This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges

Neha Agrawal and Shashikala Tapaswi, *Senior Member, IEEE*

***Abstract*—The salient features of cloud computing (such as on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service) are being exploited by attackers to launch the severe Distributed Denial of Service (DDoS) attack. Generally, the DDoS attacks in such an environment have been implemented by flooding a huge volume (high-rate) of malicious traffic to exhaust the victim servers' resources. Due to this huge volume of malicious traffic, such attacks can be easily detected. Thus, attackers are getting attracted towards the low-rate DDoS attacks, slowly. Low-rate DDoS attacks are difficult to detect due to their stealthy and low-rate traffic. In the recent years, many efforts have been devoted to defend against the low-rate DDoS attacks. By utilizing the salient features of cloud computing, it becomes easy for an attacker to launch sophisticated low-rate DDoS attacks. Thus, the study of various DDoS attacks and their corresponding defense approaches becomes essential to protect the cloud infrastructure from fatal effects of DDoS attacks. This paper presents a comprehensive taxonomy of all the possible variants of cloud DDoS attacks solutions with detailed insight into the characterization, prevention, detection, and mitigation mechanisms. The paper provides a detailed discussion on essential performance metrics to evaluate various defense solutions and their behavior in a cloud environment. The purpose of this survey paper is to excite the cloud security researchers to develop effective defense solutions against the various DDoS attacks. The research gaps and challenges are found, and described in the paper while future research directions are outlined.**

***Index Terms*—Cloud computing security, Availability, DDoS attacks, High-rate DDoS attacks, Low-rate DDoS attacks, Defense mechanisms.**

I. Introduction

CLOUD computing is a promising technology which provides a convenient platform to users for accessing cloud services and resources through the Internet. Using this technology, desktop computing is being converted into utility computing. The salient features provided by the cloud technology are on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured services [1]. The cloud provides infrastructure, platform, and software as-a-service via different delivery models such as private, public, community, and hybrid [2]. Following the lead of major cloud companies like Microsoft, Google, IBM, and Amazon, organizations such as educational institutions, hospitals, and banks have been using cloud services since last few years [3],[4].

Despite the numerous benefits of cloud computing, this technology faces several security issues [5]-[7], threats [8],[9], and challenges [10],[11]. Based on the surveys, it is observed that the security in cloud computing is a major research challenge [12],[13]. Various security issues in cloud service delivery models are reviewed in [14]-[16]. Among the security issues, availability is cited as the top-ranked critical concern [17], since the primary function of cloud computing is to offer on-demand services. The menacing threat to the availability of cloud computing services and resources is the DDoS attack [18].

The DDoS attack is a specific type of Denial-of-Service (DoS) attack [19] where multiple distributed compromised machines, also called bots [20], target the victim cloud server [21]. Based on the Arbor Networks report, the percentage of DDoS attacks targeting cloud computing services and resources is increasing every year [22],[23]. The popular cloud-based companies such as RackSpace, Amazon EC2, Microsoft, and Sony have been targeted by DDoS attacks in the recent years [24]. The attacks caused services downtime, economic losses, and many short-term and long-term effects on the victim Cloud Service Providers (CSPs).

Many variants of DDoS attacks exist in a cloud environment which differ in aim, implementation strategy, and scale [25]. The DDoS attacks can be broadly classified into two groups, brute-force and semantic [26]. In brute-force attacks (also known as flooding/high-rate DDoS attacks), attackers send a huge volume of malicious requests to exhaust the network bandwidth of the targeted cloud server [27]. The limitation of such attacks is, they can be easily detected by the defense mechanisms because of the high rate of the attack traffic [23]. On the contrary, semantic attacks (also known as vulnerability attacks), exploit the protocols weaknesses rather than exhausting the network bandwidth or cloud computing resources. The attacker generates a low volume of malicious traffic to target a specific protocol or an application. Such attacks are known as low-rate DDoS attacks. The low-rate attack traffic looks similar to the legitimate traffic. Thus, it is hard to identify the low-rate DDoS attack as compared to the high-rate DDoS attack [28].

With the technical advances, the cloud platforms are getting powerful day-by-day in terms of resources [23]. Due to this large pool of resources at the cloud side (especially, for

N. Agrawal is with the Department of Computer Science and Engineering, Amity School of Engineering and Technology (ASET), Amity University Madhya Pradesh, Gwalior, M.P., 474005, India (e-mail: nagrawal@gwa.amity.edu)

S. Tapaswi is with the Cloud Computing and Cyber Security Laboratory, Atal Bihari Vajpayee - Indian Institute of Information Technology and Management, Gwalior, M.P., 474015, India (e-mail: stapaswi@iiitm.ac.in)

large CSPs), it is difficult for an attacker to exhaust them all even with high-rate DDoS attacks. An example of such a failed DDoS attack is reported in [29] which has been launched by an anonymous group against the Amazon cloud. Consequently, the attackers are now trying to degrade the quality of cloud services without early detection by using sophisticated low-rate DDoS attacks. Based on the attack launching strategy, the low-rate DDoS attacks can be classified into four classes, namely, shrew attack [30], Reduction-of-Quality (RoQ) attack [31], Low Rate DDoS Attack against Application Server (LoRDAS) [32], and Economic Denial-of-Sustainability (EDoS) attack [33],[34]. Among the low-rate DDoS attacks, the EDoS attack has gained serious attention. A severe EDoS attack was launched against Amazon EC2 in 2015 which caused financial losses of $30,000, daily [35]. The detailed description of various forms of DDoS attacks in cloud computing is provided in Section II.

A. Motivation

Several surveys have been published on DDoS attacks and the corresponding defense approaches in a cloud environment. But, to the best of our knowledge, some forms of DDoS attacks and their defense mechanisms are not well addressed in the existing surveys. The motivation to write this survey paper is as follows.

1) The detailed classification of both high-rate and low-rate cloud DDoS attacks is not well addressed in the existing surveys.
2) The existing surveys fail to detail the attack launching strategies for various DDoS attacks and their impact on cloud services.
3) The description and comparison of the defense mechanisms for each type of DDoS attacks are not available in the existing surveys.

Thus, there is an immense need to re-look at the DDoS defense solutions in a cloud environment with the aim to minimize these attack effects.

B. Contributions

This paper presents developments related to DDoS attacks detection, prevention, and mitigation solutions in the cloud. The paper presents a comprehensive survey with detailed insight into the defense solutions of DDoS attacks. It is believed that this paper will stimulate the security researchers to develop effective defense solutions to avert the DDoS attacks in the cloud space. The novel contributions of this survey paper are as follows.

1) It considers all variants (high-rate and various forms of low-rate) of DDoS attacks in a cloud environment. A new taxonomy of DDoS attacks characterization, prevention, detection, and mitigation approaches is presented.
2) It discusses various launching strategies for DDoS attacks and their impact on cloud services.
3) It presents a comparative analysis of the defense approaches for each DDoS attack type with respect to the parameters such as the approach discussed, the deployment location, the experimental testbed used, the behavior in a cloud environment, etc.
4) It describes essential performance metrics (such as accuracy, service response time, attack detection time, victim service downtime, etc.) for effective defense solutions. A quantitative analysis of the recent approaches using these metrics is also provided.

The road-map of this survey paper is shown in Fig. 1. A DDoS attack scenario in a cloud computing environment and the detailed description of all its variants are provided in Section II. The defense mechanisms for high-rate DDoS attacks and the related discussion are given in Section III. The defense mechanisms for each category of the low-rate DDoS attacks and the related discussion are provided in Section IV. The research gaps, challenges, and future research directions are described in Section V. The essential performance metrics to study the effectiveness of any defense system is provided in Section VI. Section VII and Section VIII present open research problems and conclusions respectively.

II. DDoS Attacks in Cloud Computing

The DDoS attacks in a cloud computing environment differ from the DDoS attacks in the traditional network infrastructure [36],[37] in the way of the attack launching strategy and the attack outcome. The attackers exploit the salient features of cloud computing to launch DDoS attacks in an effective manner [13]. In the traditional network, it is difficult to infect adequate machines in a short time. By using the on-demand self-service feature of cloud computing, attackers can acquire the cloud resources, on-demand. This allows the attackers to create a powerful botnet [38]. Thus, using this powerful botnet, attackers can provide Malware-as-a-Service (such as DDoS-for-Hire [25]) in low prices [39] to other malicious users. The resource pooling feature of cloud computing helps the attackers to launch DDoS attacks easily using multi-tenant and virtualization technologies. Utilizing the broad network access feature, attackers may use a wide range of devices to launch feasible DDoS attacks. As per the report given in [40], a powerful DDoS attack was launched in 2013 using multiple devices. The rapid elasticity feature enables the CSP to scale up or down the cloud resources based on the users' requirements. The attackers exploit this feature and cause unnecessary scaling-up of the cloud resources without any intent to pay for them [41]. The associated cost for the unpaid malicious usage burdens the CSP, and over a long period, economic losses occur at the CSP end [42].

In the absence of a proper defense mechanism, the DDoS attack may cause collateral damage [43] i.e., the co-located cloud services also get affected. Thus, to reduce such attack effects, this survey is focused to review the existing variants of DDoS attacks and their defense mechanisms. According to [26], a DDoS defense mechanism can be a combination of the following four phases: (1) prevention, (2) monitoring, (3) detection, and (4) mitigation. In the prevention phase, cloud services and resources are protected from the DDoS attacks by launching appropriate security applications at several

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

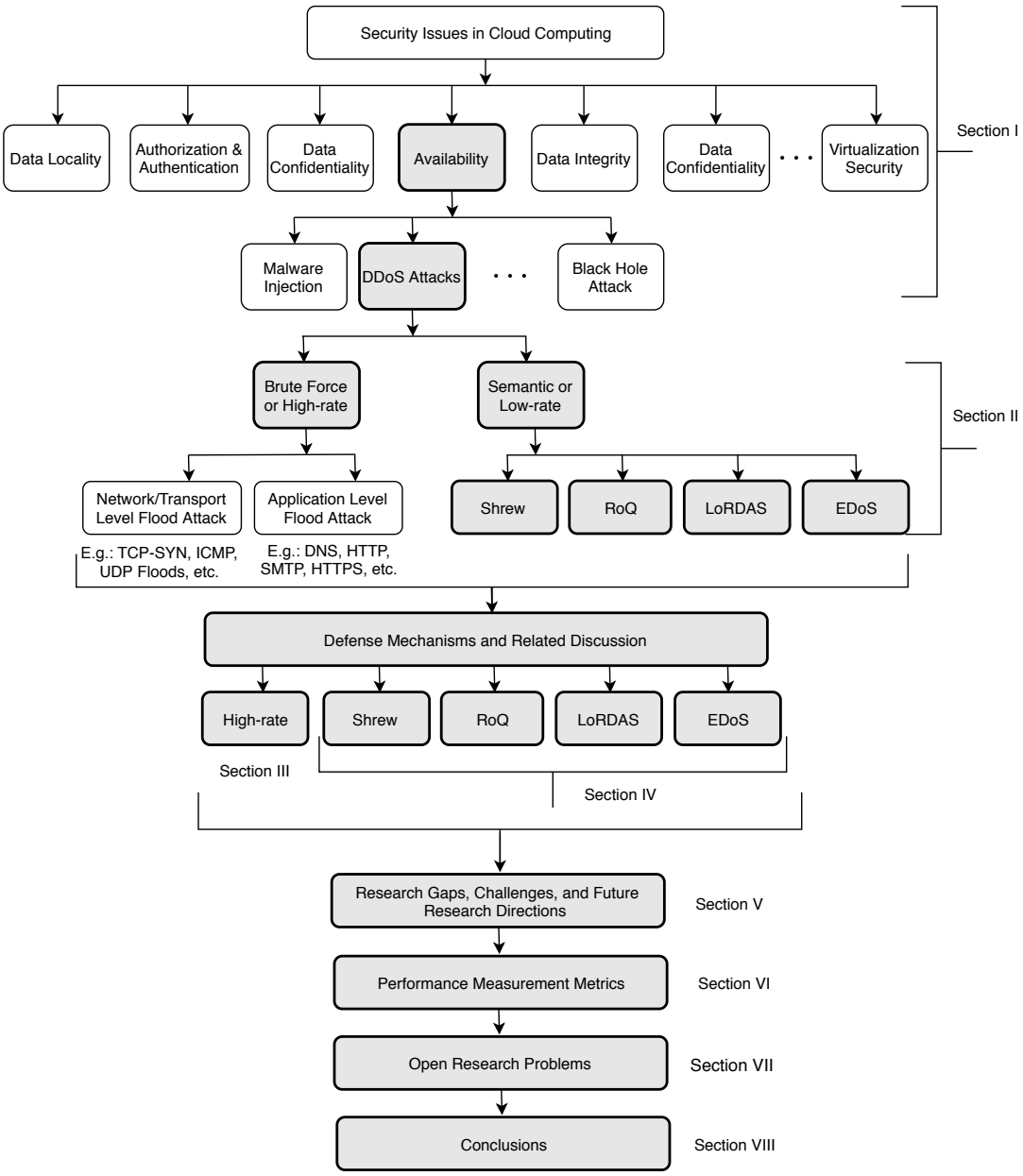

Fig. 1. Road map of the paper

locations. The monitoring phase captures useful information about hosts or network. The detection phase analyzes the captured network traffic to identify the malicious attempts. Mitigation is the last phase which calculates the attack's severity and takes a right action to control its impact. Results of the mitigation phase are forwarded to the prevention phase to regularly update the preventive measures. The monitoring phase is implicitly included in the detection phase. Thus, this paper considers only three phases - prevention, detection, and mitigation, in a DDoS defense mechanism.

Several papers, including survey papers, have been published on DDoS attacks and their corresponding defense mechanisms in a cloud computing environment. The comparative analysis of the relevant survey papers in cloud computing with this survey is given in Table I. The analysis is performed considering high-rate and low-rate DDoS attacks, and their defense mechanisms. It may be observed from Table I that this survey addresses the limitations of the existing surveys on DDoS attacks in a cloud environment.

A DDoS attack against the cloud infrastructure may be launched in two ways. A common DDoS attack scenario in a cloud computing environment is depicted in Fig. 2. The attack scenario is the same for the high-rate and the low-rate DDoS attacks, only the number and the pattern of the attack requests are different. The high-rate DDoS attack involves massive requests with attack network bandwidth greater than 500 Gbps [25]. The low-rate DDoS attack requests are periodic and pulsing, and consume less network bandwidth (in Mbps) [46]. The attack scenario consists of legitimate nodes, external and internal compromised nodes (botnets), intermediate routers,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE I
ANALYSIS OF THE EXISTING SURVEYS ON DDOS ATTACKS IN CLOUD COMPUTING

S. No.	Authors	Topics Discussed	DDoS Attacks		Defense Mechanisms			Remarks
			High-rate	Low-rate	Prevention	Detection	Mitigation	
1.	Shamelisendi et al. [26] (2015)	Mitigation approaches for the DDoS attacks in cloud computing.	✓	✗	✗	✗	✓	Taxonomy of mitigation strategies is presented only for the high-rate DDoS attacks. Mitigation solutions for the high-rate DDoS attacks are compared based on their limitations and deployment location.
2.	Osanaiye et al. [2] (2016)	DDoS attacks in cloud computing and grouped the detection approaches into three classes: signature-based, anomaly-based, and hybrid.	✓	✗	✗	✓	✗	Detection taxonomy is presented only for the high-rate DDoS attacks. Detection solutions are compared with respect to the deployment location only.
3.	Yan et al. [13] (2016)	DDoS attacks in cloud computing, their research issues, and challenges.	✓	✗	✓	✓	✓	New trends and characteristics of only high-rate DDoS attacks are presented. Defense solutions for high-rate DDoS attacks are discussed with their limitations. Detailed categorization of defense solutions and their comparisons are not provided.
4.	Somani et al. [21] (2017)	DDoS attacks in cloud computing, their issues, and taxonomy.	✓	✓ (EDoS attack only)	✓	✓	✓	DDoS attack scenario, its impact on cloud infrastructure, and defense solution taxonomy are described. DDoS defense solutions are compared with respect to the strengths, weaknesses, and limitations only.
5.	Somani et al. [25] (2017)	DDoS attacks in cloud computing, their requirements, trends, and future research directions.	✓	✓ (EDoS attack only)	✓ (Limited)	✓ (Limited)	✓ (Limited)	Fatal effects of DDoS attacks on cloud services and major requirements in designing efficient mitigation solutions are discussed. Extensive review of defense solutions is not provided.
6.	Gupta and Badve [44] (2017)	DoS and DDoS attacks with their defense mechanisms in cloud computing.	✓	✓ (Limited)	✓ (High-rate only)	✓ (High-rate only)	✓ (High-rate only)	Defense solutions only for the high-rate DDoS attacks are discussed and compared based on the deployment location. Detailed categorization of the low-rate DDoS attacks is not provided.
7.	Agrawal and Tapaswi [45] (2017)	Possible variants of DDoS attacks in cloud computing and their defense mechanisms.	✓	✓	✓ (Limited)	✓ (Limited)	✓ (Limited)	Categorization and exhaustive review of defense approaches for each DDoS attack type are not presented.
8.	**This Survey**	Various forms of DDoS attacks in cloud computing. Defense approaches for each DDoS attack type, their research gaps, challenges, and future research directions.	✓	✓	✓	✓	✓	A comprehensive taxonomy of all the possible variants of cloud DDoS attacks (high-rate and low-rate) solutions with detailed insight into the characterization, prevention, detection, and mitigation mechanisms of these attacks is presented. Detailed description, performance metrics, and comparative analysis of the defense approaches (based on the experimental testbed used, deployment location, DDoS attack type, behavior in cloud, etc.) for each DDoS attack type are described.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

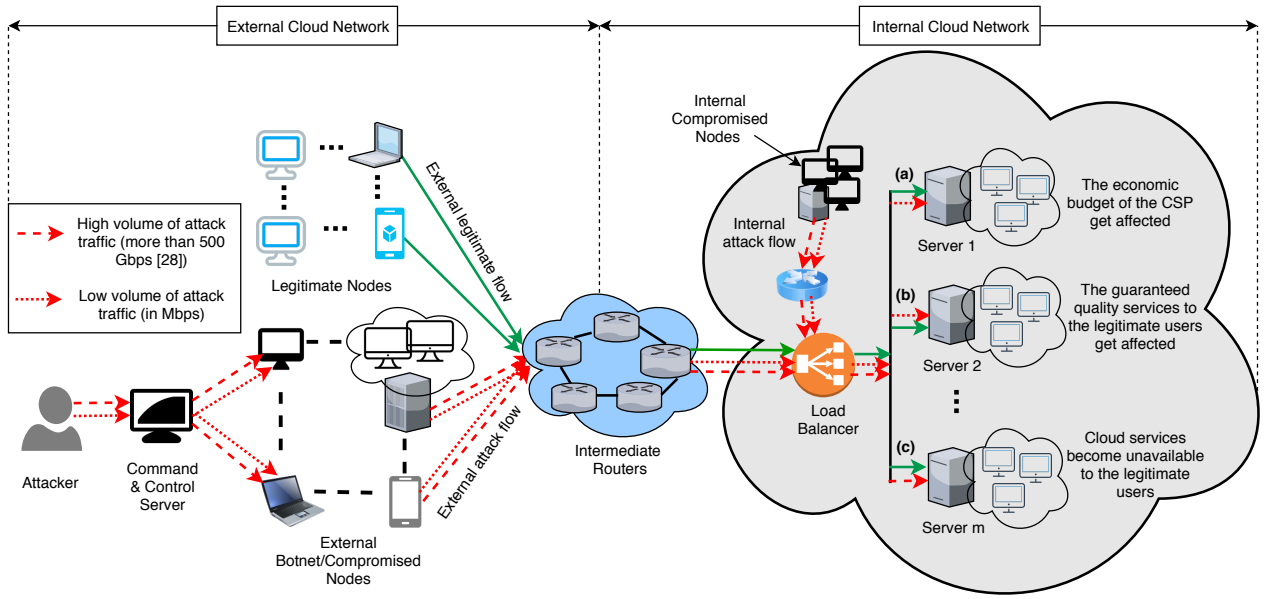

Fig. 2. DDoS attack scenario in a cloud computing environment

load-balancer, and *m* cloud web application servers.

In the external DDoS attacks, the attacker targets the cloud server via external compromised nodes which are controlled and managed by a Command & Control (C&C) server under the direction of the attacker. The aggregate traffic which is coming from the legitimate and external compromised nodes arrives at the load-balancer after passing through the intermediate routers. Similarly, the internal DDoS attacks are launched by the internal compromised nodes (VMs of the cloud infrastructure). The service providers launched several VMs and clustered together to create *m* cloud servers. The applications are installed on the cloud servers, and their services are offered to the legitimate cloud users. It can be observed from Fig. 2 that three situations ('a', 'b', and 'c') may arise here. The low-rate DDoS attack targets the economic component of the CSP (situation a) or affects the quality of cloud services to the legitimate users (situation b). The high-rate DDoS attack makes the services unavailable to the benign cloud users (situation c). Several defense approaches have been proposed against the low-rate and high-rate DDoS attacks in cloud computing. The new taxonomy of the DDoS attacks and their defense approaches is shown in Fig. 3. The description of each classification is described in Section III and Section IV. Aim, attack launching strategy, and attack impact for each DDoS attack type are explained in next subsections.

A. High-rate DDoS Attacks

In the high-rate DDoS attacks, the attackers send a flood of malicious requests either to disrupt the cloud services or the users' connectivity. The disruption of connectivity is caused by exhausting the router processing capacity, network bandwidth capacity or resources. Such attacks are called network or transport level flooding attacks [47]. Examples of such attacks are the Transmission Control Protocol (TCP)-SYN flood, the User Datagram Protocol (UDP) flood, and the Internet Control Message Protocol (ICMP) flood [44],[48]. The unavailability of cloud services to the legitimate users is performed by exhausting the server resources like CPU, memory, disk, or I/O bandwidth. These attacks are known as the application-level flooding attacks such as the Hypertext Transfer Protocol (HTTP) flood [49], the Domain Name System (DNS) flood, and the Simple Mail Transfer Protocol (SMTP) flood.

The attackers launch such attacks by exploiting the vulnerability of a huge amount of computers to create attack armies, also called botnet. The attack command is issued by the attacker to the C&C server which is forwarded to the multiple compromised hosts. The compromised hosts send a flood of requests to target one or more cloud servers. The botnet computers may use IP spoofing technique to launch DDoS attacks to hide the true origin of the attacker. Thus, to identify the actual location of the attacker is a challenging and crucial task. Since a detailed classification of high-rate DDoS attack types in cloud computing is available in [2],[26], their individual description is out of the scope of this survey paper.

B. Low-rate DDoS Attacks

Unlike the high-rate DDoS attack, the low-rate DDoS attack is a sophisticated attack and arduous to detect because of its low-rate traffic and stealthy behavior. Since the attacker sends malicious requests at a very low rate, such attacks remain undetected by the traffic volume based defense mechanisms. The attack affects the Quality-of-Service (QoS) experienced by the legitimate user rather than stopping the cloud services. Based on the exploited vulnerability, target, and values of the attack parameters, the low-rate DDoS attacks can be categorized into four types, namely, shrew attack, RoQ attack, LoRDAS, and EDoS attack. These attacks differ in attack characteristics such as the attack length *(L)*, the attack period

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

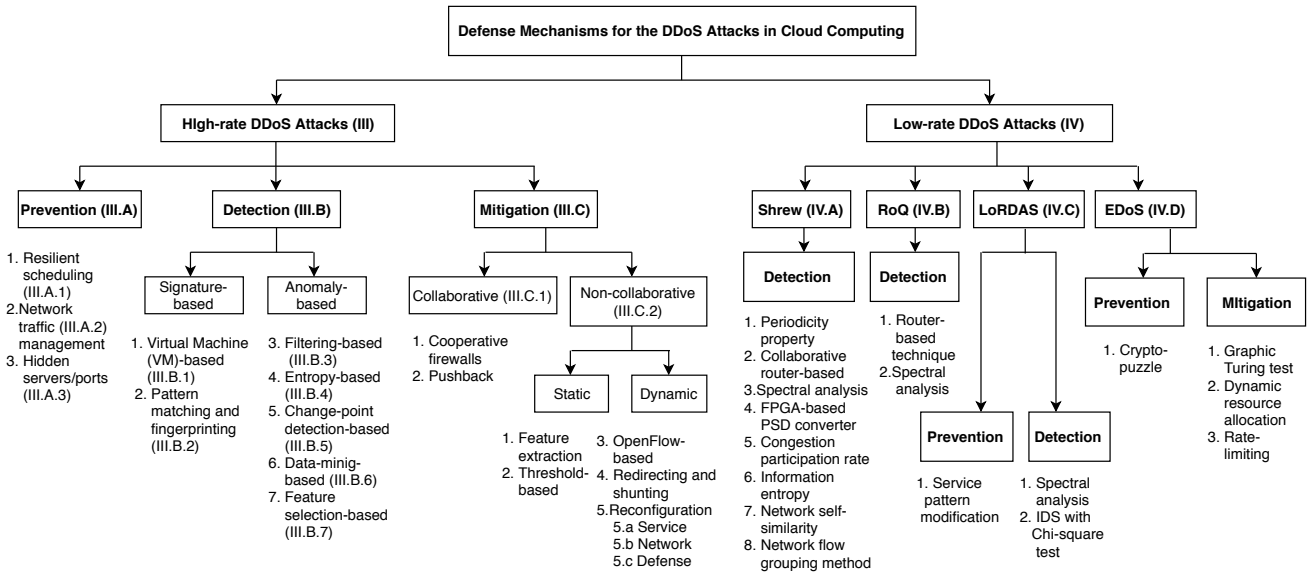

Fig. 3. DDoS attacks and their defense mechanisms taxonomy for a cloud computing environment

(T), and the attack rate *(R)*. Since the low-rate attacks send high-intensity traffic for a shorter time and repeat itself after a particular period, the attack traffic follows periodic and pulsing behavior. The description of each of its types is as follows.

1) *Shrew Attack:* In this attack, the attacker exploits the vulnerability exists in the TCP Retransmission Timeout (RTO) mechanism. The aim of the shrew attack is to avert the legitimate TCP flow and affect the cloud applications by sending the low rate attack traffic. Whenever the TCP sender recovers from the timeout, the attacker immediately sends low rate traffic to make the link congested/timeout again. Thus, it makes the legitimate TCP flow's throughput very low or nearly zero [30].
Two important properties of the shrew attack were discovered in [50], (a) the peak rate of shrew attack remains constant, while the peak rate of TCP flow increases linearly, and (b) the attack stream arrives periodically at the destination, while the TCP stream arrives continuously. Using these identified properties, the shrew attack can be detected. To estimate the characteristics of shrew attack, a mathematical model is proposed in [30]. The square-wave model for shrew attack as adapted from [30] is depicted in Fig. 4.
This attack model consists of three parameters, the attack period T_s, the attack length L_s, and the attack magnitude R_s. Hence, a shrew attack can be modeled as a triplet $\langle T_s, L_s, R_s \rangle$. The period T_s is calculated using the estimated TCP RTO timer implementation from the legitimate sources. Based on [51], the attack burst period T_s should be equal to *1 second* (initial RTO) to maximize the attack damage. Authors in [30] later proved this result inaccurate as it did not consider the TCP congestion window adaptation behavior. To sustain the attack's stealthy behavior, the attack period must be greater than *1 second*, and the values of R_s and L_s should also be high [30]. The value of burst rate R_s is based on the TCP bottleneck bandwidth. Let the bottleneck buffer size and bandwidth be B and C respectively. For the shrew attack to launch, ideally, the burst rate R_s should be equal to the bottleneck bandwidth C [52]. To make TCP retransmission timeout (typically *1 second*), length of burst L_s should be enough to fill the buffer size B or greater than equal to the maximum Round Trip Time (RTT) value, i.e., $L_s \geq RTT_{max}$ and $T_s = RTO_{min}$.

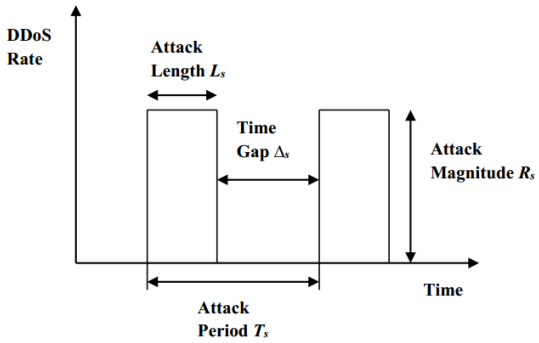

Fig. 4. The square-wave model for the shrew DDoS attack in the time-domain [Adapted from [30]]

2) *Reduction-of-Quality Attack:* In this attack, the assaulter exploits the vulnerability of TCP's congestion avoidance algorithm named Additive Increase Multiplicative Decrease (AIMD). The aim of this attack is to affect the QoS experienced by the legitimate cloud users [31]. The RoQ attack can be represented using the same model as discussed for shrew DDoS attack, only the attack parameters values are different. Thus, the RoQ attack can be modeled as a triplet $\langle T_r, L_r, R_r \rangle$. The attack period $T_r \geq 5$ *seconds* [53], the attack length L_r is equal to the time to make the network congested, and the time gap Δ_r is the time taken by the network to recover from congestion.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

3) *Low Rate DDoS Attack against Application Server:* This attack exhausts the victim cloud server resources by generating a low rate of malicious requests towards the victim server. The attacker aims to fill the service queue of the victim server with malignant requests. A mathematical model for LoRDAS is given in [32]. The work assumed a single hosted cloud server with a large finite service queue running a single application. In this scenario, when a request arrives, it waits for its turn. A new space becomes available in the queue when a request (based on the queue's discipline) is allocated to the server. The purpose of the attacker is to determine the instant when a position gets vacant in the service queue [32]. In the service queue, a position becomes vacant only after the service time of a request, $T_{service}$. The service queue is always full, if $T_{service} > \Delta_l$ (where, Δ_l is the time interval (gap) between two consecutive attack packets). Thus, the request coming from the legitimate cloud users are subsequently discarded. Fig. 5 shows the model for LoRDAS which is an offshoot of [32], and explains its waveform and attack parameters.

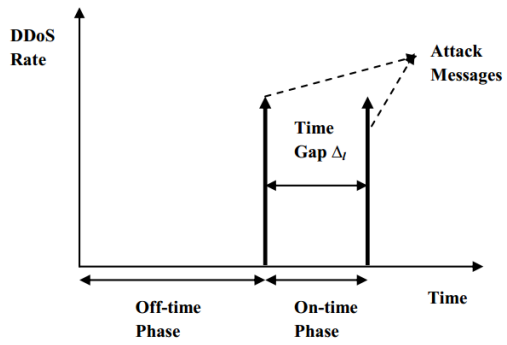

Fig. 5. The model for LoRDAS attack in the time-domain [Adapted from [32]]

The explanation of each of the parameters is as follows:

- Time Gap (Δ_l): time between two consecutive attack packets.
- On-time Phase ($t_{on-time}$): during this active interval, attacker aims to acquire the free positions in the service queue by sending attack messages.
- Off-time Phase ($t_{off-time}$): no attack packet is transferred during this inactive interval.

To maintain a low rate of attack traffic during *on-time* phase, a better prediction for the service time (or the instant in which a position of the service queue becomes vacant) should be made. The methods, (1) request-response time and (2) inter-output time were described in [32] which are used by the attackers for service time estimation. Request-response time defines the period when an attacker sends a request and waits for the corresponding response. Inter-output time is the period when an attacker sends two consecutive requests and analyzes the time elapsed between their outputs. This method provides a more accurate prediction as compared to the request-response time method.

4) *Economic Denial-of-Sustainability Attack:* The EDoS attack targets the financial component of the service provider. The cloud services are dynamically provisioned which can scale up or down according to the users' requirements. The EDoS attack exploits the auto-scaling feature of the cloud and causes unwanted installation of new VMs without willing to pay for them. The cost associated with this unpaid malicious usage burdens the CSP. Over a period, the services become unsustainable as the CSP is charged with a hefty amount [33]-[34].

Since the EDoS attack traffic looks similar to the benign traffic, its detection is a challenging task. It may be observed that among the DDoS attacks, EDoS attack is very dreadful as it targets the economic component of the cloud. Unlike other DDoS attacks which prevent the legitimate users from accessing the cloud services for a certain amount of time, the EDoS attack prevents the CSP from delivering cloud services for a long time [54].

III. Defense Mechanisms for High-rate DDoS Attacks

Due to the involvement of high volume of attack traffic, the prevention and mitigation of such attacks is difficult. However, these attacks can be easily detected because of the high attack traffic volume. In the literature, a wide variety of detection approaches are available against such attacks. The defense mechanisms for the high-rate DDoS attacks are described in further subsections.

A. Prevention

A prevention approach for DDoS attacks in cloud computing proactively filters and drops the malicious requests before the attack produces any adverse effect on the cloud services. Since the prevention approaches are applied to both legitimate and malicious traffic, the performance of the legitimate users may be affected. The prevention approaches for the high-rate DDoS attack can be classified into three categories which are described as follows.

1) Resilient Scheduling: To prevent the victim server resources from overwhelming with the malicious requests, a resilient scheduling approach is described in [55]. The approach consists of suspicion assignment and DDoS resilient scheduler. Suspicion assignment provides a continuous value to each session which is utilized by the scheduler to decide if and when to schedule the session's requests. The approach has scalability constraint in the large-scale cloud network. Thus, its performance may get affected.

2) Network Traffic Management: To prevent the consumption of network bandwidth by malicious attempts, an adaptive traffic management technique is proposed in [56]. Using this approach the shares of bandwidth are allocated to each cluster based on the packet similarity. A traffic shaping technique which limits the bandwidth by using the probability of a source to be a legitimate user is proposed in [57]. Under the high traffic load, the approach shapes source IP addresses to the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

bandwidth limits. Since the approaches limit the bandwidth, the auto-scaling feature of the cloud may get affected for legitimate users.

3) Hidden Servers/ports: This method hides the direct communication link between the client and the server (ports). This is accomplished by introducing an intermediate node (proxy) which acts as a forwarding authority. The forwarding authority balances the load among the cloud servers, monitors the incoming traffic, and responsible for fault-tolerance and recovery of the servers. The hidden proxy server method is utilized in [58] to protect the targeted server from DDoS attacks. The authors proposed a moving target approach where multiple proxy servers are involved. The proxies are dynamically assigned and changed to protect the cloud servers. The approach has several issues such as inclusion of multiple proxy servers, shuffling, and scalability.

B. Detection

DDoS attacks detection approaches can be broadly categorized into two groups: signature-based and anomaly-based [2]. In the signature-based detection method, the captured network traffic is compared with the well-defined attack patterns such as byte or packet sequence [59]. It is easier to develop and understand, and provides more accurate results as compared to the anomaly-based method. The limitation of signature-based detection approaches is, they can identify only known attacks for which the attack pattern is pre-defined.

To overcome this limitation, the anomaly-based approaches are proposed, where the behavior pattern of the traffic is used for attack detection [60]. The behavior of legitimate users is profiled, and the attack is signaled if any deviation is found in legitimate profile behavior. The method can detect unknown attacks but does not provide better accuracy. Various signature-based and anomaly-based detection approaches have been proposed. They can be further classified into several categories which are as follows.

1) VM-based: A VM-based detection approach for the DDoS flood attacks is proposed in [61]. An intrusion detection system (IDS) is installed on each VM of the cloud server to analyze the in-bound and out-bound network traffic. The installed IDS sensors detect DDoS attacks and subsequently drop the incoming traffic from the identified attack sources. Another VM-based approach which analyzes the data gathered from IDSs on various VMs is proposed in [62]. Since an IDS is installed on each VM, this approach reduces the possibility of an attack. The limitation of these approaches is, since a separate IDS is configured on each VM, the VMs may get overloaded. Thus, the guaranteed cloud services to the legitimate users may get affected.

To overcome this limitation, a distributed IDS model is proposed in [63], where a separate IDS is installed in each cloud region. When an IDS identifies the attack, an alert report is sent to other IDSs. The IDS includes a cooperative agent which is capable of deciding whether to accept the alert message. The network measurement value is used in [64]. The attack is signaled if the measured value satisfies the corresponding node's threshold value. Once the attack is detected, the traffic destined to that node is transferred to other nodes by launching one or more VMs. The limitation of the approaches is the high communication complexity.

The VM profile for the possible attacks is created and used to identify the TCP-SYN flood attacks in [65]. Each VM profile consists of the attack pattern and the detection threshold. The approach is centralized and reduces communication complexity. However, the detection of other flooding attacks is not discussed.

2) Pattern matching and fingerprinting: A detection approach based on the theory of network self-similarity is proposed in [66]. The approach discriminates the attack traffic from the legitimate traffic using the self-similar pattern. Since the majority of the DDoS attacks are TCP based, IP spoofing in TCP/IP protocol is considered as a critical issue in [67]. In spoofed DDoS attack, the attacker sends attack requests using the unreachable source IP addresses. Thus, the TCP handshake process in spoofed DDoS attack is different from the normal handshake process. The work described in [67] exploited this feature of IP spoofing and utilized the ratio of TCP *SYN* and *ACK+SYN+ACK* packets. In spoofed DDoS attack scenario, as the acknowledgment packet is not received by the attack source, this ratio is not 1. The limitation of the approach is, this ratio may not be equal to 1 in a cloud environment sometimes as the packets are coming from multiple distributed sources. Thus, the legitimate traffic may be classified as spoofed.

A path fingerprint approach to detect the spoofed DDoS attacks is described in [68]. Each packet is attached with a path fingerprint which represents its route from the source to the destination. At the receiver side, the path fingerprint is calculated, and if it is not matched with the attached fingerprint, the packet is classified as spoofed. The approach fails to detect the subnet spoofing and requires cooperation from the intermediate routers. A similar approach is proposed in [69] to identify the Operating System (OS) of a packet. The fingerprint is calculated using the fields of the TCP/IP header and attached to the packet at the source side. The packet is classified as spoofed if the attached fingerprint is not matched at the receiver side. These approaches have high computational complexity and reserve the computing resource at each intermediate node.

3) Filtering-based: HTTP, eXtensible Markup Language (XML), and REpresentational State Transfer (REST) based DDoS attacks are very dangerous and may produce harmful effects to the availability of cloud resources. A filter tree approach is proposed in [70], which consists of a sequence of filters to detect and resolve such attacks. Using this approach, only known DDoS attack can be detected. Confidence-based filtering (CBF) score is used for the attack identification in [71]. The filtering score value is evaluated using the frequency of occurrences of the attribute pairs. The results show that the approach has less memory requirement and provides comparable accuracy. Another CBF approach to defend against the IP spoofed DDoS flooding attack is proposed in [72]. It comprises of two-level filtering, in the first level, spoofed IP packets are identified by matching the Time-to-Live (TTL) value. While, in the second level, the Jensen-Shannon divergence concept is used to detect divergence in the traffic flow from the nominal

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

profile. The approach can detect the spoofed DDoS attacks, and requires less storage at the cloud infrastructure.

A hop-count based approach which filters out the spoofed DDoS attack packets is proposed in [73]. For launching the spoofed DDoS attacks, fields of the TCP/IP header are forged by the attackers. As, the attacker may forge any field of the header, but cannot falsify its TTL field. Hence, the TTL value is utilized to detect the spoofed IP packets. Since the OSs may have different initial TTL values, the approach may produce false results. A packet-marking filtering approach based on path identification (Pi) is described in [74]. The Pi mark represents the route which is traversed by a packet from the source to the destination. Based on the Pi mark, the attack packets are detected and subsequently filtered out. A two-layer filtering approach for the DDoS attacks detection is proposed in [75]. The first layer filters the high-rate DDoS attack traffic based on the IP flow count. The second layer utilizes Discrete Fourier Transform (DFT) for analyzing the difference between the inter-arrival times of the packets.

4) Entropy-based: The information distance metric and generalized entropy metric are used for attack detection in [76]. The difference in these metrics for the legitimate traffic and the attack traffic is used for the detection of DDoS attack. The approach also includes an effective traceback scheme which can trace and discard all the attack traffic. The generalized entropy and divergence metrics are utilized for the detection of flooding DDoS attacks and flash events in [77]. The approach used the difference in entropy variations for attack detection. A collaborative approach, named FireCol, is discussed in [78] for detection of the DDoS flooding attacks. In this approach, the virtual protection rings of Intrusion Prevention Systems (IPSs) are created around the victim to analyze the incoming aggregate traffic for the attack detection. The frequency and entropy values for each filtering rule are computed and using these values a score is assigned to each rule. A large value of the score indicates the DDoS attack. The limitations of the approach are scalability and high installation cost.

5) Change point detection-based: The change point detection technique is used to identify the flooding DDoS attacks in [79],[80]. The approaches detect the attack by comparing the packets' characteristics (such as IP flow count, source IP addresses, and destination IP addresses) with the normal packets' characteristics. If any deviation is observed in these characteristics, then attack is signaled. The change aggregation trees are used in [79] and a cumulative sum algorithm is utilized for analyzing the inter-arrival time of packets in [80].

6) Data-mining-based: The significant increase in traffic volume affects the performance of the aforementioned approaches. For handling a huge amount of data, the data-mining techniques are used. The Hadoop MapReduce based detection technique for HTTP GET flood attack is proposed in [81]. A robust, scalable, and reliable threat monitoring method using Hadoop MapReduce and Spark is given in [82]. It mainly consists of three components, namely, cloud infrastructure, monitoring agents, and an operation center. A Decision tree approach is utilized for the detection of high-rate cloud DDoS attacks in [83]. Another Hadoop-based security model for the spoofed DDoS attack detection is proposed in [84]. The approaches improve the processing speed by concurrently separating and processing the data streams.

7) Feature selection based: A covariance matrix based approach for the detection of flooding DDoS attack in a cloud environment is proposed in [85]. The incoming network traffic is converted into the covariance matrix and compared with the baseline profile for the attack detection. The baseline profile is generated by selecting the features from the legitimate traffic. To enhance the detection accuracy, a multi-filter approach based feature selection method is presented in [86]. The approach utilizes decision tree classifier and provides high detection accuracy with improved performance. To detect XML and HTTP based DDoS attacks, an adaptive and intelligent approach is proposed in [87]. The detection model is constructed by extracting features from the legitimate traffic and the outlier technique is used for attack identification. An event-based approach for the detection of spoofed DDoS attack packets is proposed in [88]. In this approach, an active verification method is used to verify the legitimacy of a packet. An approach which combines the merits of feature selection and statistical learning is discussed in [89]. The features such as source IP address, destination IP address, and the packet length are extracted from the packet header. The statistical method identifies the suspicious packets and forwards to the group of classifiers for attack detection. Experimental results show that the approach is scalable only in the context of CAIDA 2013 dataset. A classifier method called extreme gradient boosting (XGBoost) is used for the DDoS attack detection in [90]. The method analyzed the traffic flow features to distinguish the attack flow from the legitimate flow. XGBoost is the improved version of the traditional Gradient Boosting Decision Tree (GBDT) algorithm. The goal of constructing the tree is to minimize the target function iteratively by applying the greedy search algorithm. The approach is scalable, accurate, and has high processing speed.

The comparison of the existing prevention and detection approaches for the high-rate DDoS attacks is shown in Table II. The comparison is performed based on the objective, the approach discussed, the experimental testbed used, the deployment location, and the type of DDoS flood attack. The behavior in cloud and countermeasure for each approach are also provided in Table II. It may be observed from the table that the anomaly-based approaches addressed the limitations of the signature-based approaches. Though the anomaly detection approaches can detect the unknown attacks but fail to provide high detection accuracy. Since most of the approaches require cooperation of the intermediate routers, they have high computational and communication complexities. Because of the scalability constraint, better performance may not be achieved in a cloud environment. Thus, there is a need of effective detection approaches which can detect the DDoS attacks with improved performance.

C. Mitigation

Mitigation is the last phase of the defense life cycle. The aim of mitigation approaches is to minimize the impact of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE II
COMPARATIVE ANALYSIS OF THE PREVENTION AND DETECTION APPROACHES FOR THE HIGH-RATE DDOS ATTACKS

Authors	Objective	Approach	Experimental Testbed	Deployment Location	Attack Type	Behavior in Cloud	Countermeasure By
Ranjan et al. (2006) [55]	Prevention	Suspicion assignment and DDoS resilient scheduler	Three Apache web servers and one MySQL server	Intermediate routers	Application	Scalability constraint, performance may degrade in the large-scale cloud networks	Goldstein et al. [57]
Goldstein et al. (2008) [57]	Prevention	Traffic shaping	NA	Intermediate routers	Network	The auto-scaling feature of the cloud may be affected	–
Bakshi and Dujodwala (2010) [61]	Detection	VM-based IDS (signature-based)	SNORT, VMware ESX, and honeypot	VMs of the cloud network	Application	VMs may get overloaded	Lo et al. [63]
Lo et al. (2010) [63]	Detection	Cooperative IDS (signature-based)	SNORT	Cloud computing regions	Network	Demands extra communication costs	Karnwal et al. [70].
Francois et al. (2012) [78]	Detection	Collaborative entropy-based (signature-based)	Simulated environment	Intermediate routers	Network	Scalability constraint and high installation cost	Anomaly-based detection approaches
Lonea et al. (2013) [62]	Detection	VM-based IDS (signature-based)	Eucalyptus 2.0.3, Barnyard tool, SNORT, Stacheldraht tool, Xen hypervisor	VMs of the cloud network	Application	VMs may get overloaded	Anomaly-based detection approaches
Gupta and Kumar (2013) [65]	Detection	VM profile-based (signature-based)	NA	Intermediate routers	Network	Cannot detect unknown attacks	Anomaly-based detection approaches
Dou et al. (2013) [71]	Detection	CBF (anomaly-based)	Simulated environment	Intermediate routers	Network	Less memory requirement and provides acceptable accuracy	–
Ismail et al. (2013) [85]	Detection	Covariance matrix (anomaly-based)	VMware and AthTek NetWalk	Intermediate routers	Network	Suitable for the large-scale cloud networks	Vissers et al. [87]
Wang et al. (2014) [58]	Prevention	Hidden proxy server	MATLAB	Intermediate routers	Network	Scalability constraint, overhead may occur because of proxy redirection	–
Shamsolmoali and Zareapoor (2014) [72]	Detection	CBF (anomaly-based)	Netwag tool, JPCap tool	Intermediate routers	Network	Detects IP spoofed DDoS attack, accurate, requires small storage	Wang et al. [94]
Choi et al. (2014) [81]	Detection	Map reduce (anomaly-based)	SNORT, Hadoop	Intermediate routers	Application	Improves processing speed	Chen et al. [82]
Vissers et al. (2014) [87]	Detection	Parametric technique with Gaussian model (anomaly-based)	Eucalyptus 2.0.3	At Cloud resource broker	Application	Protects only cloud broker	Shamsolmoali and Zareapoor [72]
Karasaridis (2016) [64]	Detection	Network transaction measurement value analysis (signature-based)	NA	Intermediate routers	Network	Cannot detect unknown attacks, and has high communication complexity	Anomaly-based detection approaches
Osanaiye et al. (2016) [80]	Detection	Change point detection (anomaly-based)	CAIDA DDoS dataset	Intermediate routers	Network	May not suitable for the large cloud networks	Wang et al. [94]
Chen et al. (2016) [82]	Detection	Map reduce (anomaly-based)	Hadoop, Spark, VMware ESXi 6.0, Cloudera CD5 5.4	Cloud infrastructure	Network	Improves processing speed and increased efficiency	–
Borisenko et al. (2016) [83]	Detection	Data mining (anomaly-based)	OpenStack cloud platform	Controller node	Application	Provides better performance	–
Behal and Kumar (2017) [77]	Detection	Entropy and divergence metrics (anomaly-based)	Emulated environment	Intermediate routers	Network	Not tested for the high-scalable real environment	Boro and Bhattacharyya [89]
Boro and Bhattacharyya (2017) [89]	Detection	Feature selection and statistical learning (anomaly-based)	Emulated environment	Intermediate routers	Network	Scalable in the context of CAIDA 2013 dataset	–
Toklu and Simsek (2018) [75]	Detection	Filtering (anomaly-based)	NS-2*	Intermediate routers	Network	May not suitable for the large cloud networks	–
Chen et al. (2018) [90]	Detection	XGBoost classifier (anomaly-based)	Mininet and Hyenae tool	SDN cloud controller	Network	High processing speed, accurate, and scalable	–

NA = Not Available, * = Network Simulator 2

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

DDoS attack by taking appropriate action at the right time. The existing mitigation approaches can be broadly classified into two groups: collaborative and non-collaborative. In the collaborative mitigation approaches, multiple intermediate routers cooperate with each other to effectively mitigate the DDoS attacks. In the non-collaborative approaches, there is no cooperation among the routers. They work independently for mitigating the impact of the DDoS attacks. The discussion of these approaches is provided in further subsections as follows.

1) Collaborative: A distributed collaborative method to detect and mitigate the DDoS attacks is proposed in [91]. To defend against the attacks, multiple routers in the autonomous system are communicated via an overlay network. To drop malicious traffic, the rate-limiting tactic is used. Rate-limiting is a threshold-based technique where a fraction of incoming attack traffic is discarded. It considers both individual and aggregate flows and limits the incoming flows to a predetermined threshold. Since the approach limits the legitimate requests, it does not support the auto-scaling feature of the cloud.

A collaborative pushback defense model is proposed in [92] to defend against the link flooding attacks. In pushback mitigation strategy, one security device pushes the information of the attack traffic to other security devices. This model named Codef which involves the collaboration among routers and performs two functions, routing and rate-control. When a router is congested, it sends rate-limiting requests to other routers. The routers re-route the legitimate traffic in response to the requests from the congested routers. The limitation of the approach is, it imposes an extra communication overhead to the intermediate routers.

The load-balancer is used for the detection and mitigation of DDoS attack in [93]. The attack is detected by analyzing the performance parameters, and its effect is mitigated by isolating the victim machine. A highly programmable network monitoring DDoS attack detection and mitigation approach named DaMask (DDoS Attack Mitigation Architecture using Software-defined networKing) is proposed in [94]. It consists of two modules: detection and mitigation. The results of the detection module are forwarded to the mitigation module. As the attack is detected by the detection module, the subsequent traffic from the identified attack sources is filtered out by the mitigation module. A Turing testing based multi-stage DDoS attack detection and mitigation approach is proposed in [95]. The approach consists of four modules, source checking, counting, Turing test, and question generation modules. The first two modules are used for attack detection, while the last two modules are used for mitigation. Under heavy traffic load, the performance of these approaches may get affected.

An autonomic mitigation approach, ArOMA for the DDoS attacks is described in [96]. The approach assigns a unique identifier to each incoming IP flow. The flow statistics are collected by the OpenFlow agents and forwarded to the detection module for further processing. The generated alert messages are utilized by the mitigation module to filter the packets from the identified attack sources. A network-based approach to detect and mitigate the HTTP DDoS attacks is described in [97]. The incoming traffic is monitored on the network devices such as routers and switches for attack detection. When the web server receives the incomplete HTTP requests from the clients, it compares the number of active HTTP connections with the threshold. If the active HTTP connections exceed the threshold, an attack is identified. The limited flow-table size vulnerability of the OpenFlow switch can also be exploited by the attackers to launch flooding DDoS attacks against the cloud. A flow-table sharing approach is proposed in [98] to protect the flow-table from overloading with DDoS flood requests. Under the DDoS attack, the approach looks for the unused space of the flow-tables in the network and redirects the targeted switch flow to the other network switches. As the approaches require involvement of multiple routers, a sufficient amount of memory is reserved at each router.

2) Non-Collaborative: The non-collaborative defense approaches can be static or dynamic. The static approaches are not adapted to the attack. On the contrary, the dynamic approaches are capable of adjusting automatically according to the severity of the DDoS attack.

The static rate-limiting OpenFlow protocol-based DDoS defense approaches are proposed in [99]-[103]. The implementation of the OpenFlow switch on the NetFPGA platform for DDoS defense is described in [99]. The contents of the packets are analyzed for attack detection. If the attack is identified, the OpenFlow controller limits the incoming traffic flow. A lightweight approach based on the traffic flow features is proposed in [100]. The relevant features are extracted and the traffic is classified as malicious or legitimate by utilizing the unsupervised Artificial Neural Network (ANN) and Self-Organising Maps (SOM). The traffic of the OpenFlow switch is monitored, and the DDoS attack is detected using volume counting approach in [101]. Two static thresholds are considered, the first is *3000* packets in every five minutes. Once the traffic reaches this limit, the second threshold, *800* packets per second is verified. If the second threshold meets for five times, the subsequent incoming traffic is dropped until the system register returns to a normal state. The traffic parameters such as flow rate and flow duration are analyzed for the DDoS attack detection and mitigation in [102]. The upper and lower bounds for both parameters are defined. If the incoming flow satisfies the defined limits, the flow is classified as legitimate. Once the packet is identified as malicious, the subsequent traffic from that IP address is filtered out to mitigate the impact of the DDoS attack.

A NetFlow-based architecture for source address validation is proposed in [103]. The approach named Virtual source Address Validation Edge (VAVE) verifies whether the source of the packet is valid. If the packet is found malicious, the corresponding entry from the routing table is discarded. An adaptive traffic control mechanism for mitigating DDoS attacks is proposed in [104]. The model consists of a distributed firewall which filters the traffic at the source-end and has a traceback service to locate the origin of the attack traffic. A lightweight dynamic strategy called redirecting and shunting is proposed in [105]. When an attack is identified, the traffic is forwarded to a different physical interface where the attack traffic is filtered out. On the alternate data path, shunt hardware is configured using NetFPGA 2 platform. The in-line hardware caches rules for IP addresses and drop the attack packets using

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

IPS.

In the dynamic approaches, the cloud service or network topology is reconfigured to mitigate the effect of DDoS attacks. The reconfiguration of service is performed in [106],[107]-[109] where the cloud services are cloned to mitigate the DDoS attacks. Service cloning-based mitigation approaches utilize the resource pooling and scaling features of the cloud. Since the cloud possesses a large pool of resources, the VMs can be cloned easily at different locations to handle the increase in service demands. But the downside is the approaches have high attack mitigation cost at the service provider side.

A network topology reconfiguration based approach is discussed in [110]. In this approach, the network topology is reconfigured rather than cloning the services. An intelligent fast-flux swarm network is used to mitigate the DDoS attacks in [110]. The communication between the client and servers is performed using the decentralized swarm transport system. The high availability of resources is assured using fast-flux network by utilizing a large number of nodes. To mitigate the DDoS attack, a traffic diversion approach is proposed in [111]. The approach works in two modes, peace mode and attack mode. In peace mode, the network elements route and forward the packets based on their destination IP address. In attack mode, the malicious traffic is forwarded to the security server based on the packet diversion field, while the legitimate traffic is redirected to the destination IP address.

The comparison of the existing mitigation approaches for the high-rate DDoS attacks is shown in Table III. The comparison is conducted based on the approach used, mitigation strategy, experimental testbed, deployment location, type of DDoS flood attack, and their behavior in the cloud environment. It may be observed from the table that there is a need to design the effective mitigation approaches which can mitigate the attack in a cost-effective manner, and improve the communication and computational complexities. This can be achieved by proposing the non-collaborative proactive approaches which can detect and mitigate the DDoS attacks in the initial stage.

Discussion: The prevention approaches for the high-rate DDoS attacks are based on rescheduling, network traffic management, and hidden proxy/servers. These approaches reschedule or shape the network traffic before coming to the cloud server. The hidden proxy/server based approaches hide the direct communication link between the client and the server. Thus, the high-rate DDoS attack traffic can be prevented. Due to the involvement of a large volume of attack traffic, such attacks can be easily detected. Thus, more literature works are focused on detection as compared to prevention. The mitigation of high-rate DDoS attacks is challenging because to mitigate the attack effect, victim cloud server requires a large amount of extra resources which directly affects the financial component of the service provider. The prevention approaches for the high-rate DDoS attacks can apply to low-rate DDoS attacks. The detection approaches for the high-rate DDoS attacks are mainly based on time-domain. These approaches are not applicable to low-rate DDoS attacks detection. Due to the stealthy behavior of low-rate DDoS attacks, its detection in the time-domain is very tedious. The low-rate DDoS attacks are periodic and pulsing in behavior, and the detection of periodic pulses using traffic volume analysis method in the time-domain is difficult. Thus, the detection of low-rate DDoS attack is performed in the frequency-domain.

IV. Defense Mechanisms for Low-rate DDoS Attacks

A. Defense Mechanisms for Low-rate Shrew Attack

The shrew attack exploits the vulnerability of the TCP RTO mechanism. In the literature, only detection approaches are available for defending against the shrew attack which are described as follows.

1) Detection: The detection approaches for the shrew DDoS attacks are based on the DFT or Discrete Wavelet Transform (DWT) which are frequency-domain techniques. The existing frequency-domain approaches can be categorized into several groups, namely, spectral analysis, congestion participation rate, network flow grouping, information entropy, and self-similarity. The description of each of the approaches is as follows.

The periodic properties of the legitimate TCP flows and shrew attack flows are utilized for the attack detection in [112]. For RTT, the TCP flows possess strong periodicity property which is not true in the case of attack flows. To estimate the signal periodicity, Power Spectral Density (PSD) is utilized by the authors. The approach is implemented in a simulated environment. The experimental results show that 81.8% TCP flows are periodic, while 18.2% are non-periodic. For the shrew attack, 15.7% flows are periodic, while 84.3% flows are non-periodic. The limitation of the approach is, since the periodicity of flows is used as a signature for the attack detection, lack of periodicity in legitimate TCP traffic indicates DDoS attack. To overcome this limitation, a frequency-domain based approach is proposed in [113]. The authors observed that the shrew attack flows have high energy distribution in low-frequency bands. The frequency-domain characteristics are used to identify the shrew attack flows in the incoming traffic. The normalized cumulative amplitude spectrum distribution is used to filter the shrew attack flows.

A collaborative router-based detection approach is described in [114]. To support the collaborative detection, a network layer multicast protocol "LocalCast" with hypothesis testing is used. The local detection results are exchanged among the routers of the multicast group. Routers use these local results for the verification of their detection results. A template matching approach for the shrew DDoS attack detection is proposed in [50]. The approach detects the shrew attack traffic hidden in the legitimate TCP/UDP stream. It is a collaborative detection and filtering (CDF) approach, where the attack is detected using spectral analysis against the previously stored spectral characteristic template of the attack. The hypothesis testing and DFT are used for attack detection. Results show that the PSD for the attack stream is high in the low-frequency band. To detect the bottleneck link, statistical and spectral traffic analyses methods are used in [115]. The bottleneck occurs when a massive amount of packets with a length equal to the Maximum Transfer Unit (MTU) is forwarded to the victim server. Utilizing periodicity in packet transmission, the

TABLE III
COMPARATIVE ANALYSIS OF THE MITIGATION APPROACHES FOR THE HIGH-RATE DDOS ATTACKS

Authors	Approach	Mitigation Strategy	Experimental Testbed	Deployment Location	Attack Type	Behavior in Cloud
Gonzalez et al. (2007) [105]	Redirecting and shunting	Dynamic Non-collaborative (filtering)	NetFPGA 2	Intermediate routers	Network	Communication overhead
Naous et al. (2008) [99]	TCP/IP packet header analysis	Static Non-collaborative (rate-limiting)	OpenFlow on NetFPGA	OpenFlow switch	Network	May affect the auto-scaling feature of the legitimate users
Braga et al. (2010) [100]	Traffic flow features analysis	Static Non-collaborative (filtering)	OpenFlow	OpenFlow switch	Network	Improves the communication complexity
YuHunag et al. (2010) [101]	Network traffic threshold	Static Non-collaborative (rate-limiting)	OpenFlow	OpenFlow switch	Network	May produce false positive alarms
Yao et al. (2011) [103]	Traffic flow features analysis	Static Non-collaborative (filtering)	OpenFlow	OpenFlow switch	Network	Improves the communication and computational complexities
Lua and Yow (2011) [110]	Service reconfiguration	Dynamic Non-collaborative (filtering)	Simulated environment	Intermediate routers	Network	Communication overhead
Lee et al. (2013) [92]	Routing and rate-control	Collaborative (rate-limiting)	NS-2*	Intermediate routers	Network	Communication overhead
Yu et al. (2014) [106]	IPS VMs cloning	Dynamic Non-collaborative (filtering)	Amazon Elastic Compute Cloud	Victim end	Application	Mitigation cost at the CSP end may increase
Peng et al. (2014) [109]	Service (VMs) cloning	Dynamic Non-collaborative (filtering)	MATLAB 7	Victim end	Application	Mitigation cost at the CSP end may increase
Murthy et al. (2015) [93]	Performance parameter analysis (anomaly-based)	Collaborative (rate-limiting)	NA	Load-balancer	Application	Load-balancer may get overloaded
Wang et al. (2015) [94]	Feature selection	Collaborative (filtering)	Amazon Elastic Compute Cloud	Intermediate routers	Network	As traffic increases significantly, performance may be degraded
Chesla and Doron (2016) [111]	Traffic Diversion	Dynamic Non-collaborative (filtering)	NA	SDN Controller	Network	As the volume of traffic increases, performance may degrade
Sahay et al. (2017) [96]	Anomaly-based intrusion detection	Collaborative (filtering)	Mininet-based simulations and testbed-based experiments	Ryu controller	Network	Requires storage capacity of each intermediate router
Hong et al. (2018) [97]	Exploits the number of active HTTP connections	Collaborative (rate-limiting)	NS-3**	OpenFlow switch	Network	The controller node may itself becomes vulnerable to the DDoS attack
Bhushan and Gupta (2018) [98]	Flow-table sharing	Collaborative (traffic redirection)	Mininet	OpenFlow controller	Network	Improves the communication complexity

NA = Not Available, * = Network Simulator 2, ** = Network Simulator 3

approach identified a bottleneck link without any network overhead.

A hardware-based approach named Field Programmable Gate Array (FPGA) PSD converter is proposed in [116], [117]. The approach discussed in [116] is comprised of two modules: Auto Correlation (AC) and DFT. The reusability feature of the AC module significantly improves the performance of the approach. The correlation measure between any two samples is used for the attack detection in [117]. Based on the absolute distance and the deviation from their mean and standard deviation, the DDoS attack is identified. A congestion participation rate (CPR) based approach is proposed in [118], which detects and filters the TCP targeted low-rate DDoS attacks. The CPR approach exploits the fact that the attack traffic causes congestion in the network. Thus, the flows with high CPR value are treated as malicious, and hence will be dropped.

A New Collaborative Detection Method (NCDM) for low-rate DoS attack is described in [119]. The method used Chi-Square (χ^2) distance and mean deviation to determine the frequency distributions and fluctuations in the traffic pattern respectively. A sequence alignment detection algorithm, named Smith-Waterman is used in [120]. In this algorithm, first, the score rule is defined for two sequences then based on the rules, the score matrix is built. Utilizing the score matrix, similar sequences are identified. Experimental results show that the shrew attack sequences follow similar pattern behavior.

An entropy-based method is proposed in [46] for low-rate DDoS attacks detection and mitigation. In this method, the information entropy is integrated with power spectrum. Two information metrics such as Fourier power spectrum entropy and Wavelet power spectrum entropy are used for the attack detection. The empirical evaluation of several information

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

entropy metrics is performed in [121]. The major information metrics such as Shannon entropy, generalized entropy, and Hartley entropy, are evaluated based on their ability to detect both high-rate and low-rate DDoS attacks. The experiments are conducted in the MIT Lincoln Laboratory, CAIDA and TUIDS DDoS datasets are used to measure the performance of each metric for the DDoS attacks detection. It is observed that when the order of information divergence is increased, the information distance metric provides better results as compared to the Kullback-Leibler divergence method. Since the information metrics used minimum detection parameters, these approaches have low computational complexity. The generalized entropy is used to detect the low-rate DDoS attack against SDN data centers in [122]. The attack is detected using the probability distribution of the traffic flow. Results show that in this approach, detection accuracy is improved as compared to other information entropy metrics based methods.

To distinguish the attack traffic and the legitimate traffic, the Naive Bayes classifier with DFT and DWT is used in [123]. The Fisher g-statistic and Siegel test are utilized in [124]. The results show that the Fisher g-statistic is better for the one dominant periodicity, and the Siegel test is good for the multiple dominant periodicities. For shrew DDoS attack detection, a network flow grouping method is proposed in [125]. Using Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH) algorithm, the approach discriminates the attack flow from the legitimate flow. A network self-similarity approach for the TCP-targeted DDoS attacks is described in [126]. The effect of the low-rate DDoS attacks on the self-similar nature of the traffic is analyzed. The H-index is used to differentiate the attack traffic and the legitimate traffic. The multifractal features of network traffic are utilized in [127], and a comb-filter is designed in [128]. The limitation of the above-discussed approaches is, they do not consider the internal traffic of the cloud network for attack detection. Thus, the internal DDoS attacks remain undetected. This limitation has been overcome in [42],[28]. A PSD-based approach is described in [42] for the detection of low-rate cloud DDoS attacks. A lightweight approach for the detection of IP spoofed low-rate cloud DDoS attacks is proposed in [28]. The approach used flow count and traffic behavior for attack detection. In both approaches, real-time aggregate traffic is monitored and analyzed. Results show that the approach can detect internal and external low-rate DDoS attacks with competitive performance.

The comparative analysis of the detection approaches is provided in Table IV. The analysis is performed based on the approach referred, experimental testbed, input parameters, outcome, and their behavior in cloud. It may be observed from the table that only a few efforts have been devoted to detect the internal cloud DDoS attacks. Thus, new approaches need to be designed which can detect both internal and external shrew cloud DDoS attacks.

B. Defense Mechanisms for Low-rate RoQ Attack

The RoQ attack affects the guaranteed quality services offered to the legitimate cloud users. In the literature, limited work is available on the RoQ attack. The existing literature is based on the impact of RoQ attack and its detection approaches which are discussed as follows.

1) Impact of RoQ attack on end-systems and load-balancer: The effect of RoQ attacks on end systems using the potency metric is described in [129],[130]. The potency metric defines the ratio of the damage caused by the attack to the cost of attack implementation. The authors of [129] proposed a control theoretic model and the attack's impact is determined by using the potency metric. The proposed model is composed of an admission controller and a feedback monitor. It is observed that (a) an attacker can estimate the admission rate using the attack requests, and (b) tracing the location of an attacker is an excruciating task due to its stealthy behavior. A Discrete-time model is proposed in [130] to study the impact of RoQ attack. The experimental results show that the attack increases the service response time and degrades the performance of services and resources.

The vulnerability exists in the dynamic load balancer can be exploited to launch RoQ attack as described in [131]. Load balancers can be classified into static load balancers and dynamic load balancers. The load balancing decision of the static load balancer is based on the static information such as IP address or predefined assignment strategy. The dynamic load balancer decision depends on the delayed feedback from underlying resources. The load balancers utilize a sticky connection feature, where requests from the same client always forwarded to the same server. The approach revealed that the dynamic load balancer greatly improves the performance of services as compared to the static load balancer. The approach also discussed the impact of RoQ attack using parameters such as feedback delay, number of resources managed, and the averaging parameters.

2) Detection: A router-based approach to detect and mitigate the RoQ attack is proposed in [53]. The approach operates in two stages. In the first stage, RoQ attack is detected using per-flow information available on the routers. It uses four parameters, namely, packet count, packet size, created time, and last accessed time. In the second stage, RoQ packets are dropped using the filtering algorithm. An unexpected increase in the flow of expired packets is used for attack detection. The filtering is based on queue length, as queue size fluctuates during the *ON* period of attack. Spectral analysis is used for the detection of RoQ attack in [132]. The approach detects and filters the RoQ flows using energy spectral analysis and standard deviation. The flow level spectral analysis is combined with sequential hypothesis to save the computing time. The scheme can detect the RoQ attack accurately.

The comparison of the above-stated approaches is shown in Table V. The comparison is performed based on the objective, approach, experimental testbed, input parameters, outcome, and their behavior in cloud. It is observed from Table V that limited literature is available on the RoQ attack. The new approaches should be designed to address the limitations of the existing approaches.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE IV
COMPARATIVE ANALYSIS OF THE DETECTION APPROACHES FOR LOW-RATE SHREW ATTACK

Authors	Approach	Experimental Testbed	Input Parameters	Outcome	Behavior in Cloud
Chen and Hwang (2006) [50]	Template matching approach based on periodicity of shrew attack flows	NS-2*	T_s = 0.3-0.5 s, L_s = 30-90 ms, and R_s = 0.5-0.2 MB/s	Shrew attack traffic has high energy in the low frequency bands	Aggregate traffic flows may not follow periodicity property and produces false positive alarms
He et al. (2009) [115]	Spectral analysis	Simulated Environment	NE	Attack traffic exhibits strong periodicities based on the link bandwidth and packet size	Bottleneck occurs if packets with MTU is transferred
Zhang et al. (2012) [118]	CPR with random early detection queue management	NS-2*	T_s = 0.2 s, R_s = 5 Mb/s	A flow with a high CPR is treated as malicious	Effective to distinguish attack flow from the aggregate flows
Chen et al. (2013) [116]	FPGA-based PSD converter	Xilinu Virtex2 Pro FPGA	L_s = 20 ms, T_s and R_s are not explicitly stated	Burden of auto-correlation process is significantly reduced	Improves processing speed
Tang et al. (2014) [119]	A new collaborative detection method (NCDM) using χ^2-test	NS-2*	T_s = 1.2-2.0 s, L_s = 0.1-0.3 s, and R_s = 20-30 Mb/s	Attack flow affects the frequency distribution and fluctuation pattern of the legitimate flow	Detects attacks with low false alarm rate
Fouladi et al. (2016) [123]	Naive Bayes classification	MATLAB R2015a and Weka 3.6	NE	Naive Bayes classifier is simple and easy to implement	Provides better performance
Cotae et al. (2016) [124]	Fisher g-statistic and Siegel test	Simulated environment	NE	For shrew attack the energy distribution is high in low frequency bands	For detecting one dominant spectral line Fisher g-statistic is better, while for multiple dominant spectral lines Siegel test is better
Liu et al. (2016) [125]	Network flow grouping method	Simulated environment	T_s = 1.0 s and R_s = 200 Kb/s	Provides fast response time	High accuracy may not be achieved
Agrawal and Tapaswi (2017) [28]	Flow count and traffic flow behavior analysis	Eucalyptus 3.4.1 cloud platform	Not required	Only limited amount of IP addresses can be spoofed	Internal cloud DDoS attacks can be detected.
Hoque et al. (2017) [117]	FPGA-based PSD converter	MATLAB and FPGA	NE	Burden of auto-correlation process is significantly reduced	Improves processing speed
Kaur et al. (2017) [126]	Network self similarity	NS-2*	NE	Low-rate DDoS attacks affect the H-index of the self-similar nature of the network traffic	High accuracy may not be achieved
Agrawal and Tapaswi (2018) [42]	Power spectral density analysis	OpenStack cloud platform	T_s = 1.0 s and R_s = 200 Kb/s	Attack traffic has high energy distribution in low-frequency bands	Internal cloud DDoS attack could be identified
Chen et al. (2018) [46]	Power spectrum entropy analysis	NS-3**	T_s = 1.35 s, L_s = 100 ms, and R_s = 10 Mb/s	Attack traffic has high energy in low-frequency bands and has low entropy	Fail to detect internal cloud DDoS attack
Sahoo et al. (2018) [122]	Generalized entropy metric	Mininet 2.2.26	NE	Entropy is less for the attack flow	Provides improved accuracy
Wu et al. (2019) [120]	Smith-Waterman sequence alignment algorithm	NS-2*	T_s = 1.2 s, L_s = 200 ms, and R_s = 5 Mb/s	Low-rate DDoS attack sequences are highly correlated	Internal cloud DDoS attacks cannot be identified

NE = Not Explicitly stated, * = Network Simulator 2, ** = Network Simulator 3

C. Defense Mechanisms for Low-rate LoRDAS Attack

LoRDAS attack targets the service queue of the cloud application server. The impact, attack launching strategy, and the defense approaches for the LoRDAS attack are described as follows.

1) Impact and launching strategy of the LoRDAS attack: LoRDAS attack against the iterative servers is discussed in [133]. The vulnerability in the iterative server is explored and to evaluate the effectiveness of the attack, a mathematical model is proposed. The impact of LoRDAS attack is analyzed in both simulated and real environments. By predicting the response time of a request, the attack traffic can be minimized. The LoRDAS attack against the application server is analyzed in [134]. A mathematical model is proposed which consists of m servers and a common load-balancer. Each server is associated with a large finite service queue. If the load balancer does not find a free position in any of the queue for servicing the request, the request will be discarded, and an overflow alert message is raised. Otherwise, the request spends tq_i waiting time in the i^{th} machine before accessing the service module, where $1 \leq i \leq m$. If an attacker tries to occupy all positions of the service queue, the DDoS attack is experienced by the legitimate cloud users. As a consequence, to make the attack stealthy, the intruder must send the packets only when any of the queue positions is free. The fundamentals, strategy, and design issues of such attack against the application server are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE V
COMPARATIVE ANALYSIS OF THE DEFENSE APPROACHES FOR LOW-RATE ROQ ATTACK

Authors	Objective	Approach	Experimental Testbed	Input Parameters	Outcome	Behavior in cloud
Guirguis et al. (2005) [129]	Study the impact of RoQ attack on end-systems	Control theoretic model	Linux 2.4.20 server	NE	Attacker aims to maximize the attack damage, which increases the attack potency	The scalability and auto-scaling features of the cloud computing may get affected
Guirguis et al. (2007) [131]	Study the impact of RoQ attack on dynamic load-balancer	Queuing theory analysis	Linux 2.4.20 Server	Potency metric is used against the number of attached server with and without delay	Analyzed attack's impact based on the number of resources managed, averaging parameters, and feedback delay	The attack degrades load balancer's performance in the presence of feedback delay
Chen and Hwang (2007) [132]	Detection and filtering	Spectral analysis	NS-2*	Δ_r = 1 ms, T_r, L_r, and R_r are not explicitly stated	Energy distribution for the legitimate and attack flows is different	Cannot detect the IP spoofed cloud DDoS attack
Shevtekar and Ansari (2008) [53]	Detection and mitigation	Router-based technique	NS-2*	T_r > 5 s, L_r and R_r are not explicitly stated	Expired flows traffic load is less in non-attack period	Drops attack packets based on the queue length
Guirguis et al. (2009) [130]	Study the impact of attack on end-systems	Discrete-time model	Red Hat Linux 2.6.9-11.EL	R_r = 10 requests/sec	The attack causes high response time, degraded service, and under-utilization of resources	The attack affects the guaranteed services offered to the cloud users

NE = Not Explicitly stated, * = Network Simulator 2

presented in [135]. The authors used the same architecture as discussed in [134]. In this, the strategy for reducing the attack traffic is also discussed in [135]. To evaluate the time elapsed between the responses, the RTT between servers and attacker, the time spent in the service queue, and the service time are used. The performance of the approach is measured in both real and simulated environments.

2) Prevention: A prevention approach to prevent the attacker from gaining all service queues' positions and to estimate the server's behavior is presented in [136]. These objectives are achieved by modifying the server's pattern for servicing the incoming requests. The effectiveness of the approach is tested in real as well as simulated environments.

3) Detection: The detection of low-rate DDoS attack against HTTP server is discussed in [137],[138]. The weakness of Apache HTTP 1.1 server for handling the persistent connection is exploited in [137]. The low-rate DDoS attacks against HTTP/2 is described in [138]. The new threats to HTTP/2 are explored and the results show that HTTP/2 is more vulnerable to attacks as compared to its predecessors. An intrusion detection approach is proposed which utilizes the Chi-Square (χ^2) distance between the legitimate and attack traffic.

Comparison of the defense approaches for the LoRDAS attack is given in Table VI. The comparison is performed on the basis of the objective, approach used, experimental testbed, input parameters, outcome, and their behavior in cloud. It may be observed from the table that the LoRDAS attack is feasible to launch but difficult to identify. The smart attackers have adopted sophisticated attack launching strategies. Thus, more effective approaches need to be designed for defending against such attacks.

D. Defense Mechanisms for Low-rate EDoS Attack

The EDoS attack exploits the auto-scaling feature of the cloud and affects the financial component of the service provider. The impact of EDoS attack, their prevention, and mitigation approaches are discussed in the literature which are as follows.

1) Impact of EDoS attack: The impact of EDoS attack on cloud services is demonstrated in [139]. The authors performed EDoS attacks on popular cloud service providers such as Google, LinkedIn, and Microsoft. The characteristics of ten popular public third-party services have been observed and revealed that the EDoS attack can be easily launched at a very low cost. Therefore, the attack mitigation strategies are highly required to address the consequences of such attacks. To study the impact of EDoS attack on cloud computing services, an analytical model is described in [34]. The model is based on queuing theory and verified in a simulated environment. The Discrete Event Simulation (DES) is performed, and the performance parameters such as end-to-end delay, throughput, utilization of computing resources, and the associated cost are analyzed. The authors of [140] discovered that the effect of EDoS attack is dependent on the resource allocation strategy, attack strength, attack duration, type of the attack, and size of the cloud infrastructure. To study the impact of EDoS attack, the experiments are performed on a single physical server and the cloud infrastructure of different size. The effect of EDoS attack on CSP is described in [141]. To analyze the fraudulent resource consumption, Coral-Reefs based approach has been used which simulates the increasing demands for the cloud-based VMs. Based on the analysis, it has been observed that such attacks may induce reputation and financial losses at the CSP's end.

2) Prevention: A crypto-puzzle-based solution to prevent EDoS attack is proposed in [142]. A puzzle difficulty level is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE VI
COMPARATIVE ANALYSIS OF THE DEFENSE APPROACHES FOR LOW-RATE LORDAS ATTACK

Authors	Objective	Approach	Experimental Testbed	Input Parameters	Outcome	Behavior in Cloud
Fernandez et al. (2007) [133]	Study the impact of LoRDAS against iterative server	Queuing model	NS-2*	$t_{on-time}$ = 0.6 s, $t_{off-time}$ = 2.7 s, and Δ = 0.3 s	Rate of traffic and its efficiency are evaluated	The attack is efficient and feasible to implement against the victim cloud server
Fernandez et al. (2007) [134]	Study the impact of LoRDAS against application server	Queuing model	NS-2*	$t_{on-time} \in$ (0.1 s - 0.6 s), $\Delta \in$ (0.1 s - 0.4 s)	All taken parameters values should be keep low for launching successful LoRDAS	The attack is feasible to launch against the victim cloud server.
Fernandez et al. (2008) [135]	The fundamentals, strategy, and design issues of the attack are discussed	A mechanism is proposed to reduce the attack load	NS-2*	$t_{on-time} \in$ (0.1 s - 0.6 s), $\Delta \in$ (0.1 s - 0.4 s)	By predicting the correct service time, the attack load can be minimized	Utilizing the correct service time, the attack can bypass several IDS mechanisms
Fernandez et al. (2010) [136]	Prevention	Exploits the behavior pattern of application server	NS-2*	Attack burst = 0.4 s, Time between attack packets = 0.2 s, mean service time = 12 s, and RTT = 1s	The approach prevents the attacker from obtaining all positions of the service queue	Feasible to implement against the cloud application server
Brynielsson and Sharma (2015) [137]	Detection	Exploits HTTP 1.1 server persistent connection feature using DFT	LoRDAS Simulator	NE	To reduce the attack traffic, off-time interval should be less than KeepAliveTimeout	The attack can evade several IDS mechanism
Tripathi and Hubbali (2018) [138]	Detection	IDS with χ^2 distance between the legitimate and attack traffic	Apache 2.4.23, Nginx 1.10.1, H2O 2.0.4, and Nghttp2 1.14.0	NE	Explored new threats against HTTP/2 protocol	HTTP/2 protocol is more vulnerable to attacks as compared to its predecessors

NE = Not Explicitly stated, * = Network Simulator 2

defined by the cloud user who genuinely wants to access the cloud resources. The cloud users have to solve the crypto-puzzle for accessing the cloud services. The difficulty of solving the crypto-puzzle is increased if the request is not entertained in a given frame of time due to the resource constraints. A similar approach based on crypto-puzzle is presented in [143]. The limitations of the approaches are, they suffer from the puzzle accumulation attack (where an attacker requests for a puzzle without any intention to solve them), asymmetric power consumption, and the associated false alarm rate. The approaches may provide false negative if an attacker has sufficient computing power to solve the puzzle, and false positive if the legitimate user lacks computing resources. These approaches may affect the performance of the legitimate users. EDoS attack may also launched by downloading thousands of files from cloud storage. To protect cloud storage from such attacks, an access control approach is proposed in [144].

3) Mitigation: EDoS shield, a method which verifies the legitimacy of the incoming requests is described in [145]. The main idea behind the EDoS shield is to check whether the requests are originated from the botnets or the legitimate users. The first incoming request is forwarded to the verifier node which verifies the request using graphic Turing test, and the black/white list associated with the virtual firewall is updated accordingly. The subsequent requests are handled based on the verification result of the first request. The performance and efficacy of the EDoS shield are evaluated using queuing theory modeling in [146], and Citrix cloud platform in [147].

The enhanced EDoS shield, an extension of [145] is proposed in [148]. The objective of this approach is to mitigate the effect of IP spoofed EDoS attack. The authors used the same architecture as discussed in [145] with the addition of TTL value in the black and white lists. When a request is entered into the verification process, its TTL value is stored. Based on the verification result, the IP address along with the TTL value are added to the white/black list. An improved version of the enhanced EDoS shield is proposed in [149]. The approach identifies the legitimacy of requests by analyzing only the first packet using a graphic Turing test. The approach consists of five modules, namely, virtual firewall (VF), verifier node, client puzzle server, IPS, and reverse proxy (RP) server. Instead of checking the contents of each packet, the IPS checks only packet flow rate, which reduces the end-to-end delay. To hide the location of the protected servers and control the load balancer, the RP firewall is used. The approach consists of three layers of verification. Thus, better accuracy can be achieved.

A dynamic resource allocation strategy is proposed in [106],[150] where resources are dynamically assigned based on the auto-scaling feature of cloud computing. Several intrusion detection systems (IDSs) are placed between cloud data centers and Internet in [106]. When the attack occurs,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

extra resources are dynamically assigned to clone IDSs. The IDSs filter the attack packets, and subsequently mitigates the effect of the attack. To mitigate the effect of EDoS attack, extra resources are provided to the victim cloud server to remain its resources available as described in [150]. A service resizing method where additional resources are provided to the mitigation service is proposed in [151]. To reduce the "Resource Utilization Factor", a similar approach named Scale inside-out is proposed in [152]. The approaches [151],[152] shrink the web-service resources and allocate those resources to the mitigation service. Consequently, the attack mitigation cost is increased and the performance of the legitimate cloud users may be affected.

A rate limiting approach where a limited number of access permission is assigned to each user is proposed in [33]. The approach analyzes the requests coming from the end users. User's behavior is analyzed at the cloud provider side by comparing the number and type of requests. The architecture consists of four modules, namely, virtual firewall, VM investigator, load balancer, and database. The virtual firewall filters the packets based on the regularly updated black list. The VM investigator is used to check the legitimacy of clients through a Turing test and also keeps track the user's activities. After completion of the test, the request is forwarded to the load balancer, where the trust value is incremented if the user passes the test; otherwise, it is decremented. A challenge-response-based rate limiting approach for the EDoS attack is proposed in [153]. The approach named EDoS Armor utilized the congestion and admission control techniques. The packets from the authenticated users are forwarded to the admission and congestion controllers. The challenge server authenticates the users by giving them either image-based or cryptographic-based challenge. Congestion controller is implemented on top of admission controller. The model is deployed in a web application firewall and both controllers are simultaneously applied to mitigate the EDoS attack. Admission controller is used to limit the number of requests, and congestion controller is used for prioritizing the requests. Thus, based on the priority only a limited number of request can be serviced. Since the approaches limit the number of requests to the cloud resources, the better performance may not be achieved by the legitimate cloud users.

To mitigate the Index Page Attack (IPA) in the field of EDoS, an approach is proposed in [154]. For any website, the index page is the first page which attracts the attackers as it is freely available without any login credentials. An IPA defender is used at the provider's end to analyze each request for an index page. It is implemented using IP tables which counts every request for an index page coming from the same IP address. If the page count exceeds the defined threshold, then the subsequent requests from that IP address are dropped, and the corresponding IP address is added to the black list.

A reactive approach named EDoS-Attack Defense Shell (EDoS-ADS) is proposed in [54]. The aim of the approach is to differentiate between the legitimate and malicious clients belong to the same Network Address Translation (NAT)-based network. The approach utilized the average CPU utilization threshold and duration as detection parameters. The upper and lower thresholds are assumed as *80%* and *30%* respectively with the respective duration of *5 minutes* and *1 minute*. The EDoS-ADS works in four modes: normal, suspicion, flash overcrowd, and attack. The system is in normal mode if the average CPU utilization below the upper threshold. Once the utilization exceeds the upper threshold, the mode switches to suspicion region. If a large number of incoming requests is classified as suspicious, the mode switches to attack, otherwise, flash overcrowd. The limitations of the approach are, the auto-scaling feature of the legitimate cloud users gets affected and the attack mitigation cost is high.

The comparative summary of the above-discussed approaches is provided in Table VII. The comparison is performed based on the objective, approach, experimental testbed, and behavior in cloud. It is observed from the table that the existing mitigation approaches are reactive. Thus, the attack is detected after its successful implementation and the attack mitigation cost is high. Significant research efforts need to be done to mitigate the EDoS attack in a proactive manner.

Discussion: The defense approaches in the field of DDoS attacks are mainly for the high-rate DDoS attacks. Limited literature is available for the low-rate DDoS attacks. Thus, there is a great need of research in the field of low-rate DDoS attacks in a cloud computing environment. Though the low-rate attacks involve a less volume of attack traffic but if such attacks are not detected in time, these will lead to a huge financial loss. Since the attack traffic possesses similar behavior as the legitimate traffic, its prevention is difficult. The low-rate DDoS attack traffic is periodic and pulsing in behavior, and the detection of periodic pulses in time-domain is strenuous. Thus, the detection approaches for such attacks are based on the frequency-domain. The existing frequency-domain approaches are based on DFT which has high ($O(N^2)$) total computational complexity. Consequently, DFT-based approaches are not suitable for real-time traffic analysis. The EDoS mitigation approaches are reactive, and have high attack reporting time and victim service downtime. Thus, the associated attack mitigation cost is high. Hence, more effective approaches need to be designed to defend against the low-rate DDoS attacks in a timely manner.

The functions and transformations closely related to this paper are given in Appendix.

V. Research Gaps, Challenges, and Future Research Directions

A. Research Gaps and Challenges

Based on the literature study, several research gaps and challenging issues are found that need to be addressed. This section discusses some of the critical research issues to defend against the DDoS attacks in a cloud computing environment.

1) Communication complexity: Based on the above study, it may be observed that several defense approaches for the low-rate and high-rate DDoS attacks require cooperation of the intermediate routers. This produces an extra overhead on the intermediate nodes and the performance of the approaches may get affected. For launching any DDoS attack in a cloud computing environment, attackers may utilize the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE VII
COMPARATIVE ANALYSIS OF THE DEFENSE APPROACHES FOR LOW-RATE EDOS ATTACK

Authors	Objective	Approach	Experimental Testbed	Behavior in Cloud
Khor and Nakao (2009) [142]	Prevention	Crypto-puzzle	NA	Suffers from asymmetric power consumption, puzzle accumulation attack, false alarm rate.
Squalli et al. (2011) [145]	Mitigation	EDoS shield (graphic Turing test)	Discrete event simulation	May generate false alarms.
Masood et al. (2013) [153]	Mitigation	Congestion control and admission control	E-commerce application	The auto-scaling feature of the cloud may be affected for the benign cloud users.
Saini and Somani (2014) [154]	Mitigation	Index page attack defender	Apache web server	May produce false alarms.
Yu et al. (2014) [106]	Mitigation	Dynamic allocation of VMs (VMs cloning)	Amazon Elastic Compute Cloud (EC2)	Mitigation cost at the service provider's end may be increased.
Al-Haidari et al. (2015) [34]	Impact of EDoS attack is evaluated against single class cloud services	Queuing model	Discrete event simulation	By increasing the attack traffic, the response time, utilization of computing resources, and associated cost also increase.
Somani et al. (2015) [140]	Effect of DDoS/EDoS attacks on cloud services are analyzed	Dynamic resource allocation strategy	CloudSim 3.0.3	Other than the victim cloud server, multiple co-hosted cloud servers may be affected.
Alosaimi et al. (2015) [149]	Counteracts EDoS attack and protects targeted services	Filtering	Simulated environment	Suffers from asymmetric power consumption and puzzle accumulation attack.
Baig et al. (2016) [33]	Detection and mitigation	Rate limit technique	Citrix cloud platform 3.0.5	Limits the scalable and elastic features of cloud computing.
Alsowail et al. (2016) [147]	The effectiveness of the EDoS shield is evaluated	EDoS shield (graphic Turing test)	Citrix cloud platform	Victim resource utilization is proportional to the attack intensity.
Somani et al. (2017) [151]	Mitigation	Affinity-based victim service re-sizing algorithm	XenServer 6.5	Shrinks the web-service resources and expands the mitigation service resources. Quality of services to the legitimate cloud users may be affected.
Al-Haidari et al. (2017) [146]	The effectiveness of the EDoS shield is evaluated using queuing model	EDoS Shield (graphic Turing test)	Analytical modeling	Effective in terms of performance and cost.
Somani et al. (2017) [150]	Mitigation	Dynamic resource allocation strategy	XenServer 6.5	Additional resources are provided to the victim cloud server. The financial budget of the CSP may get affected.
Somani et al. (2017) [152]	Mitigation	Scale inside-out	XenServer 6.5	Sacrifices the web-service resources and allocates those resources to the mitigation service. The attack mitigation cost is high.
Shawahna et al. (2018) [54]	Mitigation	EDoS-ADS (monitors average CPU utilization threshold and duration)	CloudSim	Detects the attack in a reactive manner. Thus, may cause economic losses and has high attack mitigation cost.
Xue et al. (2018) [144]	Prevention	Access control	Microsoft Azure	Prevents attackers from downloading multiple files from cloud storage.
Ficco (2019) [141]	Effect of EDoS attack on CSP is described	Coral-Reefs approach	Simulated environment	Reputation and financial losses at the CSP's end

NA = Not Available

IP spoofing technique to disguise the true location of the attackers. Thus, the detection of spoofed DDoS attack is a crucial but difficult task. Existing detection approaches for the spoofed DDoS attack need the involvement of the intermediate routers as discussed in [68],[69],[74]. Thus, the approaches have high communication complexity and cannot detect the low-rate and high-rate spoofed DDoS attacks in an effective manner. Although some efforts have been done to reduce the communication complexity in [42],[28], more research is still required to reduce the communication overhead.

2) Computational complexity: As discussed in Section V-A, the detection approaches for the low-rate DDoS attacks are mainly based on DFT for power spectral calculation. For the computation of N-point DFT, the number of complex multiplications and additions required are N^2 and $N(N-1)$ respectively. Thus, the total computational complexity involved in DFT is $O(N^2)$. This affects the performance of the algorithm and makes it unsuitable for real-time traffic analysis. Due to the involvement of complex computations, DFT is slow and provides poor performance. The DFT is not efficient for the large values of N. As the value of N increases, the number of computations required also increases. Thus, the effort should be done to reduce the computational complexity of DFT, or other transformation algorithms should be used which involve less computational complexity.

3) Internal cloud DDoS attack: In most of the existing approaches, the traffic coming from the external network is mainly considered for analysis. The external network refers to the network outside the cloud infrastructure. Thus, using such approaches, only the external DDoS attacks can be detected. The DDoS attacks in cloud computing may be launched by the VMs of the same cloud infrastructure. Such attacks are known as internal DDoS attacks which are unaddressed in the literature. Thus, the possibility of DDoS attacks still exists in the existing approaches. The monitoring of both internal and external traffic of the cloud network is essential and a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

challenging task.

To capture the internal and external cloud traffic without imposing extra communication overhead is also a challenge. The significant attempts have been made in [42],[28] to address this issue. Though the approaches can detect the external as well as the internal cloud DDoS attacks, more research effort is required in this field.

4) Real-time aggregate traffic analysis: The aggregate traffic refers to the traffic coming from the external as well as internal, legitimate and compromised nodes. From the literature study, it is observed that the real-time aggregate traffic is not considered. Tables II-VII show that the performance of most of the existing approaches is evaluated only in the simulated environments which are very far from the real cloud scenario. Thus, their suitability in the large-scale cloud network cannot be assured. For the effective detection system, analysis of real-time aggregate traffic is crucial which reduces the possibility of attacks.

To improve the detection performance, some approaches have been discussed which are based on the real cloud scenario as shown in Tables II-VII. To diminish the attack possibility, whole network traffic analysis is essential. Thus, significant efforts are needed to address this issue.

5) Economic loss: Nowadays, attackers are fascinated towards the low-rate DDoS attacks. They are continuously trying to discover new stealthy attack launching strategies. Thus, the detection of such low-rate attacks is arduous. Among the low-rate DDoS attacks, early detection of EDoS attack is essential. In EDoS attack, the attacker exploits the auto-scaling feature of the cloud and causes unnecessary installation of the new VM instances. If such attacks are not detected within a time-limit, then it may cause a huge financial loss. Existing mitigation approaches for the EDoS attacks mitigate the attack reactively. Reactive approaches mitigate the attack after its successful implementation. Thus, such solutions may increase the attack mitigation cost and consequently affect the economic component of the CSP. Hence, the proactive approaches need to be designed which make the early detection of such attacks possible.

B. Future Research Directions

This section presents the research opportunities in the field of DDoS attacks in a cloud computing environment.

1) Defense against DDoS attacks in Internet-of-Things (IoT)-based cloud: Cloud computing provides the virtual computing resources to the intended users, on demand. The scope of cloud computing applications can be extended to deal with the real world using IoT [155]. IoT is a new technology in the wireless telecommunications field and is widely adopted in the development of smart homes, wearables, smart cities, etc. It is a network of physical things (such as machines, home appliances, vehicles, etc.), which uses different Application Programming Interfaces (APIs) and sensors to communicate. IoT emphasizes the use of novel protocols for communication with the Web using Internet-connected devices.

When IoT is integrated with cloud computing, the new computing paradigm is named as *Cloud-of-Things* [156]. The technology adds a new dimension (such as physical things) to the cloud computing resources, and provides new monitoring and powerful processing capabilities. Besides the advantages, the technology faces some security challenges such as reliability, heterogeneity, performance, etc. With the advancement of Cloud-of-Things technology, the DDoS attacks are growing rapidly. The DDoS attacks in such an environment are still in their infancy. Due to the newly added dimension, the existing DDoS defense approaches may not be suitable for the Cloud-of-Things environment. Thus, further research is required to defend against the DDoS attacks in the IoT-based cloud.

2) Software Defined Networking (SDN)-based defense against DDoS attacks: Cloud computing is becoming a first attraction to launch DDoS attacks because of its essential features. These features provide many alternatives to defend against DDoS attacks. The cloud computing may get benefited by an another promising technology known as Software Defined Networking (SDN). With the recent advances in SDN, this new paradigm has gained great attention in the field of networking. SDN decouples the control and data planes, logically centralizes the network intelligence and abstracts the complexity of network-infrastructure for the applications [157]. The merging of these two promising technologies may provide new captivating options to defend against the DDoS attacks in cloud [13] and Cloud-of-Things environments. SDN-based cloud is a new type of cloud where the network infrastructure is controlled by the SDN controller and may provide Networking-as-a-Service (NaaS). The features of SDN such as centralized control, software-based traffic analysis, dynamic updates in forwarding rules, etc. make it easier to defend against the DDoS attacks.

Despite numerous benefits, the SDN itself becomes vulnerable to DDoS attacks which need to be addressed while designing any defense system. The comprehensive study about the DDoS attacks against SDN-based cloud is provided in [13]. Some SDN-based defense approaches for the DDoS attacks are described in [99]-[103]. As shown in Table III, these approaches are static and unable to adjust their functions according to the severity of DDoS attacks. Hence, they may have limited success rate. Thus, new dynamic SDN-based approaches need to be designed against the DDoS attacks for cloud and Cloud-of-Things environments.

3) Defense against DDoS-for-Hire service: New players in the field of DDoS attacks are the service providers who provide DDoS-for-hire [25] service on payment basis. The on-demand self-service and rapid elasticity features of cloud computing are exploited by the attackers to build a powerful botnet and provides DDoS-for-hire as a service. This cloud model is implemented by utilizing a large amount of cloud computing resources. Such clouds are known as black or grey clouds which are administered by the attackers. Due to the rise in DDoS-for-hire service, the percentage of DDoS attacks in a cloud computing environment may increase. It may get easier to launch DDoS attacks even for the novice attackers. Thus, the design of mitigation approaches against such attacks is the focus of cyber security researchers. The mitigation of DDoS attacks (implemented using DDoS-for-hire service) is expensive as more resources are required to circumvent the

attacks. Thus, a low-cost defense against such attacks is a challenging task.

4) Defense against Detection Near Impossible (DeNy) attack: A new but sophisticated attack, named as DeNy, has been anticipated to be available in coming future [25]. This attack is evolving as an open challenge for the cloud security research community. The DeNy attack is more stealthy and uses variable rate attack traffic. Thus, its detection is nearly impossible by the existing defense methods. In this attack, the attackers send only benign traffic from a large number of attack sources. Such attack is undetectable due to its two properties, benignness and false alerts. Benignness means the attack traffic has no anomalies. Thus, the attack traffic always generates false positive. DeNy attack traffic pattern is different from the low-rate DDoS attack traffic pattern. Thus, it may remain undetected by the low-rate DDoS attacks defense mechanisms. The development of defense mechanisms against DeNy attacks is more challenging, and it requires an improvement in the existing prevention, detection, and mitigation techniques.

VI. Performance Measurement Metrics

Several prevention, detection, and mitigation approaches against low-rate and high-rate DDoS attacks have been proposed in the literature. However, their performances are not evaluated against the set of common metrics. A set of consistent metrics should be defined to measure the performance of any defense system. The essential performance measuring metrics found in the literature are discussed in this section. Using these metrics, the defense approaches can be compared with respect to certain common parameters, and their efficacy can be easily measured. Then the quantitative comparison of the existing approaches is performed using these metrics in Table VIII and Table IX. In Table VIII, the recent approaches are compared based on the experimental testbed, adaptivity, True Negative Rate (TNR), True Positive Rate (TPR), and accuracy. Another comparison is performed based on the attack detection time, service response time, victim service downtime, and estimated cost/hour as shown in Table IX.

A. Accuracy

Accuracy is the first important metric for evaluating the performance of any defense system. The accuracy can be measured using two parameters: *TPR* or Sensitivity and *TNR* or Specificity. *TPR* measures the proportion of the attack traffic which is identified correctly, and *TNR* measures the proportion of the legitimate traffic which is identified correctly. Both *TPR* and *TNR* can be defined as,

$$TPR = \frac{\text{Attack Traffic Identified Correctly (a)}}{\text{a + Attack Traffic Misclassified as Legitimate (b)}} \quad (1)$$

and,

$$TNR = \frac{\text{Legitimate Traffic Identified Correctly (c)}}{\text{c + Legitimate Traffic Misclassified as Attack (d)}} \quad (2)$$

The accuracy of the proposed approach can be calculated as,

$$Accuracy = \frac{a + c}{a + b + c + d} \quad (3)$$

For an accurate defense system, the values of TPR and TNR should be as high as possible.

B. Service Response time

Service response time is the second crucial performance measuring metric for any defense system. It defines the period when a request is sent, and the corresponding response is received by the cloud user. Service response time plays a significant role in measuring the performance of the legitimate users. The deployment of the defense system in the cloud scenario should not affect the service response time of the legitimate users.

C. Attack Detection Time

Attack detection time is the third critical metric for evaluating the performance of a defense system. It defines the time when the network traffic is classified as legitimate or malicious. For an effective defense system, the attack should be detected as early as possible, i.e., attack detection time should be very low. The attack detection time directly depends on the communication and computational complexities of the defense algorithm.

D. Victim Service Downtime

Service downtime is the forth significant metric for measuring the performance of any defense mechanism. It defines the period during which the victim cloud server becomes unavailable and fails to service the legitimate requests. The defense approaches should be designed to respond the DDoS attacks quickly and make the victim server available to the legitimate users. Thus, for an effective defense system, the victim service downtime should be low.

E. Total Estimated Cost

Attack detection and mitigation cost is the fifth predominant metric which defines the total estimated cost associated with a defense system. The cost is estimated based on the utilization of computing, bandwidth, storage, and memory resources to defend against the DDoS attacks. Ideally, the attack defense cost of any security system should be less than the losses occurred due to the DDoS attacks.

F. Experimental Testbed

For an effective defense system, it is important to capture and monitor the real-time aggregate traffic. The real-time aggregate traffic which is coming from the legitimate as well as compromised nodes should be analyzed for the attack detection. The performance of several existing defense approaches has been evaluated in the simulated environment which is very far from the real cloud scenario. Thus, their suitability for real-time traffic analysis in the large-scale cloud computing environment cannot be guaranteed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

TABLE VIII
COMPARISON OF THE EXISTING APPROACHES BASED ON THE EXPERIMENTAL TESTBED, ADAPTIVITY, TNR, TPR, AND ACCURACY

Reference	Experimental Testbed	Adaptive	TNR	TPR	Accuracy
Fouladi et al. (2016) [123]	MATLAB R2015a and Weka 3.6	No	94.6%	96.7%	95.93%
Cotae et al. (2016) [124]	Simulated environment	No	NA	NA	NA
Liu et al. (2016) [125]	Simulated environment	No	NA	85%	NA
Wu et al. (2016) [127]	NS-2*	No	91%	92%	91.7%
Agrawal and Tapaswi (2017) [28]	Eucalyptus 3.4.1 cloud platform	Yes	99.5%	99.1%	99.3%
Hoque et al. (2017) [117]	Simulated Environment	No	99.9%	99.7%	99.66%
Kaur et al. (2017) [126]	NS-2*	No	NA	NA	NA
Wu et al. (2017) [128]	NS-2*	No	92.55%	81.36%	86.99%
Chen et al. (2018) [46]	NS-3**	No	NA	95.32%	NA
Wu et al. (2019) [120]	NS-2*	No	NA	NA	86.88%

NA = Not Available, * = Network Simulator 2, ** = Network Simulator 3

TABLE IX
COMPARISON OF THE EXISTING APPROACHES BASED ON THE ATTACK DETECTION TIME, RESPONSE TIME, SERVICE DOWNTIME, AND COST/HOUR

Reference	Attack Detection Time	Service Response Time	Victim Service Downtime	Cost/hour
Baig et al. (2016) [33]	NA	93 ms	NA	$0.15
Alsowail et al. (2016) [147]	NA	661.8 ms	NA	NA
Al-Haidari et al. (2017) [146]	NA	30 ms	NA	NE
Somani et al. (2017) [150]	39.6 s	0.151 s	1174 s	NA
Somani et al. (2017) [151]	845 s	NA	1326 s	NA
Somani et al. (2017) [152]	40.84 s	0.056 s	40.75 s	NA
Shawahna et al. (2018) [54]	3.33 ms	NA	NA	$3.73

NA = Not Available, NE = Not Explicitly stated

G. Proactive vs Reactive

The proactive approaches respond to the DDoS attacks in its early stage. While the reactive approaches respond to the attack after its successful implementation. The total estimated cost involved in the reactive approaches is high as compared to the proactive ones. The proactive approaches are more suitable for the small and medium enterprises or the single-hosted cloud service providers as they have several budget constraints.

H. Adaptivity

The DDoS attacks in the cloud environment may be launched via the compromised nodes of the internal as well as external cloud networks. Thus, the monitoring of both types of network traffic is of paramount importance. To minimize the possibility of DDoS attacks, the approaches should be adaptive which monitor and analyze the whole network traffic for attack detection.

Discussion: It may be observed from Table VIII that most of the existing approaches are based on the simulated environment. Majority of the approaches do not consider the internal traffic of the cloud infrastructure for attack detection. Among the approaches discussed in Table VIII, the approach proposed in [117] achieves high TNR, TPR, and accuracy. Though [117] provides enhanced accuracy, it is implemented in a simulated environment. Thus, it may not be suitable for the real-time traffic analysis in a cloud environment. It is clear from Table IX that none of the approaches is effective in terms of detection time, response time, service downtime, and cost/hour. Thus, the new approaches should be designed against the DDoS attacks to overcome the limitations of the existing approaches.

VII. OPEN PROBLEMS

Based on the future research directions, some open problems are discussed here to signify the importance of future research efforts needed. Current cloud networks are going to become the base of future IoT networks. SDN is going to change the behavior of future Internet networks. Thus, this section discusses the future research problems with respect to IoT and SDN networks.

1) Unlike conventional botnet, IoT botnet does not involve only the dedicated computers but also other devices such as home appliances, mobile devices, etc. It is easy for an attacker to create a powerful botnet using these devices easily because most of the IoT devices are low power devices and use less sophisticated security protocols. Using such botnet, it becomes easy to launch DDoS attacks even for an average skilled attacker. Thus, there is a need to design effective and less complex security protocols to protect the IoT-enabled devices from being compromised by attackers.
2) Though new capabilities of SDN bring new opportunities to defeat against the DDoS attacks in a cloud environment, SDN itself is vulnerable to DDoS attacks. Using SDN characteristics, attackers may launch DDoS attacks against SDN-based cloud. As the SDN controller plays a significant role, attackers target the controller node to paralyze the entire network. The defense mechanisms designed for the SDN-based cloud should be deployed at the controller node to reduce the possibility of attacks.
3) Using the features of DDoS-for-Hire service, the DDoS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

attacks may significantly increase due to their low price and ease of implementation. To accomplish this goal, attackers look for cheaper ways to create a botnet for DDoS-for-hire service. The less secured IoT devices become the easy targets for the botnet creation. Thus, robust security protocols are needed for IoT devices in defense against DDoS-for-hire service.

4) DeNy attack is also a serious concern in a cloud environment and the defense against such attacks is an open challenge for the research community due to its benignness and false alerts properties. For efficient design of defense solutions for such attacks, their attack launching strategies need to be carefully studied.

VIII. Conclusions

This paper starts with a discussion of security issues in cloud computing. To offer the on-demand feature of cloud computing, availability of cloud computing services and resources is predominant. The menacing threat to such availability is the DDoS attack. The paper next discusses how the cloud computing salient features are exploited by the attackers to launch various DDoS attacks. This survey considers the high-rate and all the possible variants of low-rate DDoS attacks in a cloud computing environment. A new taxonomy of the DDoS attacks and the corresponding defense mechanisms is presented. The prevention, detection, and mitigation approaches for each type of DDoS attacks are described. The paper discusses launching strategies for various DDoS attacks and their impact on the cloud infrastructure. The comparative analysis of the defense approaches and their behavior in cloud are also provided. The essential parameters for evaluating the performance of any defense system are also discussed. To the best of our knowledge, the low-rate DDoS attacks and their defense mechanisms are not well addressed in the existing surveys. The novelty of this paper is, various forms of low-rate DDoS attacks and their defense mechanisms are categorized and described. This paper excites the security researchers to develop effective prevention, detection, and mitigation solutions against the DDoS attacks in a cloud environment.

Appendix

Description of Functions and Transformations

A. Shannon Entropy

The entropy in information theory defines the amount of information in a signal. In 1948, Claude E. Shannon introduced the concept of information entropy [158]. The information entropy measures the amount of randomness or uncertainty in a signal with a given probability distribution. Shannon defines the entropy H of a discrete random variable X as:

$$H(X) = E[I(X)] = E[-log_2 P(X)] \tag{4}$$

where E is the expected value operator, $I(X)$ is a random variable defines the information content of X, and P is the probability distribution of X. The Shannon entropy can be written in terms of the possible outcomes $\{x_1, x_2, ..., x_n\}$ of X as:

$$H(X) = \sum_{i=1}^{n} P(x_i) I(x_i) = -\sum_{i=1}^{n} P(x_i) log_2 P(x_i) \tag{5}$$

where $P(x_i)$ is the probability of the i^{th} outcome (x_i) of X such that $P(x_i) \geq 0$. Thus, the Shannon entropy of a variable X is the sum of the product of the probability of outcome x_i and the information content of x_i for all possible (n) outcomes of X.

B. Discrete Fourier Transform

DFT is used to calculate the signal's frequency spectrum and allows to analyze the signals in frequency-domain. Using DFT, the periodicities in input signal and the relative strength of any periodic signal can be determined.

The DFT [159] maps the N-point discrete time signal input sequence x[n] = $\{x_0, x_1, ..., x_{N-1}\}$ into the N-point complex discrete output sequence Y[k] = $\{Y_0, Y_1, ..., Y_{N-1}\}$. The k^{th} number of complex output sequence can be obtained using DFT as:

$$Y[k] = \sum_{n=0}^{N-1} x[n] e^{-i2\pi kn/N} \tag{6}$$

After applying the Euler's formula on Equation (3), it can be represented as:

$$Y[k] = \sum_{n=0}^{N-1} x[n] cos(2\pi nk/N) - i * sin(2\pi nk/N)] \tag{7}$$

where x and Y are the input and output sequences respectively, N is the length of both sequences, and k is a variable which belongs to $\{0, 1, 2, ..., N-1\}$.

C. Discrete Wavelet Transform

Like DFT which decomposes the signal into the complex sinusoids, DWT [160] decomposes the signal into the wavelets. The DWT of a signal x[n] is determined by passing it via sequence of filters. First, the signal x is passed through the low-pass filter with impulse response g which produces the convolution of x and g as output. The low-pass filter can be defined as:

$$y[n] = (x * g)[n] = \sum_{\delta=-\infty}^{\infty} x[\delta] g[n - \delta] \tag{8}$$

The signal is simultaneously decomposed by using a high-pass filter h as:

$$y[n] = (x * h)[n] = \sum_{\delta=-\infty}^{\infty} x[\delta] h[n - \delta] \tag{9}$$

This decomposition is performed repetitively to enhance the frequency resolution and the series of filters is represented by a filter-tree also known as filter-bank.

The implementation of filter-bank can be performed by computing the wavelet coefficients of a discrete set of child

wavelets for a given mother wavelet $\psi(t)$. In DWT, the mother wavelet is scaled and shifted by a power of 2 as:

$$\psi_{\alpha,\beta}(t) = \frac{1}{\sqrt{2^{\alpha}}}\psi\left(\frac{t - 2^{\alpha}\beta}{2^{\alpha}}\right) \tag{10}$$

where α and β are integers, and define the scale and shift parameters respectively.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[2] O. Osanaiye, K.K.R. Choo, and M. Dlodlo, "Distributed Denial of Service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147-165, May 2016.

[3] B. Varghese and R. Buyya R, "Next generation cloud computing: New trends and research directions", *Future Generation Computer Systems* vol. 79, no. 3, pp. 849-861, Feb. 2018.

[4] P.K. Senyo, E. Addae, and R. Boateng, "Cloud computing research: A review of research themes, frameworks, methods and future research directions", *International Journal of Information Management*, vol. 38, no. 1, pp. 128-139, Feb. 2018.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592, March 2012.

[6] K. Hashizume, D.G. Rosado, E. Fernndez-Medina, and E.B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 5, pp. 1-13, Feb 2013.

[7] M.A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications,* vol. 71, pp. 11-29, Aug. 2016.

[8] S. Singh, Y.S. Jeong, and J.H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200-222, Nov. 2016.

[9] L. Coppolino, S.D. Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Computers & Electrical Engineering*, vol. 59, pp. 126-140, April 2017.

[10] M. Ali, S.U. Khan, and A.V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences*, vol. 305, pp. 357-383, June 2015.

[11] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88-115, Feb. 2017.

[12] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843-859, Second Quarter 2013.

[13] Q. Yan, F.R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, First Quarter 2016.

[14] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, Jan. 2011.

[15] S. Iqbal, M.L.M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M.K. Khan, and K.K.R. Choo, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *Journal of Network and Computer Applications*, vol. 74, pp. 98-120, Oct. 2016.

[16] N.V. Juliadotter and K.K.R. Choo, "Cloud attack and risk assessment taxonomy," *IEEE Cloud Computing*, vol. 2, no. 1, pp. 14-20, Jan.-Feb. 2015.

[17] F. Gens, "New idc it cloud services survey: Top benefits and challenges," IDC exchange, pp. 17-19, 2009.

[18] C. Fachkha and M. Debbabi, "Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1197-1227, Second Quarter 2016.

[19] J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, and R.K. Thomas, "Accurately measuring denial of service in simulation and testbed experiments," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 2, pp. 81-95, April-June 2009.

[20] N. Hoque, D.K. Bhattacharyya, J.K. Kalita, "Botnet in DDoS attacks: trends and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242-2270, Fourth Quarter 2015.

[21] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications*, vol. 107, pp. 30-48, July 2017.

[22] A. Networks, "DDoS Attack Statistics," 2016. [Online]. Available: https://www:arbornetworks:com/arbor-networks-releasesglobal-ddos-attack-data-for-1h-2016

[23] A. Praseed and P.S. Thilagam, "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 661-685, First Quarter 2019.

[24] P. Nelson, "Cybercriminals moving into cloud big time, report says," March 2015. [Online]. Available: https://www.networkworld.com/article/2900125/malware-cybercrime/criminals-moving-into-cloud-big-time-says-report.html

[25] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, R. Buyya, "Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 22-32, Jan.-Feb. 2017.

[26] A. Shameli-Sendi, M. Pourzandi, M. Fekih-Ahmed, and M. Cheriet, "Taxonomy of distributed denial of service mitigation approaches for cloud computing," *Journal of Network and Computer Applications*, vol. 58, pp. 165-179, Dec. 2015.

[27] S.T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013.

[28] N. Agrawal and S. Tapaswi. "A Lightweight Approach to Detect the Low/High Rate IP Spoofed Cloud DDoS Attacks," *in Proc.* 7^{th} *IEEE International Symposium on Cloud and Service Computing (SC2)*, Kanazawa, Japan, 22-25 Nov. 2017, pp. 118-123.

[29] Anonymous attack on amazon.com appears to fail, Available: http://www.computerworld.com/article/2511711/cybercrime-hacking/anonymous-attack-on-amazon-com-appears-to-fail.html. December 2010.

[30] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for Low-Rate Shrew DDoS," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069-1083, July 2014.

[31] M. Guirguis, "Reduction-of-quality attacks on adaptation mechanisms," Boston University, 2007.

[32] G.M. Fernandez, J.E. Diaz-Verdejo, and P. Garcia-Teodoro, "Mathematical model for low rate DoS Attacks Against Application Servers," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 519-529, Sept. 2009.

[33] Z.A. Baig, S.M. Sait, and F. Binbeshr, "Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks," *Computer Networks*, vol. 97, pp. 31-47, March 2016.

[34] F. Al-Haidari, M. Sqalli, and K. Salah, "Evaluation of the impact of EDoS attacks against cloud computing services," *Arabian Journal for Science and Engineering*, vol. 40, no. 3, pp. 773-785, March 2015.

[35] L. Munson. Greatfire.org faces daily $30,000 bill from ddos attack. Available: https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/, 2015.

[36] K. Pelechrinis, M. Iliofotou, and S.V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 245-257, Second Quarter 2011.

[37] N.C. Luong, D.T. Hoang, P. Wang, D. Niyato, and Z. Han, "Applications of economic and pricing models for wireless network security: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2735-2767, Fourth Quarter 2017.

[38] J. Francois, "Cloud Computing: Weapon of Choice for DDoS?," Dec. 2012. [Online]. Available: http://www.orange-business.com/en/blogs/connecting-technology/security/cloud-computing-weapon-of-choice-for-ddos

[39] A. Gonsalves, "Prices Fall, Services Rise in Malware-as-a-Service Market," Mar. 2013. [Online]. Available: http://www.csoonline.com/article/2133045/malware-cybercrime/prices-fall-services-rise-in-malware-as-a-service-market.html

[40] A. Gonsalves, "Mobile Devices Set to Become Next DDoS Attack Tool," Jan. 2013. [Online]. Available: http://www.csoonline.com/article/2132699/mobile-security/mobile-devices-set-to-become-next-ddosattack-tool.html

[41] M. Ficco and M. Rak, "Stealthy Denial of Service strategy in cloud computing," *IEEE Transaction on Cloud Computing*, vol. 2, no. 1, pp. 80-94, Jan.-March 2015.

[42] N. Agrawal and S. Tapaswi, "Low rate cloud DDoS attack defense method based on power spectral density analysis," *Information Processing Letters*, vol. 138, pp. 44-50, Oct. 2018.

[43] G. Somani, M.S. Gaur, D. Sanghi, and M. Conti, "DDoS attacks in cloud computing: collateral damage to non-targets," *Computer Networks*, vol. 109, no. 2, pp. 157-171, Nov. 2016.

[44] B.B. Gupta and O.P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3655-3682, Dec. 2017.

[45] N. Agrawal and S. Tapaswi. "Defense Schemes for Variants of Distributed-Denial-of-Service (DDoS) Attacks in Cloud Computing: A Survey," *Information Security Journal: A Global Perspective, Taylor and Francis*, vol. 26, no. 2, pp. 61-73, Feb. 2017.

[46] Z. Chen, C.K. Yeo, B.S. Lee, and C.T. Lau, "Power Spectrum Entropy based Detection and Mitigation of Low Rate DoS Attacks," *Computer Networks*, vol. 136, pp. 80-94, May 2018.

[47] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53, April 2004.

[48] K. Kalkan, G. Gur, and F. Alagoz, "Filtering-based defense mechanisms against DDoS attacks: A survey," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2761-2773, Dec. 2017.

[49] K. Singh, P. Singh, K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," *Computers & Security*, vol. 65, pp. 344-372, March 2017.

[50] Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," *Journal of Parallel and Distributed Computing*, vol. 66, no. 9, pp. 1137-1151, Sep. 2006.

[51] F. Yu, G. Li, and M. Cui, "The Detection of Low-rate Denial-of-service attack based on feature extraction and analysis at congestion times," *in Proc. IEEE International Conference on Electrical and Control Engineering (ICECE)*, 2011, pp. 1338-1341.

[52] A. Kuzmanovic and E.W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," *in Proc. ACM Conf. on App., Technologies, Architectures, and Protocols for Computer Communications*, Karlsruhe, Germany, 25-29 Aug. 2003, pp. 75-86.

[53] A. Shevtekar and N. Ansari, "A router-based technique to mitigate reduction of quality (RoQ) attacks," *Computer Networks*, vol. 52, no. 5, pp. 957-970, April 2008.

[54] A. Shawahna, M. Abu-Amara, A. Mahmoud, and Y.E. Osais, "EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability (EDoS) Attacks," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, pp. 1-14, Feb. 2018.

[55] S. Ranjan, R. Swaminathan, M. Uysal, E.W. Knightly, "DDoS-Resilient Scheduling to Counter Application Layer Attacks Under Imperfect Detection," *in Proc. 25^{th} IEEE Int. Conf. on Computer Communications (INFOCOM)*, Barcelona, Spain, 23-29 April 2006, pp. 1-13.

[56] A. Matrawy, P. C.van Oorschot, and A. Somayaji, "Mitigating network denial-of-service through diversity-based traffic management," *in Proc. International Conference on Applied Cryptography and Network Security*, Springer, Berlin, Heidelberg, June 2005, pp. 104-121.

[57] M. Goldstein, M. Reif, A. Stahl, and T. Breuel, "High performance traffic shaping for ddos mitigation," *in Proc. ACM CoNEXT Conference*, Dec. 2008, pp. 1-2.

[58] H. Wang, Q. Jia, D. Fleck, W. Powell, F. Li, and A. Stavrou, "A moving target DDoS defense mechanism," *Computer Communications*, vol. 46, pp. 10-21, June 2014.

[59] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643-666, April 2004.

[60] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42-57, Jan. 2013.

[61] A. Bakshi and Y.B. Dudojwala, "Securing cloud from DDoS attacks using intrusion detection system in virtual machine," *in Proc. 2^{nd} IEEE International Conference on Communication Software and Networks (ICCSN)*, Singapore, 26-28 Feb. 2010, pp. 260-264.

[62] A.M. Lonea, D.E. Popescu, O. Prostean, and H. Tianfield, "Evaluation of experiments on detecting distributed denial of service (DDoS) attacks in eucalyptus private cloud," *in: Proc. 5^{th} International Workshop Soft Computing Applications (SOFA)*, Springer, Berlin, Heidelberg, vol. 195, 2013, pp. 367-379.

[63] C.C. Lo, C.C. Huang, J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," *in Proc. 39^{th} IEEE International Conference on Parallel Processing Workshops*, San Diego, CA, USA, 13-16 Sept. 2010, pp. 280-284.

[64] A. Karasaridis, "System and method to diffuse denial-of-service attacks using virtual machines," U.S. Patent 9,485,273, issued 1 November 2016.

[65] S. Gupta and P. Kumar, "Vm profile based optimized network attack pattern detection scheme for ddos attacks in cloud," *in Proc. International Symposium on Security in Computing and Communication*, Springer, Berlin, Heidelberg, Aug. 2013, pp. 255-261.

[66] A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Communications Letters*, vol. 13, no. 9, pp. 1089-7798, Oct. 2009.

[67] W. Chen and D.Y. Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing," *in Proc. IEEE International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL)*, Mauritius, 23-29 April 2006, pp. 1-6.

[68] F.Y. Lee and S. Shieh, "Defending against spoofed DDoS attacks with path fingerprint," *Computers & Security*, vol. 24, no. 7, pp. 571-586, March 2005.

[69] O.A. Osanaiye and M. Dlodlo, "TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment," *in Proc. IEEE International Conference on Computer as a Tool (EUROCON)*, Salamanca, Spain, 8-11 Sep. 2015, pp. 1-6.

[70] T. Karnwal, S. Thandapanii, and A. Gnanasekaran, "A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack," *Intelligent Informatics*, Advances in Intelligent Systems and Computing, vol 182. Springer, Berlin, Heidelberg, 2013.

[71] W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Future Generation Computer System*, vol. 29, no. 7, pp. 1838-1850, Sep. 2013.

[72] P. Shamsolmoali and M. Zareapoor, "Statistical-based filtering system against DDOS attacks in cloud computing," *in Proc. IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, New Delhi, India, 24-27 Sept. 2014, pp. 1234-1239.

[73] H. Wang, C. Jin, and K.G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 40-53, Feb. 2007.

[74] A. Yaar, A. Perrig, and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1853-1863, Oct. 2006.

[75] S. Toklu and M. Simsek, "Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service (DDoS) Attack Detection and Filtering," *Arabian Journal for Science and Engineering*, pp. 1-9, 2018.

[76] Y. Xiang, K. Li, and W. Zhou, "Low rate DDoS attack detection and traceback by using new information metrics," *IEEE Transactions on information forensics and security*, vol. 6, no. 2, pp. 426-437, Jan. 2011.

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

[78] J. Francois, I. Aib, and R. Boutaba, "FireCol: a collaborative protection network for the detection of flooding DDoS attacks," *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, pp. 1828-1841, Dec. 2012.

[79] Y. Chen, K. Hwang, and W.S. Ku, "Collaborative detection of DDoS attacks over multiple network domains," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 12, pp. 1649-1662, Nov. 2007.

[80] O. Osanaiye, K.K.R. Choo, and M. Dlodlo, "Change-point cloud DDoS detection using packet inter-arrival time," *in: Proc. 8^{th} IEEE International Conference on Computer Science and Electronic Engineering (CEEC)*, Colchester, UK, 28-30 Sept. 2016, pp. 204-209.

[81] 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," *Journal of Soft Computing*, vol. 18, no. 9, pp. 1697-1703, Sep. 2014.

[82] Z. Chen, G. Xu, V. Mahalingam, L. Ge, J. Nguyen, W. Yu, and C. Lu, "A cloud computing based network monitoring and threat detection system for critical infrastructures," *Big Data Research*, vol. 3, pp. 10-23, April 2016.

[83] K. Borisenko, A. Smirnov, E. Novikova, and A. Shorov, "DDoS attacks detection in cloud computing using data mining techniques," *in Proc. Industrial Conference on Data Mining, Advances in Data Mining, Applications and Theoretical Aspects*, vol. 9728, June 2016, 197-211.

[84] J. Zhang, P. Liu, J. He, and Y. Zhang, "A Hadoop Based Analysis and Detection Model for IP Spoofing Typed DDoS Attack," *in Proc. IEEE Trustcom/BigDataSE/ISPA*, China, 23-26 Aug. 2016, pp. 1976-1983.

[85] M.N. Ismail, A. Aborujilah, S. Musa, and A. Shahzad, "Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach," *in Proc.* 7^{th} *ACM International Conference on Ubiquitous Information Management and Communication*, Kota Kinabalu, Malaysia, 17-19 Jan. 2013, article no. 36.

[86] O. Osanaiye, H. Cai, K.K.R. Choo, A. Dehghantanha, Z. Xu, and M. Dlodlo, "Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 130-139, May 2016.

[87] T. Vissers, T.S. Somasundaram, L. Pieters, K. Govindarajan, and P. Hellinckx, "DDoS defense system for web services in a cloud environment," *Future Generation Computer Systems*, vol. 37, pp. 37-45, July 2014.

[88] N. Hubballi and N. Tripathi, "An event based technique for detecting spoofed IP packets," *Journal of Information Security and Applications*, vol. 35, pp. 32-43, Aug. 2017.

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

[90] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, "XGBoost Classifier for DDoS Attack Detection and Analysis in SDN-based Cloud," *in Proc. of IEEE International Conference on Big Data and Smart Computing (BigComp)*, Jan. 2018, pp. 251-256.

[91] S.T. Zargar and J. Joshi, "DiCoDefense: distributed collaborative defense against ddos flooding attacks," *In IEEE symposium on security and privacy*, May 2013, pp. 1-3.

[92] S.B. Lee, M.S. Kang, and V.D. Gligor, "CoDef: collaborative defense against large-scale link-flooding attacks," *in Proc.* 9^{th} *ACM conference on Emerging networking experiments and technologies*, Santa Barbara, California, USA, 09-12 Dec. 2013, pp. 417-428.

[93] A. Murthy, N.R. Karri, P.K. Patel, W. Hongyu Z. Marios Y.N. Sethuraman, and D. Bansal, "DOS detection and mitigation in a load balancer," U.S. Patent 9,055,095, issued 9 June 2015.

[94] B. Wang, Y. Zheng, W. Lou, Y.T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," *Computer Networks*, vol. 81, pp. 308-319, April 2015.

[95] V.S.M. Huang, R. Huang, and M. Chiang, "A DDoS mitigation system with multi-stage detection and text-based turing testing in cloud computing," *in Proc.* 27^{th} *IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Barcelona, Spain, 25-28 March 2013, pp. 655-662.

[96] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "ArOMA: An SDN based autonomic DDoS mitigation framework," *Computers & Security*, vol. 70, pp. 482-499, Sep. 2017.

[97] K. Hong, Y. Kim, H. Choi, and J. Park, "SDN-Assisted Slow HTTP DDoS Attack Defense Method," *IEEE Communications Letters*, vol. 22, no. 4, pp. 688-691, April 2018.

[98] K. Bhushan and B.B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-13, April 2018.

[99] J. Naous, D. Erickson, G.A. Covington, G. Appenzeller, and N. McKeown, "Implementing an OpenFlow switch on the NetFPGA platform," *in Proc.* 4^{th} *ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, San Jose, California, 06-07 Nov. 2008, pp. 1-9.

[100] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," *in Proc.* 35^{th} *IEEE Conf. on Local Comp. Net. (LCN)*, Denver, CO, USA, 10-14 Oct. 2010, pp. 408-415.

[101] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security", *in Proc.* 12^{th} *International Conference on Communication Technology (ICCT)*, Nanjing, China, 11-14 Nov. 2010, pp. 385-388.

[102] C. Buragohain and N. Medhi, "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers," *in Proc. of IEEE* 3^{rd} *International Conference on Signal Processing and Integrated Networks (SPIN)*, Feb. 2016, pp. 519-524.

[103] G. Yao, J. Bi, and P. Xiao, "Source address validation solution with OpenFlow/NOX architecture," *in Proc.* 19^{th} *IEEE International Conference on Network Protocols (ICNP)*, Vancouver, BC, Canada, 17-20 Oct. 2011, pp. 7-12.

[104] T. Dubendorfer, M. Bossardt, and B. Plattner, "Adaptive distributed traffic control service for DDoS attack mitigation," *in Proc.* 19^{th} *IEEE International Parallel and Distributed Processing Symposium*, Denver, CO, USA, 4-8 April 2005, pp. 1-8.

[105] J.M. Gonzalez, V. Paxson, and N. Weaver, "Shunting: a hardware/software architecture for flexible, high-performance network intrusion prevention," *in Proc.* 14^{th} *ACM Conf. on Comp. and Comm. security*, Alexandria, Virginia, USA, Oct. 2007, pp. 139-149.

[106] S. Yu, Y. Tian, S. Guo, and D.O. Wu, "Can we beat DDoS attacks in clouds?," *IEEE Transactions on parallel and distributed systems*, vol. 25, no. 9, pp. 2245-2254, Sep. 2014.

[107] D.K. Yau, J.C. Lui, F. Liang, and Y. Yam, "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles," *IEEE/ACM Transactions on Networking*, vol. 13, no. 1, pp. 29-42, Feb. 2005.

[108] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing", Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, vol. 4, pp. 506-522.

[109] C. Peng, M. Kim, Z. Zhang, and H. Lei, "VDN: Virtual machine image distribution network for cloud data centers," *in Proc. IEEE INFOCOM*, pp. 181-189, March 2012.

[110] R. Lua and K.C. Yow, "Mitigating ddos attacks with transparent and intelligent fast-flux swarm network," *IEEE Network*, vol. 25, no. 4, July-Aug. 2011.

[111] A. Chesla and E. Doron, "Techniques for traffic diversion in software defined networks for mitigating denial of service attacks," *United States patent application US 14/728,405*, Dec. 2016.

[112] C.M. Cheng, H.T Kung, and K.S. Tan, "Use of spectral analysis in defense against DoS attacks", *in Proc. IEEE Conference on Global Telecommunications (GLOBECOM)*, Taipei, Taiwan, 17-21 Nov. 2002, pp. 2143-2148.

[113] Y. Chen, K. Hwang, and Y.K. Kwok, "Filtering of Shrew DDoS attacks in frequency domain", *in Proc. IEEE Conference on Local Computer Networks (LCN)*, Sydney, NSW, Australia, 17 Nov. 2005, pp. 786-793.

[114] Y. Chen, K. Hwang, and Y.K. Kwok, "Collaborative defense against periodic Shrew DDoS attacks in frequency domain," *ACM Transactions on Information and System Security*, pp. 1-30, May 2005.

[115] X. He, C. Papadopoulos, J. Heidemann, U. Mitra, and U. Riaz, "Remote detection of bottleneck links using spectral and statistical methods," *Computer Networks*, vol. 53, no. 3, pp. 279-298, Feb. 2009.

[116] H. Chen, T. Gaska, Y. Chen, and D.H. Summerville, "An optimized reconfigurable power spectral density converter for real-time shrew DDoS attacks detection," *Computers & Electrical Engineering*, vol. 39, no. 2, pp. 295-308, Feb. 2013.

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

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

[119] D. Tang, K. Chen, X.S. Chen, H.Y. Liu, and X.H. Li, "A New Collaborative Detection Method for LDoS Attacks," *Journal of Networks*, vol. 9, no. 10, pp. 2674-2681, 2014.

[120] Z. Wu, Q. Pan, M. Yue, and L. Liu, "Sequence Alignment Detection of TCP-targeted Synchronous Low-rate DoS Attacks," *Computer Networks*, vol. 152, pp. 64-77, 2019.

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

[122] K.S. Sahoo, D. Puthal, M. Tiwary, J.J. Rodrigues, B. Sahoo, R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," *Future Generation Computer Systems*, vol. 89, pp. 685-697, July 2018.

[123] R.F. Fouladi, C.E. Kayatas, and E. Anarim, "Frequency based DDoS attack detection approach using naive Bayes classification," *in: Proc.* 39^{th} *IEEE International Conference on Telecommunications and Signal Processing (TSP)*, Vienna, Austria, 27-29 June 2016, pp. 104-107.

[124] P. Cotae, M. Kang, and A. Velazquez, "Spectral analysis of low rate of denial of service attacks detection based on fisher and Siegel tests," *in Proc. IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia. 22-27 May 2016, pp. 1-6.

[125] Z. Liu, X. Yin, and H.J. Lee, "A new network flow grouping method for preventing periodic shrew DDoS attacks in cloud computing," *in Proc.* 18^{th} *IEEE International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, South Korea, 31 Jan.-3 Feb. 2016, pp. 66-69.

[126] G. Kaur, V. Saxena, and J.P. Gupta, "Detection of TCP Targeted High Bandwidth Attacks Using Self-Similarity," *Journal of King Saud University-Computer and Information Sciences*, pp. 1-15, May 2017.

[127] Z. Wu, L. Zhang, and M. Yue, "Low-rate DoS attacks detection based on network multifractal," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 5, pp. 559-567, Sep.-Oct. 2016.

[128] Z. Wu, M. Wang, C. Yan, and M. Yue, "Low-Rate DoS Attack Flows Filtering Based on Frequency Spectral Analysis," *China Communications,* vol. 14, no. 6, pp. 98-112, June 2017.

[129] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on internet end-systems," *In:* 24^{th} *IEEE Annual Joint Conference of the IEEE Computer and Communications Societies*, Miami, FL, USA, 22 Aug. 2005, pp. 1362-1372.

[130] M. Guirguis, J. Tharp, A. Bestavros, and I Matta, "Assessment of vulnerability of content adaptation mechanisms to RoQ attacks," *In:* 8^{th} *IEEE International Conference on Networks (ICN'09)*, 2009, pp. 445-450.

[131] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) attacks on dynamic load balancers: Vulnerability assessment and design tradeoffs," *in Proc.* 26^{th} *IEEE International Conference on Computer Communications*, Barcelona, Spain, May 2007, pp. 857-865.

[132] Y. Chen and K. Hwang, "Spectral analysis of TCP flows for defense against Reduction-of-Quality attacks," *in Proc. IEEE Int. Conf. on Communications,* Glasgow, UK, 24-28 June 2007, pp. 1203-1210.

[133] G.M. Fernandez, J.E.D. Verdejo, and P.G. Teodoro, "Evaluation of a low-rate DoS attack against iterative servers," *Computer Networks*, vol. 51, no. 4, pp. 1013-1030, March 2007.

[134] G.M. Fernandez, J.E.D. Verdejo, P.G. Teodoro, and F.D.T. Negro, "LoRDAS: A Low-Rate DoS Attack against Application Servers," *in Proc.* 2^{nd} *International Workshop on Critical Information Infrastructures Security (CRITIS)*, Lecture Notes in Computer Science, vol 5141. Springer, Berlin, Heidelberg, Oct. 2007, pp. 197-209.

[135] G.M. Fernandez, J.E.D. Verdejo, and P.G. Teodoro, "Evaluation of a low-rate DoS attack against application servers," *Computers & Security*, vol. 27, no. 7-8, pp. 335-354, Dec. 2008.

[136] G.M. Fernandez, R.A.R. Gomez, J.E.D. Verdejo, "Defense techniques for low-rate DoS attacks against application servers," *Computer Networks*, vol. 54, no. 15, pp. 2711-2727, Oct. 2010.

[137] J. Brynielsson and R. Sharma, "Detectability of low-rate HTTP server DoS attacks using spectral analysis," *in: Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Paris, France. 25-28 Aug. 2015, pp. 954-961.

[138] N. Tripathi and N. Hubballi N, "Slow rate denial of service attacks against HTTP/2 and detection," *Computers & Security*, vol. 72, pp. 255-272, Jan. 2018.

[139] H. Wang, Z. Xi, F. Li, and S. Chen, "Abusing Public Third-Party Services for EDoS Attacks," *in* 10^{th} *USENIX Workshop on Offensive Technologies (WOOT)*, Austin, TX, 8-9 Aug. 2016, pp. 1-13.

[140] G. Somani, M.S. Gaur, and D. Sanghi, "DDoS/EDoS attack in cloud: affecting everyone out there!," *in Proc.* 8^{th} *Int. Conf. on Security of Inf. and Networks*, Sochi, Russia, 08-10 Sep. 2015, pp. 169-176.

[141] M. Ficco, "Could emerging fraudulent energy consumption attacks make the cloud infrastructure costs unsustainable?," *Information Sciences*, vol. 476, pp. 474-490, 2019.

[142] S.H. Khor and A. Nakao, "sPoW: On-demand cloud-based eddos mitigation mechanism," *in Proc.* 5^{th} *IEEE Workshop on Hot Topics in System Dependability*, Estoril, Lisbon, Portugal, June 2009, pp. 1-6.

[143] M.N. Kumar, R. Korra, P. Sujatha, and M. Kumar, "Mitigation of economic distributed denial of sustainability (eddos) in cloud computing," *in Proc. Int. Conf. on Advances in Engg. and Technology*, 2011.

[144] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062-2074, Aug. 2018.

[145] M.H. Sqalli, F. Al-Haidari, and K. Salah, "Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing" *in Proc.* 4^{th} *IEEE International Conference on Utility and Cloud Computing (UCC)*, Victoria, NSW, Australia, pp. 49-56, Dec. 2011.

[146] F. Al-Haidari, K. Salah, M. Sqalli, and S.M. Buhari, "Performance Modeling and Analysis of the EDoS-Shield Mitigation" *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 793-804, Feb. 2017.

[147] S. Alsowail, M.H. Sqalli, M. Abu-Amara, Z. Baig, and K. Salah, "An experimental evaluation of the EDoS-shield mitigation technique for securing the cloud" *Arabian Journal for Science and Engineering*, vol. 41, no. 12, pp. 5037-5047, Dec. 2016.

[148] F. Al-Haidari, M.H. Sqalli, and K. Salah, "Enhanced EDoS-shield for mitigating EDoS attacks originating from spoofed IP addresses," *in Proc.* 11^{th} *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Liverpool, UK, 25-27 June 2012, pp. 1167-1174.

[149] W. Alosaimi, M. Zak, and K. Al-Begain, "Denial of Service Attacks Mitigation in the Cloud," *in Proc.* 9^{th} *IEEE International Conference on Next Generation Mobile Applications, Services and Technologies*, Cambridge, UK, 9-11 Sept. 2015, pp. 47-53.

[150] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, "DDoS victim service containment to minimize the internal collateral damages in cloud computing," *Computers & Electrical Engineering*, vol. 59, pp. 165-179, April 2017.

[151] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "Service resizing for quick DDoS mitigation in cloud computing environment," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 237-252, June 2017.

[152] G. Somani, M.S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, "Scale Inside-out: Rapid Mitigation of Cloud DDoS Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1-14, Oct. 2017.

[153] M. Masood, Z. Anwar, S.A. Raza, and M.A. Hur, "Edos armor: a cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments," *in Proc.* 16^{th} *IEEE Multi Topic Conference*, Lahore, Pakistan, Dec. 2013, pp. 37-42.

[154] B. Saini and G. Somani, "Index page based EDoS attacks in infrastructure cloud," *in Proc. International Conference on Security in Computer Networks and Distributed Systems*, Berlin/Heidelberg Springer, vol. 420, 2014, pp. 382-395.

[155] S. Mubeen, S.A. Asadollah, A.V. Papadopoulos, M. Ashjaei, H. Pei-Breivold, and M. Behnam, "Management of Service Level Agreements for Cloud Services in IoT: A Systematic Mapping Study," *IEEE Access*, vol. 6, pp. 30184-30207, June 2018.

[156] C. Stergiou, K.E. Psannis, B.G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Generation Computer Systems*, vol. 78, no. 3, pp. 964-975, Jan. 2018.

[157] S.H. Yeganeh, A. Tootoonchian, and Y. Ganjali, "On scalability of software-defined networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 136-141, Feb. 2013.

[158] J. Lin, "Divergence measures based on the Shannon entropy," *IEEE Transactions on Information Theory*, vol. 37, no. 1, pp. 145-151, Jan. 1991.

[159] B.P. McGrath, D.G. Holmes, and J.J.H. Galloway, "Power converter line synchronization using a discrete Fourier transform (DFT) based on a variable sample rate," *IEEE Transactions on Power Electronics*, vol. 20, no. 4, pp. 877-884, July 2005.

[160] J.T Olkkonen and H. Olkkonen, "Discrete lattice wavelet transform," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 54, no. 1, pp. 71-75, Jan. 2007.