IEEE Xplore ®

Notice to Reader

"A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments"
by S. Dong, K. Abbas, and R. Jain
published in *IEEE Access,* Volume 7, pp. 80813-80828, 2019
Digital Object Identifier: 10.1109/ACCESS.2019.2922196

It is recommended by the Editor-in-Chief of IEEE *Access* that the above-mentioned article should not be considered for citation purposes. IEEE policy requires that consent to publish be obtained from all authors prior to publication.

This article was submitted by Shi Dong without the consent of Raj Jain.

We regret any inconvenience this may have caused.

Prof. Derek Abbott
Editor-in-Chief
IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 16, 2019, accepted June 7, 2019, date of publication June 12, 2019, date of current version July 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2922196

A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments

SHI DONG[1], KHUSHNOOD ABBAS[1], AND RAJ JAIN[2], (Fellow, IEEE)
[1]School of Computer Science and Technology, Zhoukou Normal University, Zhoukou 466001, China
[2]Department of Computer Science and Engineering, Washington University, St. Louis, MO 63130, USA

Corresponding author: Shi Dong (njbsok@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant U1504602, in part by the China Postdoctoral Science Foundation under Grant 2015M572141, in part by the Key Scientific and Technological Research Projects in Henan Province under Grant 192102210125, in part by the Science and Technology Department Research Project of Henan Province under Grant162102310147, and in part by the Education Department of Henan Province Science and Technology Key Project Funding under Grant 14A520065.

ABSTRACT Recently, software defined networks (SDNs) and cloud computing have been widely adopted by researchers and industry. However, widespread acceptance of these novel networking paradigms has been hampered by the security threats. Advances in the processing technologies have helped attackers in increasing the attacks too, for instance, the development of Denial of Service (DoS) attacks to distributed DoS (DDoS) attacks which are seldom identified by conventional firewalls. In this paper, we present the state of art of the DDoS attacks in SDN and cloud computing scenarios. Especially, we focus on the analysis of SDN and cloud computing architecture. Besides, we also overview the research works and open problems in identifying and tackling the DDoS attacks.

INDEX TERMS Software defined network, cloud computing, distributed denial of service attacks (DDoS), DDoS attack and detection, experimental setup, survey.

I. INTRODUCTION

Recently, Software Defined Networks (SDN) and cloud computing have gained significant attention in both, the academia and the industry. SDN decouples the network control plane from the data plane. The control plane is coherently synchronized. SDN plans to simplify the networks and empower the developments through the programmability of networks. Centralization helps disentangling the usage of system strategies by programming, not like customary systems which makes utilization of low-level device configuration. A control program can set up the high-level state approaches and rapidly distinguish the real-time network state. Centralization of the controller streamlines the advancement of network functions. Network programmability can adequately control the fundamental data plane in SDN. SDN architecture decouples the network control and forwarding capacities empowering the network control to be programmable and the fundamental framework to be preoccupied for applications and network services. SDN has helped a great deal towards the accomplishment of cloud computing networking paradigm. Cloud computing has significant points of interest contrasted with conventional computing models, for example, lessened CAPEX and OPEX [1], [67], and give dynamic and extensible virtualization assets [4]–[7], [13], [14], [52], [109]. SDN and cloud computing has developed fundamentally in both scholarly community and industry because of their basic attributes. While two innovations are creating numerous new open doors in both research and industry, security has been a significant concern for the development of the two technologies. As of late, security issues in SDN and cloud computing have attracted the attention of numerous researchers. Research works have shown that different security attacks can be directed against SDN and cloud computing through various network components. Security has been viewed as the predominant hindrance to the improvement of SDN and cloud computing [104]. It is also found that virtualization technology is commonly utilized in cloud computing to oblige the immense number of client requests. However, DDoS

The associate editor coordinating the review of this manuscript and approving it for publication was Arif Ur Rahman.

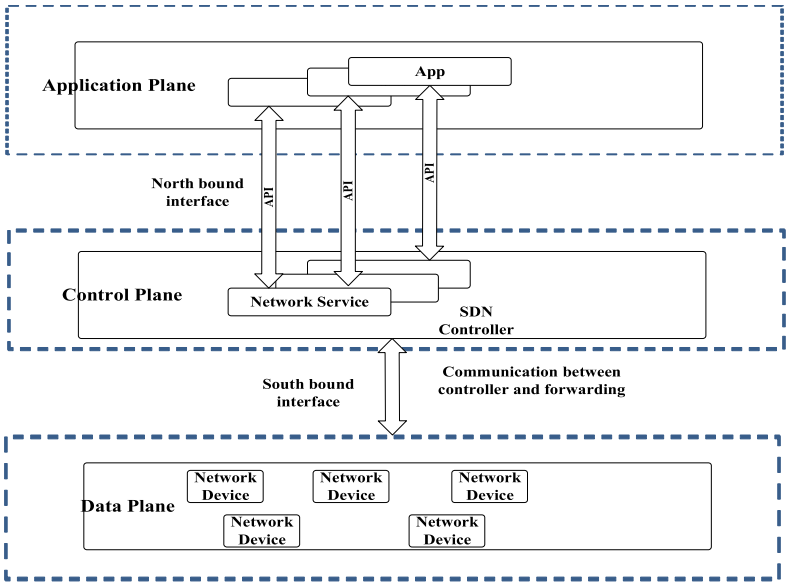

FIGURE 1. SDN architecture.

attack is a significant risk for the virtualized environment and accessibility of the assets [53], [94], [104].

In this paper, we conducted a broad survey on DDoS attacks in SDN and cloud computing environments. We think about the DDoS attacks in the scenario of SDN and cloud computing as far as their belongings and examine the new patterns and attributes of DDoS attacks in SDN and distributed computing. We at that point give a far-reaching review on defense mechanism against such attacks. Rest of the paper is organized as pursues- section 2 gives an introduction to SDN and cloud computing advances. Also, section 2 outlines the order of DDoS attacks. In section 3, we talk about the new patterns in DDoS attacks in SDN. In section 4 we overview the distinctive works done in the field of DDoS attacks from a cloud computing point of view. Section 5 talks about open issues which should be addressed to moderate the DDoS attacks. Section 6 depicts test condition in SDN and distributed computing situations for DDoS attack reproductions. At last, we concluded the paper in Section 7.

II. SOFTWARE-DEFINED NETWORKS, CLOUD COMPUTING, AND DDoS ATTACKS: A PRIMER

A. SOFTWARE DEFINED NETWORKS (SDN)

SDN is as of now drawing into consideration in both, scholarly world and also industry, which provides centralized, decoupled and programmable network switching mechanisms. Customary networking devices opt how an incoming packet ought to be dealt with dependent on its IP destination address, while SDN pursues a flow-based forwarding scheme where numerous header fields choose how the approaching bundle ought to be taken care of. SDN adopts the idea of centralized network control plane and introduces programmability, which can streamline network management and enables run-time organization of security strategies. In this way, SDN can rapidly react to network anomalies and malicious traffic. To all the more likely comprehend the SDN architecture, the three primary functional layers or SDN planes are exhibited in Figure. 1 and talked about beneath.

- Application Plane: It is the highest layer of the SDN design. It establishes different SDN applications including different functionalities, for example, policy execution, network management, and security services. The northbound interface is utilized as an interface between the application plane and control plane.
- Control Plane: It is a logically unified control structure and has a global perspective of the network. Control plane deals with the SDN switch through the commands and provides hardware abstractions to SDN applications. The control plane functionalities incorporate the system configuration, management, and exchange of routing table information. By decoupling the control plane from the network hardware and running it as software rather, the controller encourages automated network management and programmability of the systems [105].
- Data Plane: Data plane is in charge of sending the traffic flows dependent on flow rules modified by the control plane. Some network devices, such as switches lie in the data plane. Here, a switch is just utilized for packet forwarding and coordinate in fast packet matching. The southbound interface is an interface between the control between the control plane and data plane.

B. CLOUD COMPUTING

Cloud computing is a developing field that helps the IT infrastructure, network services, and applications. Formally cloud computing can be defined as ‘‘a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly

TABLE 1. Type of cloud computing.

Cloud type	ownership	Services
Private Cloud	Owned by one organization	Offered to internal users
Public Cloud	Owned by one organization	Offered to the general public
Hybrid Cloud	Owned by private organization or specific community and/or cloud service provider	Offered to the general public and internal users or/and specific community

provisioned and released with minimal management effort or service provider interaction'' [114]. Clouds can be partitioned into three noteworthy sorts, which are: public cloud, private cloud, and hybrid cloud, as appeared in Table 1. Private cloud will be cloud framework which is worked for a single client alone and in this manner gives the best command over information, security, and nature of service. The private cloud can be deployed either in big business server farms or in a colocation office and is claimed or rented by a single organization. Public cloud is an infrastructure which is possessed by an organization giving cloud services. Cloud computing services are commonly sold to common users or organizations. Hybrid cloud is a framework which is made out of at least two cloud platforms (private, Hybrid, or public), and each cloud stays independent. However, standard or restrictive technologies join them with information and application portability which can be utilized to deal with the unexpected load.

While public and a private association utilize public cloud and private cloud, respectively, the hybrid cloud is a combination of public and private cloud infrastructure. Subsequently, the hybrid cloud keeps the properties of both public and private cloud. Hybrid cloud enables organizations to keep their basic applications and information in private while outsourcing others to the public. Henceforth, we center around breaking down the effect of hybrid cloud on DDoS attack guard.

Cloud computing framework can be partitioned into two areas: the front end and the back end [45]. They both are associated with one another through a network, for the most part, the web. The front end is the thing that the customer (client) sees while the back end is computing resources such as services, storage, etc. The front end is commonly the user's PC and the application required to get to the cloud, and the back has the cloud computing administrations like different PCs, servers, and information storage. A central server manages user's requests, client demands and watching the network performance. It pursues certain guidelines, i.e., conventions and utilizations exceptional programming called the middleware [45]. Middleware permits organized PCs to speak with one another. Figure 2 demonstrates the diverse layers of cloud computing design [6]. Cloud application layer provides the service as ''software as a service (SaaS)'' through the Internet. Clients don't have to install the application to their local terminals [57]. Likewise, the SaaS model enables clients to access these applications through Internet-based remote access and industrially accessible from network management software [75]. SaaS is the most widely utilized services by Google applications. Another service offered by the cloud,

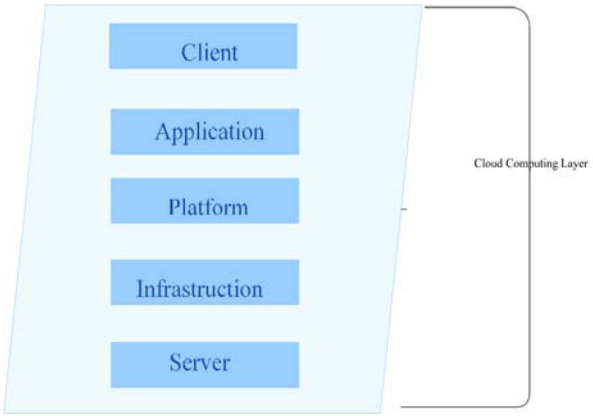

FIGURE 2. Cloud computing infrastructure.

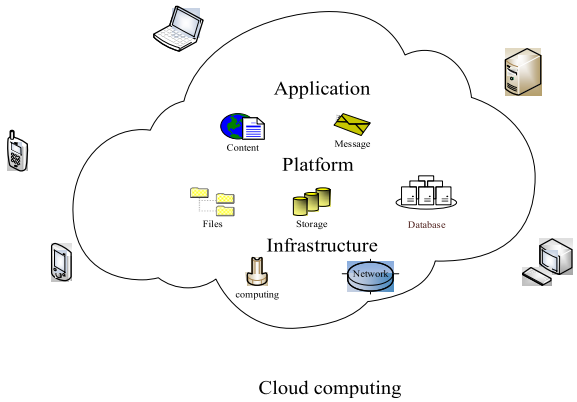

FIGURE 3. Cloud computing architecture.

is referred to as ''Platform as a service (PaaS)''. PaaS is a cloud computing model that provides a platform, which can be utilized for real application development by the end users, over the Internet. It liberates clients from installing in-house hardware and software to create or run new applications. Clients can get the opportunity to keep all the system and software lifecycle condition required by the service engineer, regardless of whether it is creating, testing, deploying and hosting Web applications.

For example, GAE, Microsoft's Azure are the real models giving PaaS benefit [75]. The following service offered by the cloud is called ''Infrastructure as a Service (IaaS)'' which gives the required framework as a service. The customers need not to buy the required servers, data centers or the network resources. Additionally, the key preferred standpoint here is that users need to pay just for the time duration they utilize the service. Subsequently, clients can accomplish

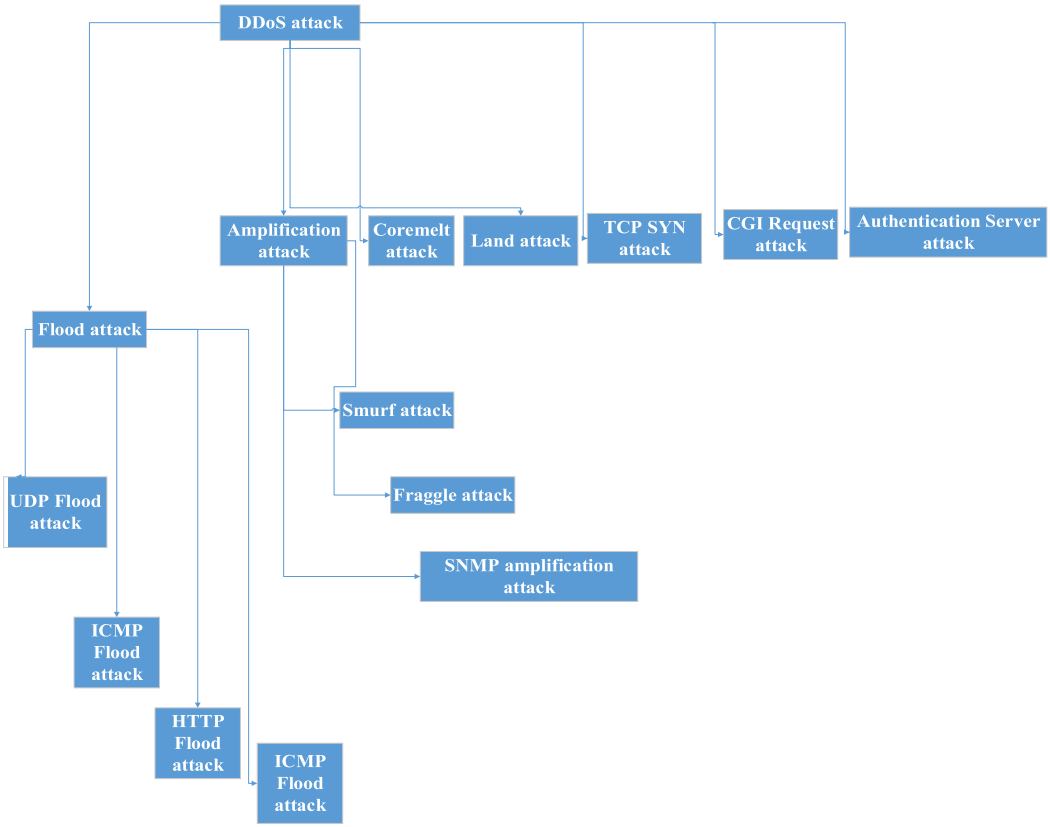

FIGURE 4. Classification of DDoS attack.

a lot quicker services conveyance at less expense. GoGrid, Flexiscale, Layered Technologies, and Rackspace are typical examples of IaaS administrations [75]. In Figure.3 we present the typical cloud architecture which includes three parts, that is, Application, Platform, and Infrastructure.

C. DDOS ATTACKS

In this segment, we present the state-of-the-art for DDoS attacks and its category. In the general terms, DDoS attack is an attack which is targeted by multiple compromised computers called as bots or zombies focusing on a single system. Its motivation is to make the objective system or network resource depletion, with the goal that the service is incidentally hindered or stopped, leading to service unavailability. DDoS attack is separated into seven noteworthy classes which are: flood attack, amplification attack, coremelt attack, land attack, TCP SYN attack, CGI request attack, and authentication server attack also depicted in Figure.4. Classification of DDoS attack and conceivable countermeasures are talked about in detail in [86]. Beneath we quickly examine these subkinds of the DDoS attack.

Flood attack: A flood attack sends an expansive number of traffic to an objective system through zombies. In this way, the objective framework's network data transfer usage is significantly expanded with IP traffic. UDP, ICMP, HTTP, and SIP packets may likewise run the flood attack, bringing about UDP flood, ICMP flood, HTTP surge, and SIP surge attacks. The injured individual is attacked by sending UDP (User Datagram Protocol) bundles persistently to an explicit or arbitrary port.

ICMP flood attack: In this substantial number of ICMP requests for packets are sent to the person of the subject. When the sent bundles surpass 65535 bytes, the host computer of the victim stops working.

HTTP Flood: The web server is overwhelmed with HTTP requests. It is a volumetric attack, and it is different from spoofing techniques.

SIP flood attack: Voice over IP (VoIP) utilizes SIP for call signaling when it is used for communication. SIP telephone can be effectively overflowed with messages, so it is unable to serve authentic requests.

Amplification attack: This attack is controlled by an attacker or the zombies by sending messages using a broadcast IP address, which compels all nodes in the subnet network to send an answer to the victim user's system. Amplification attack is additionally partitioned into Smurf attack, Fraggle attack, and SNMP enhancement attack.

Smurf attack: Reflection or amplification attack is focused against switches and servers where the ICMP packets are redirected to these amplifiers with a duplicate source IP address. The duplicate address will be used as victim user's host IP address. UDP and ICMP flood attack sources can be adequately recognized. Anyway it is difficult to pursue the Smurf attack.

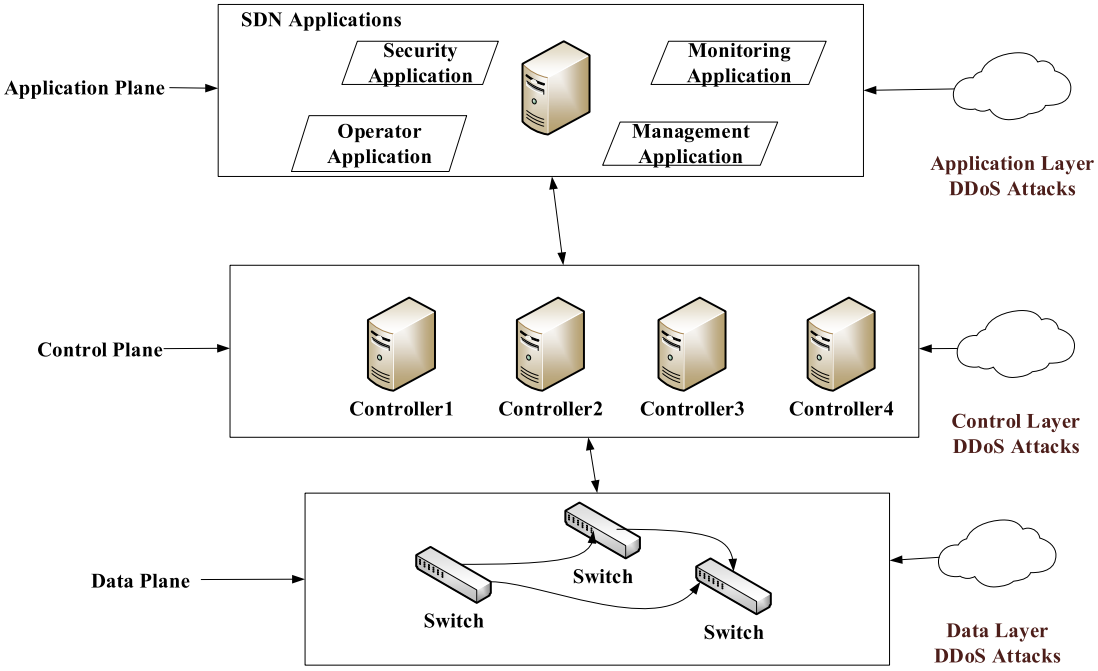

FIGURE 5. The DDoS attack in SDN.

Fraggle attack: This attack is like Smurf attack, yet utilizes UDP packet rather than ICMP packet. Here additionally the victim individual client's IP address is utilized as a spoofed source IP address in the malicious data packet.

SNMP amplification attack: SNMP (Simple Network Management Protocol) is utilized to monitor the devices in the network, for example, routers, printers and firewalls and so on. SNMP retrieves configuration information in the network using default communication channel. To achieve this SNMP sends bulk requests to retrieve information. Attackers send this request using spoofed source IP address. In this way, the victim computer flooded with responses.

Coremelt attack: In a Coremelt attack, the attacker utilizes an accumulation of subverted machines sending information to one another to surge and disable network link. With subverted machines sending information to one another, an attacker can escape capacity and filtering based DoS defenses since the receiver requests all traffic. At the point when the subverted machines are scattered over multiple networks, the attacker has a more prominent possibility of closing down a backbone link, without devastating minimal tributary connections [89], [116].

Land attack: A LAND (Local Area Network Denial) attack is a DoS (Denial of Service) attack that comprises of sending an expansive quantity of mocked poisoned packet to a targeted computer, making it cease its functioning. Expansive quantities of parcels are sent to a similar host and goal IP address and port number that crashes the framework.

TCP SYN attack: In this attack, an attacker uses the correspondence protocol of the Internet, TCP/IP, to overwhelm the target computer with SYN requests. The server answers to the demand by sending SYN + ACK bundle and waits for the ACK packet from the client. However, if the aggressor doesn't send ACK packet deliberately, the server waits for the ACK for an inconclusive measure of time. Support line of the server turns out to be full and CPU time and memory are depleted. Finally, incoming legitimate requests are likewise rejected.

CGI Request attack: The attacker sends an ample amount of CGI requests that consume CPU cycles of the victim computer, and in consequence, the victim computer ceases to take requests.

Authentication Server attack: The confirmation server checks the fake signature sent by the attacker which expends a larger number of computing resources than generating the signature.

III. DDOS ATTACKS AND DETECTION IN SOFTWARE DEFINED NETWORKS

In the section, we review the basics of DDoS attacks and DDoS detection scheme in SDN paradigm. SDN is as a novel networking architecture which might be an objective of DDoS attacks. SDN is categorized into three fundamental functional planes, which are: application plane, control plane and information plane as appeared in Figure 1. Potential DDoS attacks can be executed in these three planes of SDN architecture. Based on the possible targets, the DDoS attacks also are divided into three categories in SDN which are application-layer DDoS attacks, control layer DDoS attacks, and data layer DDoS attacks as shown in Figure 5. Some work has just been done in the research community for DDoS attack detection and ID in SDN. VizvÃąry and Vykopal [98] investigate SDN with OpenFlow convention from DDoS. Rt *et al.* [47] break down the SVM classifier and contrast

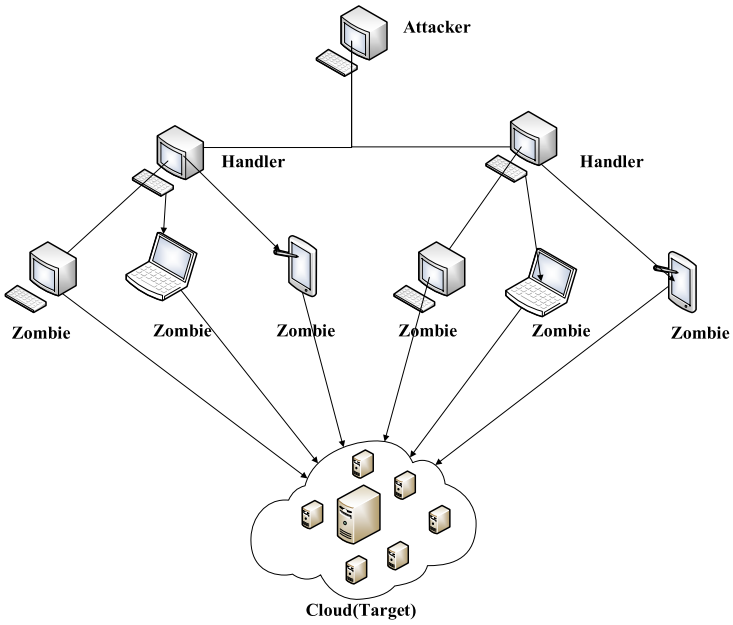

FIGURE 6. DDoS attack in cloud.

it and different classifiers for DDoS identification in SDN condition. Furthermore, DDoS attack detection mechanism and methods [22], [59] have been broadly proposed in the traditional networks, e.g., [29] and [30]. Such strategies can be received in SDN as proposed in [58]. We talk about the three classes for DDoS attack in SDN as follows.

A. APPLICATION LAYER DDoS ATTACKS

There are two different ways to implement the application layer DDoS attacks. One is the attacks focusing on some SDN applications; the other is the attack focusing on SDN northbound API. Since the separation of applications is hard to acknowledge [49], an application layer DDoS attack may influence another application which is not the objectives. Such compromised applications may cause genuine security breaches in SDN. Braga *et al.* [11] propose a self-organizing map (SOM) strategy [73] to distinguish DDoS based attacks utilizing machine learning techniques. In this strategy, the SOM model is trained by gathering factual information from OpenFlow switches. SOM training features are average packets per flow, normal bytes per stream, average duration per flow, the percentage of bidirectional flows, growth of single flow, and growth of single ports.

B. CONTROL LAYER DDoS ATTACKS

Control layer is center of SDN and furthermore the weakest connection in the entire SDN security because of a single point of failure. Control plane DDoS attacks might be controlled by three strategies which are attacking controller, attacking northbound APIs and attacking southbound APIs. Distinctive applications can make many clashing flow rules which may cause DDoS attacks in the control layer. Since controller makes decisions to forward the flows according to flow rules, when the network device finds a new network packet in the data plane, and there are no flow rules to match the existing flow information in the flow table for new packets. Either the complete packet or part of the packet header is sent to the controller, in order to resolve the query [78]. With a huge volume of network traffic, sending a total packet to the controller may expend high-data bandwidth [78]. Mousavi and St-Hilaire [62] propose to utilize the centralized control of SDN for DDoS attacks discovery and presents a solution that is successful and lightweight as far as the assets required. Dao *et al.* [18] introduce an achievable technique to secure the system against DDoS attacks all the more effective — Gde Dharma *et al.* [25] present the potential vulnerabilities in SDN controller that can be exploited for DDoS attack. Lee and Choi [31] and Lee and Choi [31] acquaint incorporated centralized monitoring Snort with identifying DDoS attacks.

C. DATA LAYER DDoS ATTACKS

Data plane should not be allowed to any pernicious applications which can install, change or adjust stream rules as the DDoS attack is launched when the routers are attacked, and southbound API is attacked. Shin *et al.* [82] propose that a if we add some minimal insight into the data plane device then some of the problems can be alleviated. Researchers in proposed in [81] to show the plausibility of DDoS attacks, another SDN arrange checking model device (named SDN scanner) to remotely fingerprint networks that convey SDN. This strategy can be effortlessly worked by modifying existing network examining instruments (e.g., ICMP checking and TCP SYN filtering). The attack can be led on the SDN network by a remote attacker, and it can fundamentally corrupt the execution of a SDN arrange without requiring superior or high capacity devices.

TABLE 2. DDOS attacks in SDN.

SDN Layer	Reference	Description
Application plane	Braga et al.[11]	this paper utilizes Self-Organizing Maps (SOM) [73] based on machine learning methods for DDoS identification
Control plane	Mousavi et al.[62]	the paper proposes to utilize the centralized control of SDN for attack discovery and presents a working solution that is viable and lightweight concerning the assets that it exploits.
	Dao et al.[18]	the paper acquaints a plausible strategy for ensuring the protection of network against Distributed Denial of Service attacks all the more successfully.
	Kandoi et al.[43]	the paper talks about DDoS attack on the control plane bandwidth.
Data plane	Shin et al.[82]	this research recommends that a portion of these issues could be settled by adding some minor insight into the data plane devices.
	Paper[72]	the paper shows that OF applications may compete/contradict, override one another, incorporate vulnerabilities or chances to be written by attackers.
	wang et al.[101]	This research proposes an entropy-based lightweight DDoS flooding attack recognition method which runs in the OF edge switch.
	Kandoi et al.[43]	This research discusses the router's stream table attack.

It is demonstrated that a DDoS attack can overpower the controller in SDN architecture [61]. One genuine situation of DDoS attack that can specifically influence the controller is overwhelming the controller with packets. Any new packet that does not have a match in the stream table will be sent to the controller for processing. Most DDoS attacks utilize spoofed source address, which switches into new incoming packets. For the centralized and separated control, this is considered as beneficial for SDN management, while it is a noteworthy disadvantage when the quantity of new approaching packet is bigger than that the secure channel bandwidth and processing power of controller. In a DDoS attack, an extensive number of parcels are sent to the host groups in the network. In the event that incoming packet's source address is produced, the switch, for the most part, can't discover a match, and information parcel is sent to the controller. Genuine packets and DDoS forged packets both combined may exhaust the resource of the controller. This keeps the controller from handling the recently arrived data packets and can prompt loss of information including reinforcement controller, which faces a similar test [61]. Writers in [72] bring up that OpenFlow applications may compete/conflict, covering one another, including the vulnerability or probability changed and written by rivals. In the most pessimistic scenario, the attacker can utilize deterministic OpenFlow applications to control the province of OpenFlow switch at the point when OpenFlow rules empower or cripple the system traffic prohibited(or permitted) contrarily through existing rules, then a conflict of standards increases. Programmers can exploit the standards struggle to run DDoS attacks — Wang *et al.* [101] propose an entropy-based lightweight DDoS flooding attack recognition demonstrate running in the OpenFlow edge switch. This accomplishes a disseminated inconsistency identification in SDN and decreases the stream gathering over-burden of the controller. Besides, Kandoi and Antikainen [43] talk about two kinds of Denial-of-Service (DoS) attacks explicit to OpenFlow SDN systems. The first sort is attacking the control plane bandwidth, and the second kind is attacking the switch flow table. Diverse DDoS attacks technique in SDN can appear in Table 2.

IV. DDoS ATTACKS AND DETECTION IN CLOUD COMPUTING

Handling DDoS attacks in cloud computing has been a challenge in the network security field, particularly with the appearances of SDN and cloud computing perspective. Because of the tremendous measure of information stored over clouds, cloud computing is susceptible to DDoS attacks. In the time of cloud computing and huge information, the measure of information is developing quickly [114]. The current safety efforts cannot meet the security requirements of distributed computing. Gartner predicts the application-layer DDoS attacks to grow three times each year in the distributed computing situations. According to the forecasting, DDoS attacks will represent 25% of the majority of the application-layer attacks. Customary defense components confront numerous difficulties in identifying DDoS attacks in cloud computing context. An ongoing Cloud Security Alliance (CSA) study demonstrates that DDoS attacks are basic dangers to cloud security [94], [74]. Distinctive scientist works, for example, works introduced in [7]–[9], [15], [48], [54], [56], [76], [80], and [96], are concentrating on making an increasingly differing stage to counter the DDoS attacks. In spite of the expanding research to recognize and anticipate DDoS attacks, the security breaks have additionally been expanding at a disturbing rate, both in the undertakings and distributed computing environments. In this segment, we talk about the explanations for the development of DDoS attacks in cloud computing conditions. We survey the fundamental qualities of cloud computing, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Besides,

we survey the DDoS attacks and discovery plots in cloud computing.

A. BOTNETS OUTBREAK

Botnet comprises an enormous number of PCs linked over the Internet and communicating with one other, known as zombies. They are not people just commanded program or robots. The master arranges the activities of zombies by passing messages or directions. Vast scale botnets (e.g. Srizbi, Kraken/Bobax, and Rustock) have been intended to perform pernicious tasks, for example, performing DDoS attacks [84]. It can taint countless in a brief time frame in the customary systems. Likewise, distributed computing condition gives computational forces to make ground-breaking botnets [50]. With the progress in the cloud computing, Malware-as-a-benefit is broadly utilized for spamming and propelling for swearing of-benefit attacks. To different rival providers, costs of malware-as-a-benefit are getting lower than previously. Today, one can purchase a 10000-PC botnet for $1,000 [90]. So with the botnets, DDoS attacks are likewise getting progressed and winding up increasingly visit in the distributed computing situations.

B. BROAD NETWORK ACCESS

Nowadays, attackers use botnets and other advanced programs to attack their victim's network structure, which may cause DDoS attacks. The quantity of DDoS attack is expanding each year. Spamhaus, an association that keeps up arrangements of spammers, went under an extensive DNS testing on DDoS attack in March 2013. Researchers reported [5] that attack volume was supposedly as high as 300 Gbps. At the same time, mobile terminal devices, for example, cell phones and tablets, have turned into a stage to dispatch DDoS attacks in a distributed computing context. Researcher in [60] brings up that Android malware could be utilized to run DDoS attacks. It is anything but difficult to make an attack for pernicious attackers, which requires nominal abilities. Since clients from the cell phone may join a DDoS attack network, therefore such attacks may spread quickly in the following couple of years. DDoS attacks are winding up increasingly visit, as well as being effective in recognizing explicit applications to attack (for instance, DNS, HTTP or VoIP) [12]. Sophisticated low-bandwidth capacity DDoS attacks utilize less traffic, and increment its viability against a weak point in the victim's system. In spite of the fact that this requires all the more comprehension of the complex attack frameworks, contrasted with high bandwidth capacity attack, low-transfer speed DDoS attacks have three points of interest: 1) bring down expense - as it utilizes less traffic; 2) little space - so it is hard to distinguish; 3) can harm by the flow control system protection [10].

C. RESOURCE POOLING

Cloud computing architecture gives processing resources including hardware and programming utilizing a multi-occupant model for various users. Diverse physical and virtual resources are designated randomly and reallocated according to users request [28]. Anyway, cloud computing likewise helps the attacker by giving dispersed processing situations. Virtualization innovation may likewise help aggressor by showing some attacking techniques and recreating the genuine attacks. In the cloud computing context, attackers may exploit virtualization technology to set up an association with at least one gathering focuses [88]. For this reason, a virtual machine (VM) will be enhanced to utilize very memory or disk space. Thus, an attacker can streamline costs and even launch more virtual machines [88]. In a DoS attack, the efficiency of the Web server running on a virtual machine may reduce by 23%, while the execution of a non-virtualized has with similar equipment may diminish by 8% just [79]. The reason is that cloud computing infrastructure is a multi-tenant framework, where the attack on a single inhabitant can without much of a stretch be disseminated to all other tenants. The tenants share public network architecture, as well as the computational resources such as memory and storage space [2]. At the point when DDoS attack happens, a virtual machine can involve all accessible physical resources [95] starving another tenant. Even though the manager alots restricted physical assets for each VM, side diverts have been utilized in ongoing attack to bypass the virtual machine isolation [27].

1) NEW SERVICE MODEL

Cloud Service Providers (CSPs) charge expenses to their users dependent on server and system resources on pay-per-use premise. This model empowers the customary DDoS attacks to advance to another type of attacks focusing on monetary assets of the CSPs, called Economic Denial of Sustainability attack(EDOS) [87], [97]. EDOS attack is a kind of deceitful asset utilization (FRC) attacks. It is unique in relation to application-layer DDoS attacks which are developed for the utilization of resources and focus on the accessibility as transient objectives. While FRC does not attempt to attack by long-term financial feasibility of open cloud estimating over expanded times of time, web content hosted under a CSP's utility model empowers an attacker to play out a FRC attack by essentially making protocol consistent requests [40]. The attacker utilizes a huge measure of network resources (through botnets) to attack the victim users undertaking false charges. In cloud computing, a focus of FRC attack is the exploited user (i.e., periodic Cloud Client) from users for their long hosted web items which is openly available.

In other words, the attacker, who is served as a legal cloud customer, ceaselessly sends requests to devour transmission capacity from the web server facilitating cloud, which is hard to distinguish authentic traffic [104]. Numerous DDoS attacks are completed in this manner. DDoS can be led by utilizing traded off vulnerable nodes on the internet(also known as zombie computers) [65]. The DDoS attack architecture is shown in Figure 6.

Ficco and Rak [23] has proposed a system to organize stealthy attack designs, which display a gradually expanding

force drift intended to deliver the greatest monetary expense to the cloud user, while regarding the activity measure and the administration entry rate forced by the recognition mechanisms. The low rate DDoS attack influences the evaluating model of cloud by sidestepping early identification. Gupta and Kumar [30] give another heading in which a similar dimension of security capacities for the system can be gotten with insignificant costs of assets which is the prime necessity for any plan for being pertinent in a cloud computing environment. It is a lightweight attack design discovery plot dependent on VM profile enhancement and is an entire plan for principle-based DDoS arrange interruption location in Clouds. Ficco and Palmieri [1] propose a DDoS attack discovery framework in an adaptable and powerful way, which can work over different system limits. Choi *et al.* [17] propose a strategy for the combination between HTTP GET flooding among DDoS attacks and MapReduce handling for a quick attack discovery in distributed computing scenario. This strategy guarantees the accessibility of the objective framework for precise and solid discovery dependent on HTTP GET flooding. Palmieri *et al.* [69] contend that the DDoS attack will cause electrical blackouts because of intensity spending weariness. Palmieri *et al.* [68] present another age of eDoS attacks described by increasingly unpretentious and less obvious conduct, yet whose potential ought not to be thought little of. Such threats, mainly relying on application-benefit level defects may remotely influence the cloud resource utilization of expansive scale cloud server farm frameworks by presenting important financial harms without influencing the general system network and the accessibility of the administrations offered by the people in question. Deshmukh and Devadkar [19] provide a short overview on DDoS attacks, at that point scientific classification of attacks, its sorts and different countermeasures to relieve the DDoS attacks. This review gives DDoS detection, prevention, and tolerance techniques. The paper closes by giving a few points to be considered while choosing DDoS protection systems to be actualized. Diverse DDoS attacks and recognition technique under distributed computing condition can be found in Table 3 and Table 4. Wahab *et al.* [123] propose a trust-based maximin game between DDoS attackers trying to minimize the cloud system's detection and hypervisor trying to maximize this minimization under limited budget of resources. Vetha and Devi [124] proposes a new solution that allows the hypervisor to establish trust - based relationships towards the guest Virtual Machines (VMs).

V. OPEN PROBLEMS

Notwithstanding the bounteous research on DDoS attacks in the SDN and cloud computing environments, there are as yet many research issues which are not very much examined and request future work from the examination network. Relieving DDoS attacks in conventional systems has been examined for quite a while. Works displayed in [71] and [113] have included the majority of these work, while we need to readdress the issue from SDN and cloud computing context because of their extraordinary architecture. In this section, we examine probably the most critical issues which should be routed to discussed to mitigate DDoS attacks in SDN and cloud computing scenarios.

A. MITIGATING DDoS ATTACK IN SDN

Naous *et al.* [64] first proposed a novel NetFPGA stage architecture based on an OpenFlow Switch to mitigate DDoS attacks. The architecture has shown a decent execution with stream processing and insertion rate. The proposed model catches the packets, which contain the substance name, extracts the asked for substance from the parcel fields, and afterward, it associates them. Finally, DDoS attacks flows are obstructed by confining the arriving rate of requests. Application-level DDoS flooding attacks are another critical DDoS attacks, which for the most part expend less data transmission than volumetric attacks. They are fundamentally the same as considerate traffic [113]. Notwithstanding, application-level DDoS flooding attacks ordinarily have a similar effect to the administrations since they make utilization of explicit qualities and conventions of uses, for example, HTTP, DNS, or SIP [113]. As per the examination by Gartner, there will be a striking increment in the application-level DDoS attacks [3]. Henceforth, it is pivotal to get to the payload data for application-level DDoS attacks alleviation. Also, this data should be acquired at significantly decreased latencies so as to react immediately. Be that as it may, neither controller nor Switches have L4-7 application awareness. SDN models, by design, provide the permeability and control which is just required to execute security at the lower layer stacks of the network [77]. For instance, in its present form, OpenFlow generally handles layer 2/3 arrange traffic data, and the whole bundle might be sent to the controller just in some exceptional cases (on account of non-accessibility of the cushions in the switch or the principal parcel of a given obscure flow) [41]. In this way, applications that need get to and to control information packets payload can't profit by the current OpenFlow implementation as both profound packet examination, and forceful surveying of the information plane can quickly cause debasement of the performance [41].

At the point when SDN is connected to layer 4-7 networking, it needs to defy critical challenges, since these layers suit a various arrangement of profoundly specialized applications that are hard to consolidate and centralize. In addition, a particular device is frequently required to superior output performance for layer 4-7 services [39]. SDN can offer progressively adaptable, simple to-oversee and more affordable programming based usefulness contrasted with conventional layer 4-7 apparatuses. Applications at these layers need to enhance the usefulness by incorporating with SDN technologies [39] for the ideal execution. L4-7 metadata and DPI motor can furnish controller and its applications with metadata and App IDs to settle on more astute choices [24]. Execution and security have likewise turned into the real research targets, and critical endeavors are required to create arrangements with great harmony among execution

TABLE 3. DDOS attacks in cloud computing environment.

Type	Category	Description
Reason of DDoS attack in the cloud computing environment		
Botnets Outbreak	Silva et al.[84]	Large-scale automated programs such as Srizbi, Kraken/Bobax, and Rustock are considered well known botnets for malicious attacks [84].
	Kutylowski et al.[50]	On-demand self-service capacities of cloud that let real organizations rapidly include or remove could be utilized to make an incredible botnet [50] in a split seconds.
Broad Network Access	Brief et al.[12]	For stealthy attacks pinpoint specific applications are being used such as DNS, HTTP or VOIP etc [12].
	Ben-Porat et al.[10]	Ability to attack the systems that are protected by flow control mechanisms [10].
Resource Pooling	Goel et al.[28]	In cloud computing the cloud server's computing resources are combined to full fill high demand of many users using multi-tenant model with different physical and virtual resources dynamically [28].
	Shea et al.[79]	Researchers in [79] found that if non-virtualized server are used for cloud service hosting on the same hardware then its performance degrades by 8%.
	Tsai et al.[95]	Researchers in [95] found a kind of attack in which one VM occupies all the available physical resources so that the server machine cannot support more VMs, and availability is denied.
	Godfrey et al.[27]	To bypass virtual machine isolation side channels have been used in cloud attacks [27].
New Service Model	Sqalli et al. [87], VivinSandar et al.[97]	Researchers [87, 97] discussed about Economic Denial of Sustainability attack (EDoS) on the server and network resources which targets on financial assets of the supplier of cloud service provider .
	Idziorek et al.[40]	A FRC attack is a significantly increasing that tries to disturb the long-term monetary feasibility of operating in the cloud by utilizing the utility pricing model over an long duration [40].
	Wahab OA et al.[123]	A trust-based maximin game between DDoS attackers is designed trying to minimize the cloud system's detection
	Vetha S et al.[124]	A new solution is proposed that allows the hypervisor to establish trust - based relationships towards the guest Virtual Machines (VMs).

and security. Klöti *et al.* [46] propose to utilize STRIDE [37] and information streamgraphs to relieve the security issues in OpenFlow systems. Wang *et al.* [99] introduce an adaptable, effective and lightweight system (OF-GUARD) for SDN networks, which can keep immersion attack from information plane to control plane by utilizing packet relocation and information storing.

Hong *et al.* [38] propose two SDN-explicit attack vectors including Host Location Hijacking Attack and Link Fabrication Attack, which truly challenge the center preferred standpoint of SDN, broad visibility, and present another security threats to the OpenFlow controllers(TopoGuard). It gives programmed and continuous identification of Network Topology Poisoning Attacks and mitigates the DDoS attacks between the control plane and data plane. Wang *et al.* [102] propose another DDoS anticipation show dependent on [38], called as FloodGuard, which contains two new strategies: packet movement and proactive stream rule analyzer. So as to guarantee to organize strategy usage, proactive stream rule analyzer progressively creates proactive stream rules as indicated by the runtime rationale of the SDN controller and its applications. To avoid over-burden to the controller, packet movement strategy can briefly reserve the flooding packets which are sent to the OpenFlow controller utilizing round-robin and rate limit planning. Mowla *et al.* [63] propose a multi-protection component to moderate DDoS attack in interconnected CDNs which are additionally checked and controlled through ALTO server and SDN controller. The method would alleviate the impact of the DDoS attack on the weak point and trace back to the bots utilized by the attacker to run the attack however the personality of the first attack may, in any case, stay hidden. Saif Saad Mohammed *et al.* [117] create a model for DDoS detection in SDN using NSL-KDD dataset and train the model. Results show the proposed the model can improve the performance and accuracy for DDoS detection. Kalkan *et al.* [118] give out the survey about several methods against DDoS attacks in SDN. After that, he proposed a hybrid mechanism, namely SDNScore [119] and a joint entropy-based security scheme (JESS) [120] to enhance the SDN security with the aim of a reinforced SDN architecture against DDoS.

B. MITIGATING DDoS ATTACK IN CLOUD COMPUTING

Work introduced in [100] proposes an exceedingly incorporated programmable network observing, monitoring the location and adaptable control structure that permits quick

TABLE 4. DDOS attack and detection.

DDoS attack and Detection	Ficco et al.[23]	A procedure to arrange stealthy attack designs, which show a slowly– expanding intensity trend. The pattern is intended to cause the most extreme money related expense to the cloud client while regarding the job size measure and the service arrival rate imposed by the recognition method. The low rate DDoS attack influences the pricing model of the cloud by avoiding early detection[23].
	Gupta et al.[30]	Another bearing in which a similar dimension of security abilities for the system can be acquired with negligible cost of resources which is the prime necessity for any plan for being relevant in cloud environment[30].
	Ficco et al. [1]	A DDoS attack in a scalable and robust way, a completely distributed command and control design, which can work over numerous network limits, is required in distributed computing infrastructure.
	Choi et al.[17]	A technique for coordination between HTTP GET flooding among DDoS attacks and MapReduce preparing for a quick attack identification in the cloud computing condition. This technique ensures the accessibility of the objective framework for exact and dependable discovery dependent on HTTP GET flooding.
	Palmieri et al.[69]	The DDoS attack is additionally causing electrical blackouts because of power budget depletion.
	Palmieri et al. [68]	Another age of eDoS attack portrayed by a progressively unobtrusive and less obvious conduct.
	Rashmi V et al.[19]	A concise study on DDoS attack is given, at that point scientific categorization of attack, its sorts and different countermeasures to alleviate the DDoS attacks[19].

information gathering and explicit attack reaction in cloud computing situations. It develops an attack recognition framework based on the graphical model, which can deal with the change issues in DDoS alleviating framework. Creators in [55] propose another way to deal with alleviate DDoS attack utilizing an intelligent fast-flux swarm network that adjusts the Intelligent Water Drop calculation for conveyed and parallel improvement. The quick motion system can keep availability among swarm nodes, clients and servers. Fast-flux service networks also enable us to conveniently build a transparent service and keep minimal modifications for existing cloud services. Researchers in [107] proposes a channel strategy named Cloud-channel to alleviate DDoS attack in cloud computing condition. The strategy is utilized to detect the source of DDoS attack in cloud computing. Tests demonstrate the defense framework which is a blend of SOA-Based Traceback Approach(SBTA) and Cloud-channel technique is found to be effective in Cloud Computing. Paper [20] proposes a technique called Confidence-Based Filtering, which decides if to dispose of a packet or not by computing the score of a specific bundle in the attack period. Yu *et al.* [110] propose a dynamic resource allocation methodology to alleviate DDoS attack for individual cloud users and set up a queuing theory model for the proposed procedure in a cloud domain. The primary thought is, when DDoS attack happens, the inert resources of the cloud are used to copy adequate interruption anticipation servers for the victim. Meanwhile, some attacking packets are immediately identified and QoS level of benign users are guaranteed all the while. Osanaiye *et al.* [65] propose a Host-Based Operating System that coordinates the working arrangement of the incoming packet from its database through both dynamic and inactive strategy. The proposed strategy can identify IP spoofing by verifying the genuine source of an approaching parcel amid DDoS attack in cloud computing condition. In addition, Osanaiye *et al.* [66] also examine existing research on DDoS attack and defense method in cloud computing and propose a reasonable cloud DDoS alleviation framework dependent on the change-point location. Pillutla and Arjunan [122] presents a Fuzzy self organizing maps-based DDoS mitigation (FSOMDM) technique that is ideally and suitably designed in cloud computing. Meanwhile, there are many research works [11], [26], [32], [34], [42], [58], [70], [71], [83], [91]–[93], [103], [106], [108], [111], [112], [121], [122] on moderating DDoS attack utilizing SDN. These techniques may give some assistance in future research on relieving DDos attack in cloud computing. Table 5 demonstrates the DDoS attacks relief in SDN and cloud computing lately.

VI. EXPERIMENTAL SETUP

In this section, we discuss tools to set up the experimental environment to perform the DDoS attacks in the simulated SDN and cloud computing environments. Tools for experimental setup for DDoS attack simulation in SDN and cloud computing environments are shown in Table 6.

A. EXPERIMENTAL ENVIRONMENT FOR SDN

Mininet [33], [51] has fundamentally lead the state-of-the-art for creating and testing new controller applications. Some scientists adopt Mininet as simulation devices for the laboratory test. Kandoiet al. have utilized Mininet to run their analyses. In Mininet, each arranges hub (switch, have, controller) keeps running as a lightweight virtual machine. The virtual machine keeps running in its own Linux portion namespace with the goal that it approaches just to the assets inside its namespace [43]. It has been widely accepted by the analysts, as it

TABLE 5. DDOS attacks mitigation in sdn and cloud computing.

Year	Reference	SDN	cloud computing
2008	J. Naou et al.(2008)[64]	√	
2011	R. Lua et al.(2011)[55]		√
2012	G. Finnie et al.(2012)[24]	√	
	L. Yang et al.(2012)[107]		√
2013	Gartner (2013)[3]	√	
	R. Kloti et al.(2013)[46]	√	
	W. Dou et al.(2013)[20]		√
2014	(2014)[77]	√	
	Y. Jarraya et al.(2014)[41]	√	
	(2014)[39]	√	
	H. Wang et al.(2014)[99]	√	
	S. Yu et al.(2014)[110]		√
	Mowla et al.(2014)[63]	√	
2015	B. Wang et al.(2015)[100]	√	
	O. A. Osanaiye et al.(2015)[65]		√
	Hong et al.(2015)[38]	√	
	Wang et al.(2015)[102]	√	
2016	O. Osanaiye et al.(2016)[66]		√
2017	Kalkan K et al.(2017)[118]	√	
	Wahab O A et al.(2017)[123]		√
	Kalkan K et al.(2017)[119]	√	
2018	Mohammed S S(2018)[117]	√	
	Kalkan K et al.(2018)[120]	√	
	Bhushan K et al.(2018)[121]		√
	Pillutla H et al.(2018)[122]		√

offers great authenticity and consistent change from development to deployment. Gupta et al. [29] portray a simulation-based method called fs-sdn that supplements and develops these existing methodologies. fs-sdn depends on the fs [85] recreation stage. Researchers in [47] receives DARPA interruption discovery situation explicit data-set given by MIT Lincoln lab to evaluation [36].

TABLE 6. DDOS attack simulation tools in SDN and cloud computing.

Category	Experiment Tools	Reference
DDoS attack in SDN	Mininet	[33,51]
	fs	[85]
	fs-sdn	[29]
DDoS attack in Cloud computing	C++	[16]
	contexts	[88]
	OMNeT++	[4]
	cloudsim	[44]

B. EXPERIMENTAL ENVIRONMENT FOR CLOUD COMPUTING

Simulation models exhibited in [16] are written in C++ and present the simulation conditions including the data source, the parameter selection for the model and diverse attack types. Paper [88] recovers the dataset from York University's Computer Science and Engineering (CSE) office and recreations are executed on a PC with Intel i7 processor and 8GB of RAM. The experiments were led utilizing the default Xen

4.2 hypervisor, where researchers have separated the reserve into 2, 4, 8, or 16 allotments. The experiments run on the IBM contexts [27]. Paper [44] utilizes Cloudsim and Eucalyptus as tools to finish the analysis. Paper [4] uses OMNeT++ to mimic a three-tier data server framework including racks holding servers associated with a best of rack (TOR) switch.

VII. CONCLUSIONS AND FUTURE RESEARCH

DDoS attacks are growing in SDN and cloud computing environments. In this paper, we initially talk about the design of SDN and cloud computing standards and further arrange the DDoS attacks. At that point, we outline DDoS attack situations and their recognition instruments in SDN and cloud computing conditions. In addition, since SDN might be a victim of DDoS attack, we survey the research work on introducing the DDoS attacks on SDN and how to solve this issue. We likewise talk about how to fabricate exploratory condition and use simulation instruments in SDN and cloud computing condition for DDoS attacks and identification.

At last, we investigate some open research problems in this direction, for example, how to alleviate DDoS attacks in SDN and cloud computing environment. In spite of bottomless research in this field, there are still some problems to be solved. That should be addressed in future research. We propose some future research as pursues:

A. DDoS ATTACK IN SDN

Albeit unified control is the real preferred advantage of SDN, it is additionally a solitary cause of failure also if it is targeted by Distributed Denial of Service(DDoS) attack. With the expansion in the DDoS attacks, traditional anomaly detection strategies face numerous troubles in alleviating the DDoS attacks. Hence, big information examination and location advancements for DDoS attacks is a noteworthy region of research in SDN. SDN and NFV(Network Function Virtualization) are mutually useful, yet are not subject to each other. SDN is an empowering influence for NFV. SDN contributes towards network automation that empowers approach based choices to coordinate system traffic flows, which is an engaging platform for network virtualization since control logic runs on a controller instead of on physical switches [21]. We forecast some DDoS attacks that will be propelled utilizing virtualization innovation later on. Hence, how to identify and alleviate DDoS attacks in virtualized SDN arrange is a critical research problem.

B. DDoS ATTACK IN CLOUD COMPUTING

Since application level and framework level DDoS attack can target distinctive cloud components, more investigation about DDoS attack is required to address this issue in cloud environments. Some marked dataset ought to be worked with optimal feature selection in current DDoS attack detection. This will enhance the precision of discovery for DDoS attack in cloud computing. In addition, different ISPs and cloud server providers ought to receive a common standard deployment approach for better co-operation.

ACKNOWLEDGMENT

The authors would also like to thank the anonymous reviewers for their comments and suggestions.

REFERENCES

[1] M. Ficco and F. Palmieri, "Introducing fraudulent energy consumption in cloud infrastructures: A new generation of denial-of-service attacks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 460–470, Jun. 2017.
[2] T. Lohman. *DDoS is Cloud's Security Achilles Heel*. Accessed: Sep. 2011. [Online]. Available: http://www.computerworld.com.au/article/401127
[3] D. Sher, "Gartner: Application layer ddos attacks to increase in 2013," Tech. Rep., 2013.
[4] Z. Anwar and A. W. Malik, "Can a DDoS attack meltdown my data center? A simulation study and defense strategies," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1175–1178, Jul. 2014.
[5] D. Anstee, D. Bussiere, and G. Sockrider, "Arbor special report: Worldwide infrastructure security report," Arbor Networks, Burlington, MA, USA, 2012. [Online]. Available: http://pages.arbornetworks.com/rs/arbor/images/wisr2012_en.pdf
[6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[7] V. Ashktorab and S. R. Taghizadeh, "Security threats and countermeasures in cloud computing," *Int. J. Appl. Innov. Eng. Manage. (IJAIEM)*, vol. 1, no. 2, pp. 234–245, 2012.
[8] R. Bace and P. Mell, "Nist special publication on intrusion detection systems," DTIC, Fort Belvoir, VA, USA, Tech. Rep., 2001.
[9] A. Bakshi and B. Yogesh, "Securing cloud from DDoS attacks using intrusion detection system in virtual machine," in *Proc. 2nd Int. Conf. Commun. Softw. Netw.*, Feb. 2010, pp. 260–264.
[10] U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Vulnerability of network mechanisms to sophisticated DDoS attacks," *IEEE Trans. Comput.*, vol. 62, no. 5, pp. 1031–1043, May 2013.
[11] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using nox/openflow," in *Proc. IEEE Local Comput. Netw. Conf.*, Oct. 2010, pp. 408–415.
[12] *Arbor Application Brief: The Growing Threat of Application-Layer DDoS Attacks*, Arbor Networks, Feb. 2011. [Online]. Available: http://www.arbornetworks.com/component/docman/doc download/467-the-growing-threat-of-application-layer-ddos-attacks?Itemid=442
[13] Y. Cai, F. R. Yu, and S. Bu, "Dynamic operations of cloud radio access networks (C-RAN) for mobile cloud computing systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1536–1548, Mar. 2016.
[14] R.-I. Chang and C.-C. Chuang, "A service-oriented cloud computing network management architecture for wireless sensor networks," *Ad-Hoc Sensor Wireless Netw.*, vol. 22, nos. 1–2, pp. 65–90, 2014.
[15] S. S. Chapade, K. U. Pandey, and D. S. Bhade, "Securing cloud servers against flooding based DDOS attacks," in *Proc. IEEE Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. 2013, pp. 524–528.
[16] Q. Chen, W. Lin, W. Dou, and S. Yu, "CBF: A packet filtering method for DDoS attack defense in cloud environment," in *Proc. IEEE 9th Int. Conf. Dependable, Autonomic Secure Comput.*, Dec. 2011, pp. 427–434.
[17] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting Web based DDoS attack using mapreduce operations in cloud computing environment," *J. Internet Services Inf. Secur.*, vol. 3, nos. 3–4, pp. 28–37, 2013.
[18] N.-N. Dao, J. Park, M. Park, and S. Cho, "A feasible method to combat against DDoS attack in SDN network," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2015, pp. 309–311.
[19] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS attack & its effect in cloud environment," *Procedia Comput. Sci.*, vol. 49, pp. 202–210, Jan. 2015.
[20] W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1838–1850, Sep. 2013.
[21] D. Drutskoy, E. Keller, and J. Rexford, "Scalable network virtualization in software-defined networks," *IEEE Internet Comput.*, vol. 17, no. 2, pp. 20–27, Mar./Apr. 2013.
[22] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in *Proc. DARPA Inf. Survivability Conf. Expo.*, vol. 1, Apr. 2003, pp. 303–314.
[23] M. Ficco and M. Rak, "Stealthy denial of service strategy in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 3, no. 1, pp. 80–94, Jan./Mar. 2015.
[24] G. Finnie. *The Role of DPI in an SDN World*. Accessed: Dec. 2012. [Online]. Available: https://www.qosmos.com/

[25] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, "Time-based DDoS detection and mitigation for SDN controller," in *Proc. 17th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Aug. 2015, pp. 550–553.
[26] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments," *Comput. Netw.*, vol. 62, no. 5, pp. 122–136, Apr. 2014.
[27] M. Godfrey and M. Zulkernine, "Preventing cache-based side-channel attacks in a cloud environment," *IEEE Trans. Cloud Comput.*, vol. 2, no. 4, pp. 395–408, Oct./Dec. 2014.
[28] R. Goel, M. Garuba, and A. Girma, "Cloud computing vulnerability: DDoS as its main security threat, and analysis of IDS as a solution model," in *Proc. 11th Int. Conf. Inf. Technol., New Gener.*, Apr. 2014, pp. 307–312.
[29] M. Gupta, J. Sommers, and P. Barford, "Fast, accurate simulation for SDN prototyping," in *Proc. 2nd ACM SIGCOMM Hot Topics Softw. Defined Netw.*, Aug. 2013, pp. 31–36.
[30] S. Gupta and P. Kumar, "VM profile based optimized network attack pattern detection scheme for DDOS attacks in cloud," in *Proc. Int. Symp. Secur. Comput. Commun.* Berlin, Germany: Springer, 2013, pp. 255–261.
[31] D. Y. Bang, D. K. Lee, and D. Choi, "A protection method on SDN using sFlow and snort for SYN flooding attack," in *Proc. 3rd Int. Conf. Smart Media Appl.*, 2014.
[32] N. Handigol, B. Heller, V. Jeyakumar, D. Mazières, and N. McKeown, "Where is the debugger for my software-defined network?" in *Proc. 1st ACM Workshop Hot Topics Softw. Defined Netw.*, Aug. 2012, pp. 55–60.
[33] N. Handigol, B. Heller, V. Jeyakumar, B. Lantz, and N. McKeown, "Reproducible network experiments using container-based emulation," in *Proc. 8th ACM Int. Conf. Emerg. Netw. Exp. Technol.*, Dec. 2012, pp. 253–264.
[34] N. Handigol, B. Heller, V. Jeyakumar, D. Mazières, and N. McKeown, "I know what your packet did last hop: Using packet histories to troubleshoot networks," in *Proc. 11th USENIX Symp. Netw. Syst. Design Implement.*, 2014, pp. 71–85.
[35] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," *Gartner Rep.*, vol. 27, pp. 29–52, Jun. 2008.
[36] J. Hendler. *DARPA, 2000 Hendler, James: DARPA Agent Mark Up Language (DAML)*. Accessed: 2001. [Online]. Available: http://dtsn.darpa.mil/iso/programtemp.asp
[37] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Uncover security design flaws using the stride approach," *MSDN Mag.-Louisville*, pp. 68–75, Nov. 2006.
[38] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures.," in *Proc. NDSS Symp.*, Feb. 2015, pp. 1–15.
[39] (Apr. 2013). *How SDN Applications Will Change Layer 4-7 Network Services*. [Online]. Available: http://searchsdn.techtarget.com/tip/HowSDN-applications-will-change-Layer-4-7-network-services
[40] J. Idziorek, M. Tannian, and D. Jacobson, "Attribution of fraudulent resource consumption in the cloud," in *Proc. IEEE 5th Int. Conf. Cloud Comput.*, Jun. 2012, pp. 99–106.
[41] Y. Jarraya, T. Madi, and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1955–1980, 4th Quart., 2014.
[42] R. Jin and B. Wang, "Malware detection for mobile devices using software-defined networking," in *Proc. 2nd GENI Res. Educ. Exp. Workshop*, Mar. 2013, pp. 81–88.
[43] R. Kandoi and M. Antikainen, "Denial-of-service attacks in openflow Sdn networks," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 1322–1326.
[44] S. Karthik and J. J. Shah, "Analysis of simulation of DDOS attack in cloud," in *Proc. Inf. Conf. Inf. Commun. Embedded Syst.*, Feb. 2014, pp. 1–5.
[45] W. Kim, "Cloud computing architecture," *Int. J. Web Grid Services*, vol. 9, no. 3, pp. 287–303, 2013.
[46] R. Klöti, V. Kotronis, and P. Smith, "Openflow: A security analysis," in *Proc. ICNP*, Oct. 2013, pp. 1–36.
[47] K. Rt, S. T. Selvi, and K. Govindarajan, "DDos detection and analysis in SDN-based environment using support vector machine classifier," in *Proc. 6th Int. Conf. Adv. Comput. (ICoAC)*, Dec. 2014, pp. 205–210.
[48] H. Kozushko, "Intrusion detection: Host-based and network-based intrusion detection systems," *Independ. Study*, vol. 11, pp. 1–23, Sep. 2003.
[49] D. Kreutz, F. M. V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, Aug. 2013, pp. 55–60.
[50] M. K. Owski and J. Vaidya, *Computer Security—ESORICS 2014*. Wroclaw, Poland, Sep. 2014.
[51] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid prototyping for software-defined networks," in *Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw.*, Oct. 2010, p. 19.
[52] Y.-D. Lin, D. Pitt, D. Hausheer, E. Johnson, and Y.-B. Lin, "Software-defined networking: Standardization for cloud computing's second wave," *Computer*, vol. 47, no. 11, pp. 19–21, Nov. 2014.
[53] D. Linthicum, "As cloud use grows, so will rate of DDoS attacks," InfoWorld, San Francisco, CA, USA, Tech. Rep., 2013.
[54] A. M. Lonea, D. E. Popescu, and H. Tianfield, "Detecting DDoS attacks in cloud computing environment," *Int. J. Comput. Commun. Control*, vol. 8, no. 1, pp. 70–78, 2013.
[55] R. Lua and K. C. Yow, "Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network," *IEEE Netw.*, vol. 25, no. 4, pp. 28–33, Jul./Aug. 2011.
[56] P. S. Mann and D. Kumar, "A reactive defense mechanism based on an analytical approach to mitigate DDoS attacks and improve network performance," *Int. J. Comput. Appl.*, vol. 12, no. 12, pp. 975–987, 2011.
[57] P. Mathur and N. Nishchal, "Cloud computing: New challenge to the entire computer industry," in *Proc. 1st Int. Conf. Parallel Distrib. Grid Comput. (PDGC)*, Oct. 2010, pp. 223–228.
[58] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Berlin, Germany: Springer, 2011, pp. 161–180.
[59] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004.
[60] A. Gonsalves. (Jan. 2013). *Mobile Devices Set to Become Next DDoS Attack Tool*. [Online]. Available: http://www.csoonline.com/article/2132699/mobilesecurity/mobile-devices-set-to-become-next-ddos-attack-tool.html
[61] S. M. Mousavi, "Early detection of DDoS attacks in software defined networks controller," Ph.D. dissertation, Carleton Univ., Ottawa, ON, Canada, 2014.
[62] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 77–81.
[63] N. I. Mowla, I. Doh, and K. Chae, "Multi-defense mechanism against DDoS in SDN based CDNi," in *Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2014, pp. 447–451.
[64] J. Naous, D. Erickson, G. A. Covington, G. Appenzeller, and N. McKeown, "Implementing an OpenFlow switch on the NetFPGA platform," in *Proc. 4th ACM/IEEE Symp. Archit. Netw. Commun. Syst.*, Nov. 2008, pp. 1–9.
[65] O. A. Osanaiye, "Short paper: IP spoofing detection for preventing DDoS attack in cloud computing," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Feb. 2015, pp. 139–141.
[66] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016.
[67] G. Pallis, "Cloud computing: The new frontier of Internet computing," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 70–73, Sep./Oct. 2010.
[68] F. Palmieri, M. Ficco, and A. Castiglione, "Adaptive stealth energy-related dos attacks against cloud data centers," in *Proc. 80th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2014, pp. 265–272.
[69] F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, and A. Castiglione, "Energy-oriented denial of service attacks: An emerging menace for large cloud infrastructures," *J. Supercomput.*, vol. 71, no. 5, pp. 1620–1641, 2015.
[70] A. Passito, E. Mota, R. Bennesby, and P. Fonseca, "AgNOS: A framework for autonomous control of software-defined networks," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, May 2014, pp. 405–412.
[71] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surv.*, vol. 39, no. 1, p. 3, Apr. 2007.
[72] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for OpenFlow networks," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, Aug. 2012, pp. 121–126.
[73] M. Ramadas, S. Ostermann, and B. Tjaden, "Detecting anomalous network traffic with self-organizing maps," in *Recent Advances in Intrusion Detection*. Berlin, Germany: Springer, 2003, pp. 36–54.
[74] W. Ren, "uLeepp: An ultra-lightweight energy-efficient and privacy-protected scheme for pervasive and mobile WBSN-cloud communications," *Ad Hoc Sensor Wireless Netw.*, vol. 27, pp. 173–195, Jan. 2015.

[75] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proc. 5th IEEE Int. Joint Conf. INC, IMS IDC*, Aug. 2009, pp. 44–51.
[76] S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in *Proc. 8th IEEE Int. Conf. Dependable, Autonomic Secure Comput.*, Dec. 2009, pp. 729–734.
[77] (Jan. 2014). *SDN and Security: Network Versus Applications*. [Online]. Available: https://devcentral.f5.com/articles/sdn-and-security-networkversus-applications
[78] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, Jul. 2013.
[79] R. Shea and J. Liu, "Performance of virtual machines under networked denial of service attacks: Experiments and analysis," *IEEE Syst. J.*, vol. 7, no. 2, pp. 335–345, Jun. 2013.
[80] M. P. K. Shelke, M. S. Sontakke, and A. D. Gawande, "Intrusion detection system for cloud computing," *Int. J. Sci. Technol. Res.*, vol. 1, no. 4, pp. 67–71, May 2012.
[81] S. Shin and G. Gu, "Attacking software-defined networks: A first feasibility study," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, Aug. 2013, pp. 165–166.
[82] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2013, pp. 413–424.
[83] S. Shin, P. A. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyson, "FRESCO: Modular composable security services for software-defined networks.," in *Proc. 20th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 2013, pp. 1–16.
[84] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," *Comput. Netw.*, vol. 57, no. 2, pp. 378–403, 2013.
[85] J. Sommers, R. Bowden, B. Eriksson, P. Barford, M. Roughan, and N. Duffield, "Efficient network-wide flow record generation," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2363–2371.
[86] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures," in *Proc. 17th Int. Conf. Parallel Distrib. Comput. Syst. (ISCA)*, 2004, pp. 543–550.
[87] M. H. Sqalli, F. Al-Haidari, and K. Salah, "EDoS-shield—A two-steps mitigation technique against EDoS attacks in cloud computing," in *Proc. 4th IEEE Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2011, pp. 49–56.
[88] D. Stevanovic and N. Vlajic, "Next generation application-layer DDoS defences: Applying the concepts of outlier detection in data streams with concept drift," in *Proc. 13th Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2014, pp. 456–462.
[89] A. Studer and A. Perrig, "The coremelt attack," in *Proc. Eur. Symp. Res. Comput. Secur.* Berlin, Germany: Springer, 2009, pp. 37–52.
[90] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 961–987, 2nd Quart., 2014.
[91] J. Suh, H.-G. Choi, W. Yoon, T. You, T. Kwon, and Y. Choi, "Implementation of content-oriented networking architecture (CONA): A focus on DDoS countermeasure," in *Proc. Eur. NetFPGA Developers Workshop*, Sep. 2010, pp. 1–6.
[92] A. TaheriMonfared and C. Rong, "Multi-tenant network monitoring based on software defined networking," in *Proc. OTM Confederated Int. Conf. 'Move Meaningful Internet Syst.'* Berlin, Germany: Springer, 2013, pp. 327–341.
[93] H. Tian and J. Bi, "An incrementally deployable flow-based scheme for IP traceback," *IEEE Commun. Lett.*, vol. 16, no. 7, pp. 1140–1143, Jul. 2012.
[94] A. Alva *et al.*, "The notorious nine cloud computing top threats in 2013," Cloud Secur. Alliance, 2013.
[95] H.-Y. Tsai, M. Siebenhaar, A. Miede, Y. Huang, and R. Steinmetz, "Threat as a service?: Virtualization's impact on cloud security," *IT Prof.*, vol. 14, no. 1, pp. 32–37, Jan./Feb. 2011.
[96] P. R. Ubhale and A. M. Sahu, "Securing cloud computing environment by means of intrusion detection and prevention system (IDPS)," *Int. J. Comput. Sci. Manage. Res.*, vol. 2, no. 5, pp. 2430–2435, 2013.
[97] S. VivinSandar and S. Shenai, "Economic denial of sustainability (EDoS) in cloud services using HTTP and XML based DDoS attacks," *Int. J. Comput. Appl.*, vol. 41, no. 20, pp. 11–16, Mar. 2012.
[98] M. Vizváry and J. Vykopal, "Future of DDoS attacks mitigation in software defined networks," in *Proc. IFIP Int. Conf. Auton. Infrastruct., Manage. Secur.* Berlin, Germany: Springer, 2014, pp. 123–127.
[99] H. Wang, L. Xu, and G. Gu, "OF-GUARD: A DoS attack prevention extension in software-defined networks," in *Proc. Poster Session Open Netw. Summit*. Santa Clara, CA, USA: USENIX, 2014, pp. 1–2.
[100] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," *Comput. Netw.*, vol. 81, pp. 308–319, Apr. 2015.
[101] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 310–317.
[102] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined networks," in *Proc. 45th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2015, pp. 239–250.
[103] A. Wundsam, D. Levin, S. Seetharaman, and A. Feldmann, "OFRewind: Enabling record and replay troubleshooting for networks," in *Proc. USENIX Annu. Tech. Conf.*, 2011, pp. 327–340.
[104] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 843–859, 2nd Quart., 2013.
[105] H. Xie, T. Tsou, D. Lopez, H. Yin, and V. Gurbani, *Use Cases for Alto with Software Defined Networks*, document draft-xie-alto-sdn-extension-use-cases-01.txt, Working Draft, IETF Secretariat, Internet-Draft, 2012.
[106] T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar, "Snortflow: A openflow-based intrusion prevention system in cloud environment," in *Proc. 2nd IEEE GENI Res. Educ. Exp. Workshop (GREE)*, Mar. 2013, pp. 89–92.
[107] L. Yang, T. Zhang, J. Song, J. Wang, and P. Chen, "Defense of DDoS attack for cloud computing," in *Proc. IEEE Int. Conf. Comput. Sci. Automat. Eng. (CSAE)*, vol. 2, May 2012, pp. 626–629.
[108] G. Yao, J. Bi, and P. Xiao, "Source address validation solution with openflow/nox architecture," in *Proc. 19th IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2011, pp. 7–12.
[109] Z. Yin, F. R. Yu, S. Bu, and Z. Han, "Joint cloud and wireless networks operations in mobile cloud computing environments with telecom operator cloud," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 4020–4033, Jul. 2015.
[110] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can we beat DDoS attacks in clouds?" *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2245–2254, Sep. 2014.
[111] Y. Yu, Q. Chen, and X. Li, "Distributed collaborative monitoring in software defined networks," Mar. 2014, *arXiv:1403.8008*. [Online]. Available: https://arxiv.org/abs/1403.8008
[112] C. YuHunag, T. MinChi, C. YaoTing, C. YuChieh, and C. YanRen, "A novel design for future on-demand service and security," in *Proc. IEEE 12th Int. Conf. Commun. Technol.*, Nov. 2010, pp. 385–388.
[113] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.
[114] D. Bhamare, R. Jain, M. Samaka, and A. Erbad, "A survey on service function chaining," *J. Netw. Comput. Appl.*, vol. 75, pp. 138–155, Nov. 2016.
[115] D. Bhamare, R. Jain, M. Samaka, G. Vaszkun, and A. Erbad, "Multi-cloud distribution of virtual functions and dynamic service deployment: Open ADN perspective," in *Proc. IEEE Int. Conf. Cloud Eng.*, Mar. 2015, pp. 299–304.
[116] A. Studer and A. Perrig, "The coremelt attack," in *Proc. 14th Eur. Conf. Res. Comput. Secur.*, 2009, pp. 37–52.
[117] S. S. Mohammed, R. Hussain, O. Senko, B. Bimaganbetov, J. Lee, F. Hussain, C. A. Kerrache, E. Barka, and M. Z. A. Bhuiyan, "A new machine learning-based collaborative DDoS mitigation mechanism in software-defined network," in *Proc. 14th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2018, pp. 1–8.
[118] K. Kalkan, G. Gur, and F. Alagoz, "Defense mechanisms against DDoS attacks in SDN environment," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 175–179, Sep. 2017.
[119] K. Kalkan, G. Gür, and F. Alagöz, "SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2017, pp. 669–675.
[120] K. Kalkan, L. Altay, G. Gür, and F. Alagöz, "JESS: Joint entropy-based DDoS defense scheme in SDN," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 10, pp. 2358–2372, Oct. 2018.
[121] K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 5, pp. 1985–1997, May 2019.

[122] H. Pillutla and A. Arjunan, "Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 4, pp. 1547–1559, Apr. 2019.
[123] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal load distribution for the detection of VM-based DDoS attacks in the cloud," *IEEE Trans. Serv. Comput.*, to be published.
[124] S. Vetha and K. V. Devi, "A trust-based hypervisor framework for preventing DDoS attacks in cloud," *Concurrency Comput., Pract. Exper.*, p. e5279. doi: 10.1002/cpe.5279.

SHI DONG received the M.S. degree in computer science from the University of Electronic and Technology of China, in 2009, and the Ph.D. degree in computer science from Southeast University. He was a Postdoctoral Researcher with the Huazhong University of Science and Technology. He was a Visiting Scholar with Washington University, St. Louis. He is currently a Distinguished Professor with Zhoukou Normal University. His current research interests include network management and network security.

KHUSHNOOD ABBAS received the bachelor's and master's degrees from Aligarh Muslim University, India, in 2011, and the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC) in 2018. He was a Visiting Scholar with the Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences.

RAJ JAIN received the B.S. degree in electrical engineering from APS University, Rewa, India, in 1972, the M.S. degree in computer science controls from IISc, Bangalore, India, in 1974, and the Ph.D. degree in applied math/computer science from Harvard University, in 1978. He was one of the Co-Founders of Nayna Networks, Inc., San Jose, CA, USA—a next generation telecommunications systems company. He was a Senior Consulting Engineer with Digital Equipment Corporation, Littleton, MA, USA, and then a Professor of computer and information sciences with Ohio State University, Columbus, OH, USA. He is currently a Professor of computer science engineering with Washington University, St. Louis. He holds 14 patents and has written or edited 12 books, 16 book chapters, more than 65 journal and magazine papers, and more than 10 e5 conference papers. He is a Fellow of ACM and AAAS. He received ACM SIGCOMM Test of Time Award, CDAC-ACCS Foundation Award 2009, and ranks among the top 100 in CiteseerX's list of Most Cited Authors in computer science.