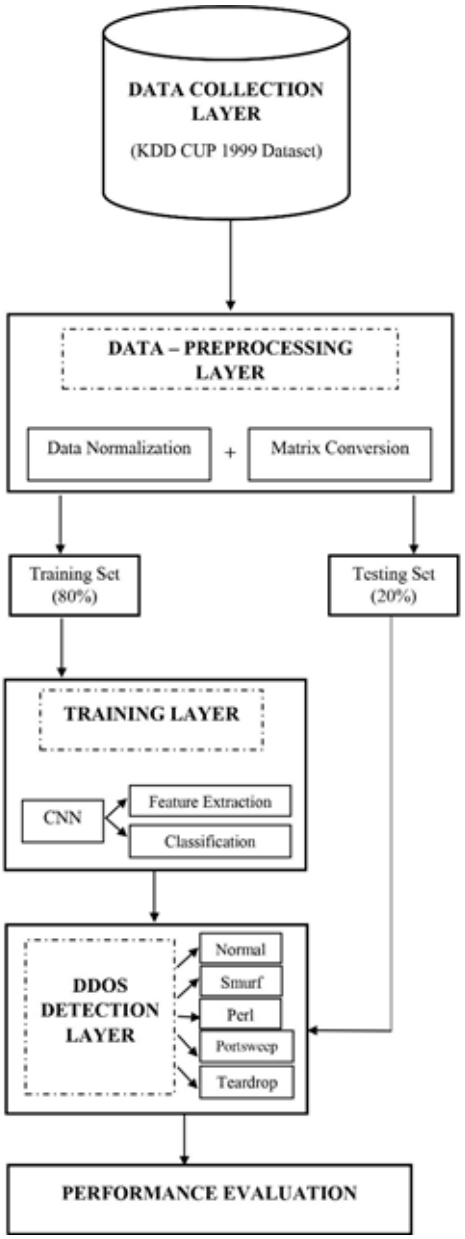

Figure 1: Architecture of the Proposed Model

2.1 DATA COLLECTION

The Data used for the research work was sourced from the KDD Cup-99 dataset in order to train and test the model. This was obtained from the University of California's online archives (http://kdd.ics.uci.edu /databases/kddcup99/kddcup99.html). The reason for using the KDD Cup 1999 dataset is based on the fact that it provides real-time network traffic and it is also a well-known dataset for intrusion detection based on a project by the Defense Advanced Research Projects Agency (DARPA) in 1998 [27]. The dataset contains about 5 million records in which the dataset is made up of 22 different attacks with 41 features of traffic in each record. For the purpose of this research, we extracted the normal traffic and four (4) of the 22 different attacks. This is shown in Table 1.

Table 1: Extracted Normal Traffic and Attack types with their Count Frequency (Instances in the Dataset)

S/N	ATTACK	FREQUENCY
1	Normal	97277
2	Smurf	280790
3	Teardrop	979
4	Portsweep	1040
5	Perl	3

The total number of samples in the obtained dataset was 380,089, which were split into training and testing sets at 80% and 20%, respectively, as shown in Table 2. The training set is the dataset that is used to train the model. It serves as a baseline for future use, while the test data is intended to assess the efficiency of the model [9]. Generally, for machine learning algorithms like convolutional neural networks, the more training datasets, the better the performance of the model and it does not easily suffer from overfitting like some other machine learning algorithms.

Table 2: Splitting of Dataset

Training Set (80%)	Testing Set (20%)
304,071	76,018

Table 3 shows the KDD Cup-99 dataset attributes. As revealed in the Table, 41 attributes were used. The attributes are carefully selected to improve classification performance as well as to reduce computational time.

Table 3: Number of Attributes and the Attributes Used

No	Network Attributes	No	Network Attributes	No	Network Attributes
1	duration	**15**	su_attempted	**29**	same_srv_rate
2	protocol_type	**16**	num_root	**30**	diff_srv_rate
3	service	**17**	num_file_creations	**31**	srv_diff_host_rate
4	flag	**18**	num_shells	**32**	dst_host_count
5	src_bytes	**19**	num_access_files	**33**	dst_host_srv_count
6	dst_bytes	**20**	num_outbound_cmds	**34**	dst_host_same_srv_rate
7	land	**21**	is_host_login	**35**	dst_host_diff_srv_rate
8	wrong_fragment	**22**	is_guest_login	**36**	dst_home_same_src_port_rate
9	urgent	**23**	count	**37**	dst_host_srv_diff_host_rate
10	hot	**24**	srv_count	**38**	dst_host_serror_rate
11	num_failed_logins	**25**	serror_rate	**39**	dst_host_srv_serror_rate
12	logged_in	**26**	srv_serror_rate	**40**	dst_host_rerror_rate
13	num_compromised	**27**	rerror_rate	**41**	dst_host_srv_rerror_rate
14	root_shell	**28**	srv_rerror_rate		

2.2 DATA PRE-PROCESSING

The data collected was preprocessed by the data pre-processing layer. The first stage in the pre-processing stage was to convert and normalize the dataset into a matrix comprising the value of each input image, with each value ranging from zero to 255 for each pixel, since the CNN algorithm is good at image classification. Furthermore, the normalization is very necessary as a large percentage of the values in the KDD dataset are less than 122, with a few being larger than 255. An algorithm is therefore needed for the normalization of the dataset.

To achieve this, two normalization algorithms were studied in [33] and [27]. The researchers adopted the algorithm in [27] because the experiment was also based on the use of the KDD Cup dataset. The algorithm is presented below:

Require: KDD Dataset
Ensure: New data with range from 0 to 255

```
c = foreachColumn()
avg = 0
r = 0
if(c is integer) then do
    new_val = Processinteger(c)
else
    avg = average(c)
    r = getRow(c)
    if( r < 122) then do
      new_val = r*2
else
    if( r < 2 * avg) then do
      new_val = (r * 123) / avg
    else
```

2.3 DATA MODELING

The dataset was trained and modeled with the CNN algorithm. The classifier contains two convolution layers, two pooling layers, and three fully connected layers. The kernel size of the convolution layers is [4*4] and [3*3] respectively. The pooling size for the two pooling layers is [2*2], while the three fully connected layers include 50, 20 and 2 neurons. The Rectified Linear Unit (ReLU) activation function was used in all the layers. In order to optimize the algorithm, the adaptive moment estimation (Adam) method was used, and the number of epochs was set to 80.

The trained CNN model classifies input traffic into five types: normal, smurf, perf, Portsweep, and

teardrop attack traffic. The model works by convolving the input data with a set of n kernels.

Considering n kernels = 5,
Then the $W\ (Kernel)\ = \{w1, w2, \dots, w5\}$ and their biases, $B = \{b1, b2, \dots, bn\}$.
Where;
W is the number of kernels
B is represented as their Biases

2.4 EVALUATION

To evaluate the proposed detection model, an experiment was conducted to show the performance of the proposed CNN based detection model using the test data. The following metrics were used to evaluate the performance of our developed model: Sensitivity, Specificity and Accuracy.

Where;

$$\text{Sensitivity} = \frac{TP}{TP+FN} \quad (1)$$

$$\text{Specificity} = \frac{TN}{TN+FP} \quad (2)$$

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

where,
TP is True positive: which implies that predictions are true and confirmation also say it is true (that is, when illegitimate traffic is correctly identified as attacks).
TN is True Negative: which implies that predictions are not true and confirmations say that is not true (That is, when legitimate traffic are correctly identified as normal traffic)
FP is False Positive: which implies predictions are true and confirmation says it is not true. (That is, when normal traffic is detected as an attack).
FN is False Negative: which implies that predictions are not true and confirmation says it is true (When attacks are detected as normal traffic).

3.0 RESULTS AND DISCUSSION

3.1 RESULTS

A total of 380,089 data were considered in this research, and 80 iterations were run on the model to determine the accuracy of the developed model. An extract of this is shown in Figure 2. From the figure, the accuracy of the model at the 80th iteration level was 99.69%.

The test loss result, which indicates the number of bad predictions, is depicted in Figure 3. In this figure, it can be observed that the test loss ranged between 0.5 - 0.11. This range of values means that the errors made were minimal and did not have any significant impact on the performance of the model. The iteration was run 80 times and the accuracy levels were measured as depicted in Figure 4. The confusion matrix as presented in Table 4 revealed that out of 282,812 attacks with 97,277 legitimate traffic instances from the overall data, the model correctly predicted 281,964 attack instances and 96,985 normal traffic instances correctly. The false positive values of 292 and false negative value of 848 were recorded for attacks and normal traffic respectively. Based on the explained equations and the matrix outcomes, the values for sensitivity, specificity and accuracy were obtained.

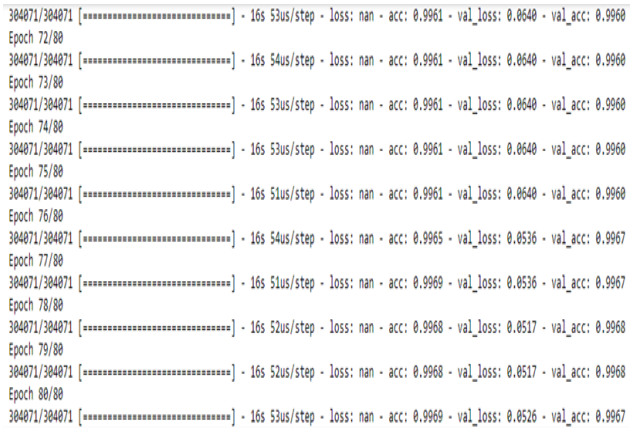

Figure 2: Extract of Iterations

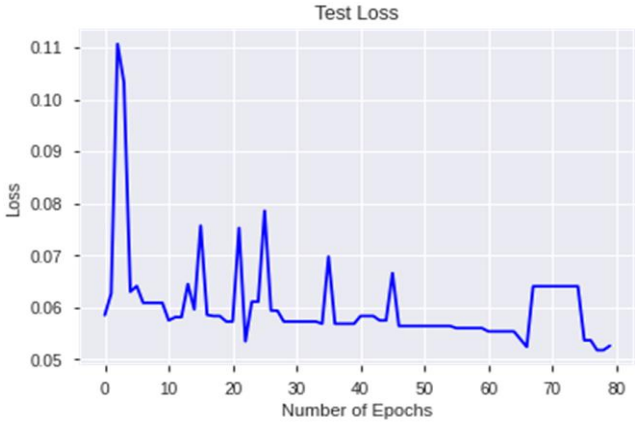

Figure 3: Test Loss of the Developed Model

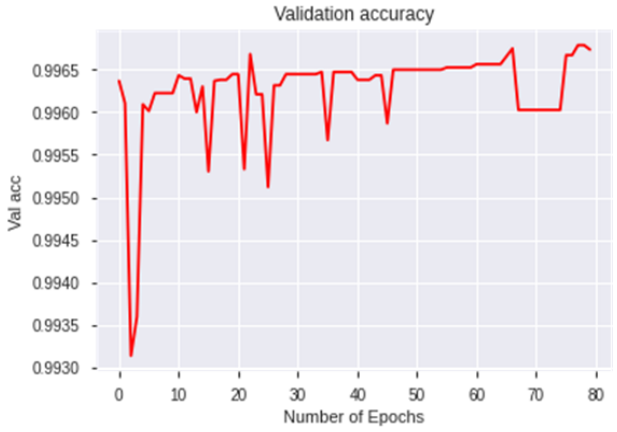

Figure 4: Accuracy at Different Iteration Levels

The developed model is shown to be effective in detecting legitimate traffic and attack instances with a specificity of 99.69% and a sensitivity of 99.71%. The general performance of the developed model on the test data was also impressive as it attained an accuracy of 99.72%.

Table 4: Confusion Matrix Result of the Developed CNN DDoS Detection Model

		Predicted Class	
		Normal Traffic	Attacks
Actual Class	Normal Traffic	TN **96,985**	FP **292**
	Attacks	FN **848**	TP **281,964**

3.2 PERFORMANCE EVALUATION

The model presented was compared to other traditional lLearning techniques, based on their accuracy, sensitivity and specificity as shown in Table 5. The graphical representation is also shown in Figure 5. The Figure reveals that the developed CNN based DDoS Detection model proved to be the most effective model with an Accuracy of 99.72%, Sensitivity of 99.71%, and Specificity of 99.69% as compared to the result from Support Vector Machines with (98.95%, 88.56% and 91.22% respectively) and Multilayer Perceptron (98.83%, 91.35% and 92.84%) respectively.

Table 5: Comparison of the Developed Model with SVM and MLP

Algorithm Model	Accuracy (%)	Sensitivity (%)	Specificity (%)
Developed CNN based DDoS Detection Model	99.72	99.71	99.69
Support Vector Machines	98.95	88.56	91.22
Multilayer Perceptron	98.83	91.35	92.84

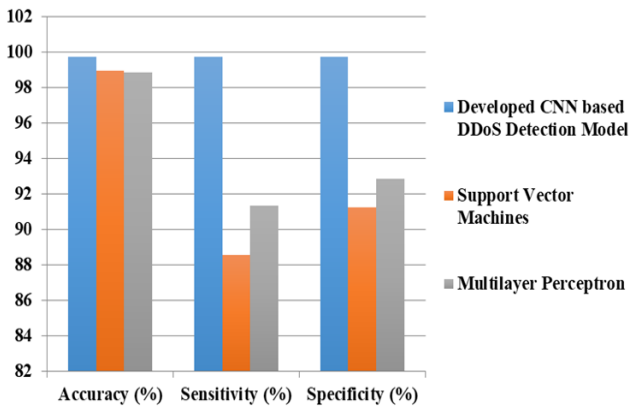

Figure 5: Comparison of Developed Model to Support Vector Machines and Multilayer Perceptron

4.0 CONCLUSION

The focus of this work was on developing a detection model to mitigate Distributed Denial of Service attacks on networks. A convolutional neural network based model to detect and predict DDoS attacks is hereby proposed. The KDD cup-99 dataset was used in the modeling. The model was tested on a LAN, and based on the performance metrics of accuracy, sensitivity and specificity, values of 99.72%, 99.71%, and 99.69% respectively, was obtained. The performance shows a relative improvement over the existing traditional machine learning techniques. The developed model is recommended for network administrators, internet users, website designers, corporate organizations, and cloud experts. However, the research also paves the way to testing the developed model on a more real dataset to further test its efficiency.

REFERENCES

[1] Alese, T., Owolafe, O., Thompson, A. F. and Alese, B. K. "A User Identity Management System for Cybercrime Control," *Nigerian Journal of Technology*, vol. 40, no. 1, pp. 129–139, 2021, doi: 10.4314/njt.v40i1.17.

[2] Rajasekharaiah, K., Dule, C. S. and Sudarshan, E. "Cyber Security Challenges and its Emerging Trends on Latest Technologies Cyber Security Challenges and its Emerging Trends on Latest Technologies," 2020, doi: 10.1088/1757-899X/981/2/022062.

[3] Najafabadi, M. M. "Machine Learning Algorithms for the Analysis and Detection of Network Attacks," Florida Atlantic University, 2017.

[4] Ibor, A. E. "Zero day exploits and national readiness for cyber-warfare," *Nigerian Journal of Technology*, vol. 36, no. 4, p. 1174, 2018, doi: 10.4314/njt.v36i4.26.

[5] Sofi, I., Mahajan, A. and Mansotra, V. "Detection And Analysis Of Ddos Attacks Using Machine Learning Techniques : A Literature," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 5, no. VI, pp. 179–185, 2017.

[6] Vishwakarma, R. and Jain, A. K. "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.

[7] Sangodoyin, A., Modu, B., Awan, I. and Disso,

J. P. "An Approach to Detecting Distributed Denial of Service Attacks in Software Defined Networks," in *Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud*, 2018, pp. 436–443, doi: 10.1109/FiCloud.2018.00069.

[8] Bawany, N. Z., Shamsi, J. A. and Salah, K. "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 425–441, 2017, doi: 10.1007/s13369-017-2414-5.

[9] Sofi, I., Mahajan, A. and Mansotra, V. "Machine Learning Techniques used for the Detection and Analysis of Modern Types of DDoS Attacks," *International Research Journal of Engineering and Technology (IRJET)*, vol. 04, no. 06, pp. 1085–1092, 2017.

[10] Ye, J., Cheng, X., Zhu, J., Feng, L. and Song, L. "A DDoS Attack Detection Method Based on SVM in Software Defined Network," *Security and Communication Networks*, vol. 2018, pp. 1–8, 2018, doi: 10.1155/2018/9804061.

[11] Li, Q., Meng, L., Zhang, Y. and Yan, J. "DDoS attacks detection using machine learning algorithms," in *Communications in Computer and Information Science*, 2019, vol. 1009, pp. 205–216, doi: 10.1007/978-981-13-8138-6_17.

[12] Mainone, "DDoS Protection Service," 2020. https://www.mainone.net/services/mainone-ddos-protection-service/ (accessed Feb. 09, 2021).

[13] Du, P. and Nakao, A. "DDoS Defense Deployment with Network Egress and Ingress Filtering," in *IEEE ICC*, 2010, p. 6.

[14] Bruce, S. *Counterpane Internet Security*, vol. 8, no. 3, pp. 10–12, 2000.

[15] Sharma, N., Mahajan, A. and Mansotra, V. "Machine Learning Techniques Used in Detection of DOS Attacks : A Literature Review," vol. 6, no. 3, pp. 100–105, 2016.

[16] Anirudh, M., Arul, T. S. and Nallathambi, D. J. "Use of Honeypots for Mitigating DoS Attacks targeted on IoT Networks," in *IEEE International Conference on Computer, Communication, and Signal Processing (ICCCSP-2017)*, 2017, pp. 8–11.

[17] Ibrahim, Y. Okafor, E. and Yahaya, B. "Optimization of RBF-SVM Hyperparameters using Genetic Algorithm for Face Recognition," *Nigerian Journal of Technology*, vol. 39, no. 4, pp. 1190–1197, 2020.

[18] Krizhevsky, A., Sutskever, I. and Hinton, G. E. "ImageNet Classification with Deep Convolutional Neural Networks," *In Advances in neural information processing systems*, pp. 1097–1105, 2012, doi: 10.1201/9781420010749.

[19] Zhang, H. *et al.*, "Towards end-to-end speech recognition with deep convolutional neural networks," *Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH*, vol. 08-12-Sept, no. September, pp. 410–414, 2016, doi: 10.21437/Interspeech.2016-1446.

[20] Luo, X., Shen, R., Hu, J., Deng, J., Hu, L. and Guan, Q. "A Deep Convolution Neural Network Model for Vehicle Recognition and Face Recognition," *Procedia Computer Science*, vol. 107, no. Icict, pp. 715–720, 2017, doi: 10.1016/j.procs.2017.03.153.

[21] Szegedy, C., Toshev, A. and Erhan, D. "Deep Neural Networks for Object Detection," *In Advances in Neural Information Processing Systems*, pp. 2553–2561, 2013, doi: 10.3928/19404921-20140820-01.

[22] Ucar, A. "Deep Convolutional Neural Networks for facial expression recognition," *Proceedings - 2017 IEEE International Conference on INnovations in Intelligent SysTems and Applications, INISTA 2017*, pp. 371–375, 2017, doi: 10.1109/INISTA.2017.8001188.

[23] Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C. and Atkinson, R. "Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey," pp. 1–43, 2017, [Online]. Available: http://arxiv.org/abs/1701.02145.

[24] Cira, "anatomy-a-ddos-attack-against-dns-infrastructure, "2019. https://cira.ca/resources/anycast/factsheet/anatomy-a-ddos-attack-against-dns-infrastructure (accessed Sep. 23, 2019).

[25] Alkasassbeh, M., Hassanat, A. and Al-naymat, G. "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques," no. February, 2016, doi: 10.14569/IJACSA.2016.070159.

[26] Mohammadpour, L., Ling, T. C., Liew, C. S. and Chong, C. Y. "A Convolutional Neural Network for Network Intrusion Detection System," in *Proceedings of the APAN – Research Workshop 2018*, 2018, pp. 50–55.

[27] Nguyen, S.,Nguyen, V., Choi, J. and Kim, K. "Design and Implementation of Intrusion Detection System using Convolutional Neural

Network for DoS Detection," in *Proceedings of the 2nd International Conference on Machine Learning and Soft Computing*, 2018, pp. 34–38.

[28] Kumar, S. and Arora, S. "Applied Soft Computing and Communication Networks," in *International Applied Soft Computing and Communication Networks*, 2019, no. December, pp. 131–157, doi: 10.1007/978-981-15-3852-0.

[29] Fang, J., Zhou, Y., Yu, Y. and Du, S. "Fine-Grained Vehicle Model Recognition Using a Coarse-to-Fine Convolutional Neural Network Architecture," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 7, pp. 1–11, 2017.

[30] Indolia, S., Goswami, A. K., Mishra, S. P. and Asopa, P. "Conceptual Understanding of Convolutional Neural Network- A Deep Learning Approach," *Procedia Computer Science*, vol. 132, pp. 679–688, 2018, doi: 10.1016/j.procs.2018.05.069.

[31] Lee, K. B., Cheon, S. and Kim, C. O. "A Convolutional Neural Network for Fault Classification and Diagnosis in Semiconductor Manufacturing Processes," *IEEE Transactions on Semiconductor Manufacturing*, vol. 30, no. 2, pp. 0–8, 2017, doi: 10.1109/TSM.2017.2676245.

[32] Liu, X. Jiao, L., Tang, X., Sun, Q. and Zhang, D. "Polarimetric Convolutional Network for PolSAR Image Classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 57, no. 5, pp. 1–15, 2019, doi: 10.1109/TGRS.2018.2879984.

[33] Akingbesote A. O., "The Use of Dijkstra Algorithm in an Ad-Hoc African Mobile Market to Determine the Optimal Route Selection", *Digital Innovations & Contemporary Research in Science Engineering & Technology*, vol. 8, no. 1, pp. 59–70, 2020.