A Comprehensive Survey On Detection And Mitigation Of DDoS Attacks Enabled With Deep Learning Techniques In Cloud Computing

2023 6th International Conference on Advances in Science and Technology (ICAST) | 979-8-3503-5981-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAST59062.2023.10454990

Yogesh B. Sanap
Research Scholar
Department of Computer Science and Engineering
Sandip University, Nashik
Maharashtra, India
sanap.yogesh@gmail.com

Pushpalata Aher
Assistant Professor
Department of Computer Science and Engineering
Sandip University, Nashik
Maharashtra, India
pushpalata.aher@sandipuniversity.edu.in

Abstract*—To detect the DDoS (Distributed Denial of Service) attack that initiates a flooding attack over a targeted server or service meanwhile causing network traffic and disrupting legitimate users from accessing the network is significant for reducing the hosting issues and time loss. Additionally, DDoS attacks have become the foremost attack in cloud computing and cause complexity in detection and mitigation appropriately as the attacks make the server down which results in the user to loss access to the Internet and causing financial loss to the cloud computing organizations. Despite the numerous solutions that exist in the current era, the attacks continue to grow in volume as well as severity. As a consequence, multiple researchers have formulated for securing the cloud servers with the help of a software-defined network(SDN) to identify and eliminate the impacts of DDoS attacks. In this research, an in-depth analysis of the DDoS detection and mitigation frameworks for securing the servers in cloud computing is exhibited to analyze the security and authentication of attack detection systems in cloud applications. A well-defined and prominent solution can be formulated by investigators through this detailed investigation based on different datasets and techniques. The research elucidates various techniques in the detection and mitigation of DDoS attacks along with their advantages, disadvantages, and research gaps, which supports the researchers in attaining deep knowledge of the techniques prevalent in DDoS attack detection in cloud networks.

***Keywords*—DDoS attacks, Cloud computing, Network security, Malicious attacks, SDN**

I. Introduction

With the enormous demand for web applications and IoT (Internet of Things) facilities, the devices have been developed but are degraded in their performance with the issues of security prominently the attacks attempted over them[1-3]. This intentional massive attack against the critical server caused problems for users like eventual shutdown or access rejection to reach the server. The chief aim of this DDoS attack is to interrupt the functioning of the server with internet traffic[2]. Once the websites become prone to the DDoS attack it interrupts the business transactions and leads to the loss of millions of dollars in a shorter period that makes them financially unstable [5-8]. Based on the target and characteristics, DDoS attacks are split into bandwidth attacks, traffic attacks as well and application attacks [9-10].

With the evolution of edge computing, the DDoS attack that attempts to control multiple desktop computers possibly with Cyber-Physical Systems along with strong passwords is getting increased in the modern days[5]. As a consequence, edge architecture remains a strong amplifying platform[6], and it is significant to utilize the traffic flow information for designing an Intrusion Detection System (IDS), following the networks employing innovative technologies in networking like SDN to detect DDoS attacks [7]. SDN is an advanced networking paradigm that disconnects the control plane (CP) and operates separately from the conventional network design [8]. Hence, the controller can regulate the network effectively against single-point failure and adopt several network policies[9].

Additionally, deep learning (DL) techniques are getting more attention in detecting and mitigating DDoS attacks [8-10]. However, some problems exist with conventional learning techniques that involve high training time, misclassification, and false alarm rates [24-25]. To overcome these issues, an innovative Machine-Learning(ML) technique was developed for handling DDoS attack mitigation [13-15]. Moreover, DL techniques were applied in intrusion detection for their high learning and generalization capability of the attributes employed [1] [16].

II. Article Screening from the Journal and Keyword Combinations

In this section, Fig 1 reflects the selection process of the research articles and the selection is carried out with the following criteria as follows,

- Articles associated with DDoS attack detection in cloud computing are collected.
- During the collection process, the review articles are eliminated
- The journals are collected by neglecting the survey papers and other irrelevant titles.
- Articles from 2020-2023 are collected.

Multiple keywords are utilized for accessing the specific articles, such as DDoS attacks, Cloud computing, SDN, network traffic, Network security, and malicious attacks.

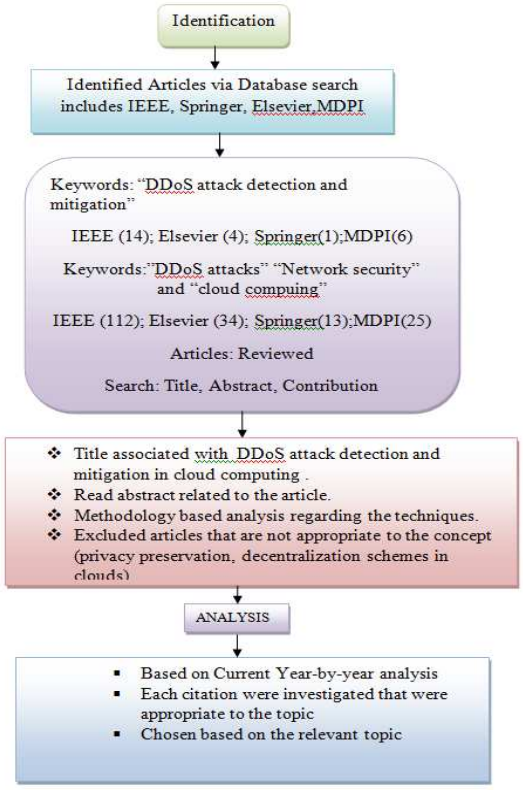

Fig.1. Refinement of the article selection process

III. Topology Categorization

The taxonomy of DDoS attack detection systems encompassing different techniques is depicted in Fig 1, which facilitates a comprehensive understanding of diverse approaches to enhance the detection process. Further, section II provides an in-depth analysis of the techniques along with their pros and cons as shown in fig 2.

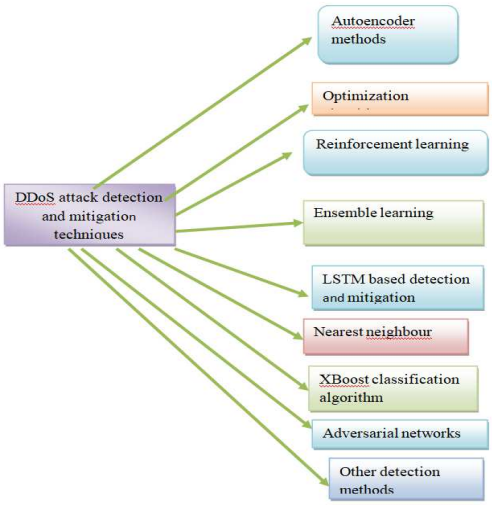

Fig.2. Categorization of DDoS attack detection and mitigation methods

A.LSTM-Based DDoS Detection

In [1], a DL-powered framework tackled DDoS attacks in Fog networks by leveraging SDN with a DDoS defender module. This module detected anomalies at the network level and employed DL-enabled traffic analysis to filter legitimate packets, blocking infected ones. Additionally in [17] an LSTM and fuzzy logic-based method detected DDoS and Portscan attacks. It predicted normal traffic flow characteristics and set threshold ranges. Fuzzy logic identified anomalies like attack floods, applying mitigation policies to enhance network operations

B. Autoencoder-Based DDoS Attack Detection

Deep neural networks [18] with stacked autoencoders (AE) were used for DDoS attack detection. AEs learned informative features and neural networks (NN) classified traffic into benign or attack categories. Decision trees, though sensitive to data changes, had limited performance on unseen data. An autoencoder-based model [15], employing a modified deep belief neural network (DBNN), achieved higher detection rates. The method allowed flexible database format alterations, benefiting the M-DBNN classifier. Enhanced optimization algorithms improved weight optimization for better prediction. A DL method addressed data security concerns in DDoS detection [19]. Categorical variables like source, destination, and switch were encoded using one-hot encoding. Stacked AE and MLP techniques were used to classify traffic based on extracted features. A hybrid DL approach was employed to detect and classify DDoS attacks [20]. Autoencoders effectively extracted relevant features without prior cybersecurity knowledge. MLP compressed features and classified attacks, reducing computational overhead and bias.

C.Optimization Enabled Detection

In [21], an effective Whale Optimization Algorithm (WOA)-based feature selection technique improved DDoS attack mitigation by reducing false alarms. The method employed data normalization for preprocessing and selected optimal features to enhance detection. A deep neural network (NN) classifier was used for categorizing normal and attacked traffic, with data stored securely via homomorphic encryption. Future work could integrate this method into IDS. In [22], an ML-enabled approach focused on mitigating attack nodes. Deep Belief Networks (DBN) were leveraged, and Sea Lion Optimization was used to adapt classifier weights and activation functions. When an infected node was detected, control was promptly transferred to a *baiting* approach to neutralize repeated attacks without disrupting normal nodes. While initially designed for performance enhancement, this method holds promise for application in cloud infrastructure security.

D.RF-Enabled DDoS Attack Detection

An ML-enabled DDoS attack detection method[23] was developed utilizing the mutual information and Random Forest (RF), which offered reduced misclassification rates by

979-8-3503-5981-7/23/$31.00 ©2023 IEEE

combining the outputs of multiple decision trees. The dataset was split based on features, and weighted voting, logistic regression, and K-NN were employed for effective attack detection. The study suggests potential improvements using wrapper methods for feature selection. Another work in [4] proposed a reliable and fast DDoS attack detection framework. It employed PCA-based feature selection and RF to reduce dataset dimensions and improve classifier performance. This method achieved high detection accuracy by applying an RF classifier across the dataset's dimensions and then reducing dimensions with attack instances.

E.Reinforcement Learning Model

In [6] employed reinforcement learning with transformers to mitigate short-time DDoS attacks in edge networks, improving service availability and reducing tail latency. This approach adapts network defenses dynamically to discernible attack patterns. Another approach [5] utilized deep CNN-enabled Q-learning that detected the DDoS attacks, specifically addressing the issues related to the Mirai botnet variant. While effective, data sparsity posed a limitation. Additionally, a study [24] focused on edge server-based DDoS detection using reinforcement learning. It optimized computing resources and reduced inspection delays while addressing privacy concerns. Future work may expand this approach to handle increased traffic.

F.Ensemble Classification Methods

In [8], a modular SDN-based architecture with ML and DL was developed to address SDN's limitations in detecting new network attacks. It employed detection modules at the transport and application layers, forwarding suspicious flow information for further classification, offering the potential for optimized mitigation. [25] Introduced a flexible SDN architecture with ML capabilities that effectively mitigated the DDoS attacks. The method utilized an intrusion prevention system with a flow management module for HTTP flow detection, attack management, and intrusion detection. Future enhancements can target different attack types. In[26] a DDoS mitigation scheme that analyzed real traffic to distinguish normal traffic from attack traffic. ML algorithms, in conjunction with SDN, detected and dropped attack traffic while preserving normal traffic. Challenges included complexity and difficulty in distinguishing normal and flood attack traffic. In [10] developed a deep CNN ensemble model for detecting the attacks in SDN. The model enhanced centralized control intelligence, and leveraged deep CNN, LSTM, and RNN classifiers, improving accuracy, reducing time consumption, and minimizing computational complexity. Further testing parameters would be added to enhance the performance.

G.Linear Regression Model

A multiple linear regression method was presented for DDoS attack detection in [2] that addressed the issues of access denial due to the attacks. The feature selection technique known as the information gain approach was deployed that acquired the informative features and determined the significant attributes for easing the prediction. Finally, the linear regression based on the learned attributes from the fit charts and residual plots classified the DDoS attacks. Although the analysis was carried out for only one-day log files, five-day log files can be implemented in the future.

H.Extreme Learning

A DDoS attack detection approach was introduced in [12], employing multiple EL machines for simultaneous detection. Each EL machine processed samples from a training dataset and majority voting was used to classify attack and normal samples based on threshold values. However, threshold evaluation proved complex, especially for heterogeneous network traffic. In [14], a DDoS attack detection system was developed using deep neural and feed-forward networks with sigmoid activation functions. The system dynamically managed network traffic entering SDN by modifying flow tables during attack simulations. Learned features enabled the classification of new instances, and the controller, guided by ML algorithms, determined routing paths and traffic blocking.

I.GAN Enabled Attack Detection

In [27] an adversarial learning approach was introduced using GAN networks in SDN to detect and prevent DDoS attacks. This method made the system less sensitive through adversarial training while incorporating modules for continuous traffic monitoring via flow analysis and anomaly detection, suggesting potential improvements using other deep neural networks.

J.Restricted Boltzmann Machine (RBM)

In [28], a hybrid DL approach was developed to detect DDoS attacks in smart city infrastructures, enhancing security by addressing authentication issues. The model, based on deep RBM, successfully identified replay and DDoS attacks by incorporating time dependencies from smart sensor data. While effective, it holds the potential for further expansion to detect additional attack types in the future.

K. Other DDoS Detection Techniques

An ML approach in [9] addressed SDN's vulnerability to DDoS attacks. The approach categorized the network traffic as benign or attacked flood traffic, using the effective Neighborhood Component Analysis (NCA) algorithm with TCP, UDP, and ICMP attack traffic data. It extracted relevant features and enabled attack diversity classification using other feature learning algorithms. In [7], a multilayer DL framework was developed for DDoS attack detection. It employed average drop rates for early detection and a mapping function for data plane-level attack detection before flood traffic overwhelmed the controller. The framework included feature extraction, training, classification, and attack mitigation, protecting local and remote nodes to prevent flood attacks from reaching ISP levels. In [13], an ML method for DDoS attack prediction utilized XGBoost and RF algorithms. It managed irrelevant data, extracted features, encoded symbolic data into numerical format, and optimized efficiency through

979-8-3503-5981-7/23/$31.00 ©2023 IEEE

kernel scaling and parameter tuning. The method also incorporated non-supervised learning for handling non-labeled datasets.

IV. Information Source and Process

The information related to DDoS attack detection, cloud computing, and network security was collected from different journals like IEEE, Elsevier, Springer, and MDPI. The papers that were utilized for analysis were selected based on the criteria, such as i) Determination of the research topic, ii) Problem definition, and iii) Accessing the uniqueness of the topic.

A. Research Questions

The research questions are framed based on the details acquired from other research articles and are stated as follows

Q1: what are the different methods used for detecting DDoS attacks?

Q2: Is detection and mitigation of DDoS attacks utilizing DL a secure method?

B. Analysis Concerning Methods

Analyzing various DDoS detection methods, including deep CNN, Regression network, LSTM, GAN, etc., is crucial for gaining in-depth knowledge. Table I and Fig 3 are the visual representation of these methods.

TABLE I. ANALYSIS CONCERNING METHODS

Methods	Paper
LSTM	[17][1][10]
RBM	[28]
MLP-AE	[20][19]
Reinforcement learning	[6][5][24]
Deep neural networks	[14]
DBN	[22][15]
RF-XBoost	[13]
RF classifier	[23][4]
GAN	[27]
Optimization algorithm	[21][22]
SVM	[25]
MLR	[2]
Extreme learning	[12]
Autoencoder	[18][15][19][20]
Fuzzy logic	[1]
Nearest neighbor	[9][23]
Ensemble learning	[8][25][26][10]

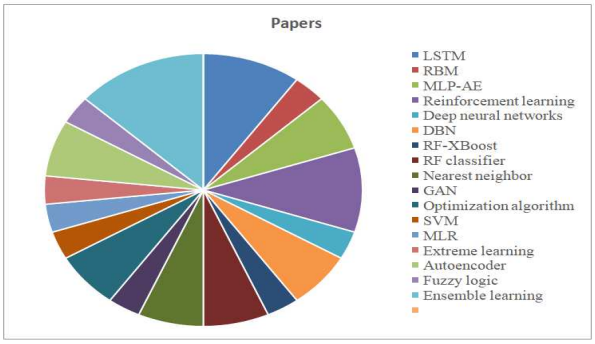

Fig.3. Analysis concerning methods

C. Analysis Concerning Metrics

The performance of the detection system is evaluated and analyzed based on the metrics. The metrics like accuracy, precision, and recall were utilized in the evaluation of the detection models. The findings are depicted in Table II and represented in Fig 4.

TABLE II. ANALYSIS CONCERNING METRICS

Metrics	Papers
Accuracy	[17][28][8][25][13][27][26][18][9][7][10][1][23][21][2][12][22][14][4][15]
precision	[19][20][13][6][25][27][26][18][16][7][10][1][22][14][4][15]
recall	[19][20][13][6][25][27][26][18][7][10][1][14][4]
F1measure	[19][20][13][25][27][26][18][9][7][10][14][4]
Detection rate	[5][22]
False negative rate(FNR)	[23][21][2][15][22]
false positive rate(FPR)	[23][21][2][15][22]
AUC score	[6]
sensitivity	[9][21][12][22]
specificity	[9][7][21][12][22]
Delay time	[24]
Error rate	[21][15]
Other measures	[15][2][27][9][1]

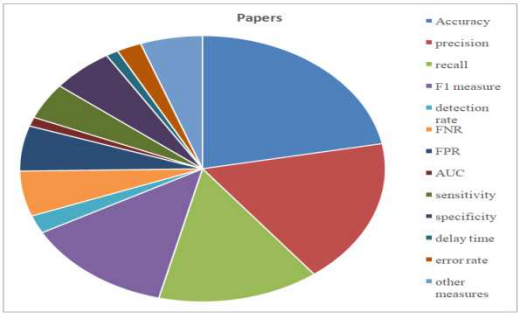

Fig.4. Analysis concerning metrics

979-8-3503-5981-7/23/$31.00 ©2023 IEEE

D. Analysis Concerning Dataset

The study helps the researchers to gain knowledge about the attack detection models. The analysis based on the dataset will assist the researchers in obtaining in-depth knowledge about the usage of datasets in various research papers. The datasets CICDDoS2019 dataset, CICDDoS2017 dataset, and so on are stated in Table III and depicted in Fig 5.

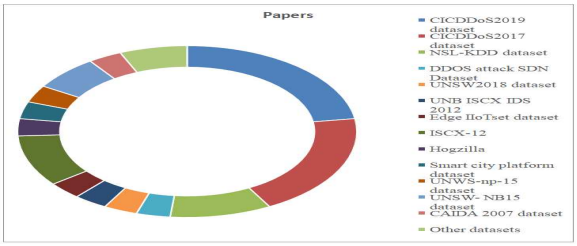

Fig.5. Analysis concerning datasets

TABLE III. ANALYSIS CONCERNING DATASETS

Dataset	paper
CICDDoS2019dataset	[20][6][25][5][27][8][1]
CICDDoS2017 dataset	[18][8][10][23][21][2]
NSL-KDD dataset	[12][18][4]
DDOS attack SDN	[9]
UNSW2018 dataset	[14]
UNB ISCX IDS 2012	[4]
Edge IIoTset dataset	[7]
ISCX-12	[19][12][14]
Hogzilla	[17]
Smart City platform	[28]
UNWS-np-15 dataset	[13]
UNSW- NB15 dataset	[6][4]
CAIDA 2007 dataset	[15]
Other datasets	[24][22]

E.Research Method

Extensive research has been exhibited on the framework, and the important factors associated with the investigation are categorized based on the objective. The articles that are investigated based on DDoS attack detection and mitigation are determined and the observations are tabulated in Table IV.

TABLE IV. ANALYSIS CONCERNINGRESEARCH FRAMEWORK

Objectives	**Papers**	**Methods**	**Dataset**	**Future work**
DDoS attack detection and mitigation	[17]	yes	yes	yes
	[28]	yes	yes	yes
	[19]	yes	yes	yes
	[20]	yes	yes	yes
	[8]	yes	yes	yes
	[13]	yes	yes	yes
	[6]	yes	yes	yes
	[25]	yes	yes	yes
	[5]	yes	yes	yes
	[26]	yes	yes	yes
	[27]	yes	yes	yes
	[18]	yes	yes	yes
	[9]	yes	yes	yes
	[7]	yes	yes	yes
	[10]	yes	yes	yes
	[24]	yes	yes	yes
	[1]	yes	yes	yes
	[23]	yes	yes	yes
	[21]	yes	yes	yes
	[2]	yes	yes	yes
	[12]	yes	yes	yes
	[22]	yes	yes	yes
	[14]	yes	yes	yes
	[15]	yes	yes	yes
	[4]	yes	yes	No

V. RESEARCH CHALLENGES

Some of the research challenges determined in the DDoS attack detection model are as follows

The major challenge that exists in the DL model is that it requires high training time for classifying the data flow and analyzing the instances during the training of the classifiers. However, evaluating the threshold was a complex task as well as difficult to apply over the heterogeneous network traffic [1] [12].DDoS attack detection using DL often demands lengthy training and suffers from elevated false alarms due to classification errors [22]. Many methods struggle to distinguish flood traffic from benign traffic, impairing detection accuracy [6][18]. The detection efficiency depends on the pre-processing that affects the quality of the model which insists on the need for integrating an advanced preprocessing method[3] [5]. Most of the research models focus and works well in binary class detection and lags in multi-class detection purpose [11]. Some existing methods work well in the offline dataset and lag when using it in the real-time dataset [8]. Most of the attacks take place on online sites in a limited time hence a computationally efficient detection model is required.

VI.Conclusion

The review examines various DDoS attack detection and mitigation strategies to enhance security in cloud computing from 2019 to 2023. After selecting 25 pertinent research papers, it thoroughly explores DDoS detection methods, including autoencoders, reinforcement learning, deep CNN, regression networks, LSTM, GAN, etc. The findings highlight the widespread use of autoencoders and reinforcement learning for cloud security against DDoS attacks. The review considers factors like existing approaches, publications, challenges, metrics, and datasets. Future research prospects include evaluating DDoS security in fog and edge computing models.

REFERENCE

[1] M.P. Novaes, L.F. Carvalho, J. Lloret, and M.L. Proenca, "Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment," IEEE Access, 8, pp.83765-83781, 2020.

[2] S. Sambangi, and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression," In Proceedings Vol. 63, No. 1, p. 51, 2020. MDPI.

[3] L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, and X. Xu, "A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. World Wide Web, 23, pp.1275-1297, 2020.

979-8-3503-5981-7/23/$31.00 ©2023 IEEE

[4] Z. Ashi, L. Aburashed, M. Al-Fawa'reh, and M. Qasaimeh, "Fast and reliable DDoS detection using dimensionality reduction and machine learning," In 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 1-10), 2020 IEEE.

[5] Z. Liu, X. Yin, and Y. Hu, "CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-learning. IEEE Access, 8, pp.42120-42130, 2020.

[6] A.B. Bhutto, X.S. Vu, E. Elmroth, W.P. Tay, and M. Bhuyan, "Reinforced Transformer Learning for VSI-DDoS Detection in Edge Clouds," IEEE Access, 10, pp.94677-94690, 2022.

[7] W.I. Khedr, A.E. Gouda, and E.R. Mohamed, FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," IEEE Access, 11, pp.28934-28954, 2023.

[8] N.M. Yungaicela-Naula, C. Vargas-Rosales, and J.A. Perez-Diaz, 2021. "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," IEEE Access, 9, pp.108495-108512.

[9] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert, and R. Kocaoğlu, "Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking," Electronics, 10(11), p.1227, 2021.

[10] S. Haider, A. Akhunzada, I. Mustafa, T.B. Patel, A. "Fernandez, K.K.R. Choo, and J. Iqbal, A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," Ieee Access, 8, pp.53972-53983, 2020.

[11] P. Upadhyay, and J.K. Chhabra, "Kapur's entropy based optimal multilevel image segmentation using crow search algorithm," Applied soft computing, 97, p.105522, 2020.

[12] G.S. Kushwah, and V. Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," Journal of Information Security and Applications, 53, p.102532, 2020.

[13] M.I. Mohmand, H. Hussain, A.A. Khan, U. Ullah, M. Zakarya, A. Ahmed, M. Raza, I.U. Rahman, and M. Haleem, "A machine learning-based classification and prediction technique for DDoS attacks," IEEE Access, 10, pp.21443-21454, 2022.

[14] A.L. Yaser, H.M. Mousa, and M. Hussein, "Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder," Future Internet, 14(8), p.240, 2022.

[15] A. Agrawal, R. Singh, M. Khari, S. Vimal, and S. Lim, 2022. "Autoencoder for design of mitigation model for DDOS attacks via M-DBNN," Wireless Communications and Mobile Computing, 2022.

[16] F.A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "ATSDL: a two-stage deep learning model for efficient network intrusion detection," Access, 7, pp.30373-30385, 2019.

[17] R. Priyadarshini, and R.K Barik, "A deep learning-based intelligent framework to mitigate DDoS attacks in fog environment," Journal of King Saud University-Computer and Information Sciences, 34(3), pp.825-831, 2022.

[18] A. Bhardwaj, V. Mangat, and R. Vig, Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud," IEEE Access, 8, pp.181916-181929, 2020.

[19] A.Nisha, G. Singal, and D.Mukhopadhyay. "DLSDN: Deep learning for DDOS attack detection in software defined networking," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2021.

[20] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, 2021. "Ae-mlp: A hybrid deep learning approach for ddos detection and classification," IEEE Access, 9, pp.146810-146821.

[21] A. Agarwal, M. Khari, and R. Singh, "Detection of DDOS attack using deep learning model in cloud storage application," Wireless Personal Communications, pp.1-21, 2021.

[22] S. Reddy, and G.K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework," Journal of King Saud University-Computer and Information Sciences, 34(7), pp.4047-4061, 2022.

[23] M. Alduailij, Q.W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," Symmetry, 14(6), p.1095, 2022.

[24] H. Zhang, J. Hao, and X. Li, "A method for deploying distributed denial of service attack defense strategies on edge servers using reinforcement learning," IEEE Access, 8, pp.78482-78491, 2020.

[25] J.A. Perez-Diaz, I.A. Valdovinos, K.K.R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," IEEE Access, 8, pp.155859-155872, 2020.

[26] N.N. Tuan, P.H. Hung, N.D. Nghia, N.V. Tho, T.V. Phan, and N.H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," Electronics, 9(3), p.413, 2020.

[27] M.P. Novaes, L.F. Carvalho, J. Lloret, and M.L. Proença Jr, "Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments," Future Generation Computer Systems, 125, pp.156-167,2021.

[28] A.A. Elsaeidy, A. Jamalipour, and K.S. Munasinghe,"A hybrid deep learning approach for replay and DDoS attack detection in a smart city," IEEE Access, 9, pp.154864-154875, 2021.

979-8-3503-5981-7/23/$31.00 ©2023 IEEE