An Explorative Analysis Sampling Deep Learning and Non-Deep Learning Approach for Detecting and Mitigating DDOS Attacks in a Network

[1]Anigbogu Kenechukwu Sylvanus*., [2]Orji Everistus Eze., [3]Mbonu Chinedu Emmanuel., [1]Anusiuba Overcomer Ifeanyi Alex

[1]Lecturer, Department of Computer Science, Nnamdi Azikiwe University Awka, Anambra State, Nigeria

[2]Lecturer, Department of Computer Science, Federal Polytechnic Ohodo Enugu State, Nigeria

[3]Researcher, Department of Computer Science, Nazarbayev University, Astana

***Corresponding Author**

DOI: https://doi.org/10.51244/IJRSI.2025.12040002

Received: 16 March 2025; Accepted: 20 March 2025; Published: 26 April 2025

ABSTRACT

The Internet is being used almost everywhere in the world now. As a result of that developing a system and network security that can detect anomalies, protect the internetwork, and predict future security threats is crucial because billions of devices are interconnected over the Internet. However, DDoS (Distributed Denial-of-Service) attacks are the most frequent and perilous threat to internet growth. New variants of DDoS attacks are highly advanced and complicated, and it is almost impossible to detect or mitigate by the existing intrusion detection systems and traditional methods. Fortunately, Machine Learning technologies enable the detection of DDoS traffic effectively. This paper reviewed the DDoS detection model based on machine learning techniques. We extracted the most used models with good deep and non-deep learning results from our literature review. We extracted the most used models with good deep and non-deep learning results from our literature review. We extracted the most used models with good deep and non-deep learning results from our literature review. APA_DDOS_Dataset which has proven results from the review was experimented with Multi-layer perceptron and Random forest, we specified the three correlated features with predicted classes that we used. It was discovered that both Multi-layer perceptron and Random forest were accurate and correctly predicted the type of network traffic with 80% and 78% accuracy with scaling. Future research can be extended by testing newer datasets on this model and then testing hybrid algorithms on the newer datasets.

Index Terms: Distributed Denial-of-Service, Random forest, Multi-layer perceptron, deep learning, non-deep learning

INTRODUCTION

Network security has become a top priority for individuals, organizations, and governments in recent years. Cyber-attacks such as DDOS, malware, phishing, ransom ware, and hacking pose a significant risk to data and network security. As a result, developing a system and network security that can detect anomalies and predict future security threats is crucial [1]. There has been an increase in the frequency and complexity of cyber-attacks, leading to significant financial losses and damage to reputation. Therefore, the need for a system and network surveillance that can provide comprehensive security measures and protect against cyber threats has become increasingly important [2].

As more individuals and organizations rely on technology to carry out their daily activities, the potential risk of network attacks increases. With the advent of advanced technologies such as artificial intelligence, machine learning, and big data analytics, the ability to detect and respond to cyber threats has improved significantly

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue IV April 2025

[3]. However, cybercriminals are also becoming more sophisticated in their attacks, making it necessary to develop advanced systems and tools to counter these threats. With the advent of technology and the proliferation of internet-connected devices, the need for secure systems and networks has become more important than ever before. Network attacks have increased in frequency, sophistication, and impact, affecting individuals, businesses, and governments alike. Network breaches can result in data loss, financial losses, and reputational damage. For instance, in 2020, the global cost of cybercrime was estimated to be $1 trillion [4].

Distributed denial of service (DDoS) attacks have become increasingly sophisticated in recent years. A single DDoS attack is now able to infect a large group of devices. More specifically, zombies target the victim and deny services to legitimate users by inundating the network with requests [5]. Attackers install malicious software, which is known as the master DDoS, to gain control over a group of compromised machines located within the same network [6]. The attackers use these zombies as an army, remotely instructing them to simultaneously attack the victim, thereby rendering the service unavailable to valid users. A related new concept, namely DDoS as a service (DDoSaaS), reduces the technical challenges associated with implementing an attack through the use of booters or stressers. The owners of pre-staged botnets allow their clients to use the DDoSaaS approach to attack specific web servers. A client has to identify a webpage link or an Internet Protocol (IP) address for a specific location to be targeted. For every hour that a system is down, businesses suffer significant revenue losses and incur additional operating expenses due to recovery efforts [7].

Machine learning is a branch of artificial intelligence that aims to enable machines to perform their jobs skillfully by using intelligent software [8]. Such jobs involve recognition, diagnosis, planning, robot control, and prediction. Machines can learn by themselves and improve their performance [9]. They do not rely on rule-based programming, but on algorithms that identify patterns in data and then predict similar patterns in new data. Machine learning algorithms that can assess the harm brought on by those packets are applied to counteract various DDoS attacks. Using machine learning techniques like decision trees, random forests, and KNN, DDoS detection has been demonstrated. A trained neural network has been found to produce less accurate results than deep learning, which combines machine learning and several abstraction layers. Deep learning has enhanced the capabilities of devices, making them appropriate for a wide range of devices, including IoT devices. One of the disciplines of artificial intelligence, machine learning, is used to find patterns in data. To develop a data-driven model, it employs algorithms. Machine learning is a fantastic option due to its versatility in situations where data is always changing and task difficulty is continually changing. Machine learning (ML) techniques are considered to be a viable means of detecting DDoS attacks [10]. Such techniques learn the patterns behind attacks to detect them before network recourses become unavailable. Modern defense systems make use of ML techniques alongside other detection models, including intrusion detection systems (IDS) and host-based intrusion detection systems (HIDS), to effectively respond to complicated cyberattacks such as DDoS attacks [11].

The literatures reviewed has provided knowledge on Distributed Denial of Service attack, and then summarized and discussed what has been done by various researchers. Some of the reviewed works explored feature extraction techniques and machine learning models that could be applied to distinguish DDOS attack behaviors correctly, while some of the works pose that a classification model using static analysis is not enough to classify the malware effectively. Some works presented that a behavioral-based malware detection system is more effective than a static-based system for the detection of new attack. It is worthy to note also that some of the work focuses on a limited number of features like API calls monitoring and file operations.

Related Works

The reviewed literature also offered a comprehensive taxonomy of machine learning-based methods for detecting anomalies, reviewing supervised, unsupervised, deep learning, and hybrid approaches, and analyzing the related challenges. Various machine learning techniques have shown promise in detecting DDOS attacks with low false-positive rates and high detection rates. The literature also presented different sets of data adopted by researchers as the case maybe in handling their solutions.

[12] Proposed a deep learning approach for identifying and thwarting flood attacks, also known as DoS-based Hello on the IoT healthcare network. They used the Deep Belief Network (DBN) model to confirm this kind of

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue IV April 2025

attack, which entailed sending plenty of Hello packets to slow down the network. The bypass-linked attacker update-based rider optimization algorithm (BAU-ROA) is a tool that the DBN approach has used to produce a variety of useful outcomes and function even better.

[13] Presented new DDoS attack detection model by using ELM. Here the NSL-KDD dataset used for experimentation. The proposed detection model produces a high detection rate and takes less computation time.

[14] Used machine learning to discover the DDoS attack and know its type to be aware of it and take the necessary measures for that. They used the CICDDoS2019 dataset. The algorithms used are Random Forest, Decision Tree, SVM, Naive Bayes, and xgboost which were used to train and test the data from the datasets. Their result showed that random forest algorithms had the highest level of accuracy (99.95426%).

Kamber et al., (2022) proposed a hybrid machine learning-based technique. Blackhole optimization and the extreme learning machine (ELM) model are combined to implement the suggested method. To test the effectiveness of our suggested technique, several experiments have been carried out using four benchmark datasets: NSL KDD, ISCX IDS 2012, CICIDS2017, and CICDDoS 2019. The accuracy is 99.23%, 92.19%, 99.50%, and 99.80% using NSL KDD, ISCX IDS 2012,CICIDS 2017, and CICDDoS 2019, respectively. It is also done to compare the performance of the proposed method with existing methods based on ELM, backpropagation ANN, artificial neural network (ANN) trained with blackhole optimization, and other cutting-edge methods (Sharafaldin, et. al., 2019).

[15] Presented a DDoS detection model based on data mining and machine learning techniques. They used the CICDDoS2019 dataset, they experimented with the following machine learning algorithms: Naïve Bayes, SVM, KNN, Random Forest, XGBoost, and AdaBoost. It is discovered that AdaBoost and XGBoost were extraordinarily accurate and correctly predicted the type of network traffic with 100% accuracy.

[16] Added a well-known DDoS dataset called CICDoS2019 that would improve the accuracy of DDoS attack identification. The DDoS dataset has also undergone preprocessing utilizing two major methods to extract the most pertinent information. The DDoS dataset will be used with four distinct machine-learning models. The Random Forest machine learning model, with an improvement over recently developed DDoS detection systems, provided the best detection accuracy with (99.9974%), according to the results of actual testing.

[17] Applied network traffic analysis and machine learning algorithms using detection of botnet and DDoS. Their model detects or predicts both botnet and DDoS attack with the highest or maximum accuracy. Highest accuracy is obtained with the selected feature and with a chosen classification algorithm. Naïve Bayes and SVM classification algorithms are used for achieving high levels of accuracy. The model detects mixed high-rate, low-rate DDOS attacks and Botnet through Network Traffic Analysis and Machine Learning.

[18] Proposed a model to detect DoS attacks based on machine learning and neural networks, then tried to maximize their model's accuracy compared to similar detection models by setting the optimum value of parameters. They achieved an accuracy of 99.95% via Random Forest algorithm with 500 trees and 50% training dataset on CIC IDS 2017 dataset.

[19] Worked on DoS/DDoS attack detection using artificial neural networks. They investigated the viability and efficiency of using deep neural networks, specifically long short-term memory (LSTM), convolutional neural networks (CNNs), and recurrent neural networks (RNNs), in the workout for detecting and eliminating DDoS attacks on SDN controllers.

[20] Investigated a novel framework for detecting DoS/DDoS attacks using deep learning techniques, and an approach to mitigate the impact of DoS/DDoS attack in network environment. The proposed Deep Learning model learns and builds binary and multiclass classification models that distinguish network attack activity from normal traffic. They looked for outliers and attack signals in traffic patterns and data. Our deep learning model is studied with accuracy and precision. In detection, the system checks for attacks or regular network data. MLP Algorithm helps this model discover items 97% of the time.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue IV April 2025

[21] Worked on Comprehensive DDoS Attack Classification Using Machine Learning Algorithms. This work is devoted to the classification of datasets with eight machine learning algorithms: naïve Bayes, logistic regression, support vector machine, k-nearest neighbors, decision tree, random forest, XGBoost, and CatBoost. In the experimental results, the Information gain and F-test feature selection methods achieved better performance with all eight ML algorithms than with the Chi-square technique. Furthermore, the accuracy values of the oversampled and SMOTE datasets were higher than that of the undersampled and imbalanced datasets. Among machine learning algorithms, the accuracy of support vector machine, logistic regression, and naïve Bayes fluctuates between 0.59 and 0.75, while decision tree, random forest, XGBoost, and CatBoost allowed achieving values around 0.99 and 1.00 with all feature selection and class balancing techniques among all the algorithms.

[22] Proposed two new algorithms, DDAML and DDADA, based on KNN and the degree of attack concept. They gathered their Dataset from a simulation environment and generated DDoS traffic withhping3, and tested their proposed algorithms as well as other traditional machine learning algorithms like SVM, KNN, and Naïve Bayes. After comparing the results of ROC curves, they found out that their proposed algorithms have better performance than the existing ones.

[23] Employed logistic regression and K Nearest Neighbor algorithms to handle DDoS attack. They compared two algorithms of Machine Learning (ML) such as Logistic Regression (LR) and K-Nearest Neighbors (KNN) and the accuracy is also compared. The accuracy of the two algorithms differs in our experimental results. The accuracy of Logistic Regression is roughly 91% and the accuracy of the KNN algorithm is roughly 99%. From the analysis, KNN is better rather than Logistic Regression.

Having reviewed literatures in detecting and mitigating DDoS attacks on a network, we extracted random forest and Multi-Layer Perceptron which represents non-deep learning and deep learning algorithm. These models has been proven to have given good results based on the literatures reviewed, therefore we are going to analysis them using our datasets to find out the better algorithm for detecting DDoS attack with respect to deep learning and non-deep learning algorithm.

MATERIALS AND METHOD

Data Collection

The dataset used in this work is APA_DDOS dataset and was extracted from kaggle containing (125008, 20). This dataset consists of feature and instances. The feature i.e., class value has three possible values: normal traffic (benign), DDoS-ACK and DDoS-PSH-ACK which are nothing but class labels.

Table 3.1: The description and features of the different events

Events	Description
Normal traffic (benign)	This label indicates normal, non-malicious network traffic. Packets labeled as `Benign` represent routine communications with no threat to network security. This traffic is generally safe and expected in regular network activity.
DDoS-ACK	This label identifies network traffic associated with a Distributed Denial of Service (DDoS) attack that primarily utilizes the ACK (Acknowledgment) flag in TCP packets. In a DDoS-ACK attack, attackers flood the target with a high volume of ACK packets, aiming to exhaust resources and disrupt normal service. This type of traffic is usually high in volume and can impact server response times.
DDoS-PSH-ACK	This label refers to traffic linked to a DDoS attack using both the PSH (Push) and ACK (Acknowledgment) flags in TCP packets. In a DDoS-PSH-ACK attack, the attacker sends numerous PSH-ACK packets to overwhelm the target. The PSH flag is used to request immediate data transmission, while the ACK flag acknowledges receipt of previous packets. This type of attack aims to congest the target network and slow down or prevent legitimate traffic from being processed.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue IV April 2025

Data Cleaning and Pre-processing

The preprocessing was done after data collection, the data collected were categorized into their respective classes, for each category, we have a good number of data prepared manually with labeling tools. The labeling tool was written with the python scripts. The effort is to make sure that, the preprocessed data meet the requirement for further analysis when applied to the machine learning algorithms. In the process of preparing the dataset, columns will be removed or retained based on their relevance to model performance and privacy concerns.

Filtering users

The amount of data that was extracted varied, this can have a negative effect on the learning of the machine learning algorithm. One solution to this was to remove data that do not comply with some constraints. A filter on each data event was created, removing data and their events when the number of sequence of events is below a certain threshold. This way data that goes against some constraints while collecting the data were removed.

The filtering techniques goes a long way of transforming the sample dataset into sizeable format by means of applying feature scaling and normalization to fit in the training model and as well to remove the missing value. This approach is done with the principle of applying statistical model such mean, mode, standard deviation in order to transform the training data for analysis.

Model Selection

Three machine learning methods viz; Multi-Layer Perceptron and Random forest were adopted in this research to determine their efficiency with regards to the dataset collected.

Choice of Programming Environment

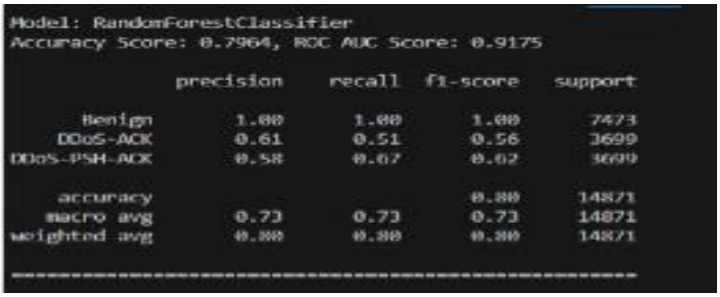
The program was developed using machine learning techniques; and the editors used for coding the system is the VS Code. Python programming language and its libraries were also used. Visual Studio Code focused mainly on the code editor. Its cross-platform supports syntaxes for a large number of programming languages. The environment is not fancy and focuses exclusively on providing flexibility and simplicity to promote compatibility across the platforms offered, beyond support for Git repositories or the ability to open multiple files iterations in one window.

RESULTS AND DISCUSSION

The system was implemented with three class labels (benign, DDOS-ACK and DDOS-PSH-ACK). Random forest and Multi-layer perceptron was used to train the data. This dataset was pre-processed and feature extracted before applying a classification algorithm to it. The classification used captured all the required training samples of data and used the test data to make detection and prediction as well as evaluate the model performance. The training data was 85% while 15% was used for testing.

Model Evaluation for Random forest

Table 4.1 Model result for Random Forest



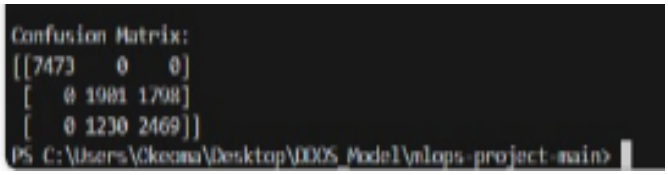
Model: RandomForestClassifier
Accuracy Score: 0.7964, ROC AUC Score: 0.9175

	precision	recall	f1-score	support
Benign	1.00	1.00	1.00	7473
DDoS-ACK	0.61	0.51	0.56	3699
DDoS-PSH-ACK	0.58	0.67	0.62	3699
accuracy			0.80	14871
macro avg	0.73	0.73	0.73	14871
weighted avg	0.80	0.80	0.80	14871

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue IV April 2025

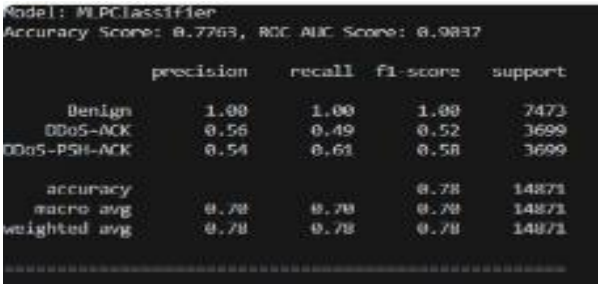
This classification result presented 100% for precision, recall, and f1-score for benign class, then 61%, 51%, and 56% for precision, recall, and f1-score respectively for DDoS-ACK, and finally 58%, 67%, and 62% for precision, recall and f1-score respectively for DDoS-PSH-ACK. The accuracy is 80% with total support of 14871.

Table 4.2 Confusion matrix for Random Forest



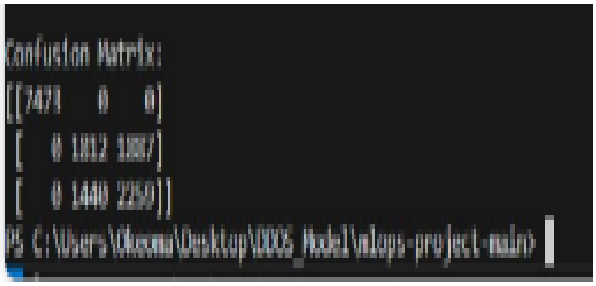
Model Evaluation for Multi-Layer Perceptron

Table 4.3 Model result for MLP



This classification result presented 100% for precision, recall, and f1-score for benign class, then 56%, 49%, and 52% for precision, recall, and f1-score respectively for DDoS-ACK, and finally 54%, 61%, and 58% for precision, recall and f1-score respectively for DDoS-PSH-ACK. The accuracy is 78% with total support of 14871.

Table 4.4 Confusion matrix for MLP



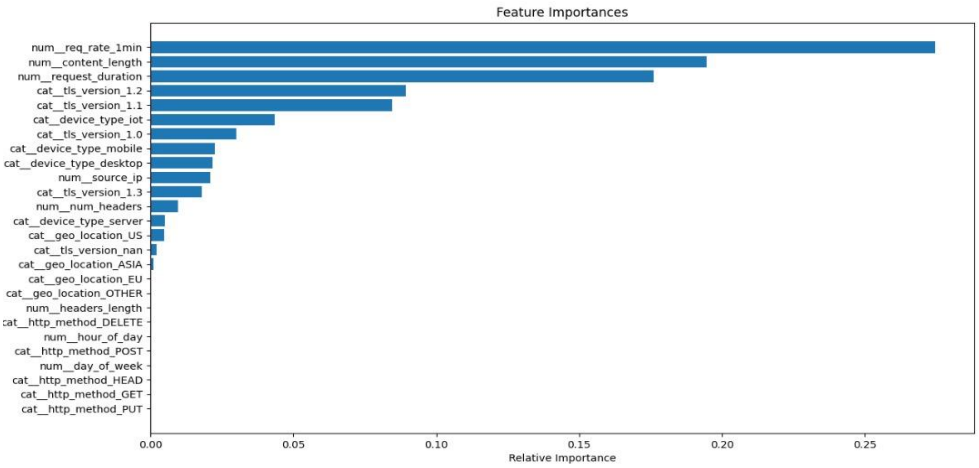


Figure 4.1. Feature graph

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue IV April 2025

CONCLUSION

Distributed Denial-of-Service (DDoS) attack constitutes a formidable form of cybercrime that unleashes havoc by inundating a server with an overwhelming barrage of requests, effectively rendering online sites and services inaccessible to legitimate users. The insidious intent behind a DDoS attack lies in its capacity to disrupt the seamless provision of both internal and external services offered by a website. What sets DDoS attacks apart in their potency is their utilization of a multitude of compromised computer systems as sources for the deluge of attack traffic. Despite their size, because of their increases in complexity, volume, and frequency, these attacks continue to threaten the network security of all the business sectors. The DDoS attacks are among the top threats due to the accessibility of business applications, services, and networks. DDoS attacks and non-malicious availability issues have similarities between them, such as system administrators performing maintenance or technical problems with the network. These problems make it extremely difficult to recognize and effectively defend against these kinds of attacks.

This research compared a deep learning model and a non-deep learning model for DDOS attacks to exploratively analyze the better model. Having reviewed other literature, we found out that there was a gap with the reviewed literature that sampled the models we adopted, and that gap is based on the data they adopted. Most researchers adopted datasets with fewer features because of their research objectives, but we are looking at sampling these datasets on these selected models so we can compare deep-learning and non-deep-learning models with this dataset. The literature reviewed presented multi-layer perceptron and Random Forest as one of the best models for deep learning and non-deep learning for DDOS attacks respectively. The APA_DDOS Dataset extracted from Kaggle has been proven to provide good results as studied in the literature. Random forest as a non-deep learning method presented itself as a better model for DDOS attacks. The data were collected, preprocessed, and prepared in a suitable format to be used by the machine learning algorithm. The results after the classification and parallel testing is encouraging as the system presented good detections and predictions for both models where Random Forest is 80% and Multi-Layer perceptron is 78% in accuracy. This was achieved using the Python Libraries, Python IDE (Jupyter notebook) and Scikit-learn. These results can be adopted by researchers seeking to work in DDOS attacks in a network environments.

REFERENCES

1. Abomhara, M., Khalifa, A., & Hassanien, A. E. (2020). A survey on network anomaly detection techniques: Taxonomy, research challenges, and future directions. Computer Networks, 178, 109470
2. Li J., Yi X., & Wei S. (2020). A study of network security situational awareness in Internet of Things,'' in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Limassol, Cyprus, Jun. 2020, pp. 1624–1629, doi: 10.1109/IWCMC48107.2020.9148549.
3. Cheng, X., Chen, Y., Li, X., Wang, H., & Yang, L. T. (2021). A comprehensive survey on cyber security using machine learning techniques. Journal of Network and Computer Applications, 181, 103026.
4. McAfee. (2020). Economic impact of cybercrime. Retrieved from https://www.mcafee.com/blogs/other-blogs/mcafee-labs/economic-impact-of-cybercrime/
5. Somani G., Gaur M., Sanghi D., Conti M., Rajarajan M., & Buyya R. (2017). Combating DDoS attacks in the cloud: Requirements, trends, and future directions,'' IEEE Cloud Comput., vol. 4, no. 1, pp. 22–32, Jan./Feb. 2017, doi: 10.1109/MCC.2017.14.
6. Vishwakarma R. & Jain A. (2019). A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks, in Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI), Tirunelveli, India, Apr. 2019, pp. 1019–1024, doi: 10.1109/ICOEI.2019.8862720.
7. Soupionis Y. & Benoist T. (2015). Cyber-physical testbed—The impact of cyber attacks and the human factor, in Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST), London, U.K., Dec. 2015, pp. 326–331, doi: 10.1109/ICITST.2015.7412114
8. Mohssen M., Muhammad B., & Eihab B. (2016). Machine Learning: Algorithms and Applications. Publisher: CRC press. ISBN: 9781498705387, edition 1. DOI: 10.1201/9781315371658.

9. Anigbogu K., Inyiama H., Onyenwe I. & Anigbogu S. (2022). Driver behavior model for healthy driving style using machine learning methods. World Journal of Advanced Engineering Technology and Sciences, 2022, 07(01), 137–148. Article DOI: https://doi.org/10.30574/wjaets.2022.7.1.0103.
10. Priya S., Sivaram S., Yuvaraj D & Jayanthiladevi A. (2020). Machine learning-based DDOS detection, in Proc. Int. Conf. Emerg. Smart Comput. Inform. (ESCI), Pune, India, Mar. 2020, pp. 234–237, doi: 10.1109/ESCI48226.2020.9167642.
11. Sultana N., Chilamkurti N., Peng W., & Alhadad R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches, Peer Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019.
12. Alzahrani R. and Alzahrani, A. (2021). "Survey of Traffic Classification Solution in IoT Networks," vol. 183, pp. 37-45, 2021.
13. Kushwah G., Ranga V., & Sciences C. (2021). "Distributed denial of service attack detection in cloud computing using hybrid extreme learning machine," vol. 29, no. 4, pp. 1852-1870, 2021 (2) (PDF) Machine Learning Techniques for Detecting DDOS Attacks. https://www.researchgate.net/publication/375128896_Machine_Learning_Techniques_for_Detecting_DDOS_Attacks
14. Mamoon M.S., Husam N.R., Othman A.H. (2023). Machine Learning Techniques for detecting DDOS attacks. Conference: 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA).
15. Alireza S., Saeid G.I., Mohammad F. (2021).A Machine Learning Approach for DDoS Detection on IoT Devices. https://arxiv.org/pdf/2110.14911.
16. Lohachab and Karambir (2018). Critical Analysis of DDoS, an Emerging Security Threat over IoT Networks Sep 2018. Journal of Communications and Information Networks 3(3):57-78. DOI: 10.1007/s41650-018-0022-5.
17. Rajesh B.Y., Rama D. G. and Prasanna P. (2023). Detection of Botnet and DDoS using Network traffic analysis and Machine Learning Algorithms. September 2023 DOI: 10.21203/rs.3.rs-3397184/v1 License: CC BY 4.0
18. Wankhede S. and Kshirsagar D. (2018). DoS Attack Detection Using Machine Learning and Neural Network. August 2018 DOI: 10.1109/ICCUBEA.2018.8697702 https://www.researchgate.net/publication/332676060 DoS Attack Detection Using Machine Learning and Neural Network
19. Osman A. and Paul C. (2018). Towards DoS/DDoS Attack Detection Using Artificial Neural Networks November. 2018 DOI: 10.1109/UEMCON.2018.8796637. https://www.researchgate.net/publication/328885982 Towards DoSDDoS Attack Detection Using Artificial Neural Networks
20. Gottapu S. R. (2024). A Novel Framework for Detection of DoS/DDoS Attack Using Deep Learning Techniques, and An Approach to Mitigate the Impact of DoS/DDoS attack in Network Environment. International Journal of Intelligent systems and Applications in Engineering.
21. Olga U., Aidana Z., Yenlik B., Eric T.M., Nikita U. (2022). Comprehensive DDoS Attack Classification Using Machine Learning Algorithms. Computers, Materials and Continua. Volume 73, issue 1, 16 May 2022, Pages 577-594 https://doi.org/10.32604/cmc.2022.026552
22. Dong S and Sarem M. (2019). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. Digital Object Identifier 10.1109/ACCESS.2019.2963077 https://www.researchgate.net/publication/338248177_DDoS_Attack_Detection_Method_Based_on_Improved_KNN_With_the_Degree_of_DDoS_Attack_in_Software-Defined_Networks
23. Priya G., Shiriam S., Jeeva S., Priya G., Balasubadra K. (2024). Detection of Distributed Denial of Service (DDOS) Attack Using Logistic Regression and K Nearest Neighbor Algorithms. International Journal of Intelligent systems and Applications in Engineering. https://ijisae.org/index.php/IJISAE/article/view/4863