IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 19, 2019, accepted March 14, 2019, date of publication April 16, 2019, date of current version April 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2908998

Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods

BASHAR AHMED KHALAF[1], SALAMA A. MOSTAFA[1], AIDA MUSTAPHA[1], MAZIN ABED MOHAMMED[2], AND WAFAA MUSTAFA ABDULLAH[3]

[1]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat 86400, Malaysia
[2]Planning and Follow-Up Department, University of Anbar, Anbar 31001, Iraq
[3]Faculty of Computers and IT, Nawroz University, Duhok 44001, Kurdistan Iraq

Corresponding author: Salama A. Mostafa (salama@uthm.edu.my)

This work was supported by the Universiti Tun Hussein Onn Malaysia (UTHM) under GPPS Vot H372, and in part by the Postdoctoral Research Grant Scheme of UTHM under Vot D004.

ABSTRACT Until now, an effective defense method against Distributed Denial of Service (DDoS) attacks is yet to be offered by security systems. Incidents of serious damage due to DDoS attacks have been increasing, thereby leading to an urgent need for new attack identification, mitigation, and prevention mechanisms. To prevent DDoS attacks, the basic features of the attacks need to be dynamically analyzed because their patterns, ports, and protocols or operation mechanisms are rapidly changed and manipulated. Most of the proposed DDoS defense methods have different types of drawbacks and limitations. Some of these methods have signature-based defense mechanisms that fail to identify new attacks and others have anomaly-based defense mechanisms that are limited to specific types of DDoS attacks and yet to be applied in open environments. Subsequently, extensive research on applying artificial intelligence and statistical techniques in the defense methods has been conducted in order to identify, mitigate, and prevent these attacks. However, the most appropriate and effective defense features, mechanisms, techniques, and methods for handling such attacks remain to be an open question. This review paper focuses on the most common defense methods against DDoS attacks that adopt artificial intelligence and statistical approaches. Additionally, the review classifies and illustrates the attack types, the testing properties, the evaluation methods and the testing datasets that are utilized in the methodology of the proposed defense methods. Finally, this review provides a guideline and possible points of encampments for developing improved solution models of defense methods against DDoS attacks.

INDEX TERMS DDoS attack, DDoS defense, artificial intelligence technique, statistical technique.

I. INTRODUCTION

Distributed Denial of Service (DDoS) attack is an intimidation trial flooded on the Internet. In DDoS attack, the network bandwidth represents victims' computer machines and resources that are depleted for sending of numerous packets toward a targeted server [1]. DDoS attack programs have been existing for quite some time, and various defense mechanisms and methods are available for countering preceding single-source of the attacks. Using a single or limited number of servers for a DDoS attack is not effective [3]. The source of these attacks with the help of tracking capabilities can be detected, identified and blocked or rejected [2]. However, due to the exponential growth of Internet usage in the last decade, attackers can select from a vast amount of vulnerable systems (hosts) and use them to start their attacks [4].

Two main steps are needed to generate DDoS attack on a system. The first step involves malicious packets sent by an attacker to victims' machines to disturb protocols or running applications, i.e., vulnerability attack that creates zombies [5]. Trojan horses, backdoors, or worms are usually used to recruit zombies [8], [9]. The second step involves the attacker use these zombies to activate flooding attacks by exhausting a server or network resources including bandwidth, memory, router's processing capacities, disk/database [6]. The DDoS attack disrupts the attacked

The associate editor coordinating the review of this manuscript and approving it for publication was Yin Zhang.

system and the services that are provided by the system to legitimate users.

DDoS attacks are launched via remotely controlled, well-organized, and widely distributed zombies' botnet computers in a network. Many traffic or service requests are simultaneously or continuously sent to the target system. The target system becomes unusable, responds slowly, or crashes completely due to the attack [7]. The identification of the original attackers is difficult for the defense methods because the attackers have spoofed IP addresses and covered within the zombies that are under their control [5]. In 2009, many zombies are used to overwhelming a victim through a DDoS attack, thereby disrupting network services for popular websites, such as Facebook, Live Journal, Twitter, and Amazon [10].

Early DDoS attacks are mostly manual, and attackers must execute several steps, including detecting compromised machines to generate zombies on the Internet, port scanning, and deploying malware, before the launch of the final attack. At present, DDoS attack tools have become automated and sophisticated, thereby allowing attackers to execute all or a few of the steps automatically with minimal human effort [11]. Attackers can also configure parameters specific to the target, whereas the rest can be managed via automated tools. These automated attack tools include Trinoo, Tribe Flood Network (TFN), TFN2K, Trinity, Knight, and Stacheldraht, most of which work on Internet Relay Chat (IRC), in which compromised machines and zombies can communicate indirectly without having to disclose their identities [2]. Other attack tools are mostly agent-based, in which zombies and handlers communicate directly given knowledge of each other's identities. Flash Crowds (FC) is described as a kind of network traffic that is similar to DDoS traffic, but it comes from legitimate users [12]. FC is like DDoS attack in terms of many users gain access to a system simultaneously. In FC there is an abnormal and sudden rise in legitimate traffic because of special events such as publishing of the Olympics schedule or companies' new products like new smartphones of Samsung or Apple. The consequence of this is an early delivery response through web service, which may require prevention actions. It is difficult for defensive systems to distinguish between FC abnormal traffic from DDoS attacks because they vary in a few parameters only [13]. The parameters are low rate, infrequent arrivals and long inter-session pauses.

Many well-established review and survey articles on DDoS attack and defense methods are available in the literature including [12], [14]–[17] and [18]. The review of Behal *et al.* [12] concentrates on defense methods that distinguish between DDoS and FC. The review of Douligeris and Mitrokotsa [14] focuses on statistical defense methods. The review of Aamir and Zaidi [15] presents numerous techniques that are used in DDoS attack methods. The review of Behal and Kumar [16] focuses on the most common datasets of DDoS attack and evaluation methods. The review of Somani *et al.* [17] emphasizes various DDoS

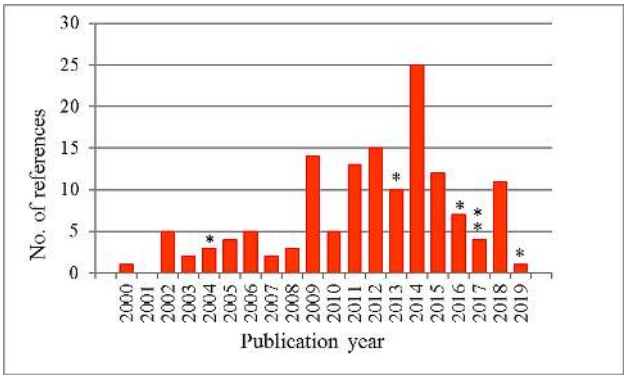

FIGURE 1. An overview of the reviewed articles.

defense methods in cloud computing. Recently, the review of Rao *et al.* [18] considers the Internet Service Provider (ISP) domain to investigate the deployment of the techniques that are used in DDoS attacks. Figure 1 shows the number of articles that are discussed in this review based on the publication year, whereas $*$ denotes the number of review articles in a particular year.

This paper offers a thorough and detailed review of various techniques for detecting and preventing DDoS attacks, according to artificial intelligence and statistical approaches that are feasible at Open Systems Interconnection (OSI) layers model. A total number of 129 research articles, 6 network security reports, 10 link of datasets and 6 review articles are covered in this review. The review investigates the defense methods that are deployed for detecting, mitigating, and/or preventing DDoS attacks. It classifies DDoS defense methods according to the class of vulnerability, the degree of automation, impact, and dynamics. The classification emphasizes a tangible view for many types of DDoS attack and DDoS defense methods and provides tables of relations. Moreover, this review includes a common testing datasets and evaluation methods. This review aims to improve the scope and shape the direction of DDoS research. It outcomes some open research challenges and provides a few suggestions for future research.

This review paper is organized into eight sections, starting with the Introduction. Section II illustrates the DDoS attack and outlines the backdrop and motivation behind such attacks. Section II categorizes the most common kinds of DDoS attacks. Section IV reviews the defense methods. Section V emphasizes and compares different evaluation approaches used for DDoS experimentation. Section VI provides a review of real, publicly available datasets on specific attributes. Section VII presents the analysis and discussion and Section VIII presents the conclusion of the paper.

II. DISTRIBUTED DENIAL OF SERVICE ATTACK

DDoS attacks have become a global menace for today's Internet. These attacks are dexterous in nature and use the same techniques of regular DoS attacks except that the former is carried out at a greater scale than the latter via botnets [14]. A botnet chain includes hundreds or thousands of compromised (bots, zombies, or slave agents) that are remotely

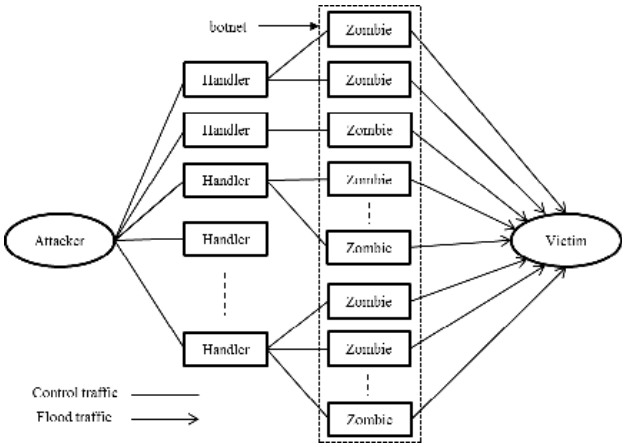

FIGURE 2. The DDoS attack architecture.

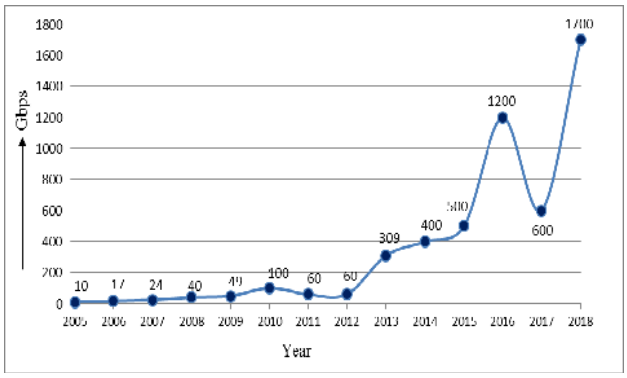

FIGURE 3. The average strength of DDoS attacks (28, 29 and 30).

controlled by one or more intruders attacking a victim. For the attackers, each computer connected to the Internet presents an attractive opportunity to create zombies and mostly without their users' knowledge. Zombies are enrolled with the help of worms, Trojan horses, or backdoors with the sending of a captivating link, e-mail content, or a trust-inspiring sender address to vulnerable machines [4].

Basically, an individual attacker or a group of attackers implements different hacking techniques to exploit the vulnerability and weaknesses of computer machines connected to the Internet. Thereby planting malicious codes that placing these computers in a vulnerable spot and assume control over these machines [4]. Some of these machines are configured as ''handlers'' and others are configured as ''zombies''. The attackers control the handlers while the handlers' software controls the zombies. The attackers attempt to control as many computer machines as possible before starting the attack. The numbers of zombies could reach hundreds or even thousands. Successively, the large groups of zombies form a ''botnet'' of the attacks as shown in Figure 2. The botnet size determines the level and magnitude of the attack's intensity. A large botnet performs disastrous and severe attacks [1].

A single zombie provides a small amount of data. However, the cumulative traffic from numerous zombies that emerge at end users' systems is enormous and thus exhausts resources. Low-rate DDoS attacks are dangerous and difficult to expose because the traffic that can be controlled by a particular link manifests as normal [19]. Thus, prevailing detection methods can result in a rapid increase in high-rate DDoS attacks. DDoS attacks are currently launched in the form of link and packet flooding. Such type of attacks has increased drastically on the Internet because attackers already know what, where, and how information is obtained. Attackers can easily launch such attacks because Internet protocols, operating systems, and web applications are constantly exposed to vulnerability. Such attacks are designed with motives, such as blackmail (to gain profit through extortion), hacktivism (to gain media attention), economic reasons (nastiness), personal reasons (disputes or revenge), and political reasons. The most usual targets for such outrageous attacks are web applications including media, gaming, online shopping and social portals [4].

DDoS attacks consider as a major threat facing web applications [20]. There are massive attacks of DDoS which are repeatedly targeted at several organizations like CNN, Amazon, Buy.com and eBay [21], [22]. In 2010 and 2011, almost 2,500 organization having 75,000 computers systems are affected by DDoS attacks in more than 100 countries with 4 million computers are attacked [20]. On a daily basis, over 7,000 DDoS attacks are launched. The number of attacks that are recorded in the first quarter of 2013 has reached 48.25Gbps, being 718% more than that of the previous year of 2012 [23]. The highest number of DDoS attacks recorded increased by about 1,000% from 40 Gbps in 2008 to 400+ Gbps in 2013. On average, these kinds of attacks occur almost 3,000 dailies. A Survey carried out by [24] revealed that on a yearly basis DDoS attacks increase by 111%. About 85% of attacks are mitigated by VeriSign network security in the fourth quarter of 2014.

In 2015, the volume of attack recorded is about 500 Gbps, and it disrupted the whole ISP network in Kenya [25]. More so, in the first quarter of 2016 BBC encountered a website attack of 602 Gbps DDoS [26]. Records by [27], showed that the biggest DDoS attacks that occurred in October 2016 are that which makes use of a novel Mirai botnet, and the attacks are targeted at Dyn servers. These servers belong to an American company engaged in the majority of the Domain Name System (DNS) infrastructure. Mirai is the main source of IoT devices attacks like digital cameras and DVR players. An estimate given by Dyn of the unusual strength of the attack is placed at 1.2 terabits (1,200 Gbps) with about ''100,000 intricate malicious agents in [28].'' As noted by [29], [30] the largest attack involving 600 Gbps occurred in 2016. In the history of DDoS attacks, the largest DDoS attack of 1.7 Tbps is targeted at North America. Figure 3 presents the average strength of the DDoS attacks.

There exist two kinds of DDoS attacks which are known as vulnerability and flooding [4], [31]. Flooding attacks involve the setting of an army of zombies by an intruder to attack packets that are headed towards their destination. This is

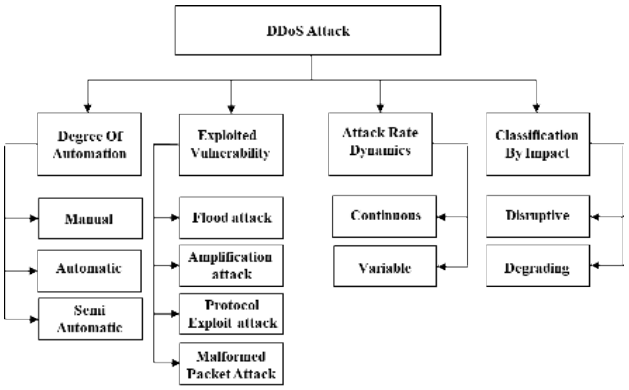

FIGURE 4. The classification of the DDoS attack.

aimed at increasing the traffic to an amount which the victim and his/her system cannot control, thereby resulting in the crashing of the victim's system [4]. Based on the method of attack, flooding attacks have been classified by [32] as direct and indirect (through reflectors) DDoS. Another classification given is that given by [17], who classified these attacks based on the protocol level that is affected; these authors classified them as Net DDoS and App-DDoS flooding attacks.

III. THE APPROACHES OF DDoS ATTACK

Proper classification is essential for recognizing DDoS attacks. Figure 4 shows a classification of the DDoS attack approaches. The approaches cover the degree of automation, exploited the vulnerability, attack rate dynamics, and impact [14], [17], [33]–[35], and [36]. Each of these approaches represents a set of attack methods. The approaches of DDoS attack are illustrated in the following points.

A. AUTOMATION DEGREE OF DDoS ATTACK

In terms of automation degree of attack, DDoS attacks can be classified as manual, semi-automatic and automatic. These categories of attacks are briefly discussed below:

- The manual DDoS attack involves the detection of loop-holes in virtual machines, penetrating them and installing attack codes. They are often executing a lot of time over other kinds of DDoS attacks. The semi-automatic and automatic DDoS attacks are employed in the subsequent of this manual attack.
- The semi-automatic DDoS is preceded by inserting the agents'/handlers' scripts into some other machines that have been compromised and possessed by the hacker/attacker. The semi-automatic attack includes two steps. The first step is made by the attacker which involves setting the type of the attack, selecting the address of the victim and organizing the attack timing/waives of the handlers' machines. The second step is deploying the handlers to automatically controlling the zombies and running the attack. The attack might be controlled through direct communication, indirect communication or both of them. The direct communication entails incorporating IP address hardcoding into the machines of the handlers. The key weakness related to direct communication is that the whole DDoS network can be revealed with the discovery of one zombie. It is because the IPs of the handlers are dynamically exchanged. Attacks which are launched in indirect communication involves the use of indirection to enhance the survival of DDoS attacks. A classic example of indirect communication is presented in the IRC-based model of DDoS attack [33].
- In the automatic DDoS attacks a periodic attack is initiated by just a single command. Here, the communication between the attack machines and the attacker are indirect. More so, pre-planning and programming of the attack attributes such as determining the beginning of the attack, setting the type of the attack, selecting the address of the victim and organizing the attack timing/waives of the handlers' machines are performed in the attack code. This way, there is only little contact from the attacker. Hence, in this type of attacks, it is difficult to discover the identity of the attacker. The main weakness of this attack is that the propagation of the attack leaves the back door of the attacker open for the zombies to trap the attacker and performs a counterattack.

B. EXPLOITED VULNERABILITY OF DDoS ATTACK

Based on the exposure that is taken advantage of, DDoS attacks can be classified as follows, protocol exploits malformed packet attacks and amplification.

- A flooding attack involves congesting the victim's system with bandwidth through the transmission of a large amount of traffic to the victim's system. If this occurs the victim's system may go through reduced speed, system breakdown or even saturation of bandwidth. Flooding attacks include User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP). In UDP attack, it is possible to transmit a large amount of UDP packets to the system of the victim, thereby leading to saturation of network and reduced availability of bandwidth for authorized service in the victim's system. UDP-based DDoS attack involves the transmission of UDP packets to ports of the victims' machines in a random or precise manner [37]. Conversely, a UDP-based flooding attack entails the random transmission of UDP packets to the ports of the victims' machines. The name of the application which is waiting in the port of the destination system is resolved by the victim's machine which receives the UDP packet. In an instance that no application is found to be waiting at the destination port, the fake address is provided with an ICMP packet of ''destination unreachable''. When UDP is adequately transmitted, the attacked machines then breakdown. The source IP address of the attacker can encounter spoofing, and this prevents the disclosure of the other victims' identities. In this event, the packets which have been sent back to the victim's system

are not transmitted back to the zombies through the use of a DDoS tool. The exploitation of ICMP-based flooding attacks occurs because the transmission of echo packets to a remote host for status verification by users is allowed in the ICMP. Specifically, when an ICMP-based DDoS flooding attack is launched, the large amounts of ICMP-ECHO-REPLY (ping) are sent to the system of the victim. These packets request for a response from the system of the victim, causing the saturation of bandwidth in the victim's network [38]. There is a high chance of the source's IP address to be spoofed when an ICMP-based attack is launched.

- When amplification attacks are launched, the features of the broadcast IP address are exploited by the attacker; the broadcast IP address is usually found on many routers. This enables the strengthening and reflection of the assault and transmission of messages towards a broadcast IP address. The routers are commanded to transmit the packets outside the network to each of the IP addresses that are found within the range of the broadcast address. Through this, the bandwidth of the victim's system decreases as a result of the extra traffic that has been generated. With this kind of DDoS attacks, the direct or indirect transmission of the broadcast message by the attacker is initiated so as to increase the traffic. When the broadcast message is directly transmitted, systems which are within the range of broadcasting network are used by the attacker without requiring the installation of any software agent. Some popularly known attacks include Smurf and Fraggle attacks. In these attacks, reflectors are the agent nodes that are used as launchers [39]. Any packet that is received by the reflector node is sent back. Therefore, DNS and web servers and routers are regarded as reflectors because they send back SYN ACKs or RSTs acknowledging SYN or other TCP packets. Packets which require acknowledgements are sent by the attacker to the reflectors. These packets spoof the address by means of the addresses of the source set to the victim's address. Reply packets are sent back by the reflectors to the victim depending on the type of packet attack. The packets used for the attack are essentially sent back in the regular packets to the victim. If the packet which is returned is considerably large, it can cause the victims' link to overflow. In the attacker packets that are received by the victim's system, it easy to recognize the reflectors as the source address. In addition, the slave which is transmitting the packets to the reflector cannot be identified by the reflector's operator, because the source address of the slave is not contained in the packets that are transmitted to the reflector, rather, it is the source address of the victim that is contained therein. The pattern of attack of the reflector attacks is similar to the one used for direct attacks. However, some notable variations exist [40]. A reflector attack needs a set of reflectors that have been prearranged. Reflectors can be spread using the internet because no installation of a software agent is required.
- The use of route-based methods cannot be employed in sorting reflected packets because they usually have verified source addresses. Smurf attacks entail the sending of an ICMP echo traffic request alongside the source address of a spoofed target victim to a specific broadcast IP address. ICMP echo requests are often received by most of the hosts that are present on an IP network [41], which then responds to the source address being the target victim in this situation. It is possible for hundreds of machines within a broadcast network to respond to each ICMP packet. The amplifier is a term used to describe the collection of several replies from a single packet using the network [42]. With this kind of attack, the damaged party which is regarded as the target victim source address is also regarded as an intermediate broadcast instrument (amplifier). The differences between Fraggle attacks and Smurf attacks are minor; one of such difference is that in Fraggle attacks, the use of UDP echoes rather than ICMP echoes is employed. More so, more dangerous traffic capable of causing more harm is produced by Fraggle as compared to Smurf attacks.
- In protocol exploit attacks, a specific attribute or the implementation bug of a certain protocol existing in the victim's system is taken advantage of, so that its extra resources can be consumed. A classic example of these kinds of attacks is TCP-SYN.
- TCP-SYN-based attacks take advantage of the natural limitations of the three-way handshake that is found in the setup connection of TCP. A server returns as an SYN/ACK (synchronize/acknowledge) echo packet and waits for the client after the first SYN (synchronize/start) request has been accepted by a client to transmit the ending ACK (acknowledge) packet. A SYN-based flooding attack is initiated by an attacker through the transmission of a large number of SYN packets without acknowledging the responses. This causes the server to wait for ACKs that do not exist [43]. By means of SYN-based flooding attack, the server becomes unable to process other requests because queue overloading occurs in the servers with a limited queue for buffering new links [44]. Some of the popularly known protocol exploit attacks that attack authentication servers include PUSH +ACK attacks.
- Attacks with malformed packets (malformed packet attacks) [45]: this kind of attack is reliant on IP packets that have been wrongly produced and transmitted from the agents to the victim's system with the aim of shutting it down. The basic categories of these attacks are IP packet and IP address attacks in which the destination of the IP packet and IP address is the same. For this reason, the OS of the victim's system is becoming confused and then crashes. In an IP packet attack, ill-formed packets may jumble the optional fields in the IP packet and set each of the quality bits to 1. Accordingly, the additional

traffic analysis time is then forcefully consumed by the victim's system. Here, when many agents are part of the attack, the victim's system crashes.

C. DYNAMIC RATE OF DDoS ATTACK

DDoS attacks are categorized into a variable- and continuous-rate attacks according to the rate dynamics of the attack as follows.

- Continuous-rate attacks are implemented at full force and without stopping or force reduction once, they begin. Such attacks produce quick impact.
- As the name suggests, variable-rate attacks "change the rate of attack," thereby making their detection and further response difficult. Different variable-rate attacks, such as fluctuating- and increasing-rate attacks, exist because various methods are used for changing the rate. Increasing-rate attacks eventually exhaust the victim's resources, hence delaying attack detection. Meanwhile, fluctuating-rate attacks have an undulating rate that changes according to the behavior and response of the victim; at times, the rate is decreased to avoid detection [35].

D. IMPACT OF DDOS ATTACK

DDoS attacks can be categorized into degrading and disruptive attacks based on their impact as follows.

- A disruptive attack results in complete DoS to the victim's clients.
- Degrading attacks aim to consume a certain portion of the resources of the victim's system. It causes a delay in attack detection, thereby resulting in tremendous damage to the victim's system.

IV. THE APPROACHES OF DDoS DEFENSE

DDoS attacks attain many challenges that are difficult to completely solved. Primarily, different DDoS attacks do not have common attributes through which they can be detected. Moreover, the distributed character of DDoS attacks renders the attacks to be exceedingly difficult to resist or trace, and automated software tools that deploy DDoS attacks can be easily obtained. Attackers may also exploit IP spoofing to hide their identity and thus render the detection of DDoS attacks to be increasingly complex. Lastly, machines connected to the Internet have inadequate levels of security, and web hosts are riddled with several security loopholes. Numerous experts have recommended the use of defense methods to defend victims against DDoS attacks. This section presents and illustrates various DDoS defense methods. Figure 5 features the most widespread statistical and artificial intelligence approaches of DDoS defense methods.

A. ARTIFICIAL INTELLIGENCE APPROACH

In the methods that follow, the system of detection can modify its process of execution according to recently collected data [46]. The system can enhance its performance on some test cases on the basis of previous outcomes.

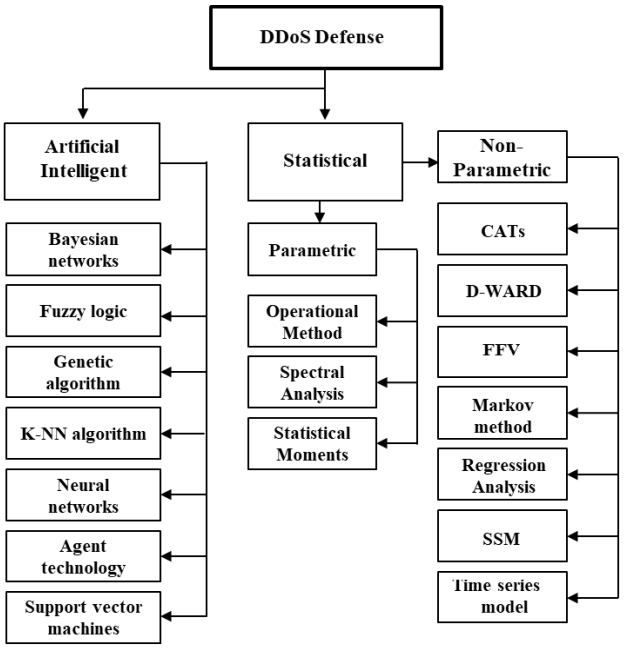

FIGURE 5. The classification of the DDoS defense.

This method coincides with artificial intelligence techniques, which concentrate on obtaining rules that produce new data [46], [47]. It provides such attributes as parallelism; robustness; and tolerance of faults, inaccuracy, and uncertainty [4]. Machine learning techniques are classified as AI-based methods. Machine learning involves such technologies as the Bayesian theory of decision, multivariate techniques, clustering, multilayer perceptron, linear discrimination, local models, classification trees, reinforcement learning, and hidden Markov models [48]. Various AI-based detection methods, namely, Bayesian networks, fuzzy logic, genetic algorithms, K-nearest neighbor (K-NN) algorithm, neural networks, software agent technology, and Support Vector Machines (SVM), are outlined as follows.

1) BAYESIAN NETWORKS

The Bayesian network is defined in [47] as a technique that determines the probabilistic associations among variables of interest. This technique is usually used for detecting attacks together with statistical schemes, which yield many advantages, such as the capability of encoding interdependencies among variables, forecasting events, and including prior data and knowledge.

Kim *et al.* [49] suggest the adoption of the pocket score, which can be defined as a programmed attack characterization, selective packet removal, and means of congestion control. The basic idea of this score is to prioritize packets according to per-packet score, which determines the packet legitimacy given the values of the attributes it contains. Then, a score-based specific packet removal process is conducted at the destination, when the packet score is calculated at detecting differentiating discarding routers using a Bayesian

TABLE 1. The defense methods based on Bayesian network.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Gonzalez et al. [50]	Trust-based approach	Accuracy, attack impact and delay	Judge router, the access router	It effectively detects malicious router access. It has a negative impact on network performance when there is no attack.	It is not able to detect IP-spoofing at the distribution routers. Also, it is difficult to develop a system at the source end.
Vijayasarathy et al. [51]	Na`ıve Bayesian classifier approach	Accuracy, time, Bandwidth, Detection Rate, Complexity and Latency	KDD, DARPA	It is carefully planned and practically detect DDoS attacks. It is lightweight and works close to line speeds.	It is efficient with only UDP and TCP protocols and cannot be tested with other types of DDoS attacks.
Katkar et al. [52]	Offline signature-based NIDS	Efficiency, Accuracy	KDD, DARPA	It is effective against HTTP flooding attack.	It can only detect limited types of DDoS attacks. Also, it is too difficult to implement this approach in actual networks.

theoretic grade. The dropping boundary for the packet removal process is dynamically adapted based on the score allocation of recent inbound packets and the present level of system congestion. Nevertheless, the work of Kim *et al.* [49] does not offer any test data to demonstrate how the timeline of updates could affect the response time. The resolution of the recommended selective packet removal process in cases of coordinated synchronized DDoS attacks is also neglected.

In the method of Gonzalez *et al.* [50], a Bayesian inference prototype is applied to evaluate the reliability of proposed access routers on the basis of forwarding packets that does not modify the IP addresses of the source. In this method, a judge router collects the traffic that passes through the access routers then calculates trust scores of the access routers. The fundamental goal of these processes is to apply trust computations, management, and trust agreements among the routers to identify and filter the hostile routers.

Bayesian networks are integrated with other statistical techniques for detecting DDoS. In this manner, Vijayasarathy *et al.* [51] present a real-time, lightweight technique for identifying a DoS attack by using a naive Bayesian classifier, which is used to classify network packets into poor or good. Furthermore, the signature-based approach is applied for attack detection using signature IDS.

Katkar *et al.* [52] propose a network intrusion detection model that is based on signatures for identifying DDoS attacks on HTTP servers. The model includes a distributed processing scheme and a naive Bayesian classifier. Observational results are given to prove the efficacy of the suggested model. The naive Bayesian is only able to classify slow attacks with a precision of 97.82% and regular attacks with a precision of 96.46%. Table 1 shows a summary of the defense methods that are based on the Bayesian network.

2) FUZZY LOGIC

The concept of fuzziness is used alongside the methods of identifying DDoS attack so that more emphasis is placed on network anomalies or attack [53]. The basis of the fuzzy set theory is used in approximating the reasoning, rather than being precisely obtained through traditional predicated logic [54], [55]. The use of fuzzy sets, as well as their rules, are employed when a large number of input parameters such as, CPU usage time, activity rate and connection duration, which can be ambiguous when handling incomplete datasets [56].

In the work done by Shiaeles *et al.* [53], the detection of DDoS attack is achieved, while the time limits are improved through the use of non-asymptotic fuzzy evaluators. The evaluator is deployed on average packet inter-arrival durations. The problem is categorized into two, which are actual DDoS attack detection and victims' IP address recognition. The attack detection is achieved through the use of strict real-time boundaries, while the recognition of victims' IP address is achieved through the use of relatively lenient constraints that are able to promptly identify the victim's IP addresses. This in return begins to add anti-attack applications on the hosts that are affected using arrival time of the packet as the major statistic of DDoS attack detection.

In order to improve the precision capabilities of DDoS attack detection, the fuzzy classification techniques are integrated with cross-correlation by [57]. Even though it is expected that the technique will improve precision, it does not satisfy real-time need due to the high cost of calculation. In research which is recently conducted by [58], "real-time" identification of DDoS attack is achieved through the use of fuzzy rules together with Hurst factor. The attack is successfully identified within 13secs; this can be considered real-time in terms of specific context. In this case, the Hurst factor is considered and computed by means of statistically analyzing the traffic, especially through Schwarz information criterion (SIC) and discrete wavelet transform (DWT). The methods of defense based on fuzzy logic are summarized in table 2.

3) GENETIC ALGORITHM

Genetic Algorithm (GA) is classified as heuristic quest techniques that are based on hypothetical thoughts of natural selection and tools used in eugenics for obtaining fairly accurate solutions or establishing optimization enigmas [55]. This algorithm adopts evolutionary statistical techniques, such as selection, crossover (recombination or mating), inheritance, mutation, and elitism [46].

It selects fine test samples as the informing dataset and reduces fake positive scales when human input is used in a feedback loop. This algorithm is a robust and flexible approach in that it is not easily influenced by noise and

TABLE 2. The defense methods based on fuzzy logic.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Shiaeles et al. [53]	Real-time DDoS attack detection approaches	Accuracy, time and complexity	DARPA	It has the ability to detect DDoS and identify malicious IPs in real-time.	It is inefficient in handling FC. Also, it is difficult to detect the attack at the source before the attack traffic aggregation.
Wei et al. [57]	Extended First Connection Density model	Accuracy and time	MIT Lincoln Laboratory	It is efficient in detecting UDP and TCP flooding attacks with high accuracy.	It can only detect limited types of DDoS attacks.
Wang and Yang [58]	Adopting variance-time plot method	Accuracy, Precision and time	DARPA	It is efficient in detecting DDoS attacks in real-time.	It can only detect limited types of DDoS attacks. Also, it is too difficult to implement this approach in actual networks.

TABLE 3. The defense methods based on genetic algorithm.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Li et al. [59]	Transductive Confidence Machines for K-NN	Accuracy Throughput efficiency and complexity	KDD Cup 1999	It is efficient in detecting DDoS attacks in a real-time.	It has high FPs and low accuracy.
Rahul et al [60]	VoIP Flood Detection System	Accuracy, Bandwidth and memory	Manually generated	It is fast and accurate in detecting DDoS attacks.	It is inefficient against FC.
Lee et al. [61]	An enhanced DDoS attacks detection approach	Accuracy, time, latency, bandwidth and detection rate	DARPA 2000	It is efficient in a real-time application.	It is inefficient against FC. Also, it is too difficult to implement this approach in actual networks.

variations in inputs. Metrics such as the detection rate (DR), false positives (FP), and the ratio of curtailed training dataset are integrated into a fitness function. Thus, the system is supposed to increase the defined fitness function (i.e., raise the DR and reduce the instances and FPs in the dataset used for training) [46].

Li *et al.* [59], develop a proficient network attack detection method that is based on an algorithm called transductive confidence machines and K-NN (TCM-KNN). Furthermore, they combine several efficient and objective anomaly impact measures from the viewpoint of clients into the TCM-KNN technique to create an efficient mechanism for the detection of an anomaly in the web server. In addition, a GA-based technique for instance selection is introduced to enhance real-time detection performance.

Rahul *et al.* [60], use a GA to identify legitimate users and specifically block VoIP and SIP flooding. Their recommended VoIP flood detection system (VFDs) is used to identify TCP and SIP flooding attacks on SIP instruments through the Hellinger distance and Jacobian fast methods. In their technique, the fast Jacobian method and Hellinger distance computation, which is a numerical anomaly-based technique, are used for fixing the boundary limit and discovering deviations in traffic, respectively.

Lee *et al.* [61], present an enhanced approach to DDoS attack detection by optimizing the traffic matrix parameters using a GA to maximize the DRs. In addition, they enhance the creation of the traffic matrix by using hash function reformation to reduce hash collisions. They also substitute the size of the time-based window with the size of a packet-based window to decrease computational expense.

Kaur *et al.* [55], follow the ''survival of the fittest'' principle so that every time several users attempt to obtain scarce resources, the fittest users take over the weak ones. A chain of iterations is carried out to replace the users with low fitness by using a fitness function. GAs are efficient in acquiring categorization rules with information collected from inbound traffic and in selecting optimal parameters for the process of detection to distinguish attacks from normal packets. Table 3 shows a summary of the defense methods that are based on GA.

4) K-NEAREST NEIGHBORS TECHNIQUE

K-Nearest Neighbors (K-NN) technique comes under an artificial intelligence technique that generates forecasts and determines by comparing the nearest graph element. Input can be categorized into groups using this nearest element, and nearby locations can be identified in real time by using this parameter geographically. Initially, K-NN has to note down IP addresses obtained to a server. Later, it has to note them down in a file and create a graph with longitude and latitude as axes. A very high density demonstrated by the graph in a particular geographical area may indicate a potential DDoS [62].

Nguyen and Choi [63], create a common anti-DDoS structure that can be used and created in real time. They also offer an appropriate method for advanced DDoS attack detection using the K-NN classifier. This process can also be used for the first phase of the anti-DDoS structure. Several studies on the detection of DDoS attacks have been performed. Nevertheless, they only concentrate on network traffic variation. Data mining-based techniques are deemed appropriate for detection but do not guarantee real-time packet transfer. This technique initially selects nine traffic/packet features that are generally found in different attack stages. Furthermore, the present status of the network is classified for determining its category. Therefore, the given method can categorize the status of the current network well to identify DDoS attacks early.

TABLE 4. The defense methods based on K-NN algorithm.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Nguyen and Choi [63]	Anti-DDoS a framework based on K-NN	Accuracy, time, efficiency and detection rate	DARPA 2000	It can correctly classify the DDoS phases and efficiently detect DDoS attacks early.	It does not ensure the real-time transfer of packets.
Barrionue et al. [64]	Anomaly detection model	Accuracy, time, F-measure and precision	Manually generated	It can avoid DDoS attacks.	It has low accuracy.

Barrionuevo *et al.* [64], suggest a model and its feasibility analysis for three known attacks, each of which is a service denial: Fraggle, land, and Smurf. The execution problem is solved by employing HPC techniques in the GPU to accelerate the procedure and obtain outcomes in a short time. The scheme is evaluated on the basis of several metrics. The suggested model reaches an accuracy of 40% to 70% and a sensitivity of 60% to 83%. The F-measure, which is used to measure the system's performance, is 0.5 to 0.83. Table 4 shows a summary of the defense methods that are based on the K-NN algorithm.

5) NEURAL NETWORKS

Neural networks are presented as a substitute for statistical techniques that categorize subsequent instructions according to a series of earlier instructions from a specific user. Neural networks are properly trained, entirely feedforward, and propagation backward networks that provide better results than do basic signature testing methods [65].

Tsai *et al.* [66], suggest the use of a so-called time delay neural network (TDNN), which is an early alarm system against DDoS attacks. It works with the time delay parameter hidden within the representative pointer. Experts create a demilitarized zone (DMZ), and TDNN is executed in a two-layer pattern. Adjacent nodes and attack information supervise the node activity sent to the expert unit for integrated assessment. The layered organization enables the system to implement appropriate actions as a positive strategy against DDoS invasion. The detection outcomes on a deployed design show that the suggested scheme can provide 82.7% accurate DR (Ordinary IDS yield 46.3 %.).

Braga *et al.* [67] recommend the adoption of a lightweight detection process for DDoS attacks. They obtain six tuple fields of the attributes of DDoS attacks using the self-sufficient mapping of the algorithm for the neural network to detect the stream of the attack using the SDN traffic information function. Meanwhile, [68] recommend a multi-vector; deep learning-based DDoS attack detection system within SDN. However, detecting these low-rate attacks using these techniques is difficult because it looks familiar to the authenticated network traffic at the victim's end. In the meantime, DDoS attacks on the victim's systems must be produced over time; otherwise, it will not be harmful to the network or the system resources. The technique we use for detection utilizes a series of continuous packets in the network and can understand the subtle difference between legitimate and attack traffic. It helps discover repeated patterns that characterize DDoS attacks and trace them in a long-term traffic sequence.

Chambers *et al.* [69], propose an innovative NLP neural network model application to detect DDoS attacks by only using social media as support. Private networks are generally slow in reporting attacks. Therefore, a detection system that uses public data could provide an improved response to a wide attack across several services. NLP models are examined to use social media as an implicit measure of the network service status. They explain two learning models for this work: a feed-forward neural network and an incompletely labelled LDA framework. Both models outshine the previous work by substantial margins (20% F1 score).

Furthermore, the model based on the topic enables the initial fine-grained reaction assessment of the public to current network attacks, thereby discovering multiple observation "stages." Ours is the very first scheme that not only detects DDoS attacks (with superior outcomes) but also provides an assessment of how and when the public explains the service outages. The models are defined, experiments on the biggest Twitter DDoS corpus to date are conducted, and the reactions of the public are assessed on the basis of the output of the learned model.

Cheng *et al.* [70] suggest a basic Extreme Learning Machine (ELM) technique that is based on arbitrary features and an ELM technique that is based on the kernel for classification using the MIB datasets collected from actual experiments of a DDoS attack. They evaluate the methods with commonly used SVM technique in dual- and multi-class classifications and used ELM techniques to classify dual- and multi-class network traffic for attack detection. The performance of the ELM technique in the dual- and multi-class situations is examined and compared with that of SVM-based classifiers.

Yan *et al.* [71], suggest a multi-level DDoS mitigation framework (MLDMF) for IoT that comprises edge-, fog-, and cloud-calculating levels. The edge-calculating level employs IoT gateways that are based on SDN to manage and secure IoT perception nodes. The fog-calculating level primarily contains an IoT management control unit (IMCU). The IMCU employs a group of SDN controllers and software and uses it to detect and neutralize DDoS attacks. The cloud-calculating level uses big data and artificial intelligence to analyze network traffic; this process constitutes an intelligent attack identification and mitigation structure that protects against DDoS attacks. Simulation results are presented to demonstrate that the combination of the edge-calculating level's quick response capability, fog-calculating level's state recognition feature, cloud-calculating level's powerful calculation capability, and SDN's network programmability could

TABLE 5. The defense methods based on neural networks.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Tsai et al. [66]	Time-delay neural network	Time-delay	Manually generated	It can detect DDoS attacks with minimal delay.	It can only detect a limited type of attacks.
Braga et al. [67]	DDoS attack detection model based on traffic flow features	Accuracy, time, Efficiency and detection rate	KDD-99	It is very efficient in detecting DDoS attacks.	It does not distinguish FC from DDoS attacks. The system not tested with a real dataset.
Chambers et al. [69]	The neural language processing model	Accuracy and precision	Manually generated	It is very efficient in detecting DDoS attacks.	It can only detect a limited type of attacks.
Cheng et al. [70]	Basic Extreme learning machines method based on random features	Accuracy and time	DAPRA 1998	It is effective in detecting and preventing DDoS attacks.	It can only detect a limited type of attacks.
Yan et al. [71]	Multi-level DDoS mitigation framework	Time and delay	Manually generated	The method is very efficient in detecting DDoS attacks in the network- and transport-layer protocols.	It does not distinguish FC from DDoS attacks.

TABLE 6. The defense methods based on software agent.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Juneja et al. [73]	An agent-based framework to counterattack DDoS Attacks	Time	Not tested	It has the ability to trace a distant source of different types of DDoS attacks.	It is still unsure about how many software agents shall be employed to work optimally. Also, it is never tested.
Kotenko et al. [1]	An agent-based approach against DDoS attack.	Time	Not tested	It has the ability to trace a distant source of different types of DDoS attacks.	It is never tested.
Kesavamoorthy and Soundar [74]	A multi-agent system (MAS)	Accuracy and time	Manually generated	It has high accuracy in detecting a DDoS attack.	It does not distinguish FC from DDoS attacks.
Singh et al. [75]	Collaborative agent-based distributed DDoS defense scheme	Accuracy, Efficiency and throughput	Tribe Flood Network tool	It is accurate and efficient to handle DDoS attacks.	It does not distinguish FC from DDoS attacks.

solve the DDoS problem in IoT. Table 5 shows a summary of the defense methods based on neural network.

6) SOFTWARE AGENT

An agent is a software entity or a mixture of software and hardware entities that can be executed in parallel on behalf of its users. It includes many useful features, such as learning capability, cooperation, reactivity, and effectiveness [72].

Kotenko and Ulanov [1], define an agent-based methodology and software environment (which is based on the framework of OMNeT++ INET) developed for modeling distributed defense techniques that can be installed on the Internet to neutralize network attacks. In the recommended approach, the cybernetic neutralization of ''malicious guys'' and security mechanisms is characterized by the interaction of various agent teams. The primary elements of the software system are highlighted. One of the tests on protection against DDoS attacks is described.

Juneja *et al.* [73] suggest a multi-agent structure for identifying, protecting, and tracking the source of DDoS attacks. This solution locates the source of a DDoS attack, but several agents are required to obtain the best results.

Kesavamoorthy and Soundar [74], recommend a new technique of detecting and protecting against DDoS attacks using a self-contained multi-agent system, where agents use particle swarm optimization among themselves to have robust communication and perfect decision making. DDoS attacks are detected using multiple agents that are connected to one another and inform the coordinator agent regarding any new attack. The suggested system, which is present in the cloud platform, can protect against different types of DDoS attacks with 98% accuracy.

Singh *et al.* [75] present a mutual agent-based distributed scheme against DDoS attacks that identifies and prevents these attacks within the ISP boundaries. The substantial task of resistance is conducted by agents and coordinating agents in all ISPs. The security system works by examining incoming traffic on the edge router and detecting the onset of DDoS attacks. The agents use an entropy-threshold-based technique for detection. The coordinating agents share information regarding the attack with adjacent ISPs so as to achieve distributed protection. Certain known metrics are adopted for assessing the defense system's performance, and the defense system efficiency is evaluated against the system's performance in the absence of such a defense system. Table 6 shows a summary of the defense methods that are based on software agents.

7) SUPPORT VECTOR MACHINE

Support vector machine (SVM) is a learning technique that is used to plot the training vectors in high-dimensional attributed space the classify them accordingly [76]. SVM considers the classification as a quadratic optimization problem. It integrates generalization control to prevent ''dimensionality curse of features'' by placing an upper limit on the margin between the various classes, thereby rendering of practical means for large and ever-changing datasets [70].

TABLE 7. The defense methods based on SVM.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Seo et al. [76]	DDoS detection model based on multiple SVMs	Accuracy	Manually generated	It can detect DDoS attacks with accuracy and lower FPR.	It can only detect limited types of attacks.
Yu et al. [77]	SVM-based hierarchical structure	Accuracy and efficiency	MIB	It can detect new and unknown types of attacks at the first level. It can easily adapt to new attacks.	It does not distinguish FC from DDoS attacks.

Seo *et al.* [76] suggest a new DDoS attack identification model that is based on several SVMs to reduce the rate of the FPs. They use traffic rate analysis to analyze the network traffic attributes during DDoS attacks, and this model yields a somewhat high detection precision and a low rate of FPs. Therefore, this technique can help provide early DDoS attack detection.

Yu *et al.* [77] recommend an SVM-based machine learning technique for attack categorization. They obtain rapid detection with high precision, and the system's overload and deployment flexibility decrease using SVM and MIB. The suggested mechanism is created with a hierarchical organization that initially distinguishes attack traffic from regular traffic and then establishes the attack type in detail. Table 7 shows a summary of the defense methods that are based on SVM.

B. STATISTICAL APPROACH

The statistical attributes of normal and attack patterns can be used in identifying DDoS attacks [78]. In general, a statistical model for regular traffic is computed, and then, a statistical deduction test is used to determine whether a new traffic instance or flow is of this model. Traffic instances that do not abide by the rules of the learning model are classified as inconsistencies (i.e., depending on the applied experimental statistics results, flows, or traffic) [4]. Research has made excellent contributions to the use of the statistical attributes of network traffic for DDoS attack detection and prevention.

The following section describes the most common statistical techniques for such attacks. The statistical techniques are used in parametric and non-parametric DDoS defense methods as follows.

1) PARAMETRIC METHODS

Parametric methods suppose that the system has knowledge of latent distribution and analyze the statistical conditions from the provided data [47]. Methods such as the operational (or threshold-based) model, statistical moment's parametric identification, and spectral analysis are categorized as parametric methods [79] of defending against DDoS attacks.

- **Operational:** Tan [80] suggest a DDoS attack identification system that uses the fundamentals of multivariate correlation analysis (MCA) and anomaly-based identification using a threshold. They furnish the detection system with the potential of accurate description for traffic behaviour and the detection of familiar and unfamiliar attacks. A triangle area method is developed to improve and boost the speed of the MCA technique. A statistical normalization method is utilized to eliminate prejudice toward the raw data. The suggested DoS detection scheme is evaluated by using the KDD Cup 99 dataset.
- **Spectral:** High-dimensional datasets are used in detection applications. Large numbers of multidimensional datasets are challenging to process, store, transmit, and analyze. Consequently, detection becomes complicated and costly to implement. Patcha and Park [46] and Purwanto and Rahardjo [81] use spectral analysis strategies to effectively handle such massive datasets. These strategies transform high-dimensional spaces into low-dimensional subspaces, including projections and embedding's, where legitimate and abnormal behavior are characterized differently and anomalies are readily recognized. The strategy is also known as wavelet analysis or signal-processing-based detection. Cheng *et al.* [82] propose a strategy for enabling DDoS exploit mitigation without harming legitimate TCP traffic using spectral analyses that recognize the flow of attacks. Li [83] introduce anomaly detection methods that are based on discrete wavelet transmutation (DWT) and probability assumptions. Dainotti *et al.* [84] present dual-phase automated detection methods that comprise change-point detection and successive alterations in wavelets for the identification of exceptional traffic profiles. This model could improve the hit rate (HR) and the false alarm ratio (FAR) trade-offs.
- **Statistical moments:** Specific confidence ranges or intervals are set in accordance with statistical properties (correlating events or moments), such as statistical mean and standard deviation, using the model. Events that range outside set interims, that is, below or above the moments, are denoted as anomalous [78]. The model provides greater flexibility when compared with operational schemes given that the confidence range follows observed events that may vary among users. Therefore, it assigns heavy weightings to recent activities. Owezarski [85], conducts analytical studies on the effect of DDoS exploits on the network's QoS. The research particularly explains how network QoS degrades during DDoS attacks by delineating the effect of such on LRD. The study relies on recent research in network monitoring that seeks to discover the features of existing traffic. Traffic characterizations markedly demonstrate the key characteristics of existing traffic in terms of dynamic properties, thereby emphasizing high-order statistical

TABLE 8. The defense methods based on parametric measures.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Tan et al. [80]	MCA-based DoS attack detection System	Accuracy	KDD Cup 99	It has the ability to distinguish known and unknown DoS attacks from legitimate traffic.	It has not been tested on DDoS attacks.
Cheng et al. [82]	Spectral analysis-based approach	Time	Manually generated	It can mitigate DOS attacks without affecting normal TCP traffic.	It can deal with limited types of DDoS attacks.
Li and Li [83]	Anomaly detection approach based on DWT technique	Precision and Time	Manually generated	It can reduce the error of identifying DDoS attacks.	It deals with a limited type of DDoS attacks.
Dainotti et al. [84]	DoS attack detection based on wavelet transform	Accuracy	DARPA and MIT	It can improve the trade-off between HR and FAR.	It has not been tested on DDoS attacks.

moments (typically second-order moments) in the characterizations. The presence of power-law invariances within the traffic is notable. Therefore, DDoS events do alter power-law relationships and particularly increase LRD in certain temporal ranges. These alterations to the LRD function, therefore, provide signatures for exploits, which can assist in their spotting within network traffic. Such differences specifically assist in the detection of exploits, which are typically transparent to a conventional anomaly or signature-based IDS. Table 8 shows a summary of the defense methods that are based on parametric measures.

2) NON-PARAMETRIC METHODS

Numerous studies have established non-parametric methods as an effective defensive approach against DDoS attacks. The following are the most common non-parametric detection approaches: D-WARD, change aggregation trees (CATs), histogram-based detection, flow feature value (FFV), regression analysis, Markov method, statistical segregation, and time series.

- **CATs:** In this technique, although the system performs modeling on the basis of observed features, no prior information on potential distribution exists [79]. Chen *et al.* [86], evolve the distributed change point architecture using CAT models. The non-parametric cumulative sum method is adopted for expressing pre- or post-change network traffic distribution. Once DDoS flooding attacks are launched, cumulative deviations will increase noticeably versus random fluctuations. The CAT mechanisms work at the router level for the efficient identification of abrupt transitions in traffic flow. The domain server exploits the traffic change patterns spotted at each attack-transit router and then constructs a CAT that characterizes the observed attack patterns.
- **D-WARD:** Mirkovic *et al.* [87], reportedly detect attacks by continuously monitoring bidirectional traffic flows among local and Internet traffic in accordance with recurring deviation analyses that are based on patterning legitimate flows. Abnormal flow types feature rate-limited characteristics proportional to their arrival rates. D-WARD allows for remarkable DRs and appreciable reductions in DDoS traffic volume. It utilizes predefined profiles to recognize legitimate traffic and spots anomalies within two-way traffic in accordance with deviation statistics. D-WARD recognizes traffic in terms of attack confirmation or invalidation and will regulate rate-limiting further in response to confirmation. However, if it is refuted, then higher traffic rates will be progressively enabled.
- **FFV:** Cheng *et al.* [88], introduce the IP FFV algorithm, which uses key DDoS attack features, including flow dis-symmetries, disruptive traffic transitions, source IP address distributions, and convergently targeted IP addresses. An ARMA prediction framework is established to assess legitimate network flows via a linear prediction technique, and a DDoS attack detection model is then derived from anomaly detection methods, in which a linear prediction scheme (DDAP) is applied.
- **Markov:** This technique uses event-counter metrics to determine the consistency of specific events according to prior events. It utilizes state transition matrices to establish the probabilities of appropriate events [65]. The model works by periodically monitoring networks and maintaining accounts of its changing states. All observations are viewed as such, where events that occur lead to system state transitions [46]. Whenever system states change and the computed probable occurrences of particular states are diminished at given points, such situations are then exceptionally disposed of [79]. The computed state change probabilities become isolating parameters in the identification of anomalies and system states that are directly observable using this scheme. The procedure searches for changes among certain activities or other commands wherein strings of such activities are especially meaningful. The scheme remains ineffective in delivering real-time services where huge amounts of traffic and increased event rates are present in high-speed networks [45]. Xie *et al.* [89] develop a novel scheme that detects patterns of app-DDoS exploits by capturing the browsing behavior of Internet users. The framework comprises three parts: (i) a new scheme that defines browsing behavior among users and detection of app-DDoS exploits in accordance with a hidden semi-Markov framework; (ii) a novel algorithm for efficient forwarding processes in HsMM and for the online detection of app-DDoS exploits; and (iii) experiments conducted through live network traffic that validates the detection technique. The scheme can be used to describe browsing behavior among legitimate users and

spot app-DDoS exploits as a result. This new algorithm can reduce memory requirements and improve computational efficiencies. Saranya *et al.* [90], recently introduce a technique known as integrated quantum flow and hidden Markov chain (IQF-HMC), which deploys broadband service provisioning. The technique measures network traffic features in terms of originating sources, data traffic characteristics, and durations. Conventional classes of traffic patterns are assessed with training samples, whereas the entropic characteristics found in the flow patterns of test traffic are comparatively analyzed for the identification and mitigation of anomalous traffic-featuring flooding attacks.

- **Regression analysis:** Prior research that takes advantage of the statistical characteristics used in the detection of DDoS exploits has contributed greatly. These works are also applied via traceback procedures (i.e., recognizing the sources of attacks and applying mitigation strategies, including rate-limiting and filtering) [91], [92]. Gupta *et al.* [93] introduce regression analysis wherein DDoS attack strengths are estimated and contrasted to actual strengths. The comparisons are promising and indicate that the technique applies to DDoS strength assessments through routers or other discrete units that communicate through routers. Two forms are analyzed: multiple and polynomial regressions. Carl *et al.* [94], review three different methods for detecting DDoS flood exploits on targeted networks: activity profiling, wavelet analysis, and change-point detection. Activity profiling is attained by examining network packet header information, which is resolved by average packet rates in packet flows that feature similar fields, including the port and address information transmitted in IP packets. The change-point detection in [95] denotes statistical analyses wherein packet traffic is initially filtered for unique fields, including protocol and address fields. The results are stored in a time series that represents clusters of activities within the time domain. The time series would show statistical transitions that can be monitored to detect exploits with DDoS attacks. Wavelet analyses in [96], [97] toward DDoS detection entails network traffic observation in terms of spectral components. When DDoS attacks occur, anomalous signaling is captured and then segregated from the noise background. However, the input signals have noise and anomalous components.
- **Statistical segregation:** Udhayan and Hamsapriya [98], present the so-called Statistical Segregation Method (SSM), which samples flow at successive intervals, contrasts the samples against attack-state condition and then sorted these conditions according to mean parameters. Legitimate traffic flows are thereby segregated from attacking types through correlational analyses.
- **Time series:** The model features the use of interlude timers and event-based counters (or resource measures). Statistical databases for threshold schemes must be prepared to reconcile in-order and inter-arrival moments along with observed values [47], [65]. Any observation (observed traffic) of a low probability of incidence should be treated as an anomaly. These anomalies are represented by data points that diverge from regular patterns using the technique. Such systems measure network behavior across time to detect various behavioral shifts [65]. Therefore, exploits performed in series are readily spotted. The detection model cannot operate effectively when rapid alterations in common network behavior occur under abnormal conditions. The move from regular packet-based analytical techniques to time series- or flow-based algorithmic methods presents promising alternatives for spotting DDoS exploits. Four measures, namely, kurtosis, periodicity, self-similarity, and skewness, are extracted from the time series to investigate the performance of these parameters in the segregation of DDoS from legitimate traffic [99]. Table 9 shows a summary of the defense methods that are based on non-parametric measures.

V. EVALUATION METHODS

Evaluation metrics assess defensive systems by measuring their performance qualitatively and quantitatively. Numerous instances realize test scenarios that rely on specific evaluation criteria and metrics. This section covers evaluation metrics across various aspects in accordance with evaluative goals, such as detection performance, attack mitigation performance, and deployment costs.

A. QUANTITATIVE METHODS

There are many evaluation methods used to evaluate the defense model against DDoS attacks. The focusing of this section on the quantitative evaluation methods as summarized in figure 6.

1) PERFORMANCE METRIC

One crucial aspect of assessing the performance of defense systems is the evaluation of the attack detection performance on the basis of accuracy, effectiveness, and speed. The metrics that are frequently deployed in the literature are presented in this paper to obtain this objective for (true positive = TP, false positive = FP, false negative = FN, true negative = TN).

- **DR or TP rate (TPR):** The percentage of attack instances that are identified and reported correctly as attacks. This metric is useful for validating the effectiveness of the detection tool [100]–[106], and [107]. It can be considered the same as the recall (or sensitivity) parameter, which stands for the retrieved fraction of relevant instances. Formula 1 is usually used to express DR:

$$DR = TPR = RECALL = \frac{TP}{TP + FN} \tag{1}$$

- **TN rate:** The percentage of instances that are classified as legitimate.

TABLE 9. The defense methods based on non-parametric measures.

Ref.	Model	Evaluation	Datasets	Advantage	Disadvantage
Mirkovic et al. [87]	D-WARD, a DDoS defense system	Accuracy, bandwidth and deployment cost	DARPA	It can detect a DDoS attack in several attack scenarios.	It is yet to be tested in real attack scenarios.
Cheng et al. [88]	IP Flow feature value algorithm	Accuracy	MIT	It is efficient in detecting DDoS attacks with high accuracy and lows FAR.	It can deal with a limited type of DDoS attacks.
Xie and Yu [89]	Large-scale hidden semi-Markov model	Accuracy	Manually generated	It can reduce memory requirement and improve computational efficiency	It can deal with a limited type of DDoS attacks.
Saranya et al. [90]	integrated quantum flow and hidden Markov chain approach	Time, accuracy and memory	KDD Cup	It improves the DDoS flooding attack conflict, reduces the time of attack detection and consumes less memory.	It deals with a limited type of DDoS attacks.
Lung-Yut et al. [95]	Distributed statistical detection of change-points	Accuracy and Detection rate	Manually generated	It is efficient in detecting and localizing DDoS attacks on Internet traffic. It is usable in high-volume network traffic	It deals with a limited type of DDoS attacks.
Udhayan and Hamsapriya [98]	Statistical Segregation Method	Accuracy, time and bandwidth	CAIDA	It blocks large numbers of zombies from the Internet and avoids blocking legitimate clients.	It deals with a limited type of DDoS attacks.

- **FP rate (FPR) or false alarm ratio:**The number of legitimate instances that are classified as attacks. Its goal is to measure the effectiveness of the system in distinguishing fake and legitimate requests [101], [105], [106], [108] and [109]. This metric can be expressed through the ROC curve (DDoS DR v/s FPR graph) to demonstrate the possible trade-offs between TPR and FPR [80], [107], [110] and [111]. The area under the ROC curve is used to compare the performance of various detection systems.
- **System precision:** The fraction of retrieved instances that is relevant to detection performance. In addition, it is the number of attack instances that are correctly reported, divided by the total number of reported attacks. This metric is useful for measuring the quality of the attack detection system [112], [113] and [114] and is depicted as follows:

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

where FP is the number of FPs.
- **Detection of overall accuracy:** The proportion of correctly classified instances. It is a basic parameter used to compare the performance of many detection methods [80], [111], [114] and [115] and can be stated as formula 3 below:

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

where TN is the number of TNs.
- **Error rate:** A reflection of the detection system's accuracy and can be expressed using Formula 4.

$$\text{Error Rate} = \frac{(FP + FN)}{(TP + FP + TN + FN)} \tag{4}$$

- **F-measure or F-score:** A reflection of the trade-off between two metrics: precision and recall. The range of its values is between 0 and 1. High values are used to indicate remarkable performance in terms of precision and recall [109]. The F-measure can be expressed as follows:

$$F - MEASURE = \frac{2 \times PRECISION \times RECALL}{PRECISION + RECALL} \tag{5}$$

- **Latency or response time:** The end-to-end communication delay used when assessing the speed of the defense system in identifying and halting an attack [116], [117] and [118] . It is used for proving the effectiveness of the defense approach when the system is going through various attack rates in defense and non-defense scenarios. The use of this metric is convenient for comparing the performance of various defense solutions. The defense system's speed is reflected through the Cloud system response time. The latency or response time metric includes the average time for request analysis or packet processing.

2) ATTACK MITIGATION

Performance metrics are needed to assess the methods for attack mitigation.

- **Packet drop rate or request dropping probability:** Its goal is to assess the performance of attack mitigation. It is helpful in proving that the defense system can identify and block attacks, thereby increasing the availability of network bandwidth and resources for service. Low drop rate values indicate good mitigation performance [115], [119] and [120]. A similar metric of success-analyzing is used by Chung *et al.* [121] to assess the capacity of the system in managing the rate of received packets.
- **Throughput or network traffic rate:** During an attack, throughput usually degrades because of the limited number of requests that the system serves. This metric, which can also be expressed as the rate of serviced requests, is used by authors to demonstrate the enhanced performance of the cloud service in defense and non-defense scenarios when detection and mitigation of attacks occur [115], [122]. Research also considers the goodput metric as a means of measuring the rate of

legitimate requests that the system serves [123]. Good performance yields high goodput rates.

- **Attack impact:** Authors usually assess the impact of the attack on the cloud for defense and non-defense scenarios so that they could illustrate the efficiency of the defense when the attack is reduced and managed. This impact is usually evaluated on the basis of the following metrics:

Application response time: Response time refers to the fact that the defense system can save the bandwidth and resources of the cloud system from congestion and unavailability as a result of attacks [115], [124]. Preetha *et al.* [125] use this metric to determine the performance of their defense technique given three kinds of application: FTP, email, and HTTP.

Cloud resource consumption: Authors use this metric in defense and non-defense scenarios as a way of demonstrating how the defense system alleviates the impact that DDoS attacks have on cloud service performance. It is typically expressed through CPU consumption [126] or network bandwidth utilization [123], [124] and [127]. It can be evaluated while the type of attack is made to vary [128].

3) DEPLOYMENT COST

The deployment cost should be assessed before assuming a defense solution against DDoS attacks given a real cloud infrastructure. To accomplish this goal, the performance overhead incurred by the identification or management technique must be examined. A defense solution can be effective when it does not result in a major overhead in the monitored system. Various forms can be taken by the performance overhead according to the kinds of functions and components of the defense architecture. The following metrics are helpful in the estimation of system overhead and deployment cost.

- **Processing time:** Authors measure the processing time involved for the defense method to conduct computational cost and time analysis [100], [101], [103], [107], [123], [129] and [130] or the testing and data training time if data classification techniques are used. Usually, the average processing time (or detection time) is measured while increasing network congestion, client request rates [119], [126], or attack intensity [131]. It can also be measured for various attack durations [108]. In a non-attack situation that has defense and non-defense cases, measuring the packet or request processing time is helpful in assessing the impact that the defense system has on a legitimate request's total response time [128]. Therefore, this metric is valuable for comparing the cost of various defense solutions. Typically, processing time is smaller when parallel processing is applied by the solution [132].
- **CPU load or processing usage**: This metric shows the system computation power that is required in the defense solution. Low processing usage is indicative of the fact that the detection or mitigation method does not use a significant number of CPU cycles. Furthermore, it means that it cannot support system overhead [121], [126] and [133].
- **Memory usage or memory overhead**: This metric refers to the quantity of memory overhead that the defense system possesses or needs for storing the models of detection and mitigation [103], [133].
- **Network load or bandwidth overhead:** One should also consider this factor when assessing deployment cost. Low communication or bandwidth overhead means that the attack can be eliminated by the defense system with minimal bandwidth utilization [107]. Dastjerdi *et al.* [134], use this metric in comparing the performance of client-server intrusion and agent-based detection systems.
- **Financial cost:** Preetha *et al.* [125] perform profit analysis using the system overhead as a basis for estimating the financial impact of the attack on the cloud service with and without the application of a defense solution. Yu *et al.* [135] estimate financial defense cost on the basis of attack rates and durations. This metric is a vital aspect of assessing defense solutions in the cloud as a result of the pay-per-use quality of the cloud environment.

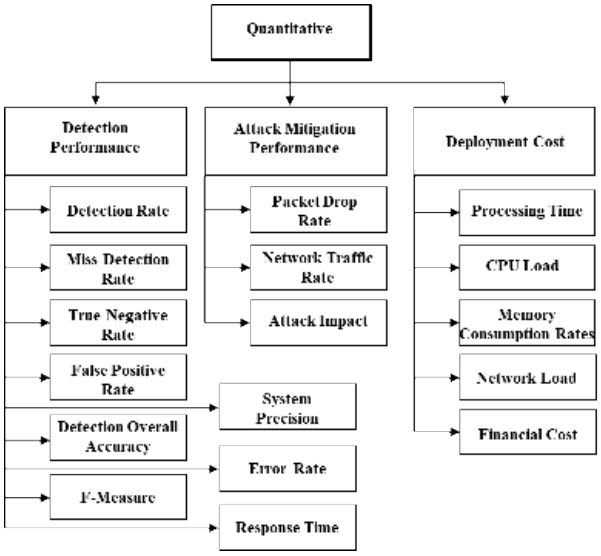

FIGURE 6. The classification of the quantitative evaluation methods.

B. QUALITATIVE METHODS

It is possible to use a quantitative approach to evaluating the defense systems built to counter DDoS attacks. Figure 7 summarized the qualitative evaluation methods.

Some of the popularly used qualitative parameters are given subsequently. By using qualitative parameters, some authors have evaluated their solutions. Jin *et al.* [120] provide a discussion on the attributes of their solution, which includes a high level of adaptability and real-time performance. Similarly, the use of a quantitative method of evaluation is employed by [112] to assess the performance of

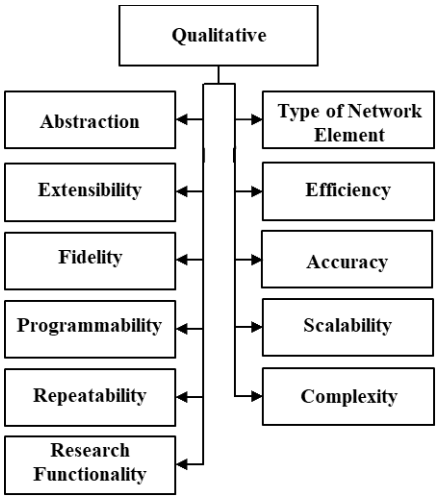

FIGURE 7. The classification of the qualitative evaluation methods.

TABLE 10. The validation attributes of the DDoS attacks [16].

Attributes	Simulation	Emulation	Real System	Real Dataset
Abstraction	Lowest	Moderate	Highest	Lowest
Extensibility	Highest	Moderate	Lowest	Highest
Fidelity	Lowest	Moderate	Highest	Highest
Functionality	Lowest	Moderate	Highest	Highest
Network Element	Virtual nodes	Real/virtual nodes	Real nodes	Real nodes
Programmability	Highest	Moderate	Highest	Lowest
Repeatability	Highest	Moderate	Lowest	Highest

the detection system. Afterwards, they presented the scalability and compatibility as the unique feature of the system. Conversely, the difficulty associated with the implementation and overhead of a novel system can be reflected through computational complexity which is a qualitative parameter. Its use in making a comparison of different approaches provides practicality [80]. Based on the suggestion made by [16], a kind of network which as elements attributes such as research functionality, extensibility, fidelity, repeatability, and programmability should be used. A comparison of previous works will provide researchers with advanced facilities for the implementation and assessments of algorithms for the detection and defense of DDoS. In Table 10, we summarized comparison of the different methods of validation used in DDoS attack research.

The qualitative attributes of all the methods of evaluation are given below:

- **Abstraction:** Abstraction is the term used to describe how complex a person perceives or programs a system. The implication of the higher level is fewer details and the other way round.
- **Extensibility:** this means that an experimental setup that is network-based must have a means of scaling the topology of experiments with regards to the wild internet. It is important for experiments to be portable with remote assessment capability.
- **Fidelity:** It is important for a network-based experimental setup to have this attribute because it proves the reliability of real networks. This dimension encompasses large topology that possesses a sufficient number of nodes, uneven combination of software and hardware, real routers, as well as a mixture of bandwidth capacities and delays.
- **Functionality:** Apart from the control of hardware and software features of experiments that are security-based, the facilitation of social and technical environments for experiments such as traffic generators, most recent tools for analysis and visualization of results, as well as diverse experimental profiles is essential.
- **Network elements Type:** It gives the form of the experimented network parameters such as the soft nodes, real nodes, or the combination of both nodes.
- **Programmability:** This term describes the flexibility that a network-based experiment setup must possess, so as to able to make use of novel personalized network techniques of monitoring, detecting, filtering, improving or making the addition of practical heterogeneous hardware and router algorithms. Nonetheless, programmers who use software routers may benefit from their flexibility.
- **Repeatability:** The experiment setup of a network environment must possess a facility that allows the reproduction or storage and repetition of experiments under similar environmental conditions. However, parameters like software and hardware improvements, Internet topology, available bandwidth and types of background and attack traffic make the repetition of an experiment using real systems challenging.

TABLE 11. The validation approaches of DDoS attacks.

Re.	Method	Accuracy	Complexity	Efficiency	Scalability
Xie [89]	HsMM	High	High	Low	Low
Oikonomou [13]	Human behavior	High	High	Low	Low
Kandula, [137]	Botz-4-Sale	Unknown	Medium	Medium	Medium
Jung et al. [138]	Traffic Analysis	Medium	Low	High	High
Lu and Ghorbani [97]	Wavelet	Medium	Medium	Low	Low
Yeung et al. [139]	Covariance	Medium	Medium	High	Low

Zhou *et al.* [136], propose the use of efficiency, scalability, accuracy, and complexity features for assessing and comparing the proposed module with previous work. Table 11 shows a comparison between the validation approaches that are utilized in DDoS attack research.

- The first study presented in the comparison is the hidden semi-Markov-based method introduced by [89]. Each visiting sequence of users is recorded in this method. This method can also detect FC and AL-DDoS attacks accurately. However, they are considered to have "low" efficiency and scalability because of their complex algorithms.
- The second work is made by [13] which models human behavior such that it can defend against AL-DDoS attacks. For this method, the visiting sequence of users on the website should also be recorded. The application of this method for most popular business web-

sites, which have large numbers of web pages, is nearly impossible.

- Botz-4-Sale of [137] requires collaboration with CAPTCHA. However, the associated cost when it comes to CPU processing time means that Botz-4-Sale can be deployed on medium-scale websites only.
- Jung et al. [138], characterize abnormal traffic as a way to detect AL-DDoS attacks. One can easily deploy this traditional method on large-scale websites. Nevertheless, modern AL-DDoS attacks are stealthy. Thus, the characters that this paper summarizes may not achieve good accuracy.
- Barford et al. [140] and Lu and Ghorbani [97], propose wavelet methods that are generally post-mortem methods that are inappropriate for the real-time detection of AL-DDoS in the backbone traffic.
- Yeung et al. [139] use a covariance matrix to detect AL-DDoS attacks. However, the implementation of such a matrix for every user on a popular website is expensive. The system proposed in the current study performs better than previous works because it uses a simple and efficient algorithm to detect AL-DDoS.
- Some experiments such as in [136] indicate that good performance is achieved when FC and AL-DDoS attacks are distinguished. Moreover, an architecture organization is performed on the basis of modules. Thus, the system and web servers are isolated from each other, and their performance will not affect the detection.

VI. TESTING DATASETS

A number of real datasets are available publicly and have even been widely used for DDoS research [16]. A summary of these real datasets follows.

A. FIFA WORLD CUP DATASET 1998

The 16th Federation International Football Association (FIFA) World Cup takes place in France from June 10, 1998, to July 12, 1998. It is commonly called France '98 and is the most largely covered media event in history. During that time, approximately 40 billion cumulative television audiences watch the 64 matches, which is more than twice the accumulated number of the television audience that watches the 1996 Summer Olympic Games in Atlanta. The website for France '98, http://www.france98.com, is also popular. It has over 1 billion client requests during the tournament. This dataset provides records of the requests that the football World Cup's website received during the period from April 1998 to July 1998. The website receives l.35 billion requests overall [141].

B. MIT LINCOLN LABORATORY DATASET 1998

As a part of this effort, the first attack scenario example dataset is created for DARPA. The dataset contains a DDoS attack run by an inexperienced attacker. In the future, more tricky attack versions will be available in future versions of this, as well as other example scenarios. This laboratory serves as the storehouse of TCP dump network trace data that are captured in real time. For example, a DDoS attack run by a novice attacker is recorded by LLDOS 1.0 dataset. More so, any attack that is launched by a crafty attacker can be recorded by the LLDOS 2.0.2 dataset. The data for all five phases of attack of a DDoS attack is recorded. Initially, the attacker scans the network. By means of exploiting the sadmind vulnerability of the Solaris operating system, the hosts are compromised. Subsequently, the stream DDoS software, which is a Trojan-based malicious program is downloaded. Then, the DDoS attack is launched [142].

C. KDD CUP DATASET 99

The KDD Cup 1999 dataset is produced [143] for the 3rd International Knowledge Discovery and Data Mining Tools Competition. This dataset is widely used for research related to malware. However, it has a very limited scope of usage. It is primarily used for assessing signature-based IDS and is not suitable for assessing DDoS detection, DDoS defense methods (KDD 99), and flash events. The KDD dataset is an important resource for assessing the performance of DDoS detection techniques. The set has 14 attacks that can be used to test and create a model. Several methods that can be used for extracting vital features have been proposed on the basis of this dataset. Furthermore, a broad range of classifiers can be obtained from areas such as statistics. Pattern recognition and machine learning have been assessed against this dataset as well. For instance, in Kim and Park [144], pre-processing of the 1999 KDD dataset is done, followed by learning and testing. During the learning process, the polynomial, radial bias function (RBF), and kernel linear function are used. It achieves a classification accuracy of 93.56%.

D. UCLA DATASET 2001

Packet traces that are gathered in August 2001 by a network research laboratory are contained in this dataset. It also contains records of UDP flood traffic with 1001 B long packets. At the end of the trace, the attack is aborted. Then, legitimate connections proceed [145].

E. CAIDA DDoS ATTACK DATASET 2007

This dataset has the traffic traces of a flooding DDoS attack lasting approximately 1 h. This attack aims to exhaust the targeted server's computing resource, and IP addresses are given pseudonyms. Furthermore, the usability of this dataset is limited because their payloads and non-attack traffic are not included in the dataset for security reasons. This dataset can be used for low stealth rates and high rates of flooding DDoS attacks [145]. The attack component in the experiments is the CAIDA dataset, and the normal traffic component is provided by the data gathered on the SSE network. Normal and attack traffic is classified using an open-source tool called Konstanz Information Miner version 3 [146].

F. WAIKATO DDoS ATTACK DATASET

The Waikato Internet Traffic Storage Project aims to gather and document all the Internet traces possessed by the WAND Group. IP addresses for this dataset have been modified and are therefore not actual. The payload of UDP packets and headers of the transport layer are not included for security reasons [147].

G. DARPA DDoS ATTACK DATASET 2009

The 2009 DARPA dataset refers to a synthesized dataset that is formed to simulate real network and Internet traffic attacks. It lasts for 10 days, that is, from November 3, 2009, to November 12, 2009. The dataset weighs approximately 6.4 TB and is partitioned into thousands of pcap files sized 954 M each. The traffic has synthetic SMTP, HTTP, and DNS background data. The attacks are considered to be large-scale network attacks that include HTTP worms, DNS worms, and DDoS attacks. The worms and DDoS attacks are parameterized for demonstrating different propagation characteristics. This method represents the latest DDoS attack-based dataset obtained from the MIT Lincoln Laboratory. The captured traffic has background traffic and an SYN-based flooding DDoS attack on one target. Approximately 100 different IPs served as the source of the DDoS traffic. These hosts are used to begin a malware DDoS attack on a non-local target [148].

H. TUIDS DDoS ATTACK DATASET 2012

The dataset is prepared using TUIDS testbed architecture and a DMZ made up of traffic from five various networks found within the Tezpur University Campus. The attackers are positioned in wireless and wired networks with reflectors. Then, the target is positioned within the internal network. This dataset can also be used to detect low stealth rates and high rates of flooding DDoS attacks [149].

I. FRGP NTP FLOW DATASET

Three months' worth of daily Network Time Protocol (NTP) traffic is presented in the form of Argus flows. These flows are found on a 10 Gb/s link found between content and a regional ISP. A number of academic and research institutions are involved in the traffic. NTP traffic gathered at a university and NTP DDoS reflection attack traffic is also part of the dataset. To trigger these attacks, the attackers send monlist queries with spoofed source IP addresses. These queries are sent to vulnerable hosts that run NTP. These vulnerable hosts then answer with a list of last clients (up to 600), which typically generates larger replies compared with smaller queries [150].

J. BOOTER DNS DATASET 2014

This dataset can detect amplification DDoS and DNS-based reflection attacks. This dataset represents the record of DNSSEC-signed domains, including traffic from approximately 70% of all active domains [151].

TABLE 12. Summary of DDoS attack datasets.

Year	Dataset	Scope	Type of traffic	Network layer
1998	FIFA World Cup	Flash	HTTP	Application
1998-2000	MIT Lincoln	DDoS	TCP	Transport
1999	KDD Cup	FC, DDoS	TCP	Transport
2001	UCLA	DDoS	UDP	Transport
2007	CAIDA	DDoS	ICMP	Network
2009	Waikato	DDoS	UDP	Transport
2009	DARPA	DDoS	HTTP, SMTP, DNS, TCP	Application, Transport
2012	TUIDS	DDoS	ICMP, TCP, UDP	Network, Transport
2013	FRGP NTP Flow Data	DDoS	NTP	Application
2014	Booter	DDoS	DNS	Application
2014	FRGP_SSDP	DDoS	SSTP, UDP and ICMP	Network, Transport

K. FRGP SSDP REFLECTION DATASET

Approximately 3 H of DDoS attack traffic is sent to a victim in the form of Argus flows. UDP simple service discovery protocol (SSDP) traffic is the form that most attack traffic assumes. ICMP and other kinds of UDP traffic protocols are included. The flows are found on a 10-GB/s link between the content and a regional ISP. These attacks are triggered by attackers via UPnP/SSDP discovery requests to vulnerable hosts that run SSDP. The attackers also use spoofed source IP addresses ([150]. The summary of the dataset is shown in Table 12.

VII. ANALYSIS AND DISCUSSION

The related literature review papers in this field have been focused on certain aspects of DDoS security threats and solutions such as the type of attacks, defense methods, evaluation methods or testing datasets. This paper offers a thorough and detailed review of various methods to detect and prevent DDoS attacks, according to the classification of statistical and artificial intelligence approaches that are feasible at the OSI layered model. A large body of research is consulted in the preparation for this comprehensive literature review paper. A total of 151 data sources and including six review papers have been studied in order to outcome this masterpiece. The aim of this review is to provide guidelines for developing improved DDoS defensive methods and strategies and integrating effective solutions. The paper contexts on attackers' motivations that prompt such persons to flood targeted networks. It exploits and classifies the common DDoS attacks and determines the targeted particular and recognizes appropriate defensive methods of each class.

The DDoS attack is a malicious incident that does not require internal system access. It entails the recruitment of a great number of zombies which inflicts the possible damage. Therefore, it is hard to be detected in its early stage. The critical types of the attack are redirecting a multitude of nodes onto a single target which can cause catastrophic effects to its victims and plague the networks. On the other hand, the solutions against DDoS attacks are mainly divided into recognition, mitigation and prevention methods. The defensive

methods that rely on statistical and artificial intelligence approaches, in general, provide improved results against DDoS attacks. The following discusses the contribution of artificial intelligence and statistical techniques in DDoS defense methods.

- Bayesian networks classifier is used to (1) detect and recognize DDoS attack in real-time as in [51]; (2) detect and defense against collective DDoS attack on HTTP as in [52] and (3) assess the reliability of access routers when forwarding packets to detect and mitigate DDoS attack as in [50].
- Fuzzy logic technique is used to (1) reduce the ambiguity and increase the accuracy of DDoS attack detection as in [57]; (2) perform self-adaptive judgment in order to improve the detection of DDoS attack in real-time as in [58]; (3) dynamically estimate the intensity of DDoS flooding attack incidents in real-time as in [53].
- Genetic algorithm is used to (1) train instances' selection and improve the classification efficiency of DDoS attack as in [59]; (2) recognize legitimate users during DDoS flooding attacks on both SIP and TCP protocols as in [60]; (3) optimize the parameters of the traffic matrix in order to enhance the recognition rates of the DDoS attack as in [61].
- The K-Nearest Neighbors classifier is used to (1) classify the network status during DDoS attack in order to accurately detect and categorize the attack as in [63]; (2) estimate the unknown class of requests in order to improve the anomaly traffic detection method as in [59] and (3) recognize anomalous in network behavior by processing large data volumes and in a shortest possible time as in [64].
- Neural networks classifier is used to (1) early detect and recognize DDoS attack of a traditional IDS as in [66] work that proposes rationale of time delay neural network for this purpose; (2) detect and defense against DDoS attack by a lightweight trainable method as in [67] and (3) automatically detect and classify DDoS attack and measure network service condition of social media servers as in [69].
- Software agent technique covers various roles in DDoS attack and defense methods. It provides various mechanisms of communication and decision-making to (1) compare current traffic with the normal traffic in real-time in order to control network traffic and mitigate DDoS attack as in [72], [73]; (2) defense against DDoS attack as in [74] and (3) make a distributed defensive scheme against DDoS attacks in the ISP domains as in [75].
- Lastly, the SVM also functions to classify different aspects of DDoS attack. It is used to (1) detect anomalies of the network traffic by deploying a set of training inputs of attack instances as in [70] and [76]; and (2) classify normal traffic from attack and determine the type of the attack as in [77].
- The statistically based defensive methods are formed in accordance with parametric and non-parametric classifications. Many researchers apparently use statistical-based approaches to mitigate and defeat DDoS attacks by implementing statistical defensive strategies. Certain studies use parametric techniques, such as [80], [82], [83] and [84], and attains excellent defensive results versus DDoS attacks. On the other hand, non-parametric methods are used by [87]–[90], [95], and [98] to defend against DDoS attacks. The non-parametric methods are useful when there is no enough description to the properties of the attack.

Table 13 shows the correlation between the defense models of both the artificial intelligence and statistical approaches and evaluation methods according to this review. From the table, we can conclude that the quantitative evaluation methods are the most popular methods among others for both artificial intelligence and statistical approaches in which the accuracy is the most usable evaluation parameter. On the other hand, the qualitative evaluation methods are the less popular evaluation methods in general.

In summary, a DDoS attack is a scalability network security problem. Although there are many detection defensive methods against DDoS attack, there is limited success in implementing them across a wide range of networks. The artificial intelligence approach is mainly used to classify the aggregated records of requests as ordinary or intrusive according to the traffic and the requests' attributes. It is mainly adopted to avoid the shortcomings assumptions of the crisp statistical approach such as the typical distribution of the traffic. The time is an important factor in selecting an appropriate artificial intelligence technique as most of the methods are used for the DDoS attack in real-time. Early detection to the DDoS attack is another importing factor for formulating effective defense methods. The K-NN is found to be one of the most time efficient technique. Agents provide mechanisms of communication and decision-making for the attack and defense methods. They compare current traffic with the normal traffic in real-time to identify anomaly traffic. Then they adjust network traffic to mitigate the DDoS attack. Some of the research gaps that are identified in this work are reviewed as follows:

- The literature lacks attempts to extract, evaluate and select optimize features of network traffic for developing advanced DDoS attack detection and prevention methods. The classifiers need to be continuously supported with new and updated features in order to cup up with new threats.
- There is a dominant need for realistic and updated datasets that can simulate heterogeneous and scalable traffic of DDoS attack.
- There is no much research have been down on distinguishing a DDoS attack from FC flooding attacks.
- Most of the reviewed methods lack defenses mechanisms against collective attacks. The distributed and dynamic nature of the multi-agent system provides the

TABLE 13. The correlation between artificial intelligence and statistical approaches with evaluation methods.

Evaluation methods	Artificial Intelligence																						Statistical									
	Bayesian Networks			Fuzzy logic			Genetic Algorithm			K-NN		Neural Network					Software Agent				SVM		Parametric				Non-parametric					
	[50]	[51]	[52]	[53]	[57]	[58]	[59]	[60]	[61]	[62]	[63]	[66]	[67]	[69]	[70]	[71]	[1]	[73]	[74]	[75]	[76]	[85]	[80]	[82]	[83]	[84]	[87]	[88]	[89]	[90]	[95]	[98]
Complexity	-	x	-	x	-	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Efficiency	-	-	x	-	-	-	x	-	-	x	-	-	x	-	-	-	-	-	-	x	-	x	-	-	-	-	-	-	-	-	-	-
Scalability	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Precision	-	-	-	-	-	x	-	-	-	-	x	-	-	x	-	-	-	-	-	-	-	-	-	x	-	x	-	-	-	-	-	-
Accuracy	x	x	x	x	x	x	x	x	x	x	x	-	x	x	x	-	-	x	x	x	x	x	x	-	-	x	x	x	x	x	x	x
F-measure	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Packet drop rate	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Throughput	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-
Attack impact	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Time	x	x	x	x	x	x	x	x	x	x	-	x	x	-	x	x	x	-	x	x	x	-	-	x	x	-	x	-	-	x	x	x
CPU load	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-
Memory usage	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	x	x	-
Bandwidth	-	x	-	-	-	-	-	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	x
Financial cost	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-
Detection Rate	-	x	-	-	-	-	x	-	x	x	x	-	x	-	-	-	-	-	x	x	-	-	-	-	-	-	-	x	-	-	x	-
Latency	x	x	-	-	-	-	-	-	x	-	-	x	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

potentials to handle collective attacks and multilevel solutions platform.

- In order to come up with a realistic solution to the DDoS attack, there is a need to combine potential DDoS defensive methods in one cybersecurity platform.

VIII. CONCLUSION

This paper attempts to provide an insight into the existing DDoS attack methodologies and a comprehensive review of the proposed solutions of numerous defense methods and techniques. The review covers a total of 129 research articles, six network security reports, ten links of the dataset and six review articles. It is applicable to web applications, web servers, web services, cloud computing, and any device with an Internet connection. The review offers a thorough and detailed review of statistical and Artificial Intelligence approaches that are utilized in detecting and preventing DDoS attacks. It segments DDoS attacks according to the class of vulnerability, the degree of automation, impact, and dynamics. The paper aims to help in emerging advanced and effective defense methods for the DDoS attacks from the accumulation of the existing research. Furthermore, the classifications of the related aspects of DDoS attack entails continuous improvements and updates in order to deal with new and multipart threats. Finally, the paper identifies five research gaps that can manifest the shape of future work.

REFERENCES

[1] I. Kotenko and A. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms," *Int. J. Comput.* , vol. 4, no. 2, pp. 113–123, 2014.

[2] K. Sharma and B. B. Gupta, "Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Present Era of Smartphone Devices," *Int. J. E-Services Mobile Appl.*, vol. 10, no. 2, pp. 58–74, 2018.

[3] 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, Jan. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S092523121501053X

[4] K. M. Prasad, A. R. Reddy, and K. V. Rao, "DoS and DDoS attacks: Defense, detection and traceback mechanisms—A survey," *Global J. Comput. Sci. Technol.*, vol. 14, no. 7, pp. 1–19, 2014.

[5] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yong, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," in *Proc. 6th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2014, pp. 63–68.

[6] H. D'Cruze, P. Wang, R.O. Sbeit, and A. Ray, "A software-defined networking (SDN) approach to mitigating DDoS attacks," *Inf. Technol.-New Gener.* Cham, Switzerland: Springer, 2018, pp. 141–145.

[7] S. Jamali and V. Shaker, "Defense against SYN flooding attacks: A particle swarm optimization approach," *Comput. Elect. Eng.*, vol. 40, no. 6, pp. 2013–2025, 2014.

[8] A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah, I. Awan, and N. B.Anuar, "Botnet detection techniques: Review, future trends, and issues," *J. Zhejiang Univ. Sci. C*, vol. 15, no. 11, pp. 943–983, Nov. 2014.

[9] G. C. Kessler, "Computer security handbook," in *Denial-of-Service Attacks*, 6th ed. London, U.K.: Wiley, 2014, ch. 18.

[10] B. Acohido and J. Swartz. *ABC News Live Journal, New York.* Accessed: Aug. 2009. [Online]. Available: https://abcnews.go.com/ /story?id=8271907&page=1

[11] M. Uysal and S. R. Ranjan Swaminathan, "DDoS-resilient scheduling to counter application layer attacks under imperfect detection," in *Proc. 25TH IEEE Int. Conf. Comput. Commun.*, Apr. 2006, pp. 1–13.

[12] S. Behal, K. Kumar, and M. Sachdeva, "Characterizing DDoS attacks and flash events: Review, research gaps and future directions," *Comput. Sci. Rev.*, vol. 25, pp. 101–114, Aug. 2017.

[13] G. Oikonomou and J. Mirkovic, "Modeling human behavior for defense against flash-crowd attacks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–6.

[14] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Netw.*, vol. 44, no. 5, pp. 643–666, Apr. 2004.

[15] M. Aamir and M. A. Zaidi, "A survey on DDoS attack and defense strategies: From traditional schemes to current techniques," *Interdiscipl. Inf. Sci.*, vol. 19, no. 2, pp. 173–200, 2013.

[16] S. Behal and K. Kumar, "Trends in validation of DDoS research," *Procedia Comput. Sci.*, vol. 85, pp. 7–15, May 2016.

[17] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Comput. Commun.*, vol. 107, pp. 30–48, Jul. 2017.

[18] N. S. Rao, K. C. Sekharaiah, and A. A. Rao, "A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains," *Innov. Comput. Sci. Eng.*, vol. 32, pp. 221–230, May 2019.

[19] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, "Flow level detection and filtering of low-rate DDoS," *Comput. Netw.*, vol. 56, no. 15, pp. 3417–3431, 2012.

[20] S. H. Li, Y. C. Kao, Z. C. Zhang, Y. P. Chuang, and D. C. Yen, "A network behavior-based botnet detection mechanism using PSO and K-means," *ACM Trans. Manage. Inf. Syst.*, vol. 6, no. 1, p. 3, Apr. 2015.

[21] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 303–336, 1st Quart., 2014.

[22] C. Buragohain, M. J. Kalita, S. Singh, and D. K. Bhattacharyya, "Anomaly based DDoS attack detection," *Int. J. Comput. Appl.*, vol. 123, p. 17, Aug. 2015.

[23] S. M. Mousavi, "Early detection of DDoS attacks in software defined networks controller," Ph.D dissertation, Dept. Elect. Comput. Eng., Carleton University Ottawa, Ottawa, Canada, 2014.

[24] Verisign. (2014). *Retrieved From.* [Online]. Available: https://www.verisign.com/en_IN/ security-services/ddos-protection/ddos-report/index.xhtml

[25] C. Baraniuk. (2015). *Retrieved From.* [Online]. Available: http://www.bbc.com/news/technology-35376327

[26] S. Khandelwal. (2016). *Retrieved From.* [Online]. Available: http://thehackernews.com/2016/ 01/biggest-ddos-attack.html

[27] Woolf. (2016). [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[28] (2018). *Akamai, U.S.*. [Online]. Available: https://www.akamai.com/uk/en/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

[29] A. Bhandari, A. L. Sangal, and K. Kumar, "Destination address entropy based detection and traceback approach against distributed denial of service attacks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 8, p. 9, Jul. 2015.

[30] (2018). *Arbor Networks, U.S.*. Accessed on: Nov. 2018. [Online]. Available: https://www.netscout.com/report/

[31] G. V. Nadiammai and M. Hemalatha, "Effective approach toward intrusion detection system using data mining techniques," *Egyptian Inform. J.*, vol. 15, no. 1, pp. 37–50, Mar. 2014.

[32] A. Aggarwal and A. Gao, "Survey on data mining and IP traceback technique in DDoS attack," *Int. J. Eng. Comput. Sci.*, vol. 4, p. 06, Feb. 2015.

[33] S. Specht and R. Lee, "Taxonomies of distributed denial of service networks, attacks, tools and countermeasures," Princeton Univ., Princeton, NJ, USA, Tech. Rep. CE-L2003-03, 2003.

[34] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004.

[35] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, Mar. 2013.

[36] K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," *Comput. Secur.*, vol. 65, pp. 344–372, Mar. 2017.

[37] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, "Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13," in *Proc. Int. Conf. Commun., Signal Process., Their Appl.*, Feb. 2015, pp. 1–5.

[38] M. V. Kumar and R. Umar, "Identifying and blocking high and low rate DDOS ICMP flooding," *Indian J. Sci. Technol.*, vol. 8, p. 32, Aug. 2015.

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

[40] R. K. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 42–51, Mar. 2002.

[41] Z. Ye, W. Shi, and D. Ye, "DDoS defense using TCP_IP header analysis and proactive tests," in *Proc. Int. Conf. Inf. Technol. Comput. Sci.*, vol. 2, Jul. 2009, pp. 548–552.

[42] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Exit from hell? reducing the impact of amplification DDoS attacks," in *Proc. USENIX Security Symp.*, Aug. 2014, pp. 111–125.

[43] W. M. Eddy, "Syn flood attack," in *Encyclopedia Cryptography Security*, New York, NY, USA: Springer, 2011, pp. 1273–1274.

[44] S. Fichera, L. Galluccio, S. C. Grancagnolo, G. Morabito, and S. Palazzo, "OPERETTA: An OPEnflow-based REmedy to mitigate TCP SYN-FLOOD attacks against web servers," *Comput. Netw.*, vol. 92, no. 1, pp. 89–100, 2015.

[45] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures," in *Proc. ISCA PDCS*, Sep. 2004, pp. 543–550.

[46] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Comput. Netw.*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007.

[47] P. Garcia-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, nos. 1–2, pp. 18–28, 2009.

[48] S.-Y. Wu and E. Yen, "Data mining-based intrusion detectors," *Expert Syst. Appl.*, vol. 36, no. 3, pp. 5605–5612, 2009.

[49] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "PacketScore: A statistics-based packet filtering scheme against distributed denial-of-service attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 2, pp. 141–155, Apr. 2006.

[50] J. M. Gonzalez, M. Anwar, and J. B. Joshi, "A trust-based approach against IP-spoofing attacks," in *Proc. 9th Annu. Int. Conf. Privacy, Secur. Trust*, Jul. 2011, pp. 63–70.

[51] R. Vijayasarathy, S. V. Raghavan, and R. B. Ravindran, "A system approach to network modeling for DDoS detection using a Naive Bayesian classifier," in *Proc. 3rd Int. Conf. Commun. Syst. Netw.*, Jan. 2011, pp. 1–10.

[52] V. Katkar, A. Zinjade, S. Dalvi, T. Bafna, and R. Mahajan, "Detection of DoS/DDoS attack against HTTP servers using naive Bayesian," in *Proc. Int. Conf. Comput. Commun. Control Automat.*, Feb. 2015, pp. 280–285

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

[54] A. Chauhan, G. Mishra, and G. Kang, "Survey on data mining techniques in intrusion detection," *Int. J. Sci. Eng. Res.*, vol. 2, no. 7, pp. 1–4, 2011.

[55] H. Kaur, G. Singh, and J. Minhas. (2016). "A review of machine learning based anomaly detection techniques." [Online]. Available: https://arxiv.org/abs/1307.7286

[56] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," in *Proc. 19th Int. Conf. North Amer. Fuzzy Inf. Process. Soc.*, Jul. 2000, pp. 301–306.

[57] W. Wei, Y. Dong, D. Lu, and G. Jin, "Combining cross-correlation and fuzzy classification to detect distributed denial-of-service attacks," in *Proc. Int. Conf. Comput. Sci.*, May 2006, pp. 57–64.

[58] J. Wang and G. Yang, "An intelligent method for real-time detection of DDoS attack based on fuzzy logic," *J. Electron.*, vol. 25, no. 4, pp. 511–518, Jul. 2008.

[59] Y. Li, L. Guo, Z. H. Tian, and T. B. Lu, "A lightweight web server anomaly detection method based on transductive scheme and genetic algorithms," *Comput. Commun.*, vol. 31, no. 17, pp. 4018–4025, Nov. 2008.

[60] A. Rahul, S. K. Prashanth, K. B. Suresh, and G. Anger, "Detection of intruders and flooding in Voip using IDS, jacobson fast and Hellinger distance algorithms," *IOSR J. Comput. Eng.*, vol. 2, no. 2, pp. 30–36, 2012.

[61] S. M. Lee, D. S. Kim, J. H. Lee, and J. S. Park, "Detection of DDoS attacks using optimized traffic matrix," *Comput. Math. Appl.*, vol. 63, no. 2, pp. 501–510, Jan. 2012.

[62] K. R. W. Bandara *et al.* "Preventing DDoS attack using data mining algorithms," *Int. J. Sci. Res.*, vol. 6, no. 10, p. 390, 2016.

[63] H. V. Nguyen and Y. Choi, "Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDoS framework," *Int. J. Electr., Comput., Syst. Eng.*, vol. 4, no. 4, pp. 247–252, Feb. 2010.

[64] M. Barrionuevo, M. Lopresti, N. Miranda, and F. Piccoli, "An anomaly detection model in a LAN using K-NN and high performance computing techniques," in *Computer Science—CACIC*. Cham, Switzerland: Springer, Oct. 2017, pp. 219–228.

[65] M. Gyanchandani, J. L. Rana, and R. N. Yadav, "Taxonomy of anomaly based intrusion detection system: A review," *Int. J. Sci. Res.*, vol. 2, no. 12, pp. 1–13, Dec. 2012.

[66] C. L. Tsai, A. Y. Chang, and M. S. Huang, "Early warning system for DDoS attacking based on multilayer deployment of time delay neural network," in *Proc. 65th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2010, pp. 704–707.

[67] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. IEEE Local Comput. Netw. Conf.*, Oct. 2010, pp. 408–415.

[68] Q. Niyaz, W. Sun, and A. Y. Javaid. (2016). "A deep learning based DDoS detection system in software-defined networking (SDN)." [Online]. Available: https://arxiv.org/abs/1611.07400

[69] N. Chambers, B. Fry, and J. Mao, "Detecting denial-of-service attacks from social media Text: Applying NLP to computer security," in *Proc. Conf. North Amer. Chapter Assoc. Comput. Linguistics Hum. Lang. Technol.*, Vol. 1, 2018, pp. 1626–1635.

[70] C. Cheng, W. P. Tay, and G. B. Huang, "Extreme learning machines for intrusion detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jun. 2012, pp. 1–8.
[71] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018.
[72] B. A. Khalaf, S. A. Mostafa, A. Mustapha, and N. Angal, "An adaptive model for detection and prevention of DDoS and flash crowd flooding attacks," In *Proc. Int. Symp. Agent, Multi-Agent Syst. Robot.*, Aug. 2018, pp. 1–6.
[73] D. Juneja, R. Chawla, and A. Singh, "An agent-based framework to counter attack DDoS attacks," *Int. J. Wireless Netw. Commun.*, vol. 1, no. 2, p. 193, 2009.
[74] R. Kesavamoorthy and K. R. Soundar, "Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system," *Cluster Comput.*, vol. 276, pp. 1–8, Mar. 2018.
[75] K. Singh, K. S. Dhindsa, and B. Bhushan, "Performance analysis of agent based distributed defense mechanisms against DDoS attacks," *Int. J. Comput.*, vol. 17, no. 1, pp. 15–24, Mar. 2018.
[76] J. Seo, C. Lee, T. Shon, K. H. Cho, and J. Moon, "A new DDoS detection model using multiple SVMs and TRA," in *Proc. Int. Conf. Embedded Ubiquitous Comput.*, Dec. 2005, pp. 976–985.
[77] J. Yu, H. Lee, M. S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Comput. Commun.*, vol. 31, no. 17, pp. 4212–4219, 2008.
[78] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016.
[79] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.
[80] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 447–456, Feb. 2014.
[81] Y. Purwanto and B. Rahardjo, "Traffic anomaly detection in DDos flooding attack," in *Proc. 8th Int. Conf. Telecommun. Syst. Services Appl.*, Oct. 2014, pp. 1–6.
[82] C. M. Cheng, H. T. Kung, and K. S. Tan, "Use of spectral analysis in defense against DoS attacks," in *Proc. Global Telecommun. Conf.*, vol. 3, Nov. 2002, pp. 2143–2148.
[83] M. Li and M. Li, "A new approach for detecting DDoS attacks based on wavelet analysis," in *Proc. 2nd Int. Congr. Image Signal Process.*, vol. 2009, pp. 1–5.
[84] A. Dainotti, A. Pescapé, and G. Ventre, "A cascade architecture for DoS attacks detection based on the wavelet transform," *J. Comput. Secur.*, vol. 17, no. 6, pp. 945–968, 2009.
[85] P. Owezarski, "On the impact of DoS attacks on Internet traffic characteristics and QoS," in *Proc. 14th Int. Conf. Comput. Commun. Netw.*, Oct. 2005, pp. 269–274.
[86] Y. Chen, K. Hwang, and W. S. Ku, "Distributed change-point detection of DDoS attacks over multiple network domains," in *Proc. Int. Symp. Collaborative Technol. Syst.*, May 2006, pp. 543–550.
[87] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," in *Proc. 10th IEEE Int. Conf. Netw. Protocols*, Nov. 2002, pp. 312–321.
[88] J. Cheng, J. Yin, C. Wu, B. Zhang, and Y. Lin, "DDoS attack detection method based on linear prediction model," In *International Conference on Intelligent Computing, Springer, Berlin, Sep.*, vol. 2009, pp. 1004–1013.
[89] Y. Xie and S. Z. Yu, "A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 54–65, Feb. 2009.
[90] R. Saranya, S. S. Kannan, and S. M. Sundaram, "Integrated quantum flow and hidden Markov chain approach for resisting DDoS attack and C-Worm,"Cluster Computing, pp. 1–12.(2018).
[91] H. Beitollahi and G. Deconinck, "Denial of Service Attacks: A Tutorial," Dept. Elect. Eng., Univ. Leuven, Leuven, Belgium, Tech. Rep. 08-2011-0115, 2011.
[92] H. Beitollahi and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," *Comput. Commun.*, vol. 35, no. 11, pp. 1312–1332, Jun. 2012.
[93] B. B. Gupta, P. K. Agrawal, R. C. Joshi, and M. Misra, "Estimating Strength of a DDoS Attack Using Multiple Regression Analysis," in *Proc. Int. Conf. Comput. Sci. Inf. Technol.*, Jan. 2011, pp. 280–289.
[94] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan. 2006.
[95] A. Lung-Yut-Fong, C. Lévy-Leduc, and O. Cappé, "Distributed detection/localization of change-points in high-dimensional network traffic data," *Statist. Comput.*, vol. 22, no. 2, pp. 485–496, Mar. 2012.
[96] L. Li and G. Lee, "DDoS attack detection and wavelets," *Telecommun. Syst.*, vol. 28, nos. 3–4, pp. 435–451, 2005.
[97] W. Lu and A. A. Ghorbani, "Network anomaly detection based on wavelet analysis," *J. Adv. Signal Process.*, vol. 44, p. 4, Jun. 2009.
[98] J. Udhayan and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks," *IJ Netw. Secur.*, vol. 13, no. 3, pp. 152–160, Nov. 2011.
[99] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Statistical measures: Promising features for time series based DDoS attack detection," *Multidisciplinary Digit. Inst. Proc.*, vol. 2, no. 2, p. 96, Jan. 2018.
[100] C. C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *Proc. 39th Int. Conf. Parallel Process. Workshops*, Sep. 2010, pp. 280–284.
[101] P. Shamsolmoali and M. Zareapoor, "Statistical-based filtering system against DDOS attacks in cloud computing," In *Proc. Int. Conf. Adv. Comput., Commun. Inform.*, Sep. 2014, pp. 1234–1239.
[102] P. R. K. Reddy and S. Bouzefrane, "Analysis and detection of DoS attacks in cloud computing by using QSE algorithm," in *Proc. IEEE Int. Conf. High Perform. Comput. Commun.*, Aug. 2014, pp. 1089–1096.
[103] H. Hamad and M. Al-Hoby, "Managing intrusion detection as a service in cloud networks," *Int. J. Comput. Appl.*, vol. 41, p. 1, Feb. 2012.
[104] S. S. Chapade, K. U. Pandey, and D. S. Bhade, "Securing cloud servers against flooding based DDoS attacks," in *Proc. Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2013, pp. 524–528.
[105] L. Yang, T. Zhang, J. Song, J. Wang, and P. Chen, "Defense of DDoS attack for cloud computing," in *Proc. IEEE Int. Conf. Comput. Sci. Automat. Eng.*, vol. 2, May 2012, pp. 626–629.
[106] A. Chonka and J. Abawajy, "Detecting and mitigating HX-DoS attacks against cloud web services," in *Proc. 15th Int. Conf. Netw.-Based Inf. Syst.*, Sep. 2012, pp. 429–434.
[107] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," *Comput. Netw.*, vol. 81, pp. 308–319, Mar. 2015.
[108] W. Lee, A. C. Squicciarini, and E. Bertino, "Detection and protection against distributed denial of service attacks in accountable grid computing systems," in *Proc. 11th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput.*, May 2011, pp. 534–543.
[109] M. Ali, S. Khattab, and R. Bahgat, "Improving detection accuracy in group testing-based identification of misbehaving data sources," in *Proc. Int. Conf. Future Internet Things Cloud*, Aug. 2014, pp. 167–174.
[110] G. Nascimento and M. Correia, "Anomaly-based intrusion detection in software as a service," in *Proc. 41st Int. Conf. Dependable Syst. Netw. Workshops*, Jun. 2011, pp. 19–24.
[111] H. Badis, G. Doyen, and R. Khatoun, "Toward a source detection of bot-clouds: A PCA-based approach," in *IFIP Int. Conf. Auto. Infrastructure, Manage. Security*. Berlin, Germany: Springer, Jun. 2014, pp. 105–117.
[112] C. N. Modi, D. R. Patel, A. Patel, and R. Muttukrishnan, "Bayesian Classifier and Snort based network intrusion detection system in cloud computing," in *Proc. 3rd Int. Conf. Comput., Commun. Netw. Technol.*, Jul. 2012, pp. 1–7.
[113] A. M. Lonea, D. E. Popescu, O. Prostean, and T. H. , "Evaluation of experiments on detecting distributed denial of service (DDoS) attacks in Eucalyptus private cloud," in *Soft Computing Applications*. Berlin, Germany: Springer, 2013, pp. 367–379.
[114] H. Wang, H. Zhou, and C. Wang, "Virtual machine-based intrusion detection system framework in cloud computing environment," *JCP*, vol. 7, no. 10, pp. 2397–2403, Oct. 2012.
[115] M. T. Khorshed, A. S. Ali, and S. A. Isimi, "Classifying different denial-of-service attacks in cloud computing using rule-based learning learning," *Secur. Commun. Netw.*, vol. 5, no. 11, pp. 1235–1247, Nov. 2012.
[116] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1097–1107, 2011.
[117] C. J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 4, pp. 198–211, 2013.

[118] A. Michalas, N. Komninos, and N. R. Prasad, "Mitigate dos and DDoS attack in mobile ad hoc networks," *Int. J. Digit. Crime Forensics (IJDCF)*, vol. 3, no. 1, pp. 14–36, 2011.
[119] R. Aishwarya and S. Malliga, "Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment," in *Proc. Int. Conf. Recent Trends Inf. Technol.*, Apr. 2014, pp. 1–6.
[120] H. Jin *et al.*, "A VMM-based intrusion prevention system in cloud computing environment," *J. Supercomput.*, vol. 66, no. 3, pp. 1133–1151, 2013.
[121] C. J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 4, pp. 198–211, Jul. 2013.
[122] M. J. Sowmya, M. S. Kumar, and D. J. Mungara, "An empirical framework to detect security attacks on the cloud data storage system," *Int. J. Comput. Sci. Issues*, vol. 9, no. 4, pp. 265–271, Jul. 2012.
[123] N. C. S. N. Iyengar, G. Ganapathy, P. C. Mogan Kumar, and A. Abraham, "A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment," *Int. J. Grid Utility Comput.*, vol. 5, no. 4, pp. 236–248, 2014.
[124] N. Jeyanthi, U. Barde, M. Sravani, V. Tiwari, and N. C. S. N. Iyengar, "Detection of distributed denial of service attacks in cloud computing by identifying spoofed IP," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 11, no. 3, pp. 262–279, Jan. 2013.
[125] G. Preetha, B. S. Devi, and S. M. Shalinie, "Autonomous agent for DDoS attack detection and defense in an experimental testbed," *Int. J. Fuzzy Syst.*, vol. 16, p. 4, Dec. 2014.
[126] R. A. Michelin, A. F. Zorzo, and C. A. de Rose, "Mitigating dos to authenticated cloud rest apis," in *Proc. 9th Int. Conf. Internet Technol. Secured Trans.*, Dec. 2014, pp. 106–111.
[127] R. Lua and K. C. Yow, "Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network," *IEEE Netw.*, vol. 25, no. 4, pp. 28-33, Aug. 2011.
[128] T. Vissers, T. S. Somasundaram, L. Pieters, K. Govindarajan, and P. Hellinckx, "DDoS defense system for web services in a cloud environment," *Future Gener. Comput. Syst.*, vol. 37, pp. 37–45, Jul. 2014.
[129] R. M. Sarhadi and V. Ghafori, "New approach to mitigate XML-DOS and HTTP-DOS attacks for cloud computing," *Int. J. Comput. Appl.*, vol. 72, no. 16, pp. 27–31, Jun. 2013.
[130] I. Gul and M. Hussain, "Distributed cloud intrusion detection model," *Int. J. Adv. Sci. Technol.*, vol. 34, no. 38, p. 135, 2011.
[131] W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1838–1850, 2013.
[132] J. Choi, C. Choi, B. Ko, and P. Kim, "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment," *Soft Comput.*, vol. 18, no. 9, pp. 1697–1703, 2014.
[133] D. Smith, Q. Guan, and S. fu, "An anomaly detection framework for autonomic management of compute cloud systems," in *Proc. 34th Annu. Comput. Softw. Appl. Conf. Workshops*, Jul. 2010, pp. 376–381.
[134] A. V. Dastjerdi, K. A. Bakar, and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," in *Proc. 3rd Int. Conf. Adv. Eng. Comput. Appl. Sci.*, Oct. 2009, pp. 175–180.
[135] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can we beat DDoS attacks in clouds?" *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2245–2254, Sep. 2014.
[136] W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic," *Future Gener. Comput. Syst.*, vol. 38, pp. 36–46, Sep. 2014.
[137] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-sale: Surviving organized DDoS attacks that mimic flash crowds," In *Proc. 2nd Conf. Symp. Networked Syst. Design Implement.-Volume*, vol. 2, May 2005, pp. 287–300.
[138] J. Jung, B. Krishnamurthy, and M. Rabinovich , "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in *Proc. 11th Int. Conf. World Wide Web*, May 2002, pp. 293–304.
[139] D. S. Yeung, S. Jin, and X. Wang, "Covariance-matrix modeling and detecting various flooding attacks," *IEEE Trans. Syst., Man, A, Syst. Hum.*, vol. 37, no. 2, pp. 157–169, Mar. 2007.
[140] P. Barford, J. Kline, D. Plonka, and R. A. , "A signal analysis of network traffic anomalies," in *Proc. 2nd ACM SIGCOMM Workshop Internet Measurment*, Nov. 2002, pp. 71–82.
[141] FIFA. (2018). *The FIFA World Cup Dataset*. [Online]. Available: http://ita.ee.lbl.gov/html/contrib/worldcup.html 1998.
[142] MIT. (2000). *Lincoln Laboratory, U.S. Lexington*. [Online]. Available: https://www.ll.mit.edu/ideval/data/2000/llsddos1.0.html
[143] KDD. (1999). *Information and Computer Science University of California, Irvine U.S. California*. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[144] D. S. Kim and J. S. Park, "Network-based intrusion detection with support vector machines," in *Proc. Int. Conf. Inf. Netw.*, 2018, pp. 747–756.
[145] UCLA. (2001). *U.S. California*. [Online]. Available: https://lasr.cs.ucla.edu/ddos/traces/
[146] CAIDA. (2007). *U.S. San Diego*. [Online]. Available: https://www.caida.org/data/passive/ddos-20070804_dataset.xml
[147] WAIKATO. (2000). *Powering Scientific Discovery and Innovation, New Zealand's*. https://wand.net.nz/wits/
[148] DARPA. (2000). *Lincoln Laboratory, U.S. Lexington*. [Online]. Available: https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets
[149] TUIDS. (2012). *Center for Machine Learning and Intelligent Systems, U.S.*. [Online]. Available: http://archive.ics.uci.edu/ml/index.php
[150] FRGP_SSDP. (2017). *USC/ISI ANT Datasets, U.S. California*. [Online]. Available: https://ant.isi.edu/index.html
[151] Booter. (2016). *Github, Netherlands*. [Online]. Available: https://github.com/jjsantanna/Booter-black-List/tree/master/Crawler

Authors' photographs and biographies not available at the time of publication.