A Review on DDoS Attacks Classifying and Detection by ML/DL Models

Haya Malooh Alqahtani*, Monir Abdullah
College of Computing and Information Technology, University of Bisha, Saudi Arabia

***Abstract*—Internet security is under serious threat due to Distributed Denial of Service (DDoS) attacks. These attacks inflict considerable damage by disrupting network services, resulting in the impairment and complete disablement of system functions. The accurate classification and detection of DDoS attacks is extremely important. We provide a review of different models of Machine Learning (ML)/Deep Learning (DL)-based DDoS attack detection used by researchers that consider different classifiers. Our analysis indicates a heightened emphasis on ML-based classifiers where 22% of studies opted for the widely recognized SVM classifier. For DL-based, 27% of the studies opted for the widely recognized CNN. While the majority of researchers have formulated their datasets, NSL-KDD was employed in 55% of the studies. In addition, we discussed the future directions and challenges of DDoS detection.**

***Keywords*—Classification; DDoS attacks; machine learning; cybersecurity; detection**

I. Introduction

Lately, there has been a noticeable surge in Distributed Denial of Service (DDoS) attacks, as attackers continually devise novel and sophisticated methods to carry out these assaults [1]. This initiates a denial-of-service attack concurrently, affecting a computer network simultaneously [2]. A DDoS attack achieves success by depleting the bandwidth, the processing capacity of routing devices, network or processing resources, memory, and database, as well as the input and output operations bandwidth of server systems [3],[4]. Preventive measures exist to counteract such attacks. Yet, it is crucial to recognize the distinctive traits of the attack to implement the most effective actions and prevent its reoccurrence [5]. Several prevalent forms of DDoS attacks include The Internet of Things (IoT), which refers to the integration of interconnected, internet-enabled objects capable of gathering and exchanging information through wireless networks without manual intervention [6]. Efficient techniques for identifying intrusions, including DoS attacks, SYN floods, and port scans. The exploration of this field has gained significant momentum as a subject of active research. Within the realm of flooding attacks, emphasis is placed on Flags—six distinct bits utilized to convey various conditions. The field of Machine Learning (ML) plays a crucial role in empowering organizations to make diverse decisions. Future classification and prediction can leverage the insights gained from all types of data. ML, an application of artificial intelligence, allows systems to autonomously comprehend and enhance their understanding without explicit programming. It focuses on refining computer programs that can independently absorb and learn from information. Utilizing supervised classification algorithms for categorical datasets is common in tasks involving classification and prediction, drawing upon existing knowledge and experience [7]. There are numerous ML algorithms, including Support Vector Machines (SVM), Artificial Neural Networks (ANN), Decision Trees (DT), Genetic Algorithms (GA), kmeans, Apriori, AdaBoost, Cluster Analysis, Naïve Bayes (NB), PageRank, k-nearest neighbors, and PageRank.

A. DDoS Attacks

Throughout the years, a DDoS attack has posed a continuous security threat to online networks and services. The primary goal of DDoS attacks is to diminish service availability by depleting network or computational resources allocated for traffic and processing. As a result, legitimate users encounter obstacles when attempting to access the intended services [8]. A DDoS attack involves utilizing a vast array of compromised devices strategically dispersed globally within a botnet. This method contrasts with traditional DoS attacks, where a single network connection and one Internet-connected device are employed to inundate the target with malicious traffic [9].

B. How DDoS Attack Works

A DDoS attack can be initiated in various ways [10], with the most prevalent method involving the assailant sending a continuous stream of packets to the targeted server. Utilizing crucial resources in this manner creates challenges for genuine users attempting to access these resources. Another frequently employed strategy involves sending a small number of malformed packets, compelling the targeted servers to freeze or reboot. A different strategy for conducting a denial-of-service involves the deliberate sabotage of devices within the targeted network, depleting crucial resources and rendering the network inaccessible for both internal and external services. Numerous other methods exist for executing such attacks, making them challenging to anticipate and only identifiable after they have been initiated. Fig. 1 shows an example of a DDoS attack.

A DDoS attack unfolds through multiple stages involving three key entities: an assailant, a botnet, and a target. The assailant initiates the attack by dispatching remote instructions to each bot, orchestrating the inundation of connection requests exceeding the server's capacity. This method involves flooding the victim's server or network with copious amounts of random data, depleting the available bandwidth. As the botnet concentrates its efforts on the target's IP address, each bot sends requests, potentially overwhelming the server or network and causing a disruption in regular traffic, resulting in a service denial.

C. Types of DDoS Attacks

There are three types into which DDoS attacks can be classified. Firstly, there are volume-based attacks, where the

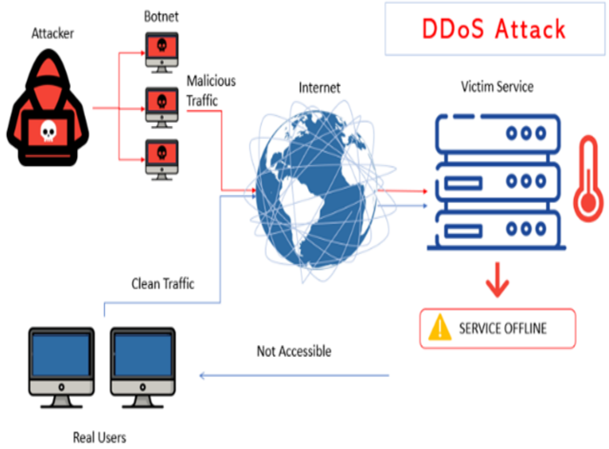

Fig. 1. Example of DDoS attacks.

aim is to overwhelm a target with a substantial amount of traffic, exploiting its bandwidth. Secondly, protocol-based attacks focus on exploiting vulnerabilities at layer 3 or layer 4, depleting the processing capabilities of the targeted system or critical resources like firewalls, leading to potential service interruptions. Lastly, application layer attacks involve connecting to a victim in a seemingly legitimate manner to exploit vulnerabilities at layer 7. These attacks utilize transactions and processes to overwhelm the server's resources excessively [11]. Fig. 2 shows the types of DDoS attacks with their examples.

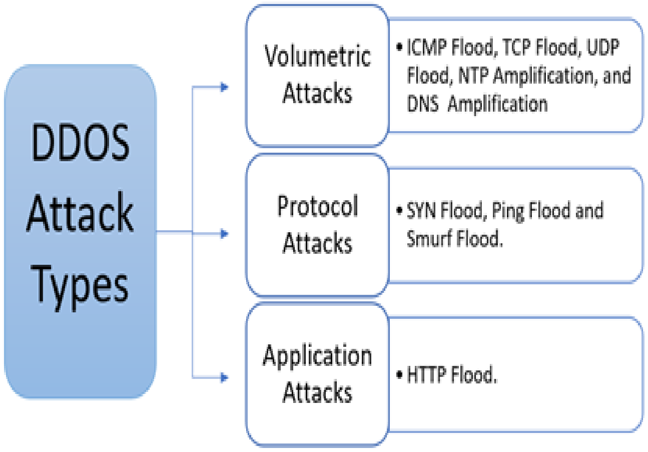
DDOS Attack Types
Volumetric Attacks
• ICMP Flood, TCP Flood, UDP Flood, NTP Amplification, and DNS Amplification
Protocol Attacks
• SYN Flood, Ping Flood and Smurf Flood.
Application Attacks
• HTTP Flood.

Fig. 2. The types of DDoS attacks.

- Attacks involving SYN Flood: In the Transmission Control Protocol (TCP) protocol, the connection is formed through a three-way handshake, during which the server and client exchange synchronization (SYN) and acknowledgment (ACK) messages. SYN Flood attacks occur when a client sends an inaccurate ACK message, containing a forged IP address, in response to the server. Consequently, the server responds to the incorrect IP address with a SYN message and awaits a reply from the client. This waiting period renders the connection idle, preventing the server from catering to legitimate users. This type of attack is particularly susceptible due to its reliance on the vulnerabilities within the three-way handshake protocol [12].
- User Datagram Protocol (UDP) flood attacks: exploiting the characteristics of the UDP, which lacks the handshake process present in the TCP. In this type of attack, packets are directly sent to the target server, allowing the attacker to leverage this property to inundate the server with a significant volume of traffic. Consequently, the network resources of the target server become depleted due to the overwhelming volume of incoming data.
- HTTP flood attack: this is a cyber-attack in which the assailant exploits legitimate HTTP GET or POST requests to target a web application or server. Typically, these attacks leverage a botnet, which is a network of interconnected computers on the Internet.
- Ping of Death: Refers to an obsolete version of an Internet Control Message Protocol (ICMP) ping flood attack. In IPv4, the IP protocol imposes a maximum packet size of 65,535 bytes for communication between two devices. Exploiting this limitation through a basic ping command to transmit malformed or excessively large packets can result in significant harm to an unpatched system.
- SMURF attacks: involve the use of spoofed PING messages, causing a surge in ICMP requests upon pinging the targeted IP address. This influx of requests not only results in the consumption of significant bandwidth but also leads to a slowdown in the computer [13].
- Fraggle attack is a form of DDoS attack wherein a substantial volume of UDP traffic is employed to overwhelm the transmission infrastructure of the switch. It bears similarity to a Smurf attack, but distinguishes itself by utilizing UDP instead of ICMP [14].
- Network Time Protocol (NTP) amplification attack involves exploiting the features of an NTP server to overwhelm a target server or network with an extensive volume of UDP traffic. Consequently, this action renders the destination infrastructure inaccessible to normal, legitimate user traffic [15].

In this paper, Section II discusses the materials and methods through a literature survey and a description of various methods. Section III shows the classification tasks in ML and the ML algorithms performance metrics used to evaluate them. Section IV illustrates the discussion of the results. Open research directions will be presented in Section V. Finally, the last section briefly concludes our paper.

II. Literature Review

In recent times, numerous reports have indicated the occurrence of DDoS attacks targeting both commercial and government websites [16]. As the technique for executing DDoS attacks has advanced, the corresponding research on detection has also progressed. Consequently, numerous approaches have been proposed to mitigate DDoS attacks. In 1990, a proposal was made for a network traffic controller that utilizes ML techniques. The objective of this controller was to optimize call completion within a circuit-switched telecommunications network [17]. This work signified a pivotal moment when ML techniques broadened their scope to encompass the telecommunications networking domain. In 1994, ML was initially employed for classifying internet flow in intrusion detection. This marked the commencement of extensive research utilizing ML techniques in the classification of internet traffic [18]. In this section, we elaborate on recent advancements and developments related to the detection of DDoS attacks. Additionally, we provide insights into the deployments and data utilized to achieve the presented findings.

A. Machine Learning Approaches

Yusof et al. [19] utilized the KDD99 dataset for attack data and employed Information Gain to assess the significance of each feature, leading to the selection of relevant features. The WEKA tool was utilized for the classification of attacks and normal traffic. The proposed ML system by Yusof et al. [19] comprises various methods applied to the dataset. Their hybrid technique, a KNN-SVM method, is proposed for the classification, detection, and prediction of DDoS attacks. The methods employed by Yusof et al. include k-nearest neighbors (KNN), SVM, DT, K-means, NB, and Fuzzy c-means (FCM). Performance metrics such as True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN), and F-Measure were used by Yusof et al. [19]. Experimental results indicate that Fuzzy c-means clustering outperforms other algorithms in terms of classification accuracy and speed. Sanmorino, A. [20] utilized secondary data collected by other researchers in the development of the ML system. The proposed ML system comprises various methods applied to the acquired information, with a focus on evaluating the accuracy of each ML classification technique in identifying DDoS attacks. Sanmorino, A. applied three methods, namely the DT method, NB, and ANN, and assessed their performance using metrics such as True Positive (TP), False Positive (FP), Precision, Recall, F-Measure, and Receiver Operator Characteristic graphs/ Area Under the Curve (ROC/AUC). The findings indicate that, among the methods employed by Sanmorino, A. [20], the ANN demonstrated the highest accuracy compared to the other two methods for the generated dataset. Radivilova et al. [21] utilized the SNMP-MIB Dataset to investigate various types of attacks, including TCP SYN, UDP flood, ICMPECHO, HTTP flood, Slowpost, Slowloris, and SSH brute force. The study involved analyzing primary approaches for detecting DDoS attacks through the realization of network traffic. The results obtained from employing ML to detect DDoS attacks were presented, with input data comprising simulated realizations of both normal and attacked network traffic exhibiting fractal properties. The classification of traffic realizations took into account various parameters such as the Hurst index, attack type, and intensity. Experimentally, attack levels of 10%, 15%, 20%, and 20% were chosen, and the initiation moment and duration of the attacks were randomly selected. The training process was conducted separately for each attack file, employing the Random Forest (RF) method as applied by Radivilova et al. The results demonstrated that the most effective method employed by Radivilova et al. [21] for detecting attacks in network traffic is RF. Nandi et al. [22] proposed a hybrid approach aimed at identifying top relevant features through the utilization of both established feature selection methods and hybrid techniques on the NSL KDD dataset. The procedure entailed employing five feature selection methods, namely Information Gain, Gain Ratio, Chi-squared, Relief, and Symmetrical Uncertainty, to identify the most pertinent features within the NSL KDD dataset. Subsequently, a hybrid feature selection method was applied to further refine the feature set, selecting the most crucial features. The dataset was then filtered to isolate DDoS packets using the chosen features, as not all anomalous instances in the dataset belonged to the DDoS category. Nandi et al. employed various methods, including NB, Bayes Net, Decision Table, J48, and RF, and their results indicated that the hybrid approach demonstrated superior detection rates compared to existing methods. In their study, Bagyalakshmi et al. [23] introduced two approaches utilizing a dataset sourced from NSL-KDD. The first approach employs Learning Vector Quantization (LVQ) as a filter method, while the second approach utilizes Principal Component Analysis (PCA) as a dimensionality reduction method. Features selected from each approach are employed in the classification process, and the outcomes are compared in relation to their effectiveness in detecting DDoS attacks. Bagyalakshmi et al. applied NB, SVM, and DT as classification methods. The findings presented by Bagyalakshmi et al. [23] indicate that the LVQ-based DT technique outperforms the others in terms of identifying attacks. In their work, Sahoo et al. [24] employed an SVM with kernel principal component analysis (KPCA) for feature selection, while a GA algorithm was utilized to optimize the SVM parameters. To address the issue of noise arising from feature variations, they introduced an enhanced kernel function (N-RBF). Sahoo et al. [24] chose SVM as the primary classifier for predicting malicious traffic, presenting an effective solution for securing Software-Defined Networking (SDN). Their proposed approach integrates SVM with KPCA and GA, using KPCA for feature extraction and SVM for attack classification. To reduce training time, they introduced an improved radial basis kernel function. The optimization of various classifier parameters was achieved through the application of a GA algorithm. The detection module was executed on the controller, and the proposed DDoS detection framework was validated in a simulated environment involving a POX controller, Open vSwitch (OVS), and Mininet emulator. Comparative analysis with other classifiers from [24] revealed that the SVM model they proposed exhibited superior effectiveness and accuracy in classification for attack detection. Chartuni et al. [2] introduced a methodology that centers around the exploration and selection of a dataset representing DDoS attack events. This involves preprocessing the data and creating a sequential neural network model for multi-class classification, utilizing the CIC DDoS2019 dataset. The approach is specifically focused on multi-classification. They highlighted the enhanced value of multi-class classification in comparison to binary classifications, contrasting their models with those presented previously. Their utilized method involves Dense Neural Networks (DNN). The model proposed by Chartuni et al. demonstrated notable performance, achieving approximately 94% in metrics such as $precision$, $accuracy$, $recall$, and $F1-score$. Jaiswar, R. [25] employed the CICIDS 2017 dataset for the attack data in their study. The model was built using correlation analysis to choose relevant features and diminish the dataset's dimensionality. Following that, K-Means Clustering was utilized on a dataset with selected features to produce clusters, subsequently designated as either Benign or Attack. The labeled clustered dataset was fed into an SVM for training and testing the model. Jaiswar, R. utilized an SVM. The findings indicate that Jaiswar, R.'s model successfully categorizes web traffic based on its nature (Benign or Attack traffic). Upon evaluation, the model demonstrated superior performance compared to other classification algorithms tested on the available dataset. Aamir et al. [26] proposed a framework comprising four key stages: dataset acquisition, feature engineering, evaluation of the machine learning (ML) model, and analysis of results. The acquisition of the dataset involves a systematic exploration of published and validated datasets that contain evidence of DDoS attacks. Feature engineering follows dataset selection and entails analyzing the dataset to understand its context, identifying duplication and collinearity among attributes, and making adjustments to render it suitable for training the chosen ML model. The model evaluation process encompasses initial training, fine-tuning hyperparameters based on results, and assessing the modified model. Aamir et al. [26] assessed five ML models—SVM, RF, ANN, NB, and K nearest neighbors (KNN). The classification results indicate that all variants of discriminant analysis and SVM demonstrate good testing accuracy. Ismail et al. [27] employed the UNWS-np-15 dataset, utilizing RF and XGBoost classification algorithms. Following the application of these ML models, a confusion matrix was generated to assess model performance. The findings indicated that XGBoost outperformed other models in terms of precision, making it the preferred choice for the dataset used by Ismail et al. [27].

Kareem et al. [28] conducted an assessment of the efficiency of rapid ML techniques for model testing and generation within communication networks, with a focus on identifying denial-of-service attacks. The CICIDS2017 dataset in the WEKA tool served as the training and testing ground for multiple ML algorithms. The evaluated methods included REP tree (REPT), random tree (RT), RF, decision stump (DS), and J48. Performance metrics such as $accuracy$, $F-score$, $precision$, and $recall$ were employed by Kareem et al. [28]. Their experiments revealed that J48 exhibited superior performance and quicker testing times, especially when utilizing 4-8 features. Alduailij et al. [29] conducted research with the primary objective of enhancing the performance in detecting DDoS attacks. The study involved experiments using the CICIDS 2017 and CICDDoS 2019 datasets. Alduailij et al. [29] employed Mutual Information (MI) and RF Feature Importance (RFFI) methods for their investigation. The methodology utilized by Alduailij et al. [29] encompassed RF, Gradient Boosting (GB), Weighted Voting Ensemble (WVE), K Nearest Neighbor (KNN), and Logistic Regression (LR). The evaluation of their approach was based on performance metrics such as $Precision$, $recall$, $F-score$, and $accuracy$. According to the experimental results, the accuracy achieved by RF, GB, WVE, and KNN with 19 features was 0.99. Table I summarizes previous studies focused on utilizing machine learning methodologies for the identification of DDoS attacks.

Classification algorithms are employed to discern DDoS attacks by classifying traffic packets. Various ML algorithms, including SVMs, ANNs, DT, GA, AdaBoost, k-means, Apriori, k-nearest neighbors, Cluster Analysis, PageRank, and NB, can be utilized for this purpose.

B. Deep Learning Approaches

Numerous DL techniques have been proposed to classify and predict Distributed Denial of Service (DDoS) attacks. Yuan et al. [30] present a DL-based approach for detecting DDoS attacks, wherein high-level features are automatically derived from low-level ones, producing a resilient representation with enhanced inference capabilities. They construct a recurrent deep neural network to identify patterns within sequences of network traffic, enabling the tracking of activities associated with network attacks. Yuan et al. [30] showcased favorable results, demonstrating a significant decrease in the error rate from 7.517

Li et al. [31] underscore the superiority of DL in comparison to traditional DL techniques for detecting DDoS attacks. They introduces a detection model and defense system rooted in DL within a Software-Defined Network framework. The experimental findings highlight the model's significantly improved performance when contrasted with conventional ML approaches. Furthermore, it diminishes reliance on the environment, streamlining real-time updates to the detection system, and easing the challenges associated with upgrading or altering the detection strategy.

In their study, Alguliyev et el. [32] presented an approach for anticipating the onset of DDoS attacks through the identification of pertinent content in social media. They employ a CNN model featuring 13 layers and an enhanced LSTM method to achieve precise classification of texts into positive and negative categories. The prediction of DDoS attacks occurring the following day relies on analyzing the negative and positive sentiments within social media texts. The effectiveness of their proposed method was assessed through experiments conducted on Twitter data.

Shurman et al. [33] introduced two approaches for identifying Distributed Reflection Denial of Service (DDoS) attacks in the context of the IoT. The initial method employs a hybrid Intrusion Detection System (IDS) designed to identify IoT-DoS attacks, while the second method utilizes DL models built on Long Short-Term Memory (LSTM), trained with the most recent dataset specifically tailored for DrDoS incidents. Shurman et al's experimental findings illustrate that implementing these methodologies effectively detects malicious activities, thereby enhancing the security of IoT networks against both Denial of Service (DOS) and DDoS attacks.

Cil et al [34] proposed the utilization of a deep neural network (DNN) as a DL model for detecting DDoS attacks. Employing the CICDDoS2019 dataset in their experiments, they observed a remarkable 99.99% success rate in detecting DDoS attacks on network traffic. Additionally, the classification of attack types achieved an accuracy rate of 94.57% based on the dataset.

In [35], they conducted traffic classification on Software-Defined Network (SDN) traffic provided by Leading India. They employed diverse DL approaches to categorize the traffic into either normal or malicious classes. The findings of Ahuja et al. [36] demonstrated remarkable success, achieving an impressive accuracy rate of 99.75% through the utilization of Stacked Auto-Encoder Multi-layer Perceptron (SAE-MLP).

Agarwal et al. [36] introduced a deep neural network-

TABLE I. SUMMARY OF MLBASED RESEARCH PAPERS

Ref.	Performance Metrics	Dataset	Contribution	Approach	Year
[19]	TP, FP, TN, FN, F-Measure.	KDD99	A hybrid method for classifying, detecting, and predicting the DDoS attack by ML.	SVM, k-nearest neighbor, K-Mean, NB, Fuzzy C Mean	2016
[20]	TTP, FP, Precision, Recall, F-Measure, ROC / AUC	Bank Data Classification of the DDOS attack by ML	DT, NB	ANN	2019
[21]	TP, FN, Accuracy.	SNMP-MIB	Classification by using fractal and recurrence features.	RF	2019
[22]	k-fold cross validation	NSL-KDD	Detection and classification of the DDoS attacking packets and normal packets.	NB, Bayes Net, Decision Table, J48, and RF	2020
[23]	Accuracy, Precision, Recall, Specificity, F-Measure	NSL-KDD	Intrusion detection for DDoS attacks cloud environment	DT, NB, SVM	2020
[24]	TP, FP, TN, FN, FMeasure.	NSLKDD, KDD	Classification of DDoS attacks SVM	GA	2020
[25]	Accuracy, Precision, Recall, F1 Score.	CICDDoS2019	Multi-class classification of the DDoS attack	Dense Neural Networks	2021
[26]	Accuracy, FP.	CICIDS 2017	Identify and classify DDoS attack	SVM	2021
[27]	k-fold cross validation	CICIDS 2017	classification of DDoS attacks	SVM	2021
[28]	Accuracy, Precision, Recall, F1 Score.	UNSW-nb15	Detection of the DDOS attack	RF, XGBoost.	2022
[29]	Accuracy, F-score, Precision, and Recall.	CICIDS 2017	Classification of DDoS attacks	REP Tree, Random Tree, RF, Decision Stump, J48.	2022
[30]	Precision, Recall, F-measure, and Accuracy.	CICIDS 2017 and CICDDoS 2019	Classification of DDoS attacks	RF, Gradient Boosting, Weighted Voting Ensemble, K-Nearest Neighbor, LR	2022

based feature selection-whale optimization algorithm (FS-WOA–DNN) for distinguishing between normal and attacked data. The chosen features undergo classification through a deep neural network classifier, utilizing the CICIDS 2017 dataset. The algorithm's performance was evaluated through simulation using the MATLAB tool, demonstrating an experimental accuracy of 95.35% in detecting DDoS attacks.

In their work, Reddy et al. [37] proposed a hybrid neural network structure that integrates a Gradient Boosting DT with a nimble Convolutional Neural Network (CNN). The results from these models are unified through an additive function to merge spatial and temporal characteristics, yielding a hybrid model proficient in differentiating between malicious and benign ultimate traffic flow. The hybrid ensemble learning model, as presented by Reddy et al, showcased enhanced accuracy compared to established detection methods. Boonchai et al. [38] proposed models leveraging deep neural networks designed for efficient multiclass classification of DDoS, utilizing the CICDDoS2019 dataset. They have introduced two models employing a straightforward DNN architecture and a Convolutional Autoencoder. The authors demonstrated enhanced classification accuracy through the application of DL techniques, achieving an accuracy of 91.9

Guo et al. [39] presented GLD-Net, a DL approach that combines topological and traffic features to achieve high accuracy in detecting DDoS attacks. These investigations collectively illustrate the effectiveness of DL in accurately categorizing DDoS attacks. Experiments conducted on the NSL-KDD2009 and CIC-IDS2017 datasets reveal that GLD-Net achieves detection accuracies of 99.3% for two classifications (normal and DDoS flow) and 94.2% for three classifications (normal, fast DDoS flow, and slow DDoS flow). Table II summarizes the papers that use DL approaches to detect DDoS assaults.

III. CLASSIFICATIONS, DATASET AND PERFORMANCE METRICS

A. Classificaton Methods

In classification tasks, the objective is to anticipate the output variable by analyzing the input features provided. The output varies across different tasks. Several frequently common classification tasks include:

- Binary Classification: involves a target variable with two possible outcomes, usually denoted as 0 or 1. Applications of this classification type include spam detection, fraud detection, and disease diagnosis. A range of studies have successfully applied ML to the binary classification of DDoS attacks. Bakhareva et al. [40] present algorithms designed to identify attacks within enterprise networks by analyzing network traffic. To assess ML methods for binary classification (distinguishing between attack and regular traffic) and multiclass classification (identifying various classes of typical attacks), the researchers utilized the CICIDS2017 dataset. The findings indicated that the CatBoost and LightGBM algorithms demonstrated effective performance in both binary and multiclass classification, successfully categorizing malicious traffic into distinct attack groups.

- Multi-class Classification involves scenarios where the target variable can have more than two potential outcomes, usually denoted as unique labels or classes. Numerous studies have investigated the application of ML in the multi-classification of DDoS attacks. In their work, Sayed et al. [41] introduced a multi-classifier model based on a stacking ensemble deep neural network. This model effectively identifies various types of DDoS attacks, achieving an accuracy rate of 89.4% when evaluated on the CIC-DDoS2019 dataset. Parfenov et al. [42] expanded the feature set for detecting attacks through the application of ML techniques. They explored methods for binary and

TABLE II. SUMMARY OF DLBASED RESEARCH PAPERS

Ref.	Performance Metrics	Dataset	Contribution	Approach	Year
[36]	Error Rate, Accuracy, Precision, Recall, F1, AUC.	ISCX2012	Classification DDOS Attacks by DL	CNN, RNN, LSTM, and GRU.	2017
[37]	Accuracy, Precision, F1 Score.	ISCX2012	Detection and defense system from the DDoS attack by DL in SDN environment.	RNN, LSTM, and CNN.	2018
[38]	Recall, Precision, F-measure, Training loss, Training accuracy, Testing loss, and Test accuracy.	Data collected from social media	Predicts DDoS attack occurrence by finding relevant texts in social media.	CNN, and LSTM.	2019
[39]	TP, FP, TN, FN	CICDDoS2019	DDoS attacks Detection in IoT.	RNN, and LSTM.	2020
[40]	TP, FP, TN, FN	CICDDoS2019	Detection of DDoS attacks on the packets captured from network traffic.	DNN	2021
[41]	Accuracy, Precision, Recall, F-score, False positive rate, and False negative rate.	Dataset provided by leadingindia.ai.	Detection of DDOS Attack on software-defined networking traffic.	CNN, LSTM, CNN-LSTM, SVC-SOM, SAE-MLP.	2021
[42]	Accuracy, Sensitivity, Specificity, Error, False Positive Rate (FPR), False Negative Rate (FNR), Positive Predictive Value (PPV), and Negative predictive value (NPV).	CIC-IDS 2017	Detection of DDOS Attack Using DL Model in Cloud Storage Application.	SVM, KNN, ANN, DNN and FS-WOA–DNN.	2021
[43]	Accuracy, Precision, Recall, F-measure.	CICDDoS2019	Detection of DDOS Attack Using DL	GBDT, CNN.	2021
[44]	Accuracy, Precision, Recall, F-1score.	CICDDoS2019	classification of DDoS attacks Using DL	DNN	2022
[45]	TP, FP, TN, FN NSL-KDD2009	CIC-IDS2017	Detection of DDoS Attacks via Topological and Traffic Feature Fusion using DL.	GLD-Net, DT, RF, Stacked-DNN, FastGRNN, FastGRNN.	2022

multiclass classification of network traffic to identify potential attack patterns. Additionally, a comparative analysis was conducted on ML algorithms including Gradient Boosting, AdaBoost, and CatBoost, utilizing the CICDDoS2019 dataset. The findings revealed that CatBoost demonstrated superior performance in both binary and multiclass classification, achieving accuracies of 99.3% and 97%, respectively. In their study, Mungwarakarama et al. [43] applied an Optimized K-Nearest Neighbor (OKNN) model to a real network dataset. By tuning parameters such as $n_neighbors$, $metrics$, $weights$, and n_jobs, the model demonstrated a notable proficiency in accurately distinguishing between normal traffic flow and DDoS attacks. The experimental outcomes showcased a high level of accuracy in the identification of both normal traffic and DDoS attacks.

- Hierarchical Classification: This classification method involves a target variable with a hierarchical or nested arrangement, where classes are structured in a tree-like form. Instances of hierarchical classification can be observed in species classification and product categorization. Various ML techniques have been suggested for the hierarchical classification of DDoS attacks. In their study, Kang et al. [44] presented a taxonomy that relies on similarity and hierarchical clustering to categorize 12 real DDoS attack tools. The effectiveness of this taxonomy was assessed, revealing its capability to accurately classify complex attack instances. Table III summarizes the papers on classification Tasks in ML approaches.

TABLE III. SUMMARY OF CLASSIFICATION TASKS ML-BASED RESEARCH PAPERS

Ref.	Classification Tasks	Approach	Dataset
[30]	Binary Classification	CatBoost, LightGBM.	CICIDS2017
[31]	Multi-class Classification	Convolution Neural Networks (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU).	CIC-DDoS2019
[32]	Multi-class Classification	Gradient Boosting, AdaBoost, and CatBoost	CICDDoS2019
[33]	Multi-class Classification	Optimized K-Nearest Neighbor (OKNN)	LRN
[34]	Hierarchical Classification	Characteristic tree, and Hierarchical Clustering.	

B. Available Benchmarked DDoS Datasets

The studies analyzed for DDoS attack detection employed datasets listed in Tables I, II, and III, which were commonly utilized across most of the studies. The subsequent section provides descriptions of these datasets: The NSL-KDD dataset: Is an enhanced version of the KDD Cup99 dataset, where several fundamental issues have been addressed and rectified through modifications and removals. Comprising 41 features, this dataset categorizes attacks into four groups [45]. ISCX2012: This dataset, created in 2012 by Ali Shiravi and colleagues, encompasses a comprehensive collection of network data. It spans seven days, specifically from June 11 to June 17, 2010, capturing a spectrum of network activities, ranging from legitimate to malicious traffic. Examples of malicious activities within the dataset include DDoS, HTTP Denial of Service, and Brute Force SSH. Formulated within the framework of a simulated network environment, this dataset comprises both sorted and unbalanced data. It employs two overarching profiles: one delineates attack patterns, while the other characterizes typical user scenarios within the ISCX dataset [46]. UNSW-NB15: This dataset was produced by the Australian Center for Cyber Security. Generated the UNSW-NB15 dataset, employing Bro-IDS and Argus tools alongside several newly developed methods. The dataset comprises around two million records featuring a total of 49 characteristics. It encompasses various attack types [47]. CICIDS 2017: This was generated by the Canadian Institute for Cybersecurity (CIC) in the year 2017. It encompasses a variety of real-time attacks as well as typical network flows. CIC Flow Meter utilizes information derived from logs, source and destination IP addresses, protocols, and identified attacks to assess network traffic [48]. CICIDS 2017 encompasses common attack scenarios, including but not limited to brute force attacks, HeartBleed attacks, botnets, DDoS, DoS, web attacks, and exfiltration attacks [49]. CSE-CIC-IDS2018: In 2018, a collaboration between the Communications Security Foundation (CSE) and CIC resulted in the development of the CSE-CIC-IDS2018 dataset. This dataset was constructed by generating user profiles containing abstract descriptions of various events, which were subsequently amalgamated with a distinctive set of attributes. The dataset encompasses seven different attack scenarios, such as Brute Force, Heartbleed, Botnet, DoS, DDoS, web attacks, and insider network compromise [50]. CICDoS2019: This dataset created by Sharafeldin et al. [51] in 2019, was generated by extracting over 80 traffic features from the original data using the CICFlowMeter-V3 feature extraction software. Table IV summarizes the Datasets and their features.

TABLE IV. SUMMARY OF DATASETS AND FEATURES

Ref.	Dataset	Attacks	Features
[45]	NSL-KDD	4	41
[46]	ISCX2012	6	-
[47]	UNSW-NB15	9	43
[48]	CICIDS 2017	14	77
[50]	CSE-CIC-IDS2018	7	80
[51]	CICDoS2019	13	88

C. Performance Metrics

Performance metrics used in studies to detect DDoS attacks are listed, with a focus on performance indicators as the predominant measures. In binary classification scenarios, common metrics encompass $Precision$, $recall$, $F1_score$, and area under the curve, among others. The confusion matrix serves as a comprehensive summary of the classification model's predictions, incorporating True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) [52]. Eq. (1) defines the true positive rate (TPR), which is alternatively referred to as recall or sensitivity [53]. The TPR should be as high as possible.

$$recall = \frac{TP}{TP + FN} \tag{1}$$

The Precision of the model is determined using Eq. (2), which involves checking the number of correctly predicted positive classes by the model that are truly positive instances.

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Eq. (3) presents the false positive rate (FPR), which quantifies the proportion of negative occurrences that the model erroneously identifies as positive.

$$FPR = \frac{FP}{TN + FP} \tag{3}$$

The false negative rate (FNR) is the percentage of positive cases wrongly identified as negative. It is calculated using Eq. (4).

$$FNR = \frac{FN}{TP + FN} \tag{4}$$

Eq. (5) illustrates the TNR, also known as Privacy, representing the percentage of accurately predicted negative as negative.

$$TNR = \frac{TN}{TN + FP} \tag{5}$$

In Eq. (6), $accuracy$ is characterized as the proportion of true predictions made by the model across all classes. A preference is given to achieving the highest level.

$$Accuracy = \frac{TP + TN}{Total} \tag{6}$$

Comparing two models becomes challenging when one exhibits high $recall$ and low precision, or vice versa. To address this issue, the $F1 - score$ is employed as a metric for comparison, providing a balanced evaluation of both memory and accuracy. Eq. (7) is utilized for the calculation of the $F1 - score$.

$$F1 - Score = \frac{2 * Recall * Precision}{Recall + Precision} \tag{7}$$

The AUC-ROC curve measures the efficiency of classification problems at various threshold levels. A model is considered to offer more accurate predictions when the area under the curve approaches 1.

IV. DISCUSSION AND ANALYSIS

Detecting DDoS attacks with varying rates and patterns from legitimate traffic poses a significant challenge. Numerous ML/DL techniques have been suggested by researchers to identify DDoS attacks over the years. However, the effectiveness of these methods is constrained due to attackers consistently evolving their strategies and rapidly enhancing their skills, enabling them to execute unknown DDoS or zero-day attacks characterized by distinctive traffic patterns. Our analysis of prevailing classification methods centers on various aspects, such as the commonly employed classifiers and their influence on classification accuracy, as well as the datasets utilized for testing purposes. Researchers employed various ML classifiers in their methodologies, encompassing SVM, KNN, NB, DT, ANN, RF, J48, GA, LR, CatBoost, AdaBoost, and XGBoost. Among these, 22% of studies opted for the widely recognized SVM classifier, 10% employed the KNN classifier, 13% utilized the NB classifier, 9% applied the DT classifier, 6% implemented the ANN classifier, 16% employed the RF dataset, 3% each utilized the J48, GA, LR, CatBoost,

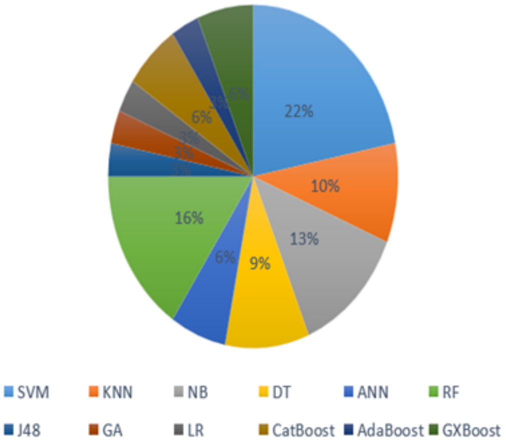

Fig. 3. Classification methods of ML approaches.

AdaBoost, and XGBoost classifiers. Fig. 3 illustrates ML classification methods in the studies.

In recent years, our observations indicate a heightened emphasis on ML-based classifiers. Specifically, in 2021, the SVM classifier took precedence, followed by the RF classifier in 2022, and the NB classifier in 2020, as illustrated in Fig. 4.

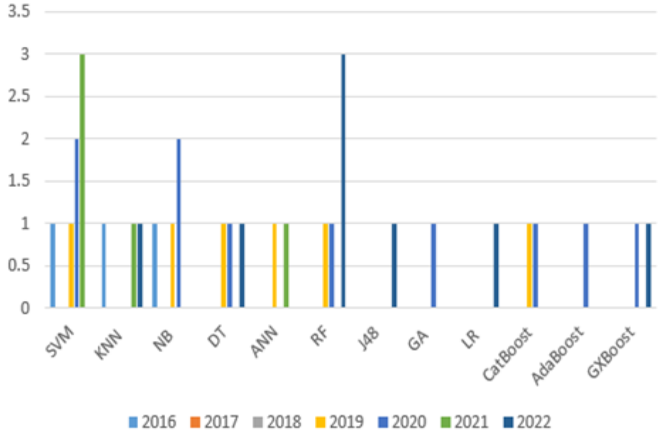

Fig. 4. Classification methods of ML approaches during past years.

The researchers have employed various DL classifiers, such as CNN, RNN, DNN, LSTM, GBDT, and GRU. Notably, 27% of the studies opted for the widely recognized CNN, while 14% utilized RNN, 18% employed DNN, 27% incorporated LSTM, 5% implemented GBDT, and 9% utilized GRU. Fig. 5 visually illustrates the distribution of DL classification methods in the research approaches.

Our analysis indicates that many researchers have formulated their datasets. In various studies conducted over recent years, several researchers employed widely recognized standard datasets, including KDDCUP99, NSL-KDD, UNSW-NB15, CIC-IDS2017, CSE-CIC-IDS2018, ISCX2012, and CICDDoS2019 in most of the studies over the past years, as Fig. 6.

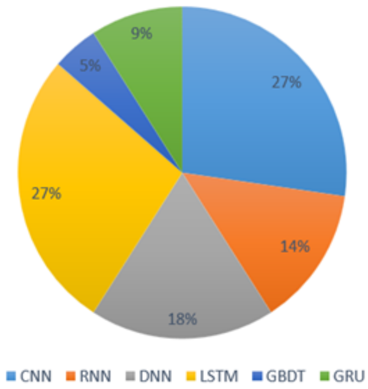

Fig. 5. Classification methods of DL approaches.

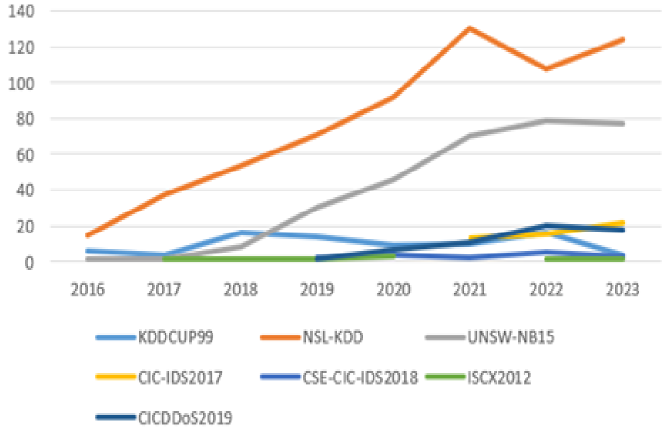

Fig. 6. Dataset that has been used over the past years.

Among the frequently utilized datasets in the literature, NSL-KDD was employed in 55% of the studies, UNSW-NB15 in 28%, KDDCUP99 in 6%, CIC-IDS2017 in 4%, CICDDoS2019 in 5%, CSE-CIC-IDS2018 in 1%, and ISCX2012 in 1%. Fig. 7 presents the distribution of different datasets used for classification.

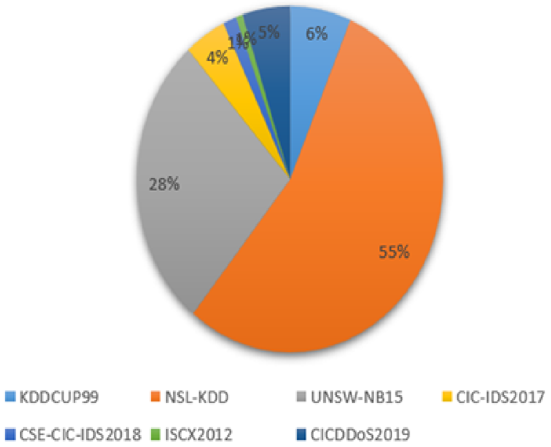

Fig. 7. The different datasets for classification methods.

V. Future Directions

The DDoS detection future research includes using advanced and improved DDoS mitigation techniques as follows:

- ML/DL Models: DL/ML models continue to be used to detect signs of DDoS attacks or analyze behaviors to detect anomalies. In addition to the possibility of mitigating its effects.
- Blockchain Technology: Using blockchain technology to detect DDoS, reducing its effects, and adopting it to raise trust between various entities and facilitate the safe exchange of information.
- Edge and fog computing: Use DDoS detection methods at the network edge to speed up response time. As for fog computing, it will be used to quickly distribute detection tasks and reduce risks.
- Human-centred approach: Develop DDoS detection interfaces based on user experience to increase user effectiveness and integrate experience into decision-making processes, especially when facing DDoS attacks.
- Quantum computing: With the advent of quantum computing, which is thought to break current algorithms, we need to develop DDoS detection techniques, and here quantum-resistant encryption methods must be used.

Continuing research and leveraging AI technologies is crucial to reducing DDoS threats. In addition, the combination of modern technologies and human expertise has a promising future for DDoS detection and reduction.

VI. Conclusion

Differentiating between DDoS attacks exhibiting various rates and patterns and regular traffic poses a considerable challenge. Numerous ML/DL approaches for detecting such attacks have been suggested by various researchers over the years. However, the constant evolution of attackers' tactics significantly restricts the effectiveness of these techniques. This paper provides a summary of the literature, adhering to the recommended taxonomy for DDoS attack detection through ML/DL methods. Our analysis indicates a heightened emphasis on ML-based classifiers where 22% of studies opted for the widely recognized SVM classifier. For DL-based, 27% of the studies opted for the widely recognized CNN. While the majority of researchers have formulated their datasets, NSL-KDD was employed in 55% of the studies. By addressing these future research areas, the field of DDoS detection can evolve to better cope with the increasingly sophisticated nature of cyber threats. Continuous research, and innovation will be key in staying ahead of evolving DDoS attack techniques.

Acknowledgment

The authors are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for the financial support through the Graduate Students Research Support Program.

References

[1] G. Kaur, S. Varma, and A. Jain, "August). a novel statistical technique for detection of ddos attacks in kdd dataset," in *InSixth International Conference on Contemporary Computing (IC3)*. IEEE, 2013, pp. 393–398.

[2] A. Chartuni and J. Márquez, "Multi-classifier of ddos attacks in computer networks built on neural networks," *Applied Sciences*, vol. 11, no. 22, p. 10609, 2021.

[3] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[4] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE communications surveys & tutorials*, vol. 18, no. 1, pp. 602–622, 2015.

[5] D. K. Bhattacharyya and J. K. Kalita, *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. CRC Press, 2016.

[6] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "Bat: Deep learning methods on network intrusion detection using nsl-kdd dataset," *IEEE Access*, vol. 8, pp. 29 575–29 585, 2020.

[7] I. M. Nasser and S. S. Abu-Naser, "Lung cancer detection using artificial neural network," *International Journal of Engineering and Information Systems (IJEAIS)*, vol. 3, no. 3, pp. 17–23, 2019.

[8] A. F. Alsirhani, Master's thesis, DDOS DETECTION MODELS USING MACHINE AND DEEP LEARNING ALGORITHMS AND DISTRIBUTED SYSTEMS (), 2021.

[9] Y. S. Sabir and F. Gebali, *DDoS Attacks Detection using Machine Learning(Doctoral Master)*. emantic Scholar, 2022.

[10] K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A survey of distributed denial of service attack," in *In10th International Conference on Intelligent Systems and Control (ISCO)*. IEEE, 2016, pp. 1–6.

[11] M. A. Al-Shareeda, S. Manickam, and M. Ali, "Ddos attacks detection using machine learning and deep learning techniques: Analysis and comparison," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 930–939, 2023.

[12] N. Sharma, A. Mahajan, and V. Mansotra, "Machine learning techniques used in detection of dos attacks: a literature review," *International Journal of Advance Research in Computer Science and Software Engineering*, vol. 6, no. 3, pp. 100–105, 2016.

[13] S. Sambangi and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression," *In Proceedings (, p. 51). MDPI*, vol. 63, p. 1, 2020.

[14] L. D'hooge, T. Wauters, B. Volckaert, and F. De Turck, "Classification hardness for supervised learners on 20 years of intrusion detection data," *IEEE Access*, vol. 7, no. 19, pp. 67 455–16 746, 2019.

[15] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *Ieee Access*, vol. 7, pp. 82 512–82 521, 2019.

[16] D. Gavrilis and E. Dermatas, "Real-time detection of distributed denial-of-service attacks using rbf networks and statistical features," *Computer Networks*, vol. 48, no. 2, pp. 235–245, 2005.

[17] B. Silver, "1990," in *Netman: A learning network traffic controller*. In Proceedings of the 3rd international conference on Industrial and engineering applications of artificial intelligence and expert systems-Volume 2, pp. 923–931.

[18] T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE communications surveys & tutorials*, vol. 10, no. 4, pp. 56–76, 2008.

[19] A. R. A. Yusof, N. I. Udzir, and A. Selamat, "An evaluation on knn-svm algorithm for detection and prediction of ddos attack," in *Trends in Applied Knowledge-Based Systems and Data Science: 29th International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2016, Morioka, Japan, August, 2016, Proceedings 29 (pp. 95-102) International Publishing*, 2016, pp. 2–4.

[20] A. Sanmorino, "March). a study for ddos attack classification method," *In Journal of Physics: Conference Series*, vol. 1175, p. 012025, 2019.

[21] T. Radivilova, L. Kirichenko, D. Ageiev, and V. Bulakh, "Classification methods of machine learning to detect ddos attacks," in *In 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol.* IEEE: 1, 2019, pp. 207–210.

[22] S. Nandi, S. Phadikar, and K. Majumder, "Detection of ddos attack and classification using a hybrid approach," in *Conference on Security and Privacy (ISEA-ISAP).* IEEE, 2020, pp. 41–47.

[23] C. Bagyalakshmi and E. S. Samundeeswari, "Ddos attack classification on cloud environment using machine learning techniques with different feature selection methods," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, p. 5, 2020.

[24] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary svm model for ddos attack detection in software defined networks," *IEEE Access*, vol. 8, no. 13, pp. 32 502–13 251, 2020.

[25] R. Jaiswar, *DDoS Attack prediction and classification at Application Layer for Web protocol using Kmeans – SVM Machine Learning Algorithm*, 2021.

[26] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. Ahmad, "Machine learning classification of port scanning and ddos attacks: A comparative analysis," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 1, pp. 215–229, 2021.

[27] M. I. Mohmand, H. Hussain, A. A. Khan, U. Ullah, M. Zakarya, A. Ahmed, M. Raza, I. U. Rahman, M. Haleem *et al.*, "A machine learning-based classification and prediction technique for ddos attacks," *IEEE Access*, vol. 10, pp. 21 443–21 454, 2022.

[28] M. I. Kareem and M. N. Jasim, *Fast and accurate classifying model for denial-of-service attacks by using machine learning*. Bulletin of Electrical Engineering and Informatics, 2022.

[29] M. A. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. A. Alduailij, and F. Malik, "Machine-learning-based ddos attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, p. 1095, 2022.

[30] X. Yuan, C. Li, and X. Li, "Deepdefense: Identifying ddos attack via deep learning." *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 1–8, 2017.

[31] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, and L. Gong, "Detection and defense of ddos attack–based on deep learning in openflow-based sdn," *International Journal of Communication Systems*, vol. 31, 2018.

[32] R. M. Alguliyev, R. M. Aliguliyev, and F. J. Abdullayeva, "Deep learning method for prediction of ddos attacks on social media," *AdvData Sci. Adapt. Anal.*, vol. 11, no. 19500, pp. 1–19 500, 2019.

[33] M. M. Shurman, R. Khrais, and A. A. Yateem, "Dos and ddos attack detection using deep learning and ids," *Int Arab J. Inf. Technol*, vol. 17, pp. 655–661, 2020.

[34] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of ddos attacks with feed forward based deep neural network model," *Expert Syst. Appl.*, vol. 169, p. 11452, 2021.

[35] N. Ahuja, 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 and Engineering (Confluence)*, pp. 683–688, 2021.

[36] A. Agarwal, M. Khari, and R. Singh, "Detection of ddos attack using deep learning model in cloud storage application," *Wirel. Pers. Commun.*, vol. 127, pp. 419–439, 2021.

[37] K. P. Reddy, S. Kodati, M. Swetha, M. Parimala, and S. Velliangiri, "A hybrid neural network architecture for early detection of ddos attacks using deep learning models." *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 323–327, 2021.

[38] J. Boonchai, K. Kitchat, and S. Nonsiri, "The classification of ddos attacks using deep learning techniques." *2022 7th International Conference on Business and Industrial Research (ICBIR)*, pp. 544–550, 2022.

[39] W. Guo, H. Qiu, Z. Liu, J. Zhu, and Q. Wang, "Gld-net: Deep learning to detect ddos attack via topological and traffic feature fusion," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[40] N. F. Bakhareva, A. Shukhman, A. Matveev, P. N. Polezhaev, Y. A. Ushakov, and L. V. Legashev, "Attack detection in enterprise networks by machine learning methods," vol. 2019, 2019.

[41] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, "A multi-classifier for ddos attacks using stacking ensemble deep neural network." *2022 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1125–1130, 2022.

[42] D. I. Parfenov, L. Kuznetsova, N. Yanishevskaya, I. P. Bolodurina, A. Zhigalov, and L. V. Legashev, "Research application of ensemble machine learning methods to the problem of multiclass classification of ddos attacks identification." *2020 International Conference Engineering and Telecommunication (EnT)*, pp. 1–7, 2020.

[43] I. Mungwarakarama, X. Hei, Y. Wang, W. Ji, and X. Jiang, "Network flow analytics: Multi-class classification of ddos attacks based on oknn." *2020 International Conference on Networking and Network Applications (NaNA)*, pp. 271–276, 2020.

[44] J. Kang, Y. Zhang, and J. Ju, "Classifying ddos attacks by hierarchical clustering based on similarity." *2006 International Conference on Machine Learning and Cybernetics*, pp. 2712–2717, 2006.

[45] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *2009 IEEE symposium on computational intelligence for security and defense applications*. Ieee, 2009, pp. 1–6.

[46] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *computers & security*, vol. 31, no. 3, pp. 357–374, 2012.

[47] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 military communications and information systems conference (MilCIS)*. IEEE, 2015, pp. 1–6.

[48] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." *ICISSp*, vol. 1, pp. 108–116, 2018.

[49] C. I. for Cybersecurity, "Canadian Institute for Cybersecurity Intrusion Detection Evaluation Datasets," https://www.unb.ca/cic/datasets/ids-2018.html, 2023, accessed on 14 December 2023.

[50] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–8.

[51] A. Mishra, "Metrics to evaluate your machine learning algorithm," *Towards data science*, pp. 1–8, 2018.

[52] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, "Deep learning and big data technologies for iot security," *Computer Communications*, vol. 151, pp. 495–517, 2020.

[53] U. C. Matrix, "Available online:." [Online]. Available: https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62