Journal of Cyber Security
DOI:10.32604/jcs.2021.018623
Article

Computational Intelligent Techniques To Detect DDOS Attacks : A Survey

Isha Sood* and Varsha Sharma

School of Information Technology, Rajiv Gandhi Prodyogiki Vishvavidyalya, Bhopal, India
*Corresponding Author: Isha Sood. Email: Ishasweet1984@gmail.com
Received: 06 July 2021; Accepted: 15 July 2021

Abstract: The Internet is often targeted by the Distributed Denial of Service (DDOS) Attacks that deliberately utilize resources and bandwidth to prohibit access to potential users. The attack possibility is that the packets are filled massively. A DOS attack is launched by a single source, while a DDOS attack is originated from numerous resources. DDoS attacks are not capable of stealing website user's information. The prime motive of the DDoS attacks is to devastate the website resources. Distributed Denial of Service (DDoS) attacks are disruptive to internet access on the Network. The attitude of the customer to get fast and reliable services can be seriously influenced by DDoS attackers. In the digital era of today, cases of DDoS attacks have also been exceeded in the wireless, smartphone, and IoT attacks with catastrophic implications. We will soon be experiencing the 5G smartphone rebellion, but there are indications that 5G networks too are becoming victim to DDoS attacks but the existing DDoS detection and protection strategies are not able to handle DDOS attacks successfully therefore, thorough research on implementing computational intelligent strategies in the detection and defense techniques has been performed to recognize, mitigate, and avoid these attacks. But the most suitable and efficient defense strategy for these attacks remains an issue to be addressed in the future. This review article concentrates on the most prevalent methods of detection and defense against DDoS attacks that incorporate computational intelligence. The analysis describes attacks and explains them. The key factors relevant to the detection of DDOS attacks are included in this research like methods, tools, and detection accuracy. Finally, various challenges attached to the detection of DDOS attacks and research gaps are depicted.

Keywords: 5G; DDoS; IoT

1 Introduction

Denial-of-Service (DDoS) attack relates to the need for client/server infrastructure to combine multiple devices as an attack tool to promote attacks on one or more objectives to maximize the attack power [1]. It is hard to differentiate attack or acceptable behavior via protocol and services. It becomes difficult to identify a distributed denial-of-service attack [2]. A study on security methods against DDoS attacks at various points in history is largely based on the strategy of detecting network intrusions. Based on the features of many-to-one attacks in the DDoS attack method, three characteristics involving the numbers of source IP addresses, the numbers of target ports as well as the flow density were used to characterize the features of the attack. There are mainly three types of attacks, i.e., Application layer attacks, Protocol attacks, and Volumetric attacks [3].

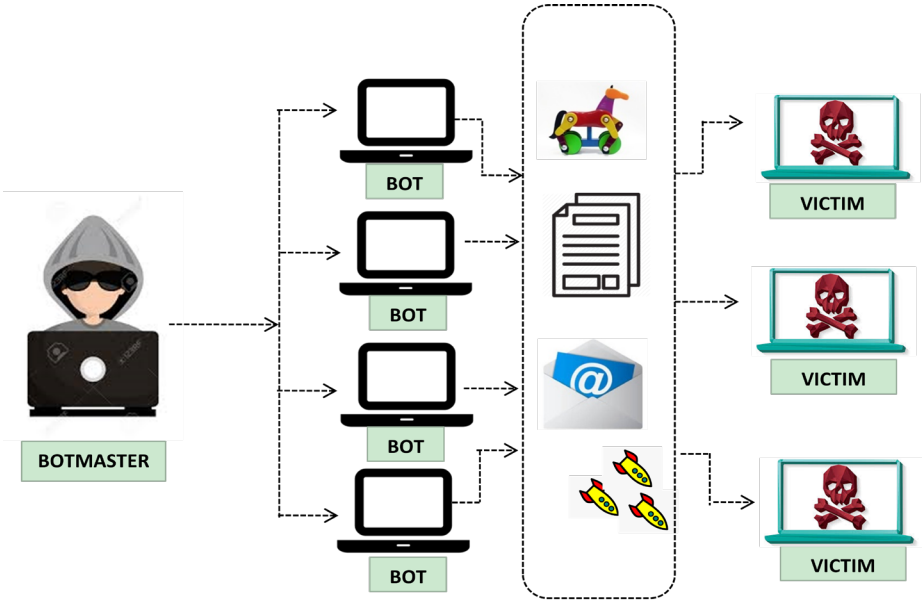

Figure 1: DDOS attack

Due to the debilitating effects of a DDoS attack, it is compared with the Tsunami attack [4]. These attacks are a persistent risk to modern industry and cause serious business disruptions, consumer problems, and monetary expenses. Regardless of research and industrial efforts to improve DDoS defense, DDoS attacks have become a severe challenge, many researchers were focusing their attention on the study of factors that are involved in the identification of DDoS attacks. A comprehensive survey of attacks and protection techniques was performed in with an overview of avoidance, identification, and response. On the other hand, a paper explaining the features of the frameworks used to identify network detection [5]. A deep study of DDoS attacks, defense techniques used during networks is described in [6]. While these researches analyze the identification processes, they are restricted to a study at the stage of the network layer but the depth application layer is not considered in which the attacks had a significant adverse effect in modern times, as shown by recent studies [7–9]. Besides, these researches have not considered the perspective that characterizes the detection of DDoS attacks for a probable betterment of it.

Hence, this paper gives the aspects that describe the detection of DDoS attacks, these perspectives include methods, tools used, observation of detection method, the dataset used, and the type of DDOS attack it can detect. The prime intention of this paper is to survey the research to examine certain aspects of the detection of DDoS attacks. The rest of the paper is organized as follows: Section 2 tells about the types of DDOS attacks, Section 3 provides a review of existing work, Section 4 provides the summary of DDOS attack detection and Section 5 presents the challenges associated with DDOS attack detection, Section 6 summarizes the research gaps and Section 7 concludes the paper and section 8 presents the future directions in the research area.

2 Review of Existing Work

In the past decade, many classification techniques for DDoS attack detection have been proposed by the authors. Few classification techniques are being discussed here:

The author proposed Enhanced Multi-Class Support Vector Machines for the classification of HTTP flooding, session flooding, and IP flooding attacks, ICMP flooding, TCP flooding, UDP flooding, Smurf flooding, port scan, land flooding, attacks with 99% accuracy on the KDDCUP 99 dataset [1].

In this paper, the author suggested Multilayer Perceptron (MLP) model classify Smurf, UDP Flood, SIDDOS, HTTP Flood attacks in a new dataset that includes modern attacks, that have never been used in prior research with 98.63% accuracy [2].

In this research, a detection mechanism based on the web user's dynamism is presented. To do so, user features such as mouse functions and right-clicking are tested by the author and it is shown that it can detect the application layer DDOS attacks with 100% accuracy. The author employed CIC-DoS, CICIDS, and CSE-CIC-IDS, and modified the data set for evaluation purposes [4].

Gradient Boosting Decision Tree (GBDT) is proposed here which is capable of detecting TCP flood, UDP flood attacks with 99.97% and 100% accuracy. It uses the RFPW feature selection algorithm that combines random forest scores with Pearson correlation coefficients as a search approach, and it also uses the GBDT algorithm as the evaluation criteria. RFPW selects a small number of features, making GBDT detection speed fast [10].

The authors propose the hidden semi-Markov model to explain the behaviors of web users that may be described by web object click rates. The observational data of usual web traffic is trained with the forward and backward algorithm to obtain the secret semi-Markov model variables. The average entropies of sequences observed that match the HsMM model is used to detect application-layer DDoS attacks with 97% detection accuracy [11].

The author uses traffic cluster entropy as detection metric not exclusively to detect DDoS attacks but in addition to distinguish between DDoS attacks and flash events. It is observed that if the flash event is enabled, the source address entropy rises whereas the traffic cluster entropy does not rise. However, when the DDoS attack is launched, entropy for the traffic cluster increases together with entropy for the source address. This technique has the capability of detecting UDP and TCP DDOS Attacks and flash events [12].

This paper provided a packet filtering scheme based on IP-traceback to combat DDoS attack and utilizes the attack graph obtained from IP traceback to calculate the costs and efficiency of filtering routers and deploys filters on the appropriate routers accordingly. The results indicate that the scheme is very successful in protecting both the victim's resources and the link resources while maintaining resource usage filtering and normal traffic loss within a reasonable limit [5].

The author introduces a new model for detecting SVM-based DDoS attacks in SDN. Firstly, the model selects multiple major characteristics from of the packet-in messages and tests the distribution of each feature by using entropy, then employs a qualified Support Vector Machine (SVM) technique to find the DDoS attack. This method can detect Syn flooding attack, ICMP flooding, UDP flooding attack with 93% accuracy by calculating the entropy distribution of 5 features [6].

This research article introduces and develops a novel protective system for the defeat of DoS/DDoS attacks based on HTTP, such as the flexible, collaborative, multilayer, DDoS prevention framework (FCMDPF). The innovation of this framework addresses and overcomes all the drawbacks of existing related works. It offers a new alternative security mechanism to defend web applications from HTTP DoS/DDoS attacks of all sorts, including high-rate DDoS (HR-DDoS) and the flash crowd (FC). It is also able to authenticate and monitor back (TB and CV) when attacking IP sources and block them at the edge router (OB). Ultimately, the FCMDPF system is analyzed based on the optimal requirements [7].

The implications of the DDoS attacks were discussed in this paper, and important factors influencing the attack were compared. The authors used a trained MLP with GA learning algorithm to detect the DDoS attack based on the volume of HTTP GET requests, the entropy of requests, and the variance of entropy in EPA-HTTP (environmental protection agency-hypertext transfer protocol) datasets with 98.13% detection accuracy [8].

The author suggested a hybrid detection method, known as a hybrid intrusion detection system (H-IDS), to detect DDoS attacks in this article. The proposed detection system makes separate but combined use of both anomaly-based and signature-based detection methods and integrates the findings of both detectors to improve overall detection accuracy [9].

This paper provides a semi-supervised clustering method Multiple-Features-Based Constrained-K-Means (MF-CKM) algorithm for detecting DDoS attacks, this method integrates the benefits of supervised and unsupervised learning methods and consider the actual application scenes that have small amounts of labeled data and large amounts of unlabeled data. The algorithm given employs the feature

vector as the feature detection to reduce the low detection performance problems caused by the use of a single feature. Simultaneously MF-CKM utilizes the labeled data to guide initial clustering center collection to increase the convergence rate [13].

Here Enhanced Support Vector Machines have been used to detect non-spoofed IPs while spoofed IPs are detected using the Hop Count Filtering (HCF) process. This technique can detect TCP flooding, UDP flooding, ICMP flooding, land flooding, HTTP flooding, and session flooding using only two filtering methods i.e. rate-based filtering and history-based filtering [14].

They have analyzed the DDOS attacks from the perspective of hybrid heterogeneous multi-classifier learning. To gain maximum generalization and complementarily, the authors proposed a heterogeneous model of the detection method and designed the component classifiers based on Bagging, Random Forest, and KNN algorithms. Simultaneously a heterogeneous classification ensemble model based on Singular Value Decomposition (SVD) has been designed which is capable to detect DDOS attacks with 99.9% accuracy [15].

The research article shows that artificial neural networks are used to effectively detect and identify three types of DDoS attacks, i.e., DNS DDoS Attack, CharGen DDoS Attack, UDP DDoS Attack, and Legal 95.6% network traffic [16].

This proposed research aims at developing a detection system based on machine learning that uses four features proposed to classify strategies for GET flood attacks by separating bots from legitimate users. These apps take benefit of bot-specific browsing behavior to catch fake clients, who are portrayed as genuine users. An emulated testbed has been set up to establish evidence of attack traffic by utilizing Publicly accessible weblogs such as WorldCup98, Clarknet, and NASA along with records of their university traffic. A selected set of classification algorithms for machine learning is used to create models that can capture bot sources effectively. SVM achieved a detection rate of 97.4% across various machine learning classifiers used [17].

The proposed method allows inferences based on signatures collected earlier from network traffic samples to accomplish a detection rate of 96 percent in TCP flood detection, UDP flood detection, and HTTP flood detection, as well as stealth attacks such as HTTP slow headers, HTTP slowcore, and HTTP slow read attacks. The program makes use of the Random Forest algorithm to identify network congestion directly through network devices depending on samples collected from the sFlow protocol [18].

Lyapunov's largest exponent has been used by the authors in this paper for validating the theory of chaos. An exponential smoothing model has been used for the prediction of the network traffic rather than NADA's predictive method. To evaluate the prediction errors chaos theory, and back propagation neural networks have been used. This proposed model can detect DDOS attacks with 98.04 % accuracy [19].

In this article, the author suggested a method to detect the anomalies based on both the exponent Tsallis Entropy and Lyapunov. Here Source IPs and Destination IPs entropy is measured by evaluating the exponent separation rate with 100% accuracy (no false negatives) and 100% precision (no false positives). The experiment findings show that the Exponent Separation Detection Algorithm is very effective in DDoS attack detection. The impact of source IPs and destination IPs in network traffic is merged by the researchers of this research, while the traditional entropy-based approach concentrates merely on the separate data packet field function [20].

The suggested technique consists of, a spoofed module for traffic analysis, an interface-based rate limiting algorithm (IBRL), and an online monitoring system (OMS). Spoofed packets are filtered out by the HCF-SVM algorithm at the victim's end. There is no requirement of coordination among the forwarding routers and the ISPs. Moreover, the Protocol header is used to derive limited traffic attributes such as source IP addresses and its related TTL values that makes it possible to detect TCP SYN, SMURF, UDP, and ICMP DDOS attacks with 98.99% accuracy of identification in the real-time scenario [21].

The authors have used a novel collection of information theory-based φ Entropy and φ Divergence metrics for early detection of DDoS attacks and Flash Events FEs. The novel metrics φ-Entropy and φ-Divergence are particularly reactive and have elevated cost of convergence. The suggested detection

method makes the detection of different forms of DDoS attacks and FEs more effective. The entropy gap between traffic flows is used in this detection algorithm to detect various types of DDoS attacks and FEs with nearly 100% accuracy [22].

In this paper Packet Threshold Algorithm (PTA) coupled with SVM is used to detect four types of DDoS attacks such as TCP SYN flood, UDP flood, Ping of Death, and Smurf attacks with 99.1% accuracy. The incoming packets are valid packets or DDoS attacks can be detected by the Packet Threshold Algorithm and SVM technique. The packet threshold is the main criteria used here to detect DDoS attack [23].

In this article, the authors suggested a New Intrusion Detection System NIDS that can track both current and new forms of DDoS attacks. It incorporates different classifiers, i.e., MLP, SMO, IBK, J48, IBK using ensemble models, with the assumption that each classifier will address unique aspects/types of intrusions, this offers a more efficient defense mechanism towards new intrusion. A 10-folds cross-validation along with preferential voting allows us to merge these classifiers and gives 99.10% detection accuracy [24].

Here a New Intrusion Detection System NIDS is anticipated. It uses ensemble classifiers and a reduced function data set to detect a DDoS attack. The NSL-KDD dataset with a lesser number of features is used in the experiment to detect only DDoS attacks. Depending on the familiarity of the domain, they used the most significant feature that can impact only the DDoS attack [25].

A system consisting of the three key components such as classification algorithms, a hierarchical method, and a fuzzy logic system is suggested by the authors. This method picks the algorithms form the prepared algorithms list, i.e., Naive Bayes, Tree Decision (Entropy), Tree Decision (Gini), and Random Trees, which detect specific DDOS attack types using fuzzy logic technique. Naive Bayes, Tree Decision (Entropy), Tree Decision (Gini), and Random Trees, which detect specific DDOS attack types. The findings put forward that fuzzy logic can easily pick classification algorithms based on the traffic situation despite the trade-off between the accuracies of the classification algorithms used and their delays [26].

A Fuzzy estimator on the mean time between network incidents is used by the authors to detect a DDoS attack. The DDoS attack and the malicious IPs are detected by the suggested technique before the resources of the victim server get exhausted. Since the approach suggested uses the time of arrival as the key metric for discerning DDoS traffic rather than port. This approach is usually very effective in detecting the DDoS attack and relatively reliable in locating offensive IP addresses under critical time limits which enable the machine to react in real-time [27].

This paper suggests a method based on the neuro-fuzzy hybrid system. It includes a novel weight update distribution approach, and the solution varies from current weight update distribution strategy approaches, error cost minimization, and a hybrid method for ensemble efficiency. This proposed detection technique can accommodate discrete as well as continuous database attributes which are theoretically important for real-time network datasets. The most considerable contribution of this research is to provide an effective false-positive reduction approach to reduce false alarms, i.e., Neyman approach that can detect DDoS attacks with 99.20% detection accuracy [28].

In this paper, authors first analyzed data center flow correlation information. Second, he proposes an efficient identification method focused on CKNN (traffic grouping with similarity analysis of K-nearest neighbors) in DDoS attacks detection. The technique takes benefit of training correlation knowledge to enhance classification efficiency by reducing the overload-induced by training data size as this strategy is focused on flows [29].

The authors presented a novel version of the original Multiagent Router Throttling method known as Coordinated Team Learning (CTL). The most innovative aspects of the anticipated solution is that it imparts a structured, collaborative reaction to the DDoS attack problem. Hierarchical team-based communication, activity decomposition, and team rewards are integrated into this technique and are also scalable [30].

In this work, the researcher embraces a bio inspired method with enormously high speed known as Bat algorithm. The author initially identified feature metrics to determine the behavior of the demand flow is of attack or regular. Here evaluation of feature metrics done on request stream observed rather in a session at an absolute time interval. Secondly, the author uses the Bat classification algorithm to train and evaluate. The model developed in this paper is exceptionally accurate and holds the high accuracy of prediction, i.e., 94.8% [31].

The aim of the author here is to detect and mitigate known and unknown DDoS attacks in real-time environments. Authors detected TCP, UDP, and ICMP DDoS attacks depending on characteristic patterns that distinguish legitimate traffic from DDoS attacks with the help of a trained Artificial Neural Network (ANN) algorithm. The ANN learning process begins with the simulation of a network system which represents the real-life scenario. This approach gives 98% detection accuracy [32].

This work presented an incoming traffic-based Multi Layer Perceptron Genetic Algorithms MLP-GA method for application-layer DDoS attacks detection. The authors have mainly taken into account four features of incoming traffic which show momentous variations in their properties. In this paper, authors considered a system for distinguishing between an attacker, a genuine client, and a suspicious mode of all the possible combinations of the attack structures and features. In suspicious mode, the IP addresses are further authenticated using a standard CAPTCHA check [33].

In this research, the author anticipated a Bio-Inspired Anomaly-based Real-Time. Detection technique for the detection of low rated App-DDoS attacks. The Cuckoo search which is a bio-inspired methodology with the extravagant rate of search has been adopted for this paper. The overall paper contribution is split into three groups. The first involvement is to characterize feature metrics to determine whether or not the request flow is of attack intent. In this the evaluation of function metrics performed in an absolute period on the stream of queries observed. The second contribution is that the Cuckoo search hierarchical order is used to train a The second contribution is that the Cuckoo search hierarchical order is used to train and detect App-DDos attacks with 95.1% accuracy [34].

This paper provides an efficient correlation mechanism that is flexible and able to manage both changing and varying correlations between a pair of samples. The suggested NaHiDVERC manages a standard traffic profile dynamically and measures its correlation value across the action with the incoming traffic sample. Whenever the measured correlation size is lesser than a user-defined NaHiDVERC is incorporated on both software and hardware using FPGA, an attack alarm is generated. Over benchmark datasets, it can achieve 100% attack detection accuracy [35].

In this paper, incremental learning based on the data stream approach has been proposed. It is a novel hybrid method for detecting DDoS attacks. The Authors used a strategy that separates the computation overhead between customer and server sides depending on their resources to coordinate the activity at a fast speed. Divergence checking is conducted on the client-side and if divergence crosses the threshold, that means an attack is detected or data is forwarded to the server-side. On the server-side, the Naïve Bayes, random forest, decision tree, multilayer Perceptron (MLP), and K-nearest neighbors (KNN) techniques are used to obtain better detection results with 98.9% accuracy [36].

In this paper, the potential of Artificial Neural Network (ANN) for evaluating the strength of a DDoS attack is being explored. The strength of the DDoS attack is evaluated using 10, 15, and 20 sized feed-forward neural networks. For a two-layer feed-forward network, the Entropy variance and DDoS attack intensity are taken as input and output. The outcomes are quite encouraging, as the strength of a DDoS attack evaluated using a feed-forward neural network is very similar to the DDoS attack's actual strength [37].

This paper application-layer DDoS attacks are detected using a model mining. The authors also suggested a security architecture that includes a novel real-time Frequency Vector (RFV) detection approach. When detecting Application Layer DDOS (AL-DDoS) attacks, the proposed framework can quickly spot suspicious sources and utilize an effective filter to avoid the traffic that does not seems normal accurately [38].

The main objective of this paper is to demonstrate the prototype detection method for DDoS attacks. A supervised learning technique Support Vector Machines (SVM) is used for capturing network traffic, filtering HTTP headers, normalizing data based on operational variables such as false positives rate, false negatives rate, classification rate, and then send the details to the respective SVM training and testing datasets. The results indicate that the suggested SVM prototype has a high detection accuracy of 99% [39].

In this paper, the author developed a hierarchical Cuckoo Search approach. It is a bio-inspired approach with magnified search speed. The paper's overall contribution is divided into three stages. The main contribution is to find out function metrics to decide whether the request stream activity is of attack intensity or not. For this developed framework, the similarity assessment is based on the Jaccard index and the evaluation of function metrics performed on the stream of requests encountered at an absolute time interval rather than in a session. Therefore the model developed in this paper significantly minimizes the processing overhead and maintains the maximum detection accuracy [40].

The use of KD-Tree in storing packet information was also shown to be quite successful. But the approach used in this paper is independently using a specified data structure for the storage and retrieval of IP addresses. This approach does not block an IP address automatically, but it explicitly blocks the protocol. If the IP address is considered guilty then it is fully blocked. Two analyzer stages, including filter engine and classifier Particle Swarm Optimization with K Nearest Neighbors (PSO KNN), are used for testing the IP. This function is useful to an enterprise that is constantly sacrificing clients [41].

This research intended to investigate some methods of protection against DoS and DDoS attacks performed using LOIC and Slowloris, emphasizing which one is the most successful. This tool supports three types of attacks, i.e., TCP, UDP, or HTTP DDOS Attacks. The authors used SNORT method, which already has a set of rules to defend against DDoS attacks carried out using LOIC or Slowloris, the detection accuracy rate has grown with suggested new rules [42].

The issue of DDoS detection and mitigation is addressed in this paper with an improved machine learning strategic-level framework. Feature engineering and machine learning with enhancements and assessment are two important components used in the proposed framework to detect DDoS attacks that avoiding over fitting and Colinearity. Experimental data indicates that by compromising 0.3% on accuracy nearly 68% reduced feature space is possible [43].

In this study, the author suggested an efficient scheme based on the non-parametric CUSUM algorithm for the detection of DoS attacks in the application layer. This algorithm uses the actual traffic traces of DoS attacks in application-level DDOS attacks. The universal application of sampling is used by the author to verify the proposed approach's performance. The authors also provided a comprehensive study of 13 different sampling techniques constructed for diverse traffic estimation and subsequently adapted for the detection of anomalies. The sketch guided sampling method has shown the best performance [44].

3 Summary of Research Review

Tab. 1 given below summarizes the various research findings done like the method used, type of DDOS attack it can detect, detection accuracy or other observations, the dataset used, and tools used for the implementation of the method.

Table 1: Summarizes the various research findings done like the method used

S.No.	Name of the Paper	Method Used	Types of DDOS Attacks detected	Data set used	Observation /Accuracy	Ref. No.
1	A unified approach for detection of DDoS attacks using enhanced support vector machines and filtering mechanisms	Enhanced Support Vector Machines	ICMP flooding, TCP flooding, UDP flooding, Smurf flooding, port scan, land flooding, HTTP flooding, session flooding and IP flooding attacks	KDDcup 99 dataset	The attack detection accuracy is 99% in this technique	[1]
2	Detecting Distributed Denial of Service Attacks Using Data Mining Technique	Multilayer Perceptron (MLP)	Smurf , UDP Flood,SIDDOS,HTTP Flood attacks	New data set containing Smurf , UDP Flood,SIDDOS,HT TP Flood attack data	98.63% dertection accuracy has been achieved in this method	[2]
3	New Features of User' s Behavior to Distributed Denial of Service Attacks Detection in Application Layer	User Dynamism	TCP flood, UDP flood, HTTP flood,	CIC-DoS, CICIDS, and CSE-CIC-IDS and customized dataset	The detection accuracy observed in this method is 99.9%	[4]
4	A Feature Analysis Based Identifying Scheme Using GBDT for DDoS with Multiple Attack Vectors	Gradient Boosting Decision Tree	TCP flood, UDP flood detection	MAWI (Measurement and Analysis on the WIDE Internet) datasets and KDD cup 99 Dataset	Atuthors have achieved 99.97% accuracy of DDOS attack detection	[10]
5	Mining Web User Behaviors to Detect Application Layer DDoS Attacks	Hidden semi-Markov model	DDOS Attacks in Application Layer detection	Real time dataset	The authors have achieved 97% detection accuracy.	[11]
6	A Traffic Cluster Entropy Based Approach to Distinguish DDoS Attacks from Flash Event Using DETER Testbed	Traffic cluster entropy	UDP and TCP DDOS Attacks and flash event detection with	Real time dataset	It can effectively classify the FEs and DDOS attacks by considering the Cluster entropy in case of DDOS attacks increased whereas it is stable in case of FE's.	[12]
7	An IP-Traceback-based Packet Filtering Scheme for Eliminating DDoS Attacks	IP-traceback-based packet filtering scheme	DDOS Attacks	CAIDA	The presented method can effectively minimize the harm produced by DDoS attacks and keep normal traffic loss to an adequate level.	[5]

S. No.	Name of the Paper	Method Used	Types of DDOS Attacks	Data set used	Observation /Accuracy	Ref.. No.
8	Using SVM to Detect DDoS Attack in SDN Network	Support Vector Machine(SVM)	Syn flooding attack, ICMP flooding, UDP flooding attack	DARPA1999	This technique guarantees 93% attack detection accuracy	[6]
9	A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks	Flexible advanced entropy based(FAEB)scheme	HTTP-based DoS/DDoS attacks	Real time dataset	It provides an excellent alternate protective safeguards to ensure web applications from HTTP DoS / DDoS attacks of all kinds, such as high-rate DDoS (HR-DDoS) and flash crowd (FC).	[7]
10	Hybrid Intrusion Detection System for DDoS Attacks	Hybrid intrusion detection system (H-IDS)	DDOS Attacks in Application Layer detection	DARPA2000 and a commercial bank penetration test Datasets	Attack detection is with 98.7% TPR and 0.73% FPR by utilizing the proposed H-IDS	[8]
11	Entropy-Based Application Layer DDoS Attack Detection Using Artificial Neural Networks	Artificial Neural Networks	HTTP-based DoS/DDoS attacks	EPA-HTTP (environmental protection agency-hypertext transfer protocol) datasets	98.31% is the accuracy of DDOS attack.	[9]
12	Multiple-Features-Based Semi-supervised Clustering DDoS Detection Method	Multiple-Features-Based Constrained-K-Means (MF-CKM)	DDOS attack detection	DARPA	Presents a semi-supervised clustering approach for MF-CKM algorithms to detect DDoS attacks. The algorithm provided utilizes the feature vector as a function detection to decrease the detection effectiveness condition faced by the use of a single feature.	[13]
13	A UNIFIED APPROACH FOR DETECTION AND PREVENTION OF DDOS ATTACKS USING ENHANCED SUPPORT VECTOR MACHINES AND FILTERING MECHANISMS	Enhanced Support Vector Machines (ESVM) Hop Count Filtering (HCF) mechanism	TCP flooding, UDP flooding, ICMP flooding, Land flooding, HTTP flooding attacks	Real time dataset	Non spoofed IP' s are detected using Enhanced Support Vector Machines (ESVM) and spoofed IP' s are detected using Hop Count Filtering (HCF) mechanism. The detected IP' s are maintained separately to initiate the defense process.	[14]
14	A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multi-classifier Ensemble Learning	Hybrid Heterogeneous Multi-classifier Ensemble Learning	TCP flooding, UDP flooding, ICMP flooding attacks	KDD CUP 1999	This technique achieved 99.8% detection accuracy	[15]

S. No.	Name of the Paper	Method Used	Types of DDOS Attacks	Data set used	Observation /Accuracy	Ref. No.
15	Model for Detection and Classification of DDoS Traffic Based on Artificial Neural Network	Artificial Neural Network	DNS DDoS attack ,CharGen DDoS attack , UDP DDoS attack	DARPA1999	By using this method 95.6% detection accuracy can be acchieved.	[16]
16	Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning	Random Forest	TCP flood, UDP flood, and HTTP flood, as well as stealth Attacks	CICIDS2017, CSE-CIC-IDS2018 and CIC-DoS	Highest accuracy achieved is 96% using this technique	[18]
17	Validation of chaos hypothesis in NADA and improved DDoS detection algorithm	Chaos Hypothesis in NADA	DDOS Attack	DARPA1998	This technique gives 98.04% DDOS detection accuracy	[19]
18	DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy	Chaos Analysis of Network Traffic Entropy	DDOS Attacks	MIT dataset	DDOS attacks can be detected with 100% accuracy using this technique	[20]
19	An Impact Analysis: Real Time DDoS Attack Detection and Mitigation using Machine Learning	HCF coupled with support vector machine (SVM)	TCP SYN, SMURF, UDP and ICMP DDOS Attacks	real time dataset	The detection accuracy of DDOS attacks is 98.99% using this technique	[21]
20	Detection of DDoS Attacks and Flash Events using Novel Information Theory Metrics	Information Theory Metric using Generalized Information Divergence (GID) metrics	DDoS attacks and Flash Events Fes	MIT Lincoln, CAIDA, FIFA and synthetically generated DDoSTB dataset	This method can detect DDOS attacks with 100% detection accuracy	[22]
21	Detection and Defense Algorithms of Deferent Types of DDoS Attacks Using Machine Learning	Packet Threshold Algorithm (PTA) coupled with SVM	TCP SYN flood, UDP flood, Ping of Death and Smurf attacks	Synthetic data type	Highest accuracy achieved with this technique is 99.1%.	[23]

S. No.	Name of the Paper	Method Used	Types of DDOS Attacks	Data set used	Observation /Accuracy	Ref. No.
22	Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest	Based on Information Theoretic Entropy and Random Forest	HTTP DDoS attacks	CIDDS-001	This technique ensured 99.54% detection accuracy.	[24]
23	DDoS Intrusion Detection through Machine Learning Ensemble	Machine Learning Ensemble	LR DDOS and HR DDOS attacks	NSL-KDD dataset	The suggested detection algorithm detect FEs and HRDDoS attacks with 100% detection accuracy	[25]
24	DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark	Classification Algorithms Controlled by Fuzzy Logic System	Syn flooding, UDP flooding ,Ping of Death and Denial of sleep attack	CAIDA	This detection scheme detects DDOS attacks with 98% accuracy	[26]
25	Real time DDoS detection using fuzzy estimators Computers & Security	Fuzzy estimators	HTTP DDoS attacks	MIT DARPA, 2000	the proposed method can detect the DDOS attack with in the real time just in a detection window of 3 seconds	[27]
26	Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems	Ensemble of adaptive and hybrid neuro-fuzzy systems	ICMP flooding, TCP flooding and HTTP flooding attacks	KDD Cup, CAIDA DDOS Attack 2007, CONFICKER worm, UNINA traffic traces, and UCI Datasets	this methods ensures 99.2% DDOS attack detection accuracy.	[28]
27	Detecting DDoS attacks against data center with correlation analysis	Correlation analysis	TCP,UDP and ICMP DDOS attacks	KDD' 99 data set	DDOS attack detection accuracy is 100 % when selected features are 6 as the number of features become 20 accuracy decrecses	[29]
28	Distributed response to network intrusions using multiagent reinforcement learning	Multiagent reinforcement learning	DDoS attacks in small-scale network topologies	Realtime dataset	This approach is more resilient and adaptable than the existing throttling approaches which deals with the scalability challenge in an efficient way.	[30]
29	An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection	information Metrics Information Entropy and Information Distance Measure	High rate and low rate DDOS attacks	MIT Lincoln Laboratory, CAIDA and TUIDS DDoS datasets	The use of appropriate information matrixc helps to magnifythe spacing between legtimate and attack traffic for both Low Rate and High Rate DDOS attacks with very low computing overhead	[31]
30	Detection of known and unknown DDoS attacks using Artificial Neural Networks	Artificial Neural Networks	High rate and low rate DDOS attacks	New data set containing Smurf , UDP Flood,SIDDOS,HTTP Flood attack data	Accuracy of 98% is achieved with this detction method.	[32]

S. No.	Name of the Paper	Method Used	Types of DDOS Attacks	Data set used	Observation /Accuracy	Reference No.
31	HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm	Bio inspired Bat algorithm	HTTP Flood attack Detection in Application Layer	CAIDA	This method provides 94.8% detection accuracy	[33]
32	MLP-GA based algorithm to detect application layer DDoS attack	Multilayer Perceptron with a Genetic Algorithm	Application layer DDoS attack.	CAIDA 2007,KDD CUP 99 ,DARPA 2009 (FRGPNTP) 2013	98.04% detcetion accuracy can be achieved using this technique	[34]
33	BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web	Bio-inspired Cuckoo search	HTTP flood attacks	synthetic data set	This technique gurantees 95.1% DDOS attack detection accuracy.	[35]
34	Real-time DDoS attack detection using FPGA	FPGA	DDOS Attacks	CAIDA, TUIDS and DARPA	FPGA provides 100% attack detection accuracy	[36]
35	The hybrid technique for DDoS detection with supervised learning algorithms	Hybrid technique using supervised learning algorithms	UDP-Flood, Smurf, SIDDOS, HTTP-FLOOD	NSL KDDD	this framework guarantees 98.9% detection accuracy.	[37]
36	Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme	ANN Artificial Neural Network	DDOS attack strength	Real time dataset	Obeserved the potential of Artificial Neural Network (ANN) for estimating strength of a DDoS attack.	[38]
37	Detection and defense of application-layer DDoS attacks in backbone web traffic	Real time Frequency Vector	Application-layer DDoS attacks nd Flash Crowd	Realtime dataset	This method is capable of being deployed in the traffic of backbone and can effectively distinguish between the AL -DDOS attacks and Flash Crowd	[39]
38	Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype	Support Vector Machine(SVM)	DDOS attacks	DARPA	99% DDOS attack detection accuracy can be cahieved by this technique	[40]
39	BIFAD: Bio-Inspired Anomaly Based HTTP-Flood Attack Detection	Bio-inspired Cuckoo search	HTTP ,application layer DDOS attack	JMETER Dataset	It provides 99.5% DDOS attack detection accuracy	[41]

S. No.	Name of the Paper	Method Used	Types of DDOS Attacks	Data set used	Observation /Accuracy	Ref. No.
40	DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks	Particle Swarm Optimization with K Nearest Neighbours (PSO KNN)	High rate DDOS (HDDOS) Attacks	CAIDA 2007, 2013; MIT Lincoln Laboratory Datasets 1999) and Tezpur University (TU) DDoS	The detection accuracy of 99.95% is achieved by suggested technique	[42]
41	An Approach for Detecting and Preventing DDoS Attacks in Campus	SNORT Intrision Detection Tool with additional features	TCP, UDP or HTTP attacks	Real time dataset	45 % better accuracy than previours LOIC abd Slowris Models	[43]
42	DDoS attack detection with feature engineering and machine learning: the frame work and performance evaluation	Feature engineering and Machine learning Algorithms	HTTP flood, UDP flood, Smurf, and Normal	KDD, CAIDA, NSL-KDD, ISOT, and ISC	68% reduction in feature make 0 .03% impact on accuracy of DDOS attacks	[44]
43	Detecting HTTP-based Application Layer DoS attacks on Web Servers in the presence of sampling	CUSUM algorithm	Application layer DoS attacks	ISCX dataset	It presents a novel detection approach for application layer DDOS attack detection nonparametric CUSUM algorithms	[45]
44	User behavior analytics-based classification of application layer HTTP-GET flood attacks	User behavior analytics and SVM classifier	HTTP-based DoS/DDoS attacks	WorldCup98, Clarknet, and NASA and University	This technique ensures 97.4% of detection accuracy.	[46]

Evaluation Matrices Used:

- Precision (Pr) or Positive Predictive value: It is the ratio of correctly classified attacks flows (TP), in front of all the classified flows (TP+FP).
- Recall (Rc) or Sensitivity: It is the ratio of correctly classified attack flows (TP), in front of all generated flows (TP+FN).
- F-Measure (F1): It is a harmonic combination of the precision and recall into a single measure [45].

$$Rc = \frac{TP}{TP+FN}$$

$$Pr = \frac{TP}{TP+FP}$$

$$\mathrm{F} = \frac{2}{\frac{1}{Rc}+\frac{1}{Pr}}$$

- Accuracy: Accuracy (ACC) is defined by equation 6. and it is calculated as the number of all correct predictions divided by the total number of packets in the data set [46].

$$ACC = \frac{TP+TN}{TP+TN+FP+F}$$

4 Challenges Associated with Ddos Detection

- Growing Internet and availability of insecure IoT devices
- Challenge to establish a trade-off between the efficiency of online (real-time) security strategies and the use of victim resources
- Interoperability of the devices
- Zero-day attack

The accelerating growth of the Internet and the introduction of insecure IoT gadgets are a serious challenge to the modern cyber world. Most recent massive DDoS attacks are carried by IoT botnets. The consumers of such large networks are often not conscious of the protection of their applications. The key protection against the development of such a massive botnet is to guarantee the safety of the system from the consumer.

Making sure the defense against IoT-based DDoS attacks is an enormously significant field of research in which several specific unanswered problems are requiring particular consideration. Avoiding the development of IoT botnets, detecting and rejecting flows from non-sophisticated IoT devices (like surveillance cameras, intelligent refrigerators, home routers) are a few examples of concerns in which more research work needs to be done.

It is still difficult to establish a trade-off between the efficiency of electronic (real-time) security strategies and usage of consumer services. Because DDoS attacks have already placed a significant strain on the victim's network infrastructure (processing capacity, storage, and bandwidth), it is also very important to make sure the accurate results of DDoS protection techniques. In other words, it is necessary to maintain the minimum use of the victim's assets through protection mechanisms when combating DDoS. It is an incredibly critical research direction as the greatest-performance defense method guarantees minimal downtime.

The interoperability is also another problem identified in the DDoS study. DDoS attacks include a variety of attack scenarios and fingerprints. The authors are however attempting to establish the absolute best response in the light of the various dimensions of the attacks. It is quite necessary to check the real-life output of such work. It is therefore important to check the output in real-time because various methods operate together to address the challenge in various situations. Predetermined datasets and stabilized attack signatures make the real-life attack environment quite divergent from the test environment. Hence interoperability of the protection methods in real-time attack scenarios must be ensured [47].

There will always be a research concern on how to protect against a zero-day attack. DDoS attackers are often focusing on introducing new kinds of attacks of enhanced strength and sophistication. Analysis to protect against such a zero-day attack is thus the most complicated. Along with massive technical skills, this analysis often involves understanding the mentality of attackers and the abilities that carry forth new kinds of DDoS attack.

5 Research Gaps

After the existing literature review, the following research gaps are drawn to plan our future framework for three-fold contribution such that:

- Almost all of the researchers used publicly accessible real data sets to authenticate their suggested methods. They used the KDD cup 99 and CAIDA dataset mostly for DDOS traffic in their researches. These datasets are outdated and the proposed model may not identify recent DDOS attacks efficiently.
- In order to simulate heterogeneous and scalable traffic of DDoS attack there is a prime requirement of realistic and updated datasets.
- To distinguish between DDoS attack and FC flooding attacks more research is required.
- There is a need to combine potential DDoS defensive methods in one Cyber security platform to come up with a realistic solution to the DDoS attack.
- It is noticeable that even after various research efforts to detect DDoS attacks with machine learning techniques we lack a strategic approach to implement such methods so that thorough assessment can avoid generally embedded difficulties such as colinearity, multicollinearity, and duplication associated with machine learning-based data.
- When we try to apply Computational Intelligent Techniques almost all the important aspects of data science-driven methods have to be integrated. The simple execution of a framework with default parameters is not sufficient but instead, it introduces the over fitting elements.
- There is also a need to combine the feature engineering framework with intelligent techniques as we have seen that a lesser number of features by an algorithm is used then detection of DDOS attacks if more efficient, therefore it is necessary to use them simultaneously in all-inclusive experiments and reliable results.
- The presented systems are widely designed to visualize static network traffic data, these systems have the potential of collecting and storing network traffic data, but a mechanism for handling real streaming data from all sources needs to be developed so that we can detect the DDoS attack in real-time.
- Detection of Encrypted header DDOS attacks in real-time is still a challenge as there is not an efficient method to detect it.

6 Conclusions

A survey of various techniques to detect DDOS attacks has been conducted in this paper. Which type of detection method should be implemented for an empirical situation is quite complex and difficult to discern. With the low false notification, few frameworks can recognize known attacks only and lead to higher detection accuracy, but the attacker can amend the attack signatures quickly or can launch the attack with little modification. Thus the attacks remain unidentified by these techniques. A significant obstacle in DDOS attack detection is the analysis and manipulation of enormous amounts of online data, and the growing false signal ratio due to the existence of data uncertainty. The survey has taken into account DDOS attack detection and defense strategies in web applications web services cloud computing and any device that has internet. This survey paper offers a comprehensive review of computational intelligent techniques that are being used in detection and prevention from DDOS attacks from the accretion of the work already being done. The research paper also enlisted the challenges associated with the DDoS attacks detection and prevention. Finally the paper identifies various research gaps that can contribute to the future work

Future Directions: We will work on building a defense mechanism for encrypted header attacks which is closer to the source of the attack with avoidable assistance of different service providers. We strongly believe that the best and most efficient technique to combat DDoS attacks might be an optimal, complete,

and accurate real-time defensive system. Our detection algorithm could also distinguish between DDOS attacks and Flash Events (FEs).

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Subbulakshmi, P. Parameswaran, C. Parthiban, M. Mariselvi, J. A. Anusha *et al.,* "A unified approach for detection of DDoS attacks using enhanced support vector machines and filtering mechanisms," *ICTACT Journal on Communication Technology*, vol. 4, no. 2, pp. 737, 2014.

[2] M. Alkasassbeh, G. Al-Naymat, A. Hassanat and M. Almseidin, "Detecting distributed denial of service attacks using data mining techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 1, pp. 436–445, 2016.

[3] D. Beckett and S. Sezer, "HTTP/2 Tsunami: Investigating HTTP/2 proxy amplification DDoS attacks," in *2017 Seventh Int. Conf. on Emerging Security Technologies*, 2017.

[4] S. Bravo and D. Mauricio, "New features of user's behavior to distributed denial of service attacks detection in application layer," *International Journal of Online Engineering*, vol. 14, no. 12, pp. 164–178, 2018.

[5] J. Zhang, Q. Liang, R. Jiang and X. Li, "A feature analysis based identifying scheme using GBDT for DDoS with multiple attack vectors," *Applied Sciences*, vol. 9, no. 21, 2019.

[6] C. Huang, J. Wang, G. Wu and J. Chen, "Mining web user behaviors to detect application layer DDoS attacks," *Journal Software*, vol. 9, no. 4, pp. 985–990, 2014.

[7] M. Sachdeva and K. Kumar, "A traffic cluster entropy based approach to distinguish DDoS attacks from flash event using DETER testbed," *International Scholarly Research Notices Communications & Networking*, 2014.

[8] Y. Wang and R. Sun, "An IP-traceback-based packet filtering scheme for eliminating DDoS attacks," *Journal of Networks*, vol. 9, no. 4, pp. 874–881, 2014.

[9] D. Li, C. Yu, Q. Zhou, and J. Yu, "Using SVM to detect DDoS attack in SDN network," *IOP Conference Series: Materials Science and Engineering*, vol. 466, no. 1, 2018.

[10] M. A. Saleh and A. Abdul Manaf, "A novel protective framework for defeating HTTP-based denial of service and distributed denial of service attacks," *The Scientific World Journal*, 2015.

[11] K. J. Singh, K. Thongam and T. de, "Entropy-based application layer DDoS attack detection using artificial neural networks," *Entropy*, vol. 18, no. 10, 2016.

[12] Ö. Cepheli, S. Büyükçorak, and G. Karabulut Kurt, "Hybrid intrusion detection system for DDoS attacks," *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[13] Y. Gu, Y. Wang, Z. Yang, F. Xiong and Y. Gao, "Multiple-features-based semisupervised clustering DDoS detection method," *Mathematical Problems in Engineering*, vol. 2017, 2017.

[14] T. Subbulakshmi, K. Balakrishnan, S. M. Shalinie, D. Anandkumar, V. Ganapathisubramanian *et al,* "Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset," in 2011 *Third Int. Conf. on Advanced Computing*, pp. 17–22, 2011.

[15] B. Jia, X. Huang, R. Liu and Y. Ma, "A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning," *Journal of Electrical and Computer Engineering*, vol. 2017, 2017.

[16] D. Peraković, M. Periša, I. Cvitić and S. Husnjak, "Model for detection and classification of DDoS traffic based on artificial neural network," *Telfor Journal*, vol. 9, no. 1, pp. 26–31, 2017.

[17] K. Singh, S. Paramvir and K. Krishan, "User behavior analytics-based classification of application layer HTTP-GET flood attacks," *Journal of Network and Computer Applications*, pp. 97–114, 2018.

[18] F. S. de Lima Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar and L. F. Silveira, "Smart detection: an online approach for DoS/DDoS attack detection using machine learning," *Security and Communication Networks*, vol. 2019, 2019.

[19] X. Wu and Y. Chen, "Validation of chaos hypothesis in NADA and improved DDoS detection algorithm," *Institute of Electrical and Electronics Engineers Communications Letters*, vol. 17, no. 12, pp. 2396–2399, 2013.

[20] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," *Institute of Electrical and Electronics Engineers communications letters*, vol. 18, no. 1, pp. 114–117, 2014.

[21] B. S. Kiruthika Devi, G. Preetha, G. Selvaram and S. Mercy Shalinie, "An impact analysis: real time DDoS attack detection and mitigation using machine learning," in *Int. Conf. on Recent Trends in Information Technology*, 2014.

[22] S. Behal and K. Kumar, "Detection of DDoS attacks and flash events using novel information theory metrics," *Computer Networks*, vol. 116, pp. 96–110, 2017.

[23] M. A. M. Yusof, F. H. M. Ali and M. Y. Darus, "Detection and defense algorithms of different types of DDoS attacks," *International Journal of Engineering Science*, vol. 9, pp. 5, 2017.

[24] M. Idhammad, K. Afdel and M. Belouch, "Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest," *Security and Communication Networks*, vol. 2018, 2018.

[25] S. Das, D. Venugopal and Shiva, "A holistic approach for detecting ddos attacks by using ensemble unsupervised machine learning," in *Future of Information and Communication Conf.*, 2020.

[26] A. Alsirhani, S. Sampalli and P. Bodorik, "DDoS attack detection system: Utilizing classification algorithms with apache spark," in *2018 9th IFIP Int. Conf. on New Technologies, Mobility and Security*, pp. 1–7, 2018.

[27] S. N. Shiaeles, V. Katos, A. S. Karakos and B. K. Papadopoulos, "Real time DDoS detection using fuzzy estimators," *Computer Security*, vol. 31, no. 6, pp. 782–790, 2012.

[28] P. Arun Raj Kumar and S. Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems," *Computer and Communications*, vol. 36, no. 3, pp. 303–319, 2013.

[29] P. Xiao, W. Qu, H. Qi and Z. Li, "Detecting DDoS attacks against data center with correlation analysis," *Computer Communications*, vol. 67, pp. 66–74, 2015.

[30] K. Malialis and D. Kudenko, "Distributed response to network intrusions using multiagent reinforcement learning," *Engineering Applications of Artificial Intelligence*, vol. 41, pp. 270–284, 2015.

[31] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection," *Pattern Recognition Letters*, vol. 51, pp. 1–7, 2015.

[32] A. Saied, R. E. Overill and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385–393, 2016.

[33] K. J. Singh and T. De, "MLP-GA based algorithm to detect application layer DDoS attack," *Journal of Information Security and Applications*, vol. 36, pp. 145–153, 2017.

[34] K. M. Prasad, A. R. M. Reddy and K. V. Rao, "BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web," *Journal of King Saud University–Computer and Information Sciences*, vol. 32, no. 1, pp. 73–87, 2020.

[35] N. Hoque, H. Kashyap and D. K. Bhattacharyya, "Real-time DDoS attack detection using FPGA," *Computer Communications*, vol. 110, pp. 48–58, 2017.

[36] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Computer Networks*, vol. 158, pp. 35–45, 2019.

[37] P. K. Agrawal, B. B. Gupta, S. Jain and M. K. Pattanshetti, "Estimating strength of a DDoS attack in real time using ANN based scheme," *International Conference on Information Processing*, vol. 157 pp. 301–310, 2011.

[38] W. Zhou, W. Jia, S. Wen, Y. Xiang and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic," *Future Generation Computer Systems*, vol. 38, pp. 36–46, 2014. DOI 10.1016/j.future.2013.08.002.

[39] M. S. H. Li, J. I. Vélez and L. Castillo, "Distributed denial of service (ddos) attacks detection using machine learning prototype," in *13th Int. Conf. on Distributed Computing and Artificial Intelligence*, 2016, pp. 33–41.

[40] K. M. Prasad, A. R. M. Reddy and K. V. Rao, "BIFAD: bio-inspired anomaly based HTTP-flood attack detection," *Wireless Personal Communications*, vol. 97, no. 1, pp. 281–308, 2017.

[41] D. Boro and D. K. Bhattacharyya, "DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks," *Microsystem Technologies*, vol. 23, no. 3, pp. 593–611, 2017.

[42] M. Merouane, "An approach for detecting and preventing DDoS attacks in campus," *Automatic Control and Computer Sciences*, vol. 51, no. 1, pp. 13–23, 2017.

[43] M. Aamir and S. M. A. Zaidi, "DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation," *International Journal of Information Security*, vol. 18, no. 6, pp. 761–785, 2019.

[44] S. M. Mallikarjunan, K. N. Bhuvaneshwaran, A. Sundarakantham and K. Shalinie, "DDAM: detecting DDoS attacks using machine learning approach," *Computational Intelligence: Theories, Applications and Future Directions*, vol. 1, pp. 261–273, 2019.

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

[46] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861–874, 2006.

[47] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *Institute of Electrical and Electronics Engineers Access,* vol. 7, pp. 51691–51713, 2019.