SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:3724–3751
Published online 13 July 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1539

REVIEW ARTICLE

A survey and taxonomy of DoS attacks in cloud computing

Mohammad Masdari* and Marzie Jalali

Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

ABSTRACT

Denial-of-service (DoS) attacks are one of the major security challenges in the emerging cloud computing models. Currently, numerous types of DoS attacks are conducted against the various cloud services and resources, which target their availability, service level agreements, and performance. This paper presents an in-depth study of the various types of the DoS attacks proposed for the cloud computing environment and classifies them based on the cloud components or services, which they target. Besides, it provides a comprehensive analysis of the vulnerabilities utilized in these DoS attacks and investigates about the state-of-the-art solutions presented in the literature to prevent, detect, or deal with each kind of DoS attacks in the cloud. Finally, it presents open research issues. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS

denial of service; DDoS; CIDoS; EDOS; virtual machine; security

***Correspondence**

Mohammad Masdari, Department of Computer Engineering, Islamic Azad University of Urmia, Urmia, Iran.
E-mail: m.masdari@laurmia.ac.ir

1. INTRODUCTION

Cloud computing is a network-based environment, which focuses on providing virtualized resources for its customers based on the pay-for-uses model [1]. It is an innovative information system architecture, which by combining emerging technologies such as service-oriented architecture (SOA) and virtualization is considered as the future of computing technologies. The main deployment models for the cloud computing are as follows [2]:

- Private cloud, whose services are only available for the cloud owner.
- Community cloud, which is shared between several organizations.
- Public cloud, which is created for large set of public clients and the owner is the organization that sells the cloud services.
- Hybrid cloud, which is a combination of two or more clouds that may be public, private, or community clouds.
- Clouds federation, which is the interconnection of multiple clouds to accommodate sudden spikes of demand.

Also, cloud service providers offer services that are mainly separated into three categories as follows [3]:

- Software as a service: It provides users access to software application over the internet using the cloud services. These software applications are in the cloud and are used for enormous ranges of tasks.
- Platform as a service: Platform as a service provides all the hardware and software components required to build cloud-based application.
- Infrastructure as a service: It provides services such as storage, security tools, and networking to the end users.

Although the paradigm of cloud computing is not mature enough, numerous critical security attacks are designed and proposed against the various cloud deployment models, which pose severe security risks to its adopters. For example, several attacks such as wrapping, malware injection, flooding [4], side channel, authentication, and man-in-the-middle cryptographic attacks can be conducted against the cloud computing [5,6]. One of these security threats is denial-of-service (DoS) attack, which is any event or malicious behavior that mitigates or prevents a cloud's capacity to perform its expected functions and services [7]. Distributed form of DoS attacks is called distributed DoS (DDoS) attack, which applies numerous network hosts to inflict more devastating effects to its victim. Other kinds of DoS attacks in the cloud computing environment are bandwidth DoS

(BW DoS) (SYN flood, Internet Control Message Protocol (ICMP) ping flood or User Datagram Protocol (UDP) flood attacks), reflection-based DoS, and amplification-based DoS attacks, which are used by attackers to overwhelm the cloud resources under heavy traffic and load.

The main reason for these security problems is that cloud computing is a network-based technology and is based on its deployment model and services and resources may be exposed to the many internal and external attackers. Virtualization, which is used to place multiple virtual machines (VMs) on each physical machines or servers, is one of those cloud features, which is favored by the DoS attackers in the cloud environment. For example, the attacks such as cloud-internal DoS (CIDoS), VM sprawl attack, and the VM neighbor attacks misuse the VM migration. Also, DoS attacks are designed against other cloud components such as VM monitors (hypervisor), cloud schedulers, and even cloud customers. For example, in the economic DoS attacks, the attacker tries to increase the cost of cloud usage for cloud users and customers. Generally, the vulnerabilities of cloud to these attacks partly depend on the cloud deployment model. For example, public clouds expose more attack surface to the attackers and can be attacked more by the external attackers. However, DoS attacks may be initiated by the internal malicious hosts and users in various cloud deployment models. The growing use of security threats against the cloud computing services, and the shared infrastructure increases the need for having a security plan to deal with various kinds of DoS attacks. Otherwise, the cloud may be throttled under the attacks or may even be applied as part of some DoS attacks against other clouds.

This paper investigates the DoS attacks related to the cloud computing providers, systems, and customers. It first illustrates the major types of DoS attacks and the vulnerabilities, which are utilized to launch each attack. Then, it classifies the DoS attacks based on the components, which they attack and categorizes them into the DoS attacks on the cloud components and the DoS attacks on the cloud networking infrastructure. The DoS attacks on the cloud components mainly target the VM migration feature of the cloud and try to overwhelm the cloud by causing high number of VM migrations. Furthermore, the DoS attacks on the networking protocols are investigated, and the weaknesses and vulnerabilities of each attacked network protocol are specified. After analyzing the techniques applied by major DoS attacks, various countermeasures presented in the literature to prevent, detect, and deal with each type of the studied DoS attacks are discussed and compared.

To the best of our knowledge, no previously proposed papers have fully investigated the DoS problem in the cloud computing, and our paper is the first one, which studies this problem in detail. Conducting this research is very important for illuminating various DoS attacks in the cloud and designing new solutions to deal with this problem.

The rest of this paper is organized as follows: Sections 2 defines the DoS attacks and their variants. Section 3 explains different types of DoS attacks on the cloud components, Section 4 classifies the existing DoS attacks on the cloud networking infrastructure, and Section 5 explains various defense mechanisms. Finally, Section 6 presents the comparison and discussion about the schemes, and finally, Section 7 provides the concluding remarks and future research directions.

Table I shows the acronyms and abbreviations that are used in the rest of this paper.

2. DENIAL-OF-SERVICE ATTACKS

In cloud computing, a DoS attack can be described as an attack designed to prevent some cloud computing service or resource from providing its normal services for a period of time. DoS attacks compromise the availability of the cloud resources and services and often target the computer networks' bandwidth or connectivity. Generally, DoS attacks come in the following categories:

- Bandwidth attacks
- Connectivity attacks
- Resource exhaustion
- Limitation exploitation
- Process disruption
- Data corruption
- Physical disruption

The bandwidth attacks are aimed to forward large traffic to consume all the available network resources. Moreover, connectivity attacks flood the victim by sending a high volume of connection requests that cause all the available operating system resources in the victim to be consumed and as a result the legitimate user requests cannot be handled [8,9].

2.1. Distributed denial of service

In remote DoS attacks, it is very important that the attacker remains undetected, otherwise it can be blocked by firewalls or intrusion detection systems located at the victim's site. To achieve this purpose, attacker utilizes many intermediate systems to perform the DoS attacks on behalf of them, that, in this case, the DoS attack is called distributed DoS (DDoS) attack. Figure 1 indicates the

Table I. Acronyms and abbreviations.

Abbreviation	Description
VM	Virtual machine
VMM	Virtual machine monitor
DoS	Denial of service
DDoS	Distributed denial of service
EDoS	Economic denial of service
CIDoS	Cloud-internal denial of service
XDoS	XML denial of service
HDoS	HTTP denial of service
LDoS	Low-rate denial of service
ADoS	Application denial of service

architecture of the DDoS attack. In the DDoS attacks, the attacker sends its orders to a system called command and control server (C&C server) that coordinates and triggers a botnet. Generally, a botnet is a collection of compromised hosts, which obscure the attacker by providing a level of indirection. The C&C server orders the botnet to launch DDoS attack against the victim, and afterwards, bots send attack packets to the victim whose content depends on the type of attack [10]. Thus, attacker host is separated from its victim by one or more intermediate layers of zombie hosts [11,12]. Generally, botnet-based DDoS attack networks fall under the following three categories [13]:

- Agent-handler Model: It comprises clients, handlers, and agents where the client or attacker uses the handlers to communicate with the agents. Also, the owners of the agent systems are unaware that their system has been compromised and is used to launch DDoS attacks, and they may be in contact with multiple handlers. Attackers often attempt to install the handler software on a compromised router or network server.
- Internet Relay Chat (IRC) Model: The client is connected to the agents through an IRC communication channel to hinder the tracking DDoS command packets.
- Web-based Model: It simply reports statistics to a web site and has some advantages over IRC such as ease of set-up, less bandwidth requirement, acceptance of large botnets for the distributed load, concealment of traffic, and hindrance of filtering and resistance to botnet hijacking.

The current popular DDoS attack bots are as follows [14]:

- AgoBot: It is one of the most popular bots with the anti-virus vendor, Sophos, listing over 600 different versions. Its variants are Gaobot, Nortonbot, Phatbot, and Polybot.
- SDBot: It has over 1800 variants and comes with ping and UDP flooding tools, whereas the "SYN Flood Edition" includes Transmission Control Protocol (TCP) SYN flooding attacks. SDBot is written in C++ to target Windows systems.
- RBot: RBot has over 1600 variants and is written in C++ to target Windows systems.
- SpyBot: Spybot is written in C programming language, and also affects Windows systems.

These botnets have a few hundred to thousand variants due to multiple authors working to enhance their features.

As outlined before, one of the important factors in conducting the DoS attack is that the attacker and various attack components such as C&C server and botnets remain undetected. The following methods are used in the current DoS attacks to keep the attackers hidden:

- Spoofing the source IP addresses of attack packets
- IP fluxing and domain fluxing
- Using botnet
- Diversity of the IP addresses in the botnet
- Using protocol specific proxies
- Using other uncompromised systems at the network, in the reflection and amplification attacks
- Using more intermediate layers of compromised systems and DoS attack components to attack the victim
- Preventing detection of the DoS attacking components such as botnets

The severity of DoS attacks depends on the following issues:

- Type of attack
- Type of protocol or event misused in the attack
- Number of compromised attacking hosts
- Number of uncompromised hosts applied in the attack
- The amount of resources at the victim's site
- Topology and defense mechanism at victim's site
- The amount of resource at the attacker components
- The amount of resource at the victim
- Type of cloud, often public clouds, which are accessible to public have more attack surfaces than private clouds

Also, to successfully launch DoS attacks, attackers try to represent themselves legal to the security components by applying the following methods:

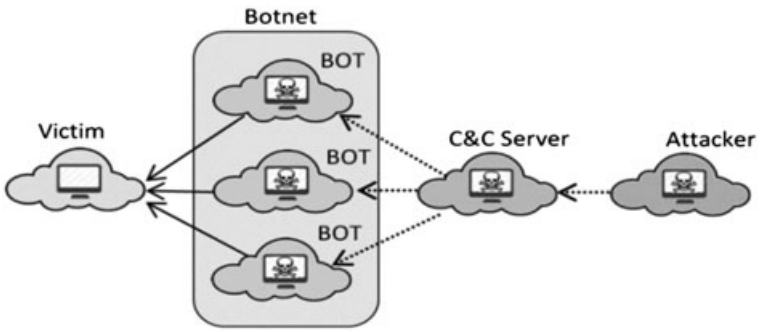

Figure 1. Architecture of distributed denial-of-service (DDoS) attack in the federated cloud environment.

- Mimicking legal network traffic.
- Mimicking flash crowds attack.
- Mimicking some legal event in the cloud computing.
- Obfuscation, for example by encrypting the content of attack messages.

However, the DDoS attacks can be more devastating in the cloud computing environment because the cloud consists of new concepts, components, and protocols, which have new vulnerabilities that can be misused to conduct new DoS attacks. Also, one major difference of DDoS attacks in conventional networks and the federated cloud computing environment is indicated in Figure 1 where all participants in the DDoS attack may be a cloud. For example, the attacker itself can be a cloud, C&C server can be a cloud, and botnet and the victim can be a cloud themselves. This makes DDoS attacks' detection, prevention, and handling more complicated because, by using clouds, attackers will have more available resources to launch their attacks. Generally, when a cloud is the victim of a DDoS attack, the first goal of the attacker is to saturate the Internet gateway of the cloud infrastructure. However, if it cannot be saturated, then the attackers will try to saturate the cloud servers.

2.2. Classification of distributed denial-of-service attacks

Distributed denial-of-service attacks can be classified based on their various features. For example, based on the attack origin, the DDoS attacks can be classified as internal DDoS attacks and external DDoS attacks.

- External DDoS attacks: Where the attacker should be able to load a trojan horse in the clients' VMs running in the cloud. If the trojan horse is able to spread over hundreds or thousands of the VMs, a botnet will be created for the attacker, which can be used as the origin of the DDoS attacks to the external victims.
- Internal DDoS attacks: The internal botnet will attack an internal victim. These attacks are more serious than the external attacks and may cause a complete breakdown of all the cloud infrastructures [15].

Thus, when the cloud security is neglected, the cloud may become the origin of many internal and external DDoS attacks. Figure 2 indicates an exploit-based classification of DDoS attacks [16]. The rest of this section describes these types of DDoS attacks in detail.

2.2.1. Protocol vulnerability exploitation

These attacks take advantage of known protocol vulnerabilities such as design or implementation flaws to cause inappropriate behaviors and modify the information going to or from a specific target [17]. Depending on its design, certain protocol steps may create the potential for DoS attacks. Moreover, although protocol may be well designed and secure, applying it with other protocols may lead to a bad situation [16]. The ping of death is caused by the protocol vulnerability.

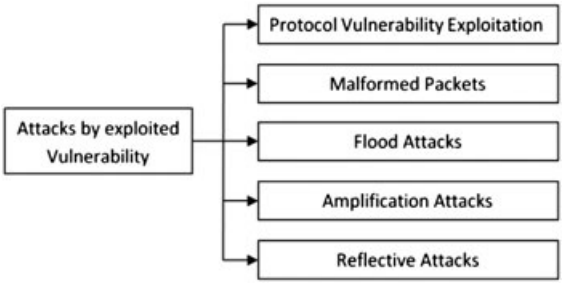

Figure 2. Classification of denial-of-service (DoS) attacks.

2.2.2. Malformed packet

Normally, these attacks rely on sending the incorrectly formed packets from attackers to the victim in order to crash the victim system. Malformed packet attack can be launched against many protocols. For example, malformed packet attack against IP protocol can be classified into IP address attack and IP packet option attack. In an IP address attack, the attack packets contain the same source and destination IP addresses, which confuse the victim's operating system and may crash it. However, in IP packet options attacks, malformed packets may randomize the optional fields within an IP packet and set all the quality of service bits to one, which may cause more processing in the victim for packet handling [18].

2.2.3. Flooding attacks

In a flooding attack, which also is called bandwidth-distributed DoS (BW-DDoS), the attacker floods the victim with unwanted traffic to prevent legitimate traffic to reach the victim system [19]. The flooding attacks differ in the type of the protocol used to flood the victim [20]. Strong attacking agent includes privileged zombie that has complete control over its host, with the ability of sending spoofed IP packets. However, weak agents include programs downloaded automatically and run in sandboxes [21]. Also, some BW-DDoS attacks create more complicated attacks using reflection and amplification techniques, which have more devastating effects on the victim and are harder to deal with [22].

2.2.4. Reflection-based denial of service

Another method applied by the DDoS attackers is the reflection method, which uncompromised servers are used to forward traffic to the victim and assist in consuming the victim's bandwidth. This method helps the attacker to send traffic to the victim indirectly and helps the attacker to remain undetected. In this method, all attack packets, which the attacker sends contain the IP address of the victim in the source address field of IP packets. When server receives these service requests, it sends its response to the victim node, not to the actual source node of packet.

Distributed reflective DoS (DRDoS) attack is a sophisticated type of DoS attack in which, as indicated in Figure 3, the attacker controls the master and slave zombies and instruct them to flood the request packets to the reflector node to bring down the target [23]. To prevent detection, the attackers can utilize botnets to conduct more serious reflective attacks. DRDoS attacks are used to exploit the protocols such as TCP, UDP, Domain Name System (DNS), and ICMP [24]. Smurf is a well-known DRDoS attack [25].

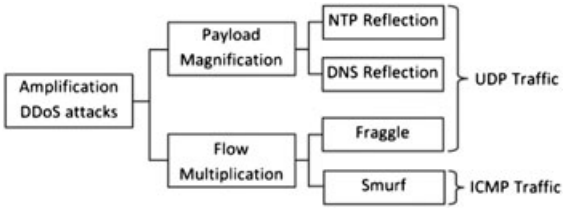

Figure 4. Classification of amplification distributed denial-of-service (DDoS) attacks.

2.2.5. Amplification distributed denial-of-service attacks

Amplification attacks are a more devastating version of reflective DoS attacks, which utilize the inherent nature of some network protocols to increase the amount of traffic that are reflected to the victim. In this attack, the volume of the response traffic generated by the applied reflector servers is more than the request message traffic issued from the attacker. As a result, traffic, which reaches the victim, is amplified by the reflector server, and this overwhelms the victim's resources and bandwidth [26]. This empowers the attacker to launch the DoS attack even with smaller botnets. To launch amplification attacks, an amplifier reflector server is needed that runs a protocol such as Network Time Protocol (NTP) or DNS. When this server receives a query packet, it responds with one or more packets whose aggregate size is larger than the size of query it receives. As indicated in Figure 4, the amplification DDoS attacks are created by the amplification through flow multiplication attacks or through payload magnification where a large number of responses are reproduced or response messages bigger than the corresponding requests are issued by the reflector.

Also, in the amplification attacks, attackers may misuse the UDP-based protocols to launch DDoS attacks, because, often they lack handshake mechanisms to verify the source node [27,28]. Thus, the amplification attacks can forward more traffic to victim with less number of intermediate zombies and are more serious than reflexive attacks and DDoS attacks (Figure 5).

3. ATTACKS ON THE CLOUD COMPONENTS

Cloud computing largely consists of technologies such as SOA and virtualization, which are vulnerable to various internal and external security problems. Security problems are significant especially in public clouds [29]. Figure 6 shows the classification of common DoS attacks on the cloud computing environment.

3.1. Attacks against virtual machines

Virtualization has become an indispensable technology for today's cloud infrastructure and provides numerous advantages in sharing, managing, and isolation of the cloud resources [30]. Virtualization allows multiple VMs to reside on a single physical machine [31], and VMs can be created, expanded, shrunk, or moved dynamically as demand varies. Figure 5 indicates the organization of the hosted virtualization. A software layer is named VM monitor (VMM) (hypervisor), which creates and manages them and maintains the isolation between the VMs [32].

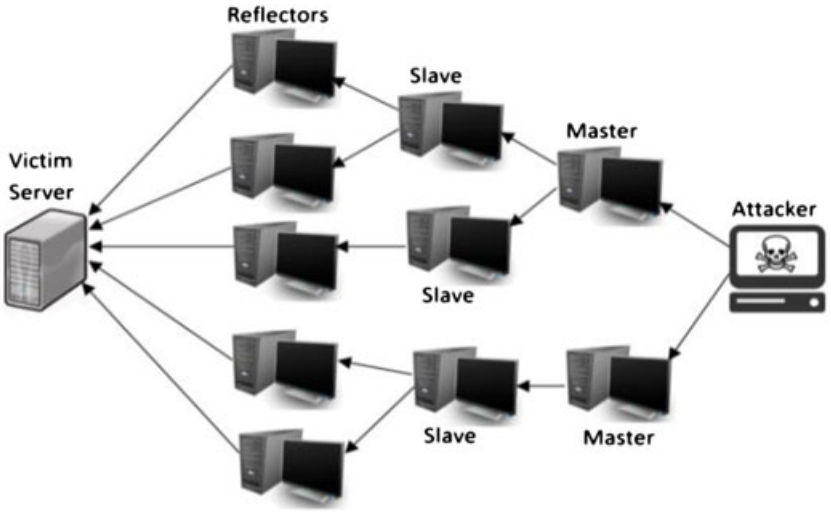

Figure 3. Architecture of distributed reflective denial-of-service (DRDoS) attack.

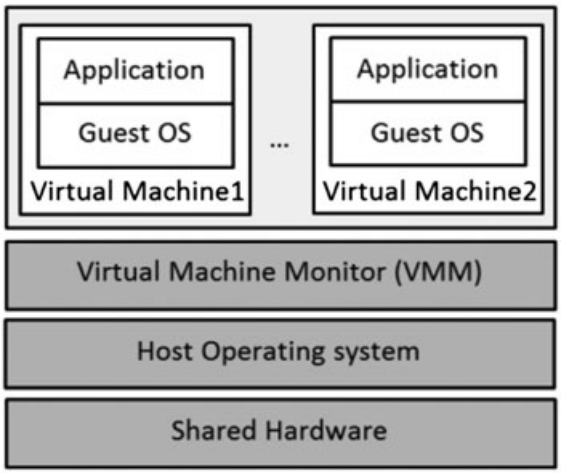

Figure 5. Hosted virtualization.

Hypervisor should also monitor the guest operating systems and their applications to detect any malicious behavior [33].

Security threats in a VM environment are the same as security flaws in the physical system. Generally, in a virtual environment, security attacks may be conducted between the following items [34]:

- Between the VMs
- Between the VMs and their host
- VM monitor from the host
- VM monitor from another VM
- Guest-to-guest attack
- External modification of a VM
- External modification of a hypervisor

Because the guest operating system (OS) can access the network, security methods are needed in each VM [35]. Some DoS attacks in the clouds are conducted by misusing the VM migration feature and degrade the service provider's ability to satisfy the service level agreement (SLA) requirements. VM migration provides efficient resource utilization and improves power saving in the cloud data centers. Normally, when a server is overloaded, its VMs can be migrated to lightly loaded servers. Moreover, when some servers are underutilized, their VMs can be consolidated into fewer numbers of servers for power saving. But VM migration is a costly operation in which a VM state is transferred from one host to another [36].

3.1.1. Virtual machine migration attacks

When a physical server is overloaded with DDoS attacks, VM migration not only does not alleviate the problem, but also it may deteriorate the system's situation [37]. VM Migration attack is conducted by the malicious increasing of the resource consumption of the VMs. It causes many costly VM migrations and degrades the performance of the cloud [38].

3.1.2. Cloud-internal denial-of-service attacks

Cloud-internal DoS attack is a cloud-specific DoS attack in which a number of malicious VMs in the same physical host try to attack their host [39]. These VMs apply covert channels and a protocol for coordination. To launch this attack, each VM increases its resource usage to break the host's ability to cope with the load. CIDoS is hard to detect because the attackers' behaviors are similar to normal workload of a very busy host. In [40] Alarifi *et al.* present a coordination protocol based on the broadcast primitives in memory-based covert channels for dynamic attack group membership and attack initiation based on a broadcast variant of the Jarecki–Kim–Tsudik protocol. This attack utilizes resource overcommitment and the migration cost and the power management issues.

3.1.3. Virtual machine sprawling attacks

In a virtual system, inappropriate VM management policy may cause VM sprawling attack in which the number of VMs is continuously increasing, while they are idle or do not back from sleep [41,42]. This attack wastes cloud resources and creates more entry points for attackers [43].

3.1.4. Neighbor attacks

One of the potential DoS attacks to cloud virtualization system is the neighbor attack, which is indicated in Figure 7.

Any VM can attack its neighboring VMs in the same physical machine by causing maximum workload to it. This DoS attack can reduce the cloud performance and may cause harmful effects on the other servers [44]. These attacks are caused by bad configurations and vulnerabilities in the hypervisor [45].

3.1.5. Virtual machine escape attacks

In a VM escape attack, the malicious application executed in a VM will be able to completely bypass the hypervisor and get access to the host machine. When it gains access to the host system, it also gains the root privileges and escapes from the VM privileges. This results in complete breakdown of the security framework of the host system. However, this problem can be solved by properly configuring the host/guest interactions [34].

3.2. Attacks on the hypervisors

A cloud customer can lease a guest VM to install a malicious guest OS, to attack the hypervisor by changing its source code and gaining access to the memory contents of the neighboring VMs [46].

3.2.1. Mimicking distributed denial-of-service attacks

To prevent detection, DDoS attacker may hide its attacks by mimicking legitimate traffic [47]. Attackers are mimicking network traffic patterns to deceive the DoS attack detection methods based on the network traffic monitoring. However, it is an open problem to discriminate the mimicking DDoS attacks from high traffic of the legitimate users.

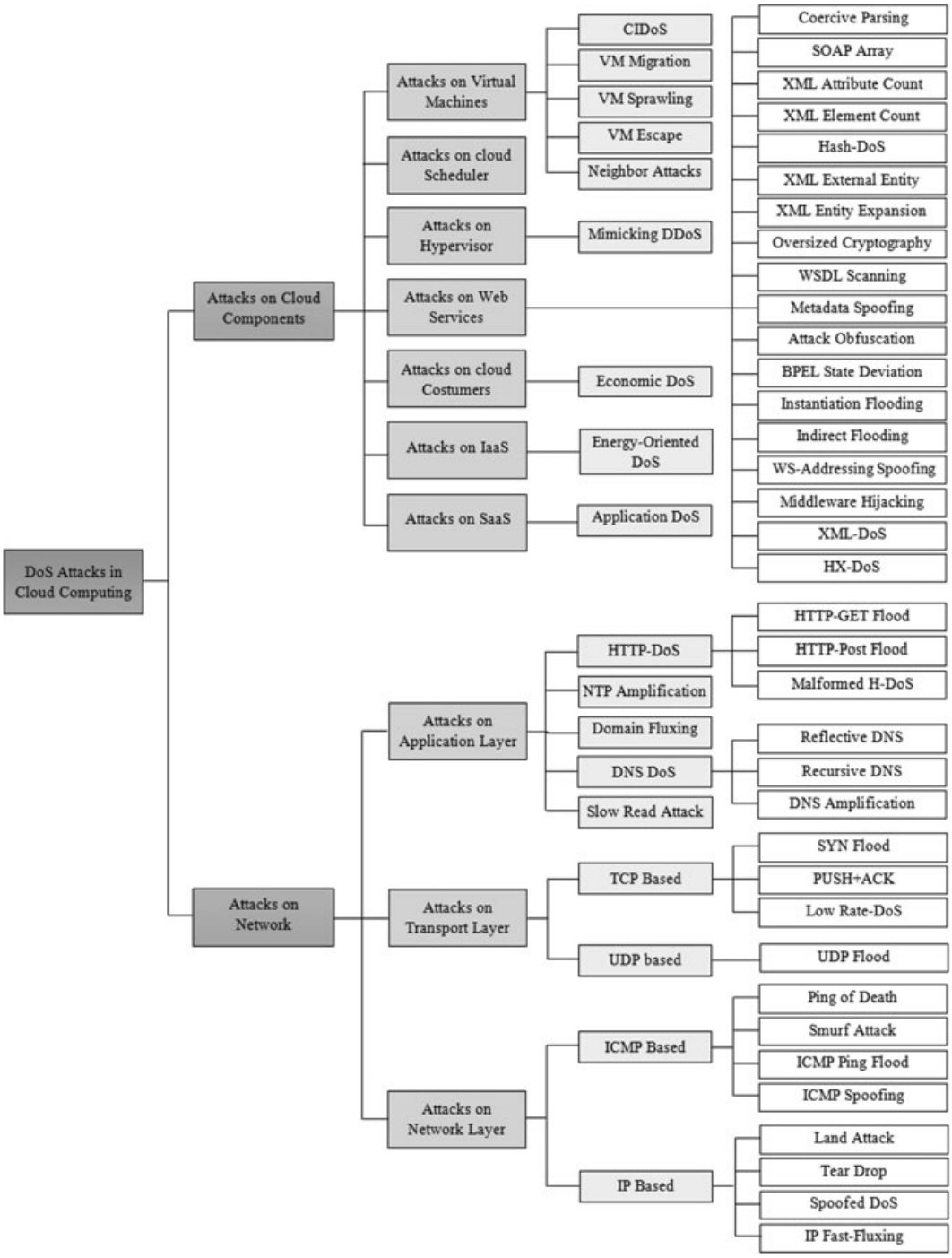

Figure 6. Classification of the denial-of-service (DoS) attacks in the cloud computing environment.

3.3. Attacks on cloud customers

In economic denial of sustainability (EDoS) attack, the attacker sends many fake requests to the cloud services and increases the load on the cloud to increase the user's bill. EDoS attack depends upon the server configuration, resources available for the cloud users, and the affordability of the resources [48–50]. Cloud services are provided in the form of SLA, which define the level of service required by the user [51]. EDoS attacks are more harmful to SLA and to meet the SLA, cloud service providers activate more resources for the availability of the service to the attacked user, which causes extra cost [52]. Table II indicates the different attacks on cloud components.

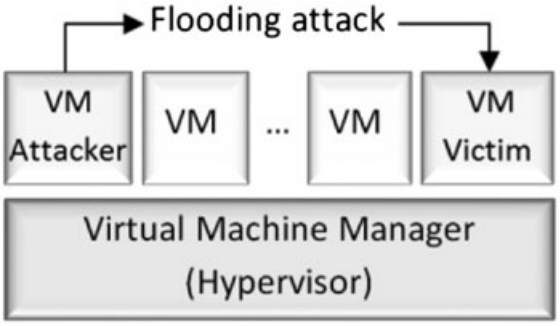

Figure 7. Neighbor attacks between virtual machines (VMs).

3.4. Attacks on cloud scheduler

Virtual machine monitor or hypervisor can manage several VMs, but its scheduler may be vulnerable to the malicious behaviors of the VMs, and this may result in an unfair or inaccurate scheduling. For example, Xen is an open-source VMM for the ×86/×64 platform, which uses a scheduling mechanism that may fail to account for CPU usage by poorly behaved VMs. Fangfei *et al.* in [35] introduce a vulnerability in Amazon's Elastic Compute Cloud (EC2), which allows malicious customers to obtain enhanced service at the expense of others. They have found that the applications, which exploit this problem, are able to utilize up to 98% of a CPU core, regardless of competition from other VMs. To solve this problem, Amazon Elastic Compute Cloud uses a patched version of Xen [53].

3.5. Denial-of-service attacks on software as a service

Application DoS attacks concentrate on software as a service clouds. They exploit flaws in the applications to prevent legitimate access to the victim's different services. These attacks are harder to trace back, and the existing security monitoring solutions may not detect them. Often, these attacks use HTTP or HTTPS protocols and apply proxy servers to obfuscate the origin of the attacker [54].

3.6. Denial-of-service attacks on infrastructure as a service

Energy-oriented DoS attack is a new kind of security attack that can seriously affect the cloud infrastructures and data centers to waste energy as much as possible. The malicious activities of this attack cause a high workload on the target and keep them fully busy. The results of this attack are the increased costs of the energy consumption and penalization because of the greenhouse gas emissions for the cloud providers [55].

3.7. Denial-of-service attacks on web services

Web services are software components that utilize various XML-based protocols and standards such as Simple Object Access Protocol (SOAP) to exchange data. The common DoS attacks conducted against the web service are as follows:

- Coercive parsing attack: In this attack, highly nested XML documents are sent to the server that may cause memory errors or even a high CPU usage when a Document Object Model-based parser processes them [56].
- SOAP array attack: It forces the web service to send very large SOAP messages [57].
- XML attribute count attack: SOAP messages with high number of attributes are sent to the server.
- XML element count attack: SOAP messages with many nonnested elements are sent to the server [56].
- Hash collision attack (Hash DoS): Large POST filled with many form variables is sent, which need hash-related processing [58].
- XML external entity DoS: It forces the server to resolve a large external entity defined in a document-type definition [59].
- XML entity expansion: Known as "XML bombing", it causes by misusing the nesting capability of XML [60].
- Oversized cryptography: Attacker attaches large amount of the encrypted or digitally signed fragments in messages [61].

Table II. Attacks on the cloud components.

Attack	Protocol vulnerability exploitation	Spoofing	Using VM migration	Incurring high load	Flooding	Gain access to hypervisor
VM migration	–	–	✓	✓	–	–
CIDoS	✓	–	–	✓	–	–
VM sprawling	–	–	–	✓	–	–
Neighbor attacks	–	–	–	✓	–	–
VM escape	–	–	–	–	–	✓
Mimicking DoS	–	–	–	–	–	✓
EDoS	–	✓	–	✓	✓	✓
ADoS	✓	–	–	–	–	–
Energy-oriented DoS	–	–	–	✓	–	–

VM, virtual machine; CIDoS, cloud-internal denial of service; DoS, denial of service; EDoS, economic denial of service; ADos, application denial of service.

- Web Services Description Language (WSDL) scanning: WSDL is an advertising method for web services to specify the parameters used to connect the specific methods. The information specified by a WSDL interface reveals sensitive information, which allows the attacker to launch other attacks [62].
- Metadata spoofing: This attack is aimed to reengineer the web service's metadata descriptions [63].
- Attack obfuscation: It uses XML encryption to mask message content from being inspected by the firewall or IDS. These encrypted contents can be used to launch other attacks such as oversize payload, coercive parsing or XML injection, and encryption [64].
- Business Process Execution Language (BPEL) state deviation attack: BPEL engine can provide the web service endpoints, which accept the service request. Each BPEL process has more than one process instance; thus, the endpoints will be able to accept the request messages at all times. An attacker can send a flood of request not related to any existing process instances [65].
- Instantiation flooding attack: When a new request message arrives, a new instance of the BPEL process is created and executes the instructions given in the process description. An attacker can attack the BPEL engine by sending a flood of requests to a BPEL process [65].
- Indirect flooding: This attack is possible because of the compositionality feature of the web service. If a web service composition is targeted with a flooding attack of valid requests, it will create workflow contexts for every incoming message; thus, it will start executing a huge amount of workflows, concurrently. Each of these workflows causes calling other web services, and the BPEL engine causes a flooding of the requests at these web services, too [66].
- Web Service (WS)-addressing spoofing: The SOAP requests sent to the server contain a WS-addressing header, which causes the server to issue the SOAP response for a different endpoint used to flood another web service [67,68].
- Middleware hijacking: This attack applies WS-addressing spoofing, but it points the attacker's endpoint URL to an existing target system running a real service at the URL specified. As a result, the web service server will repeatedly try to answer the attacker's requests [56].

3.7.1. XML-based denial-of-service attacks

XML-based DoS (X-DoS) attacks send flooding XML messages to a web service to use up all the server side resources. DX-DoS attacks are the distributed version of the X-DoS attacks, which use multiple hosts to launch the attack [69]. In this attack, often the message content is manipulated to cause a crash in the web server. Because of the complexity of XML documents and parsing them, even a small malformed XML message can consume large number of server resources [57].

3.7.2. HX-DoS attacks

The cloud web services operate based on the HTTP and XML protocols such as SOAP. One of the threats that the cloud provider struggles with is the HX-DoS attack or HX-DDoS attack, which operates based on the HTTP and XML protocols [70]. HX-DoS attack is a combination of HTTP and XML messages that are used to flood the communication channel of the cloud provider. To address the problem of HX-DoS attacks against the cloud web services, the illegitimate messages should be distinguished [71]. The comparison of the attacks on the web services is shown in Table III.

4. DENIAL-OF-SERVICE ON THE CLOUD NETWORKING INFRASTRUCTURE

This section analyzes DoS attacks conducted against the networking infrastructure of clouds and classifies them based on the network layer, which they target.

4.1. Denial-of-service attacks on the application layer

Because the services provided by the cloud are mainly supported by using the application layer, this layer's protocols have been focused by many DDoS attacks. The application layer-based DDoS attacks are major threats to the security of the cloud computing and harder to detect because the monitoring techniques should perform deep packet inspection of the received packets.

Also, sometimes these attacks use techniques such as protocol specific proxies and content encryption to make the attack detected tracing back the operations more difficult.

4.1.1. HTTP-based denial-of-service attacks

One of the critical threats to the web-based applications is the HTTP-based DoS (H-DoS) attack [72] that attackers break through the web proxy restrictions using the attack browser program and launch the H-DoS attack on the web server. Web server cannot detect malicious client penetrate through the web proxies because of the hidden information of attacker identity [73].

4.1.1.1. Malformed HTTP-based denial-of-service attacks. In these DoS attacks, the attacker floods the victim by sending HTTP messages, which contain malformed elements with the malformed fields. This attack may cause the vulnerabilities, such as buffer overflow or other security problems. Moreover, it requires smaller traffic than H-DoS and may be considered as normal flow. However, detecting malformed H-DoS is more costly than detecting regular H-DoS, because IDS must apply deep

Security Comm. Networks 2016; **9**:3724–3751 © 2016 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

Table III. DoS attacks on web services.

Attack	Protocol vulnerability exploitation	Malformed packet	Spoofing	Flooding
X-DoS	✓	✓	✓	✓
Coercive parsing attack	–	–	–	✓
SOAP array attack	–	–	–	✓
XML attribute count attack	–	–	–	✓
XML element count attack	–	–	–	✓
Hash collision attack (Hash-DoS)	–	–	–	✓
XML external entity DoS	–	–	–	✓
XML entity expansion	–	–	–	✓
Oversized cryptography	–	–	–	✓
WSDL scanning	–	–	✓	–
Metadata spoofing	–	–	✓	–
Attack obfuscation	–	–	–	–
BPEL state deviation attack	–	–	✓	✓
Instantiation flooding attack	–	–	–	✓
Indirect flooding	–	–	–	✓
WS-addressing spoofing	–	–	✓	–
Middleware hijacking	–	–	✓	✓

XDoS, XML-based denial of service; SOAP, Simple Object Access Protocol; DoS, denial of service; WSDL, Web Services Description Language; BPEL, Business Process Execution Language.

packet inspection (DPI), which consumes a lot of computing resources. Also, performing the deep packet inspection prolongs the delay of HTTP requests and reduces the quality of service (QoS) of HTTP services [74].

4.1.1.2. HTTP-GET flood attacks. In this attack the attacker utilizes HTTP-GET request of HTTP protocol to send a large number of malicious requests to a target server. Because these GET request packets have legitimate HTTP payloads, firewalls, and IDS located at the victim cannot distinguish them and processes all of them whose resources this issue exhausts [75]. Attacks on the application layer are compared in Table IV.

4.1.1.3. HTTP-POST flood attacks. In this attack, a flood of HTTP-POST messages is sent to the victim. Generally, a POST request contains a message body, which can use any encoding. The attacker first sends the HTTP header portion in full to the web server. Then, he sends HTTP message body in sequences, for example, one byte per 110 s. The web server obeys the content-length field in the HTTP header and waits for the remaining of the message body to be sent and such type of connections may cause DDoS attacks [76].

4.1.2. Domain Name System-based denial-of-service attacks

Domain Name System is vulnerable to the spoofing-based DDoS attacks. In this case, a server cannot tell whether a request packet really comes from the IP address as indicated in the request or not. Spoofed attacks result in DoS attack, which may overload the DNS servers themselves or saturate the victim's bandwidth via the amplified DNS responses [77].

4.1.2.1. Reflective Domain Name System attacks. The reflective DNS attacks do not target the DNS servers themselves, but utilize them to conduct attack against another system whose IP address is spoofed in the DNS queries. As shown in Figure 8, in the reflective DNS attack, DNS requests are issued to the DNS servers, which forward their response to the victim. However, this

Table IV. DoS attacks on application layer.

Attack	Protocol vulnerability exploitation	Malformed packet	Spoofing	Reflection	Amplification	Flooding
H-DoS	✓	–	–	–	–	✓
HTTP-GET flood attack	–	–	–	–	–	✓
HTTP-POST flood attack	–	–	–	–	–	✓
HX-DoS	✓	–	–	–	–	✓
Malformed H-DoS	–	✓	–	–	–	✓
DNS server DoS	–	–	✓	✓	✓	–
NTP amplification	–	–	–	✓	✓	–
Domain fluxing	–	–	–	–	–	✓
Slow read attack	–	–	–	–	–	✓

H-DoS, HTTP-based denial of service; DoS, denial of service; DNS, Domain Name System; NTP, Network Time Protocol.

response is amplified, and its size is larger than the DNS requests [16].

4.1.2.2. Recursive Domain Name System attacks. Recursive DNS attacks target the DNS servers themselves and reduce their availability for the network users. These attacks take advantage of recursive DNS querying and issue numerous DNS requests for non-existent domain names to the victim DNS server, which consequently are not found and require further processing and communication, causing more resource exhaustion [16].

4.1.2.3. Domain Name System amplification attacks. The target of this attack is not the DNS servers but another victim system, which is specified in the source IP address of the attack packets. In DNS amplification attack, the attacker can direct a large volume of network traffic to the victim by sending DNS queries. In this attack, the attacker spoofs the IP address of the victim to direct the DNS server response message to it [78,79]. For this purpose, a flood of DNS queries of a type called "ANY" is sent to an authoritative or non-authoritative DNS server. This returns all the information about a DNS zone. To increase the traffic, attackers can use botnets for creating a large number of spoofed DNS queries [80].

4.1.3. Network Time Protocol amplification attacks

Network Time Protocol is prone to the amplification attacks because one of its commands sends a long reply to a short request, which makes it ideal for DDoS attacks. NTP contains a command called monlist (MON_GETLIST), which can be sent to an NTP server for monitoring purposes. It returns the addresses of up to the last 600 machines that the NTP server has communicated. This response is much bigger than the request, making it ideal for the amplification attacks [81].

4.1.4. Domain fluxing

In this attack, each bot generates many domain names and starts to query them until one is resolved. Afterwards, the bot contacts the corresponding IP, which is used to host the C&C server. Thus, for various attack components such as C&C random domain names are generated to avoid detection [82].

4.1.5. Slow read attack

In this attack, the attacker sends legitimate application layer requests but it reads responses very slowly by advertising small TCP receive Window size to conduct a slow communication with the destination. If the attacker can send many requests for a web server, it will reach its maximum capacity and may become unavailable for new requests [83].

4.2. Attacks on transport layer

Denial-of-service attacks on this layer can be classified as TCP-based attacks and UDP-based attacks.

4.2.1. Transmission Control Protocol-based denial-of-service attacks

Various features of TCP protocol are used to launch DoS attacks. The most common TCP-based DoS attacks are as follows:

- SYN flood attacks
- PUSH + acknowledgement (ACK) attacks
- Low-rate DoS (LDoS) attacks

SYN flood is a DoS attack targeting the availability of web servers [84]. As shown in Figure 9, these attacks occur when a host sends a flood of TCP/SYN packets, with a fake sender's address. Each of these packets is handled as a connection request, which causes the server to create a half-open connection, by transmitting a TCP/SYN-ACK packet and waiting for a packet in response from the fake sender, which never comes. These half-open connections saturate the number of available connections that the server can make and must be kept for at least 75 s in the queue and as a result, newer connections cannot be accepted temporarily [85].

In PUSH + ACK attack, the server is flooded with the IP packets whose PUSH or ACK bits are set [86]. These packets

Figure 8. Reflective Domain Name System (DNS) attack.

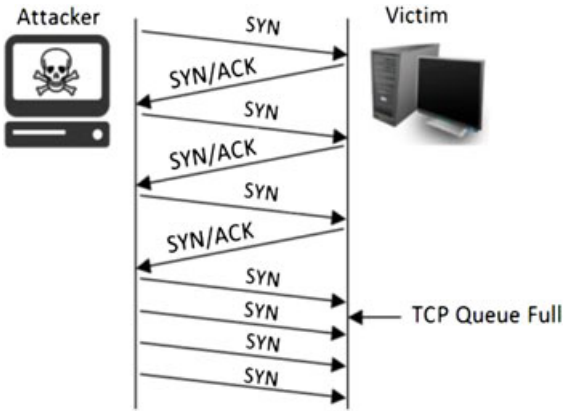

Figure 9. SYN flood attack.

cause the victim to unload all the data in its TCP buffer and send an acknowledgement. If multiple agents repeat this process, then victim system will not be able to process the large volume of such incoming packets and may crash [87].

A low-rate DDoS (LR-DDoS) attack is an intelligent attack that saturates the victim by packets with a low rate to avoid the anomaly based IDS systems. LDoS is also known as the "shrew attacks" [88] and is conducted by the attacker in the ON/OFF pattern, so that the victim may not block them. The attacker will send large number of the same requests from the same sources to the victim to degrade its performance. LDoS attack [89] can be divided into attack on the TCP protocol, and attack on the Active Queue Management mechanism of routers [90]. TCP's deterministic retransmission time-out mechanism is vulnerable to periodical low-rate DoS traffic [91].

4.2.2. User Datagram Protocol-based denial-of-service attacks

In UDP-based flooding, many UDP packets are sent to the random or specified or random ports on the victim to saturate it in the traffic. When the victim processes these incoming data, if there is no application on the specified port, the victim sends a "destination unreachable" message back. However, to hide the identity of the attacker, the previously outlined solutions such as the source IP address spoofing are used by the attackers [92,93]. Table V shows the attacks on the transport layer.

4.3. Attacks on network layer

Network layer DoS attacks misuse the IP and ICMP protocols to attack the victim. The attacks on network layer and types of the attacks are shown in Table VI.

4.3.1. IP-based denial-of-service attacks

One of the major problems faced by the Internet hosts is the DoS attacks caused by IP packet flooding [94]. Some IP-based DoS attacks are as follows:

- LAND attack: Which is similar to SYN flood, but in this attack the SYN packet source address and the destination address are both IP address of the targeted server, which may cause the server to lock up [95].
- Teardrop: Where the mangled IP fragments are sent with overlapping, oversized payload data packets to the victim [54].

4.3.1.1. IP-spoofed denial-of-service attack. In the IP spoofing DoS attack, the attackers employ spoofing to misrepresent the source IP address of DoS packets and to obscure its identity [96]. In general, when the attackers and victims are positions in the different networks the victim cannot distinguish between the spoofed packets and the legitimate ones, so the victim should respond to the spoofed packets like the others. These response packets, which are produced for the spoofed IP packets are often known as "backscatter" [97].

4.3.1.2. IP fast fluxing. IP fast flux is a method to frequently change the IP address, which belongs to a domain name. This method prevents the detection of botnets and the C&C server. Networks, which utilize the fast-fluxing techniques, are called as fast-fluxing networks. Fast fluxing can be classified into the following categories:

- Single flux: A domain is resolved to different IPs in different times.
- Double flux: It is a more sophisticated way of counter-detection and involves the repeated changing of both the flux agents and the registration in DNS servers.

Fast-fluxing network techniques are applied by attackers to maintain their attacking components hidden from the victim's security elements, which try to trace back [98].

4.3.2. Internet Control Message Protocol-based denial-of-service attacks

Internet Control Message Protocol is one of the popular protocols, which has been utilized in various DoS attacks [99,100]. Some of the ICMP-based flooding attacks are as follows:

- ICMP ping flood attack
- Ping of death attack
- Smurf attack
- ICMP spoofing attack

In ICMP ping flood, attacker spoofs the source IP address and sends huge number of ping packets, usually using ping command to the victim [101]. By sending a flood of such requests, resource starvation usually happens on the host computer [102]. A simple ping-based DDoS attack can exhaust the victim by making it busy with the ping requests.

Table V. DoS attacks on transport layer.

Attack	Malformed packet	Spoofing	Reflection	Amplification	Flooding
ACK attack	–	✓	–	–	–
SYN flood	–	✓	–	–	✓
PUSH + ACK	–	✓	–	–	✓
LDoS	–	–	–	–	✓
UDP flood	–	✓	–	–	✓

ACK, acknowledgement; DoS, denial of service; LDoS, low-rate denial of service; UDP, User Datagram Protocol.

Table VI. DoS attacks on network layer.

Attack	Protocol vulnerability exploitation	Malformed packet	Spoofing	Reflection	Amplification	Flooding
LAND attack	–	–	✓	–	–	✓
Teardrop	–	–	✓	–	–	✓
Spoofed DoS	–	–	✓	–	–	–
IP fast fluxing	–	–	–	–	–	–
Ping of death	✓	✓	–	–	–	–
Smurf attack	–	–	–	✓	✓	✓
ICMP ping flood	–	–	✓	–	–	✓
ICMP spoofing	–	–	✓	–	–	–

LAND, local area network denial; DoS, denial of service; ICMP, Internet Control Message Protocol.

Ping of death is another ping-based DoS attack, which involves sending a malformed or otherwise malicious ping to a computer. Some systems could not correctly handle a ping packet larger than the maximum IPv4 packet size of 65 535 bytes and try to reassemble the packet, which may cause buffer overflow error and system may crash [103,104].

Smurf attack is an ICMP-based amplification attack that the attacker uses unprotected intermediate networks to amplify the attack traffic [105]. As shown in Figure 10, first the attacker sends one ICMP echo request packet to the network broadcast address, which is forwarded to all hosts within the intermediary network and they send the ICMP echo replies to the victim [99].

5. DEFENSE AGAINST DENIAL-OF-SERVICE ATTACKS

As DoS attacks become more common against the cloud computing, a greater need is sensed for solutions to deal with such important attacks. Generally, defense against DoS attacks can be divided into the three main categories, which are attack prevention, attack detection, and attack response (Figure 11) [106]. This section discusses the solutions, which have been proposed in the literature to prevent, detect, or deal against various types of DoS attacks. Attack prevention methods are aimed to prevent DoS attacks to happen or at least mitigate their effect. For this purpose, some schemes try to protect the cloud services from attackers by adding intermediate components, which should deal with the clients' request for the cloud services. When they recognize that the request is valid, the access is granted, otherwise it is dropped. However, attack detection methods permit the Dos attacks to happen and then detect them. Often, these schemes learn the attack pattern and try to prevent the future similar DDoS attacks.

Often, the DDoS attack detection process is differentiating between the flash crowd (legitimate traffic) and the attack traffic. Generally, flash crowd is a sudden spike in the request for a cloud service, which is issued by legitimate users simultaneously. Flash crowd may overwhelm the cloud services and decrease their performance [72]. After a kind of DoS is detected to happen against the cloud, some actions should be performed to prevent or mitigate its effects. To mitigate BW-DoS attacks, solutions such as rate-limiting/throttling, filtering, and changing the topology are proposed in the literature [22]. The following techniques are applied in these methods:

- Limiting the connections per IP address
- Limiting the requests per IP address

To be effective, the DDoS detection process should have low false positive and low false negative. In false positive, a flash crowd is detected as DoS attack, and in false negative, a DoS attack is not recognized and the attack traffic is assumed to be a flash crowd. However, false positive

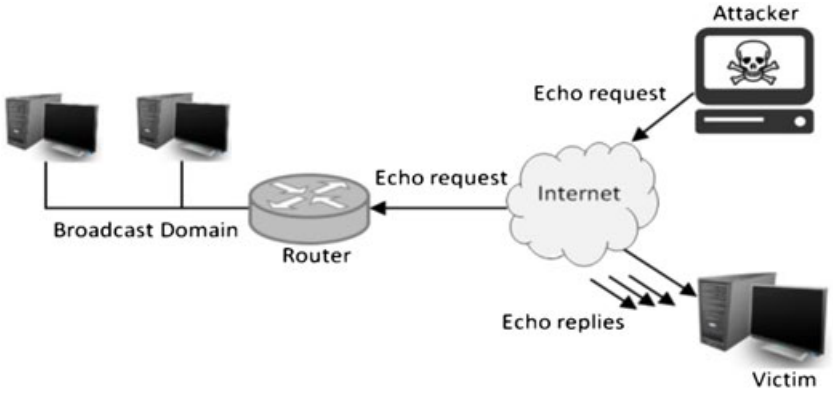

Figure 10. Architecture of smurf attack.

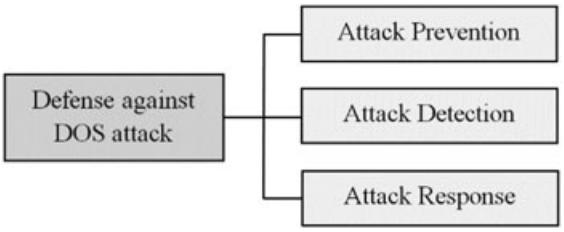

Figure 11. Defense types against DoS attacks.

problem has more negative effects on the availability of the cloud resources because without any DoS attack on the cloud, DoS attack handling mechanism itself acts as a DoS attacker and denies the cloud resource to the cloud customers.

Also, after a DoS attack is detected to happen on the cloud, some security solutions are aimed to detect the source of DDoS attacks and try to trace back and detect various attack components such as the bots, C&C server, or ideally the attacker itself. One important factor in the DoS handling schemes is the location, which DoS attack handling component is placed. Often, the security components of these schemes should be positioned at the following locations:

- At the victim's system
- At the victim's network
- At the edge of the victim's network
- At the network or Internet routers
- At the edge of the attacker's site

Also, in the cloud servers, the proposed security mechanisms can be placed in different locations such as the VMM, VM, and host OS or it can be distributed between all of them. However, when the security mechanism is located in VMM, it can get accurate system state from lower level to monitor privileged entities in guest OS because the VMM has higher privilege than guest OS. Ideally, defense solutions proposed against the DoS attacks in the cloud computing should have these properties:

- Low processing overhead
- Low bandwidth consumption
- Low impact on the network and its services
- Less modification to the existing protocols
- Need for fewer networking hardware
- Minimum additional software components
- Minimum number of cooperating nodes
- High scalability
- Low deployment cost
- Effectiveness in public and private clouds
- Adaptability to network topology changes
- Low false positive and false negative in detecting DoS attacks

Because DDoS attack mitigation poses a challenge, more stress should be laid on the prevention of such attacks. This would require more conscious effort to be put into the security of an organization and its internal networks. Each organization should come up with a security policy, which is dedicated to DDoS attack prevention and mitigation. There should be explicit mentioning of the steps that are to be taken before, during, and after a DDoS attack.

- Before the attack: The first step to prevent a DDoS attack is to prevent compromise and use of hosts as agents. To achieve this, the network should be guarded by the firewall.
- During the attack: it becomes difficult or impossible for the sysadmins to acquire access to the routers and servers of their network.
- After the attack: An intrusion response team should be in place to identify the type of attack. This analysis can aid in tracking down the hosts that form the DDoS network so that they can be shut down [107].

In the rest of this section, we discuss the defense solutions presented against the main DoS attacks.

5.1. Defense against economic denial of sustainability attack

In [108] Ramana *et al*. propose DDoS and EDoS shield which checks each request's source. It uses virtual firewalls and the verifier cloud nodes (V-Nodes) in which the virtual firewalls filter based on the black listed IP addresses updated by the verifier cloud nodes and is a VM that has filtering and routing capabilities. The virtual firewall holds a white list and a blacklist. The white list is applied for tracing the acknowledged source IP addresses that pass the firewall, and the blacklist is utilized for holding unauthenticated IP addresses that will be eliminated. If the request gets confirmed, then the source IP address is added to the white list, otherwise the blacklist is updated.

The authors in [109] present the EDDoS mitigation service. As depicted in Figure 12, in this scheme, first the client sends its request to the service provider, then the resource depletion acceptable limit is compared with the resource consumption threshold limits, and if resource depletion acceptable limit is bigger than this threshold, k-bit puzzle is given to the clients. Then, the client solves the puzzle and returns it. If the puzzle is solved, the request is forwarded to the service provider; otherwise, the puzzle hardness should be increased.

Masood *et al*. in [52] propose a defense mechanism called EDoS armor, which is a twofold solution consisting of admission control and congestion control. First, they restrict the number of users that can simultaneously issue requests, allowing enough clients that can be served easily within the existing resources on the web server. Then, the precedence of the allowed users is changed based on the type of resources, which users use and the type of operations they do, and make the system resources available to good users and limit access for bad users.

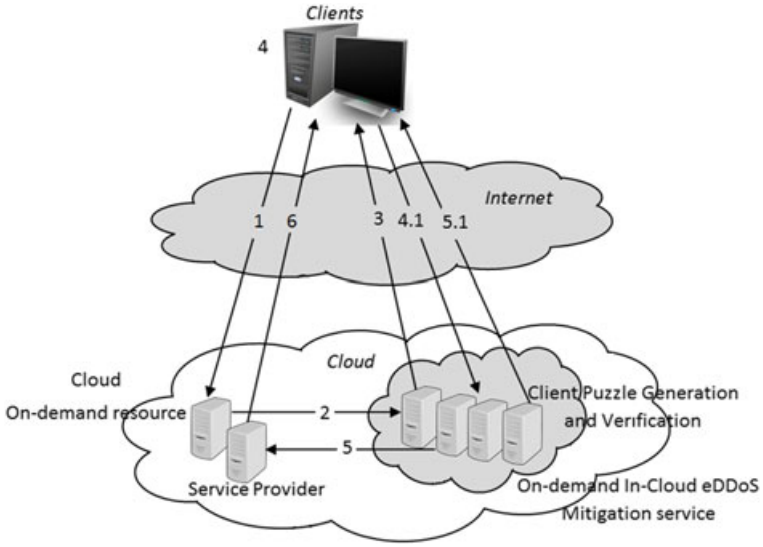

Figure 12. Scrubber service.

Alosaimi *et al*. in [110] present the DDoS-mitigation system used to deal with EDoS attacks by testing two packets from the source instead of testing all the received packets. Moreover, they use two types of tests for the user and packet authentications. This scheme applies a firewall, a verifier node, a client puzzle server, green nodes, and a router for filtering. White and black lists exist in firewall for the sources of packets related to the verification procedure. Green nodes conceal the position of the protected server, which receives only the packets sent by these nodes through the filtering router. The router sends the packets that come from the green nodes and denies other packets.

5.2. Defense against cloud-internal denial-of-service

In [39] Alarifi *et al*. introduce signals processing-based mitigation strategies against the cloud-specific CIDoS attacks. The main strategy to detect the attack is the computation of connection measurement and distances between attackers workload patters; discrete cosine transform is used to fulfill this task. They also suggest some prevention and response strategies and use one dimensional discrete cosine transform and Euclidean distance to measure the correlation between malicious VMs workload patterns.

5.3. Defense against virtual machine migration

AMAD framework is designed by Lazri *et al*. in [38] to detect anomalies in the use of dynamic VM migration. AMAD detects the occurrence of abusive VM migration attack and pinpoints the VMs at the origin of the attack. AMAD collects resource consumption-related metrics at the hypervisor level and runs without any help from the running VMs.

By exploiting the under-provisioning, Liu *et al*. in [111] indicate how an adversary can bring down a subnet in the cloud data center with a minimal cost. Even against the counter-measures against large-scale attacks, a smaller scale attack is still possible because an attack differs from a normal bandwidth-hungry application only by intent. They propose dynamic migration architecture, which applies the dynamic provisioning feature of a cloud to detect and prevent similar kind of DoS attacks.

5.4. Defense against layer 7 attacks

A mechanism called defense and offense wall (DOW) is proposed in [112], which defends against layer 7 DDoS attacks. An anomaly detection method based on K-means clustering is applied to detect and filter the request flooding and asymmetric attacks. To defend against session-flooding attacks, an encouragement model is proposed that uses the client's session rate as currency. Detection model drops doubtful sessions, and currency model amplifies more legitimate sessions. By using these models, normal clients could achieve a higher service rate and lower delay of response time.

5.5. Defense against XML-based denial-of-service

Santhi *et al*. in [113] introduce a distributed defense filter called XDetector. DPM methodology is applied to the service-oriented traceback mark (SOTA) framework by placing the service-oriented traceback mark (SOTM) within web service messages. If any other web security services are already employed, SOTM would replace the token that has the client identification. Real source message identifications are stored within SOTM and located inside the SOAP message. The structure of SOTM is made up of one XML tag so as not to weigh down the message

and stored within a SOAP header. Upon discovery of an XDoS or DXDoS attack, SOTM can be used to identify the true source of fake messages. In this architecture, service oriented trace back mark is available. It contains a proxy that marks the incoming packets with source message identification to identify the real client. Then, the SOAP message travels via XDetector. The XDetector is used to monitor and filter DDoS attacks such as HTTP and XML DDoS attack. Finally, the filtered real client message is transmitted to the cloud service provider, and the corresponding services are given to the client in a secured way [114].

To defend against HTTP or XML-based DDoS attacks, a solution called filtering tree is presented by Karnwal *et al*. in [115], which operates like a service broker within a SOA model. It converts the client's request to XML tree form and uses a virtual cloud defender to protect from these types of attacks. In this scheme, the cloud defender is responsible to detect the suspicious message, detect HTTP DDoS attack, and detecting coercive parsing/XML DDoS.

A SOA-based scheme is proposed in [116] by Xinfeng *et al*., which prevents the DoS attacks by hiding the web services providers from public and authenticating the request messages. This scheme operates in the normal and the under-attack modes. In the normal mode, an operations provider detects no attack; otherwise, it operates in under-attack mode when the requests should be authenticated. As Figure 13 indicates, in this scheme, an operations provider subscribes to a ServiceHub, and the public perceives its operations as being hosted by the ServiceHub.

Packet-based marking can detect HDoS or X-DoS attacks on the attacker side and is able to filter the detected packets.

In [71] attack messages can be detected by using the rule set-based detection, called CLASSIE. Also, the packet marking method is used to avoid the spoofing attack. CLASSIE should place one hop away from the host, and its rule set should be created over time to recognize the known HDoS and X-DoS messages. CLASSIE is able to identify the attributes of known HX-DoS attacks such as XML injection attack or XML Payload Overload attack. The packet that matches the rules is dropped by the CLASSIE upon the detection of HX-DoS. After tested by the CLASSIE, packets are marked on the edge and core routers. At the edge router, one bit is required for demonstrating that the packet and a few other bits for marking code are marked.

To detect XML vulnerabilities, in [117] Sarhadi *et al*. provide CSQD, which should be placed close to the ingress router. This scheme uses a trace back solution to detect the attack source and when an attack is launched against the server, it adds the information of request to its database to prevent the future attacks. When a client sends a request, it is checked whether the server is up or not. For normal conditions, the request is forwarded to the XML Vulnerability Detection System to check the request for XML attacks. Afterwards, when no negative response is received, it is directed to the request scheduling. When an attack is detected, it is sent to the Response System. This system prepares a suitable message and inserts the sender's IP address into the blacklist database. After request processing, the web service directs the results to check response, which accredits the response and deletes the processed request from its list.

5.6. Defense against HTTP-based denial-of-service

Choi *et al*. in [118] propose an integration of HTTP-GET flooding and MapReduce processing methods for fast attack detection in the cloud computing. In this scheme, the suspected IP of the DDoS attack gets challenging values. Then, IP by a normal reply is allowed a connection, but suspicious IP is filtered over a period of time. Whether

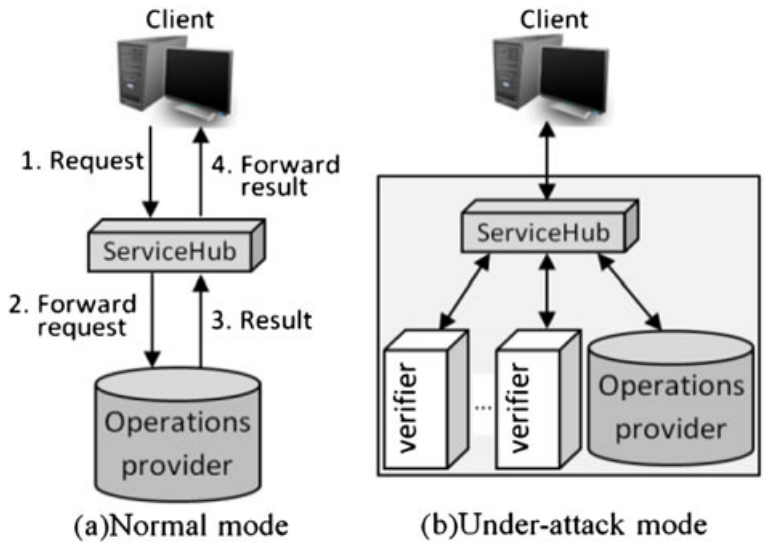

Figure 13. A system against distributed denial-of-service (DDoS) and XML-based denial-of-service (XDoS) attack.

TCP connection depletion occurs is checked, and the existence of huge number of HTTP requests is confirmed. The detection of a DDoS attack through a packet analysis uses the input values of MapReduce for a strange detection rule analysis using a statistical analysis and threshold. GET flooding can be caused by the traffic of normal users and botnets. These traffics can be recognized by the calculation of the GRPS (GET request per second) because normal users do not recurrently request the same page at the same time.

To deal with malformed HTTP headers, in [74] Wang *et al*. present a solution called Fast malformed Http message Detection Algorithm (FHDA), which gives priority to the more frequent malformed elements and tunes the detection priority of each field according to the previous detection results. This scheme is able to complete the detection in a shorter time by maintaining the detection accuracy. It is suitable for the cloud platform, which usually responds to the intensive HTTP requests and provides high QoS.

5.7. Defense against Domain Name System attacks

In [119] Herzberg *et al*. introduce DNS authentication system, which consists of request–authentication and resolver–authentication phases. The request–authentication phase filters the requests sent from the spoofed IP addresses, and tries to detect amplification DoS. Resolver–authentication identifies compatible resolvers and maintains a list of potentially compromised hosts. They propose an anti-reflection method, which prevents the amplification factor of DNS responses when the server is abused for the amplified DoS.

5.8. Defense against SYN flooding

SYN flooding is launched against the TCP protocol and many defenses have been proposed to deal with that [120]. In [121] authors propose the following solutions to deal with SYN flood attacks:

- Ingress filtering
- Firewalls and proxies: A firewall or proxy protects systems and network from SYN flooding, which spoofs SYN-ACKs to the initiators or spoofs the ACKs to the listener.
- Active monitors.

Generally, solutions designed to deal with the SYN attacks can be classified as network-based and end point-based solutions. Network-based solutions such as firewall proxies only forward the connection request after the client side ACK is received. The end point-based solutions include SYN cookies and SYN caches, which allocate the minimum amount of data required when a SYN packet arrives and only allocate full state when the client's ACK arrives [121]. SYN cookies allocate no state at all until the client's ACK arrives. For this purpose, the connection states are encoded into the TCP SYN-ACK packet's sequence number. On receipt of the ACK, the state can be recreated by the ACK's header information [120].

In [3] Udendhran *et al*. propose a framework, which monitors the flow of SYN packets by using a correlation engine or a flow traffic tool like snort or wireshark. To detect the attack source, TTL and packet marking techniques are used and a honeypot method is applied for the prevention.

Also, Siris *et al*. in [122] study statistical anomaly detection to detect SYN flooding and presents an adaptive threshold algorithm and a special application of the cumulative sum algorithm for the change point detection. Both algorithms detect changes in some statistic of the traffic flow, based on the measurements of the statistic in consecutive intervals of the same duration.

5.9. Defense against the low-rate denial-of-service attacks attacks

Random early detection (RED) is applied for active queue management, and when the average queue length exceeds the maximum threshold, it randomly drops the packets to control the average queue length. LDoS attack on the RED affects all the links connected to router through sending pulse high-intensity attacks to the router periodically. It is found that the fair random early detection algorithm can effectively resist the non-adaptive flows' LDoS attacks. For example, Ma *et al*. in [90] improve RED algorithm based on the two characteristics of LDoS attack. The first one is that the strength of each attack is very high. Most of the queue space is occupied by attack data stream. The second is that attack pulse has cycles. This scheme improves the RED algorithm to identify LDoS attack and take appropriate treatment.

5.10. Defense against the IP spoofing

Guo *et al*. in [77] propose spoof detection solutions to protect DNS servers from DoS attacks. In these strategies some kind of cookies is created for DNS server to check that the incoming requests are actually from the specified source or not. These are performed as a firewall module called DNS guard. Measurements on the DNS guard prototype indicate that it can deliver up to 80 K requests/s to legitimate users in DoS attacks at a rate of 250 K requests/s. By using this scheme, when the spoofed requests are identified, a DNS server can drop the spoofed requests without any collateral damage.

To solve the spoofed source IP address problem, Yaar *et al*. in [123] propose a new packet marking scheme called "path identifier," which includes a path fingerprint in the packets that enables the victim node to identify packets, which are forwarded through the same paths in the Internet on a per packet basis. By using this information, the victim can detect packets matching the attackers' identifiers on a per packet basis. But in PI scheme, routers should take part

in packet marking, and it is practical when only half of the network routers participate in this process.

Although an attacker can forge any field in the IP header, he cannot forge the hop count of the attack packets. Moreover, an attacker cannot randomly spoof IP addresses while preserving constant hop counts. In [124] Chouhan *et al*. store hop-count value to prevent DOS attack in the cloud environment. The server can recognize legitimate IP packets from the spoofed ones by using a mapping between IP addresses and their hop counts.

In addition, Wang *et al*. in [125] present a new and easy to deploy filtering method, called hop-count filtering, which does not need any support from the underlying network. It builds a precise IP-to-hop-count mapping table to detect and discard the spoofed IP packets.

5.11. Defense against the distributed denial-of-service attacks

5.11.1. General defense

In [126] Siqin *et al*. present a defense scheme against DoS attacks, applied in VMM. In this scheme, VMM can monitor how much operating system uses resources and can lively migrate the guest operating systems. The defending system adds the function of monitoring the available resources into VM monitor to detect DoS attack. When the attack deprives resource beyond tolerable, VM monitor selectively live duplicates operating system and tagged application to isolated environment that reserved TCB resources.

In [127] Shui *et al*. recognize that the zombies use controlled functions to transmit packets to the victim, the attack flows to the victim always share properties, such as packages distribution behaviors, which are not possessed by legitimate flows. Based on these studies, once suspicious flows are appeared to a server, they calculate the distance of the package distribution behavior between the suspicious flows. If the distance is less than a given threshold, then a DDoS attack happens; otherwise, it is a legitimate accessing.

In [128] Qi *et al*. propose a confidence-based filtering method (CBF), which is able to be deployed in non-attack period and attack period. Legitimate packets are gathered to extract the attribute pairs to generate a nominal profile, at non-attack period. The CBF method with the nominal profile is elevated by calculating the score of a particular packet at attack period to decide whether to discard it or not. Correlation pattern is the main idea of CBF, which refers to some concurrently appeared features in the legitimate packets.

Client Puzzle Protocol is a DoS attack prevention method. In this scheme, when a client requests some services, it should solve a puzzle before connecting to the server. Based on this result, server may confirm or reject the client's connection. The puzzle should be simple to solve but should require a little amount of computation or human intervention by the client. Although nonmalicious users may experience a little computational cost, but attackers that try to establish large numbers of connections will be unable to perform their attacks because of the computational cost of puzzle [76].

To avoid DoS attacks in cloud servers, in [129] Panja *et al*. propose DOSBAD. It first finds the server's available bandwidth and periodically sends a number of packets to each path within the cloud and monitors how much of the bandwidth is used by the routers. In this scheme, incoming packets' number and the ACKs are measured where the number of the received packets should match the number of ACKs. Otherwise, this may indicate that the bandwidth limit is reached and some malicious activities are attempted. Then, DOSBAD considers the return addresses of the incoming packets at the attacked routers and sends a ping to those addresses. If no response is received, it may be a sign of a DoS attack and DOSBAD order the router to drop all packets from that address.

Lee *et al*. in [130] specify several network parameters that can be applied to detect the DDoS attacks. The distribution of the source IP, destination IP, source port, and destination port provides additional information about each step of the DDoS attack. During the attack period the destination IP address becomes common in each packet trace.

In [131] a hybrid fuzzy DDoS defense mechanism is presented based on the statistical behavior of the parameters of network protocols, which consider the following parameters for DDoS detection:

- Entropy of the source IP addresses and ports
- Entropy of packet type
- Number of packets and their rate
- Http packet timeline and request rate
- Destination IP address and port

If the http request data is very small it may be a sign of the slow read packets. Http packet timeline is applied to mitigate slow http request attack. Attacker machine requests with an extremely slow packet transfer rate that keeps the server's resources always busy. This model is a similarity-based learning mechanism to detect the attack traffic. In attack detection phase, the traffic class is defined, which recognizes if the traffic is normal or attack traffic. Traffic class is the output parameter for the given network parameters as input. The system's architecture is shown in Figure 14 [131].

Zhiyuan *et al*. in [132] propose a solution to detect DoS attack, which utilizes multivariate correlation analysis for correct network traffic detection by achieving the geometrical correlations between the network traffic features. This scheme applies the anomaly based attack detection for detecting DoS attacks by learning the patterns of legitimate network traffic. In addition, a triangle area-based method is used to enhance the process of multivariate correlation analysis and to extract the correlative information between the features within an observed data object.

In [133] Du *et al*. present a DDoS defense scheme, named network egress and ingress filtering, which should be deployed at the ISP edge routers to prevent DDoS attacks in and out of the ISPs' networks. They present a

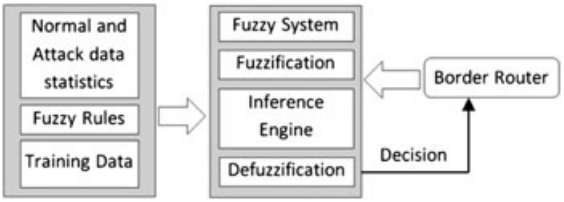

Figure 14. Architecture of fuzzy-based defense system.

bloom filter-based scheme to recognize and measure large flows. Then, these flows are rate-limited to their fair share based on the packet symmetry or the ratio of the received and sent packets of a host. The dropping decision of each flow is made based on the observed counters and has low implementation complexity.

To identify the DDoS attack source, in [134] Joshi *et al*. present Cloud Trace Back (CTB), which uses back propagation neural network. As indicated in Figure 15, CTB is deployed at the edge routers to be near to the source end of the cloud network [69]. In this scheme, to access a WS, a client sends a SOAP request message, based on the service description to CTB, which places a Cloud Trace Back Mark within the header. Then, SOAP message is sent to the web server. When an attack is detected, the victim requests for reconstruction to extract the mark and warn them of the origin of the message and the reconstruction begins to filter out the attack traffic. If the SOAP message is normal, it is forwarded to the request handler. web service prepares a SOAP response, which web server transmits to the client. Moreover, CTB utilizes a defense system called "cloud protector," which is a trained back propagation neural network to control messages that are aimed to launch X-DoS attacks.

In [85] Chapade *et al*. present average distance estimation-based DDoS detection technique. In this technique, the average value of the distance in the next period of time is calculated by the exponential smoothing estimation method. This distance-based traffic separation DDoS detection technique uses minimum mean square error linear predictor to estimate the traffic rates from different distances. They compute the distance, based on the time-to-live (TTL) value of an IP header, directly during the transmision. Consequently, the distance of the packet is computed as the final TTL value subtracted from the initial value. The challenge in distance estimation is how the victim should derive the initial TTL from the final TTL value.

5.11.2. Packet scoring-based defense

Belenky *et al*. in [135] provide a solution named deterministic packet marking (DPM). By proper establishment on the Internet, it can mark all packets at ingress interfaces and can trace the slaves that involve reflectors and conduct the DDoS attacks. In DPM, most of the required processes are executed at the victim. The traceback method can be conducted post-mortem to allow tracing back the attacks that may not have been detected, or the attacks, which would reject service to the victim. The DPM operates without exposing the topology of the providers' network and the involvement of the ISPs is limited and few changes are required to deploy the DPM.

The authors in [136] present Hierarchical Indirect Mapping System (HIMS), which provides a flat identifier space to stamp the received packets to endpoint identifier. HIMS can limit the DoS floods and provides properties such as network utilization low latency and scalability. Based on an effective merging rule, this scheme builds a hierarchical Chord architecture, which can scale to Internet level and preserve the locality and convergence of the inter-domain path. In DoS attacks, the sending host knows the IP address of the receiver and the malicious node can obtain the IP addresses of both the sender and the receiver, and then attaches a destination attack to the sender or the receiver.

Yoohwan *et al*. in [137] propose a distributed online attack detection scheme named PacketScore. In this approach, the victim is recognized by monitoring four main traffic statistics of each secured objectives while keeping minimum per-target states. The malcious packets are detected based on the Bayesian-theoretic metric of each packet. The metric is the conditional legitimate probability (CLP). This scheme, discards packets by measuring the CLP of each packet with a dynamic threshold, which is regulated according to the distribution of CLP of all doubtful packets and the congestion level of the victim. Prioritization of various kinds of suspicious packets is enabled in

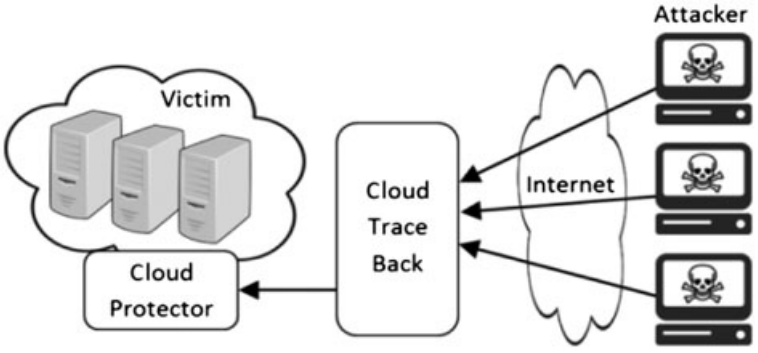

Figure 15. Cloud trace back scheme.

Security Comm. Networks 2016; **9**:3724–3751 © 2016 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

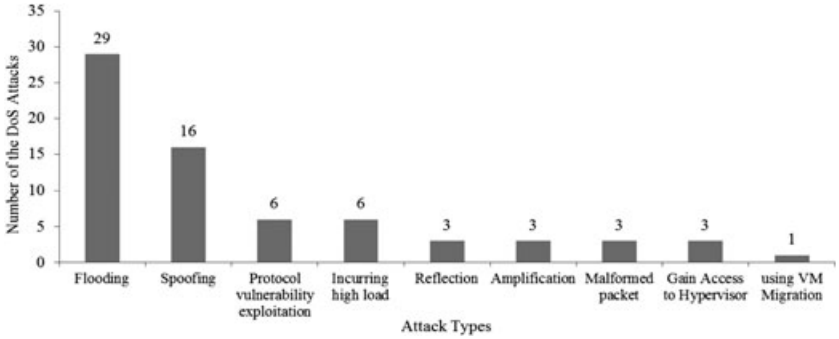

Figure 16. Attack types on the network and cloud infrastructure.

this approach. By connecting the CLP discard threshold to the congestion level of the victim, packetscore permits the victim to accept more legitimate traffic as its capacity permits.

Generally, an intense pulse in the network traffic indicates the existence of anomalies caused by DDoS attacks or flash crowds. The authors in [15] present a solution named CALD, which tries to protect the web servers against the DDoS attacks, which masquerade as flash crowds. In CALD, front-end sensor is used to monitor the traffic that may have DDoS attacks or flash crowds. When unusual traffic is recognized, an ATTENTION signal is sent by the sensor to activate the attack detection module. Also, CALD records the mean frequency of each source IP and checks the total mess extent that the mess extent of DDoS attacks is larger than the one of the flash crowds. With some parameters from the attack detection module, this scheme is able to stop the attack traffic and forward the legitimate requests. Moreover, the security modules may be divided away from the web servers. As a result, it preserves maximum efficiency on the kernel web services, irrespective of the disturbance from DDoS.

5.11.3. Neural networks-based defense

Chonka *et al*. in [47] develop a neural network detector trained by their DDoS prediction algorithm. They use the theory of network self-similarity to recognize the DDoS flooding attack from legitimate similar traffic. This method not only detects attack traffic during the transmission, but also filters it. They apply real network traffic information to recognize the self-similar pattern for legitimate users' traffic and use this information as a benchmark for the prediction algorithm to determine if any new traffic is DDoS traffic or legitimate traffic. This trained neural network can filter out any anomalous traffic that has the DDoS attack characteristics.

Another solution to detect DDoS is presented in [138], which provides training and evaluating of unsupervised neural nets for intrusion detection. This scheme applies the neural networks to analyze the network traffic in on-line and off-line modes and classifies the traffic into normal and attack. Then, these network traffics are further split into small time intervals, which include all packets whose timestamps agree with that interval. Then, they extract the statistical attributes from these intervals that create the training vector. Neural net processes and clusters them as normal or DDoS attack.

5.11.4. Honeypot-based defense

A honeypot is a DoS defense method, which performs as a detective server among a number of servers in a network where any packet honeypot received is likely to be a packet from the attackers. In [139] Khattab *et al*. propose a useful hop-by-hop traceback technique named as honeypot back-propagation, in which precise attack signatures are received by a novel leverage of the roaming honeypots approach. The acceptance of DoS attack packets by a roaming honeypot, which is a decoy machine concealed in a server

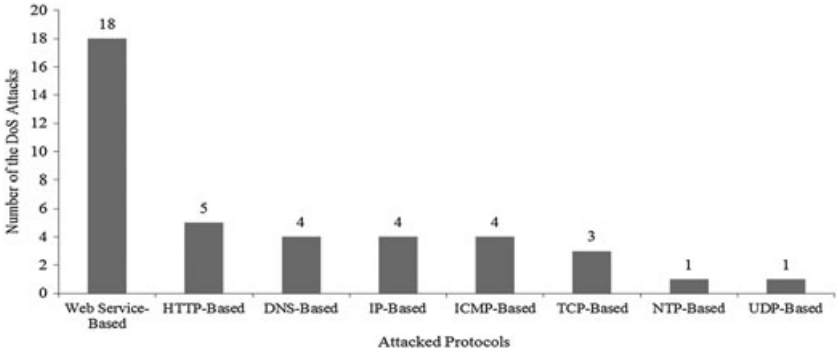

Figure 17. Attacks based on different protocols.

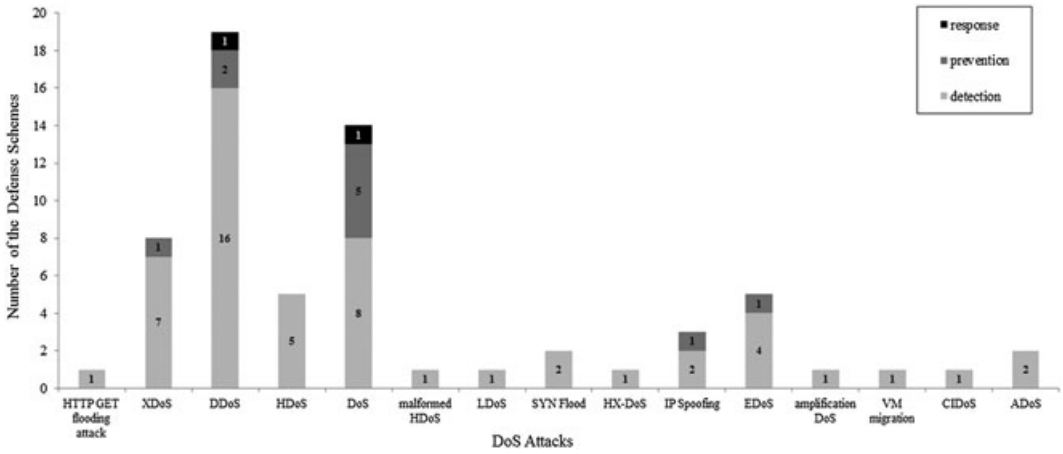

Figure 18. Defense schemes against different attacks and the type of defense method.

pool initiates the activation of a tree of honeypot sessions rooted at the honeypot. At autonomous system level, the tree is created hierarchically, and then at router level. Incremental deployment is provided by honeypot back-propagation by supplying the incentives for ISPs even with partial deployment. They can be physical or VMs and in order to find out worm signatures they have been successfully used as intrusion detection tools. For special time intervals each server performs as a honeypot. The duration of honeypot periods is not predictable to attackers.

In [140] Das *et al*. propose a new efficient honeypot model to solve all the existing problems by opening a virtual communication port for any specific communication between an authorized client and server and by providing facility to act as an active server for any honeypot. Roaming honeypot schemes are generally used as defense mechanisms against no spoofed service-level DoS attacks. For a time period one or more servers may act as honeypot from a pool of servers, without consuming service interruption. In other words, one or more legitimate services in the pool, in coordination with legitimate clients and remaining peer replicas, assume the role of a honeypot for specific intervals of time called honeypot period. Such kind of roaming honeypot services makes it difficult for attackers to recognize active servers, so results in them to be trapped in.

5.11.5. Intrusion detection system-based defense

A distributed and data-driven IDPS is proposed in [141] by Zargar *et al*. for all the cloud service providers that cooperate with each other to respond to attacks. Also, this solution applies a general trust management framework to support the establishment and improvement of trust among different cloud service providers. The proposed framework integrates IDPS in all three layers of cloud.

In [142] Goyal *et al*. present a behavior-based defense in which the client actions are compared with the usual behavior. In this scheme, to detect the attack traffic over the IP addresses or ports the deviance in the entropy is used. The value of entropy lies in the range [0, log n]. More random is the data, the more entropy it has. The entropy will be smaller if the data belongs to one class, otherwise it will be larger. A threshold value of the entropy will be set to detect the deviance in the behavior of the packets. If the value of the entropy of the packet mismatches the threshold, it will be the sign of an attack or a change in the randomness. This anomaly based detection system should be located in every router.

In [143] Lonea *et al*. focus on detecting the DDoS attacks by combining the evidence achieved from IDSs deployed in the VMs with a data fusion method in the front-end server. The VM-based IDS produces the alerts in the event of attacks, which are stored in the database

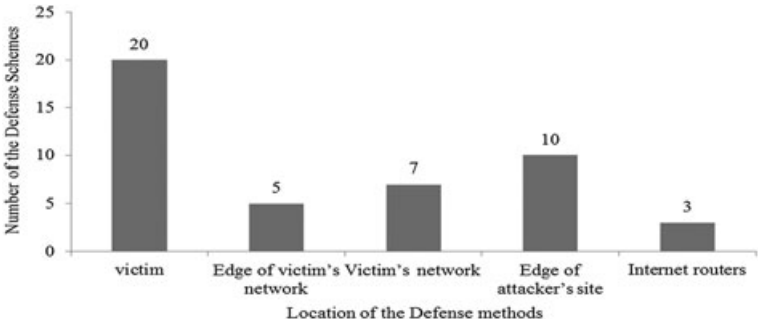

Figure 19. Classification of the defense schemes based on the position of the defense method.

placed within the Cloud Fusion Unit of the front-end server. They propose a quantitative solution and analyze alerts using the Dempster–Shafer theory operations in three-valued logic. The proposed DST solution provides these advantages:

- Accommodating the uncertain state
- Reducing the false negative rates
- Increasing the detection rate
- Alleviating the work for cloud administrators.

Also in [144] authors focus on NIDSs' weaknesses in analyzing high-speed network connectivity. They present a software development that utilizes QoS and parallel technologies in Cisco Catalyst Switches to improve the performance of a network IDS and to reduce the number of dropped packets that may be caused by several types of attacks.

5.12. Botnet detection based on network behavior

The botnet detection approach proposed in [15] is to test flow properties such as bandwidth, packet timing, and burst duration for evidence of botnet command and control activity. An approach that resolves traffic is created that is likely to be part of a botnet, and then correlates the likely traffic to find common communication patterns that would suggest the activity of a botnet.

6. DISCUSSIONS

This section presents a complete comparative analysis of the various attacks on the network infrastructure and on the cloud components and also the defense schemes that are proposed to prevent, detect, or response them. The information provided by this section can be utilized in future researches and to design new DoS attacks defense methods. Figure 16 indicates the number of the DoS attacks on the network and cloud components.

As indicated in this figure, most of the studied DoS attacks apply flooding for consuming the victim's resources and also use source IP address spoofing for masquerading themselves.

Figure 17 shows the number of the attacks conducted against the various protocols. As shown in this figure, the web services are the main target of the DoS attacks in cloud environment. As outlined before, this is because of the XML vulnerabilities of the base protocols such as SOAP that web services apply. Figure 18 indicates the number of defense schemes against different attacks and also classifies them based on the type of the defense method.

From Figures 17 and 18, it can be concluded that the number of the defense solution proposed for XML-based DoS attacks, are much fewer than the proposed XML-based attacks. As a result, more research should be performed on web service security in future, to provide robust and secure cloud services.

Also, Figure 19 classifies the defense schemes based on the location where the security components of these schemes should be positioned. As exhibited in this figure, most of the defense solutions are designed to operate on the victim's site, which the attacks traffics converge. Table VII presents summary of the defense mechanisms proposed in the literature against the different DoS attacks. One of the important issues, which cloud systems should deal with them, is to prevent the attackers from utilizing the cloud as part of the botnet to attack other clouds and system. However, as indicated in Figure 19, fewer defense solutions are proposed to operate on the attacker side and most defense solution are designed to operate on victim's site.

7. CONCLUSION

Cloud computing security is the main obstacle, which prevents the adoption of the cloud technology by many organizations. One of the critical security threats to the cloud computing is the DoS attacks. These attacks are malicious attempts performed to cause some cloud services or resources temporarily become unavailable for the cloud customers. However, DoS attacks are more serious in the cloud because an attacker can utilize extensive cloud resources to conduct his attacks and can also benefit from vulnerabilities of the new protocols and features applied in the cloud computing environment. As a result, various types of DoS attacks are designed and conducted against the cloud customers, web services, and protocols.

In this paper, the DoS attack problem in the cloud computing environment is investigated and discussed. Besides, a classification of DoS attacks in the cloud computing is presented and the properties and capabilities of each DoS attack is illuminated and compared in detail. Moreover, various states of the art security solutions presented in the literature to deal with DoS attacks in the clouds are analyzed and numerous attack handling methods, DoS attack prevention, and attack detection are illustrated and discussed.

However, the proposed security solutions for DoS attack in the cloud have low scalability and are used to deal with DoS attacks in single clouds. But, considering the importance and increasing the deployment of the federated clouds, more complete security schemes should be designed in the future studies and researches to provide security and availability for various services and resources presented in the federated clouds.

Also, most defense solutions are designed to deal with external DoS attacks. Thus, DoS attacks launched by the internal attackers are one of the issues that can be considered in the future studies. Moreover, in DoS attack detection solutions, most schemes rely on the history of access to services and resources, which can only be applied to less dynamic contents and their usage pattern is almost

constant. Thus, the main issue, which should be considered in the future researches of the DoS attack detection, is how to differentiate between the flash crowds and DoS attacks in the clouds with dynamic contents.

REFERENCES

1. Mell P, Grance T. *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology (NIST): Gaithersburg, MD, 2011.
2. Zissis D, Lekkas D. Addressing cloud computing security issues. *Future Generation Computer Systems* 2012; **28**(3): 583–592.
3. Udendhran R. New framework to detect and prevent denial-of-service attack in cloud computing environment. *Asian Journal of Computer Science and Information Technology* 2014; **4**(12): 87–91.
4. Zunnurhain K, Vrbsky S. Security attacks and solutions in clouds. In *Proceedings of the 1st International Conference on Cloud Computing*. Citeseer, 2010.
5. Singh S. Cloud computing attacks: a discussion with solutions. *Open Journal Of Mobile Computing And Cloud Computing* 2014; **1**.
6. Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. *Security & privacy, IEEE* 2011; **9**(2): 50–57.
7. Kozlov D, Veijalainen J, Ali Y. Security and privacy threats in IoT architectures. In *Proceedings of the 7th International Conference on Body Area Networks*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012.
8. Alao OD, Adekunle YA, Joshua JV, Adebayo AO. Wireless networks: overview, security issues and challenges.
9. Jamil D, Zaki H. Security issues in cloud computing and countermeasures. *International Journal of Engineering Science and Technology (IJEST)* 2011; **3**(4): 2672–2676.
10. Yu S. *Distributed Denial of Service Attack and Defence*. Springer: London, UK, 2014.
11. Strayer WT, Lapsely D, Walsh R, Livadas C. Botnet detection based on network behavior. In *Botnet Detection*. Springer: US, 2008; 1–24.
12. Massi J, Panda S, Rajappa G, Selvaraj S, Revankar S. Botnet detection and mitigation. Student-Faculty Research Day, CSIS. Pace University, White Plains, NY, 2010.
13. Alomari E, Manickam S, Gupta BB, Karuppayah S, Alfaris R. *Botnet-based distributed denial of service* (*DDoS*) *attacks on web servers*: *classification and art*. arXiv preprint arXiv:1208.0403, 2012.
14. Thing VL, Sloman M, Dulay N. A survey of bots used for distributed denial of service attacks. In *New Approaches for Security, Privacy and Trust in Complex Environments*. Springer, 2007; 229–240.
15. Latanicki J, Massonet P, Naqvi S, Rochwerger B, Villari M. Scalable cloud defenses for detection, analysis and mitigation of DDoS attacks. In *Future Internet Assembly*, 2010; 127–137.
16. Zlomislic V, Fertalj K, Sruk V. Denial of service attacks: an overview. In *Information Systems and Technologies* (*CISTI*), *2014 9th Iberian Conference on*. 2014.
17. Harrison K, White G. A taxonomy of cyber events affecting communities. In *System Sciences* (*HICSS*), *2011 44th Hawaii International Conference on*. IEEE, 2011.
18. Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks* 2004; **44**(5): 643–666.
19. Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: a classification. In *Signal Processing and Information Technology*, *2003. ISSPIT 2003. Proceedings of the 3rd IEEE International Symposium on*. IEEE, 2003.
20. Studer R. Economic and technical analysis of botnets and denial-of-service attacks. Communication systems IV, 2011. **19**.
21. Geva M, Herzberg A, Gev Y. Bandwidth distributed denial of service: attacks and defenses. *IEEE Security & Privacy* 2014; **12**(1): 54–61.
22. Deshmukh MSR, Chouragade P. Prevention against Bandwidth DDoS Attack. ▪▪▪ .
23. Revathi P. *Flow and rank correlation-based detection against Distributed Reflection Denial of Service attack*. in *Recent Trends in Information Technology* (*ICRTIT*), *2014 International Conference on*. IEEE, 2014.
24. Priya PM, Akilandeswari V, Shalinie SM, Lavanya V, Priya MS. The Protocol Independent Detection and Classification (PIDC) system for DRDoS attack. In *Recent Trends in Information Technology (ICRTIT), 2014 International Conference on*, IEEE, 2014: 1–7.
25. Tsunoda H, Ohta K, Yamamoto A, Ansari N, Waizumi Y, Nemoto Y. Detecting DRDoS attacks by a simple response packet confirmation mechanism. *Computer Communications* 2008; **31**(14): 3299–3306.
26. Colella A, Colombini CM. *Amplification DDoS Attacks: Emerging Threats and Defense Strategies, in Availability, Reliability, and Security in Information Systems*. Springer, 2014; 298–310.
27. Röpke C. Malicious Code and Access Control in Software-Defined Networks. In *9. GI FG SIDAR*

Graduierten-Workshop über Reaktive Sicherheit 2014; 4.
28. Czyz J, Kallitsis M, Gharaibeh M, Papadopoulos C, Bailey M, Karir M. Taming the 800-pound gorilla: The rise and decline of NTP DDoS attacks. In *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014; 435–448.
29. Komu M, Sethi M, Mallavarapu R, Oirola H, Khan RH, Tarkoma S. Secure Networking for Virtual Machines in the Cloud. In *CLUSTER Workshops*, 2012; 88–96.
30. Bakshi A, Yogesh B. Securing cloud from DDoS attacks using intrusion detection system in virtual machine. In *Communication Software and Networks*, *2010. ICCSN'10. Second International Conference on*. IEEE, 2010.
31. Shea R, Liu J. Understanding the impact of denial-of-service attacks on virtual machines. In *Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service*. IEEE Press, 2012.
32. Szefer J, Keller E, Lee RB, Rexford J. Eliminating the hypervisor attack surface for a more secure cloud. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011; 401–412.
33. Szefer J, Lee RB. A case for hardware protection of guest vms from compromised hypervisors in cloud computing. In *Distributed Computing Systems Workshops* (*ICDCSW*), *2011 31st International Conference on*. IEEE, 2011.
34. Reuben JS. *A Survey on Virtual Machine Security*, Vol. **2**. Helsinki University of Technology: Helsinki, 2007; 36.
35. Fangfei Z, Goel M, Desnoyers P, Sundaram R. Scheduler vulnerabilities and coordinated attacks in cloud computing. *Journal of Computer Security*. 2013; **21**(4): 533–559.
36. Masdari M, Nabavi SS, Ahmadi V. An overview of virtual machine placement schemes in cloud computing. *Journal of Network and Computer Applications* 2016; **66**: 106–127.
37. Wang Y, Ma J, Lu D, Lu X, Zhang L. From high-availability to collapse: quantitative analysis of "Cloud-Droplet-Freezing" attack threats to virtual machine migration in cloud computing. *Cluster Computing* 2014; **17**(4): 1369–1381.
38. Lazri K, Laniepce S, Zheng H, Ben-Othman J. AMAD: Resource Consumption Profile-Aware Attack Detection in IaaS Cloud. In *Utility and Cloud Computing* (*UCC*), *2014 IEEE/ACM 7th International Conference on*. IEEE, 2014; 379–386.
39. Alarifi S, Wolthusen SD. Mitigation of cloud-internal denial of service attacks. in *Service Oriented System Engineering* (*SOSE*), *2014 IEEE 8th International Symposium on*. IEEE, 2014.
40. Alarifi S, Wolthusen SD. Robust coordination of cloud-internal denial of service attacks. In *Cloud and Green Computing* (*CGC*), *2013 Third International Conference on*. 2013.
41. Luo S, Lin Z, Chen X, Yang Z, Chen J. Virtualization security for cloud computing service. In *Cloud and Service Computing* (*CSC*), *2011 International Conference on*. IEEE, 2011; 174–179.
42. Zardari MA, Jung LT, Zakaria N. A quantitative analysis of cloud users' satisfaction and data security in cloud models. In *Science and Information Conference* (*SAI*), *2014*. IEEE, 2014.
43. Krishna EP, Sandhya E, Karthik MG. Managing DDoS attacks on virtual machines by segregated policy management. *Global Journal of Computer Science and Technology* 2014; **14**(6); 20–24.
44. Ismail MN, Aborujilah A, Musa S, Shahzad A. New framework to detect and prevent denial of service attack in cloud computing environment. *International Journal of Computer Science and Security (IJCSS)* 2012; **6**(4): 226.
45. Abazari F, Analoui M. Exploring the effects of virtual machine placement on the transmission of infections in cloud. In *Telecommunications* (*IST*), *2014 7th International Symposium on*. IEEE, 2014.
46. Kazim M, Masood R, Shibli MA, Abbasi AG. Security aspects of virtualization in cloud computing. In *IFIP International Conference on Computer Information Systems and Industrial Management*, Springer: Berlin Heidelberg, 2013; 229–240.
47. Chonka A, Singh J, Wanlei Z. Chaos theory-based detection against network mimicking DDoS attacks. *Communications Letters, IEEE* 2009; **13**(9): 717–719.
48. Saini B, Somani G. Index Page-based EDoS Attacks in Infrastructure Cloud*, in* Recent Trends in Computer Networks and Distributed Systems Security. Springer: Springer Berlin Heidelberg, 2014; 382–395.
49. Sqalli MH, Al-Haidari F, Salah K. EDoS-shield—a two-steps mitigation technique against EDoS attacks in cloud computing. In *Utility and Cloud Computing* (*UCC*), *2011 Fourth IEEE International Conference on*. 2011.
50. Koduru A, Neelakantam T, Saira Bhanu S. Detection of economic denial of sustainability using time spent on a web page in cloud. In *Cloud Computing in Emerging Markets* (*CCEM*), *2013 IEEE International Conference on*. IEEE, 2013.
51. VivinSandar S, Shenai S. Economic denial of sustainability (EDoS) in cloud services using http and xml-based DDoS attacks. *International Journal of Computer Applications* 2012; **41**(20): 11–16.

52. Masdari M, Salehi F, Jalali M, Bidaki M. A Survey of PSO-Based Scheduling Algorithms in Cloud Computing. *Journal of Network and Systems Management* 2016; 1–37.
53. Masdari M *et al.* Towards workflow scheduling in cloud computing: a comprehensive analysis. *Journal of Network and Computer Applications* 2016; **66**: 64–82.
54. Siva T, E.S.P.K. Controlling various network-based ADoS attacks in cloud computing environment : by using port hopping technique. *International Journal of Engineering Trends and Technology (IJETT)* 2013; **4**(5); 2099–2104.
55. Palmieri F Ricciardi S, Fiore U, Ficco M, Castiglione A. Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures. *The Journal of Supercomputing* 2015; **71**(5): 1620–1641.
56. Jensen M, Gruschka N, Herkenhöner R. A survey of attacks on web services. *Computer Science-Research and Development* 2009; **24**(4): 185–197.
57. Falkenberg, A., Mainka C, Somorovsky J, Schwenk J. A new approach towards DoS penetration testing on web services. In *Web Services* (*ICWS*), *2013 IEEE 20th International Conference on*. IEEE, 2013; 491–498.
58. Holmes D. Mitigating DDoS attacks with F5 technology. F5 Networks, Inc, 2013; 2099–2104.
59. Siriwardena P. Security by Design*, in* Advanced API Security. Springer, 2014; 11–31.
60. Siddavatam I, Gadge J. Comprehensive test mechanism to detect attack on web services. In *Networks*, *2008. ICON 2008. 16th IEEE International Conference on*. IEEE, 2008.
61. Tiwari S, Singh P. Survey of potential attacks on web services and web service compositions. In *Electronics Computer Technology* (*ICECT*), *2011 3rd International Conference on*. IEEE, 2011.
62. Lindstrom P. Attacking and defending web services. White paper, 2004. Available from: http://www.spiresecurity. com [Accessed onDecember 2004].
63. Younis M, Kifayat K. *Secure cloud computing for critical infrastructure: a survey*. Liverpool John Moores University, United Kingdom, Tech. Rep, 2013.
64. Masood A. Cyber security for service oriented architectures in a Web 2.0 world: an overview of SOA vulnerabilities in financial services. In *Technologies for Homeland Security* (*HST*), *2013 IEEE International Conference on*. IEEE, 2013.
65. Gupta AN, Thilagam DPS. Attacks on web services need to secure XML on web. *Computer Science & Engineering* 2013; **3**(5): 1.
66. Jensen M, Gruschka N, Luttenberger N. *The impact of flooding attacks on network-based services*. in *Availability*, *Reliability and Security*, *2008. ARES 08. Third International Conference on*. IEEE, 2008.
67. Mainka C, Somorovsky J, Schwenk J. Penetration testing tool for web services security. In *Services* (*SERVICES*), *2012 IEEE Eighth World Congress on*. IEEE, 2012.
68. Jensen M, Gruschka N, Herkenhoner R, Luttenberger N. Soa and web services: New technologies, new standards-new attacks. In *Web Services*, *2007. ECOWS'07. Fifth European Conference on*. IEEE, 2007; 35–44.
69. Chonka A, Xiang Y, Zhou W, Bonti A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications* 2011; **34**(4): 1097–1107.
70. Farahmandian S, Zamani M, Akbarabadi A, Moghimi Y, Mirhosseini Zadeh SM, Farahmandian S. A survey on methods to defend against DDoS attack in cloud computing. *System* 2013; **6**(22): 26.
71. Anitha E, Malliga S. A packet marking approach to protect cloud environment against DDoS attacks. In *Information Communication and Embedded Systems* (*ICICES*), *2013 International Conference on*. IEEE, 2013.
72. Saleh MA, Abdul Manaf A. Optimal specifications for a protective framework against HTTP-based DoS and DDoS attacks. In *Biometrics and Security Technologies* (*ISBAST*), *2014 International Symposium on*. 2014.
73. Jayan D, Babu P. Detection of malicious client-based HTTP/DoS attack on web server. *International Journal of Science and Research (IJSR)* 2014:3(7).
74. Wang Y, Wang F, Guo J. A rapid detection algorithm for malformed H-DoS in the cloud platform. *International Journal of Advancements in Computing Technology* 2013; **5**(9); 474–481.
75. Yatagai T, Isohara T, Sasase I. Detection of HTTP-GET flood attack based on analysis of page access behavior. In *Communications*, *Computers and Signal Processing*, *2007. PacRim 2007. IEEE Pacific Rim Conference on*. IEEE, 2007.
76. Durcekova V, Schwartz L, Shahmehri N. Sophisticated denial-of-service attacks aimed at application layer. in *ELEKTRO*, *2012*. IEEE, 2012.
77. Guo F, Chen J, Chiueh T-c. Spoof detection for preventing dos attacks against DNS servers. in *Distributed Computing Systems*, *2006. ICDCS 2006. 26th IEEE International Conference on*. IEEE, 2006.
78. Yu H, Dai X, Baxliey T, Yuan X, Bassett T. A visualization analysis tool for DNS amplification attack.

In *2010 3rd International Conference on Biomedical Engineering and Informatics*. IEEE, 2010; **7**: 2834–2838.
79. Rozekrans T, Mekking M, de Koning J. *Defending against DNS reflection amplification attacks*. University of Amsterdam System & Network Engineering RP1, 2013.
80. Iracleous DP, Doukas N, Bourro K. Analysis and measurements of DNS amplification attacks. and Applications in the Armed Forces, 2014.
81. Graham-Cumming J. Understanding and mitigating NTP-based DDoS attacks. *CloudFlare*, 2014.
82. Yadav S, Reddy AKK, Ranjan S. Detecting algorithmically generated domain-flux attacks with DNS traffic analysis. *Networking, IEEE/ACM Transactions on* 2012; **20**(5): 1663–1677.
83. Ameyed D, Jaafar F, Fattahi J. A slow read attack using cloud. 2015.
84. Aborujilah A, Ismail MN, Musa S. Detecting TCP SYN-based flooding attacks by analyzing CPU and network resources performance. In *Advanced Computer Science Applications and Technologies* (*ACSAT*), *2014 3rd International Conference on*. EEE, 2014.
85. Chapade S, Pandey K, Bhade D. Securing cloud servers against flooding-based DDoS attacks. In *Communication Systems and Network Technologies* (*CSNT*), *2013 International Conference on*. IEEE, 2013.
86. Kaur G, Chaba Y, Jain V. Distributed denial of service attacks in mobile ad hoc networks. *World Academy of Science, Engineering and Technology* 2011; **73**:725–727.
87. Vineetha S, Ranjani PS. Review of distributed denial of service attacks and its prevention.
88. Kuzmanovic A, Knightly EW. Low-rate TCP-targeted denial of service attacks and counter strategies. *IEEE/ACM Transactions on Networking (TON)* 2006; **14**(4): 683–696.
89. Wu Z-j, Zhang L, Yue M. Low-rate DoS attacks detection based on network multifractal 2015.
90. Ma L, Chen J, Zhang B. In Improved RED Algorithm for Low-Rate DoS Attack*, in* Advances in Electronic Commerce*,* Web Application and Communication, Jin D, Lin S (eds). Springer: Berlin Heidelberg, 2012; 311–316.
91. Kurar B, Tahboub R. Internet scale DoS attacks. *International Journal of Applied Mathematics, Electronics and Computers* 2015; **3**(2): 83–89.
92. Xiaoming VSL, Chowdhury H. *Denial-of-Service (DoS) Attack with UDP Flood*. School of Computer Science, University of Windsor: Windsor, Ontario, Canada, 2007.
93. Hussain SM, Beigh GR. Impact of DDoS attack (UDP Flooding) on queuing models. In *Computer and Communication Technology* (*ICCCT*), *2013 4th International Conference on*. 2013.
94. Lakshminarayanan K *et al.* Taming IP packet flooding attacks. *ACM SIGCOMM Computer Communication Review* 2004; **34**(1): 45–50.
95. Dai H, Wang Y, Fan J, Liu B. Mitigate DDoS attacks in ndn by interest traceback. In *Computer Communications Workshops* (*INFOCOM WKSHPS*), *2013 IEEE Conference on*. IEEE, 2013: 381–386.
96. Ehrlich WK, Futamura K, Liu D. An Entropy-based Method to Detect Spoofed Denial of Service *(*DoS*)* Attacks*, in* Telecommunications Modeling*,* Policy*,* and Technology. Springer, 2008; 101–122.
97. Balkanli E. A comprehensive study on one-way backscatter traffic analysis. 2015.
98. Zhang L, Yu S, Wu D, Watters P. A survey on latest botnet attack and defense. In *Trust*, *Security and Privacy in Computing and Communications* (*TrustCom*), *2011 IEEE 10th International Conference on*. IEEE, 2011; 53–60.
99. Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)* 2007; **39**(1): 3.
100. Prabadevi B, Jeyanthi N. Distributed denial-of-service attacks and its effects on cloud environment—a survey. In *Networks*, *Computers and Communications*, *The 2014 International Symposium on*. 2014.
101. Bogdanoski M, Risteski A. Wireless network behavior under ICMP ping flood dos attack and mitigation techniques. *International Journal of Communication Networks and Information Security (IJCNIS)* 2011; **3**(1): 17–24.
102. Surisetty S, Kumar S. Is McAfee securitycenter/firewall software providing complete security for your computer? In *Digital Society*, *2010. ICDS'10. Fourth International Conference on*. IEEE, 2010.
103. Tawari HJ, Wankhade JS. Network security: attacks & component.
104. Dzurenda P, Martinasek Z, Malina L. Network protection against DDoS attacks. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems* 2015; **4**(1): 8–14.
105. Kumar S. Smurf-based distributed denial of service (DDoS) attack amplification in internet. In *Internet Monitoring and Protection*, *2007. ICIMP 2007. Second International Conference on*. IEEE, 2007.
106. Alenezi M, Reed M. Methodologies for detecting DoS/DDoS attacks against network servers. In *ICSNC 2012*, *The Seventh International Conference on Systems and Networks Communications*. 2012.

107. Zaroo P. A survey of DDoS attacks and some DDoS defense mechanisms. Advanced Information Assurance (CS 626), 2002.
108. Ramana VS. Secure cloud computing environment against DDoS and EDoS attacks. In *International Journal of Engineering Research and Technology*. ESRSA Publications, 2014.
109. Naresh Kumar M, *et al*. Mitigating economic denial of sustainability (EDoS) in cloud computing using in-cloud scrubber service. In *Computational Intelligence and Communication Networks* (*CICN*), *2012 Fourth International Conference on*. IEEE, 2012: 535–539.
110. Alosaimi W, Al-Begain K. A new method to mitigate the impacts of the economical denial of sustainability attacks against the cloud. In *Proceedings of the 14th Annual Post Graduates Symposium on the convergence of Telecommunication*, *Networking and Broadcasting* (*PGNet*). 2013.
111. Liu H. A new form of DoS attack in a cloud and its avoidance mechanism. In Proceedings of the *2010* ACM workshop on Cloud computing security workshop. ACM: Chicago, Illinois, USA, 2010; 65–76.
112. Yu J, Li Z, Chen H, Chen X. A detection and offense mechanism to defend against application layer DDoS attacks. In *Networking and Services*, *2007. ICNS. Third International Conference on*. IEEE, 2007: 54.
113. Santhi K. A defense mechanism to protect cloud computing against distributed denial of service attacks. *International Journal of Advanced Research in Computer Science and Software Engineering* 2013; **3**(5): 416–420.
114. Krishnaraj N. Securing Cloud From DDoS Attacks Using Intrusion Detection System In Virtual Machine. 2010.
115. Karnwal T, Sivakumar T, Aghila G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In *Electrical*, *Electronics and Computer Science* (*SCEECS*), 2012 *IEEE Students' Conference on*. 2012.
116. Xinfeng Y. Countering DDoS and XDoS attacks against web services. In *Embedded and Ubiquitous Computing*, *2008. EUC '08. IEEE/IFIP International Conference on*. 2008.
117. Sarhadi RM, Ghafori V. New approach to mitigate XML-DOS and HTTP-DOS attacks for cloud computing. *International Journal of Computer Applications* 2013; **72**(16): 27–31.
118. Choi J, Choi C, Ko B, Kim P. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. *Soft Computing* 2014; **18**(9): 1697–1703.
119. Herzberg A, Shulman H. DNS authentication as a service: preventing amplification attacks. In *Proceedings of the 30th Annual Computer Security Applications Conference*. ACM, 2014.
120. Shea R, Jiangchuan L. Performance of virtual machines under networked denial of service attacks: experiments and analysis. *Systems Journal, IEEE* 2013; **7**(2): 335–345.
121. Eddy WM. Defenses against TCP SYN flooding attacks. *The Internet Protocol Journal* 2006; **9**(4): 2–16.
122. Siris VA, Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks. *Computer Communications* 2006; **29**(9): 1433–1442.
123. Yaar A, Perrig A, Song D. Pi: A path identification mechanism to defend against DDoS attacks. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, IEEE, 2003: 93–107.
124. Chouhan V, Peddoju SK. Hierarchical storage technique for maintaining hop count to prevent DDoS attack in cloud computing. In *Proceedings of International Conference on Advances in Computing*. Springer: India, 2012.
125. Wang H, Jin C, Shin KG. Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM Transaction on Networking* 2007; **15**(1): 40–53.
126. Siqin Z, Kang C, Weimin Z. Defend against denial-of-service attack with VMM. In *Grid and Cooperative Computing*, *2009. GCC '09. Eighth International Conference on*. 2009.
127. Shui Y, Wanlei Z, Doss R. Information theory-based detection against network behavior mimicking DDoS attacks. *Communications Letters, IEEE* 2008; **12**(4): 318–321.
128. Qi C, Lin W, Dou W, Yu S. CBF: a packet filtering method for DDoS attack defense in cloud environment. In *Dependable*, *Autonomic and Secure Computing* (*DASC*), *2011 IEEE Ninth International Conference on*, IEEE, 2011: 427–434.
129. Panja B *et al*. Monitoring and managing cloud computing security using denial of service bandwidth allowance. *Recent Patents on Computer Science* 2013; **6**(1): 73–81.
130. Lee K, Kim J, Kwon KH, Han Y, Kim S. DDoS attack detection method using cluster analysis. *Expert Systems with Applications* 2008; **34**(3): 1659–1665.
131. Iyengar NCS, Banerjee A, Ganapathy G. A fuzzy logic-based defense mechanism against distributed denial-of-services attack in cloud environment. *International Journal of Communication Networks and Information Security (IJCNIS)* 2014; **6**(3): 233–245.
132. Zhiyuan T, Jamdagni A, He X, Nanda P, Liu RP. A system for denial-of-service attack detection based

on multivariate correlation analysis. *IEEE transactions on parallel and distributed systems* 2014; **25**(2): 447–456.
133. Du P, Nakao A. DDoS defense deployment with network egress and ingress filtering. In *Communications* (*ICC*), *2010 IEEE International Conference on*. IEEE, 2010.
134. Joshi B, Vijayan AS, Joshi BK. Securing cloud computing environment against DDoS attacks. In *Computer Communication and Informatics* (*ICCCI*), *2012 International Conference on*. IEEE, 2012.
135. Belenky A, Ansari N. On deterministic packet marking. *Computer Networks* 2007; **51**(10): 2677–2700.
136. Huang D, Yang D, Zhang H, Lin F. Efficient DoS-limiting support by indirect mapping in networks with locator/identifier separation. *Journal of Networks* 2013; **8**(1): 92–99.
137. Kim Y, Lau WC, Chuah MC, Chao HJ. PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. *Dependable and Secure Computing, IEEE Transactions on* 2006; **3**(2): 141–155.
138. Jalili R, Imani-Mehr F, Amini M, Shahriari HR. Detection of distributed denial of service attacks using statistical Pre-processor and unsupervised neural networks. In *Information Security Practice and Experience*, Deng R *et al.* (eds). Springer: Berlin Heidelberg, 2005; 192–203.
139. Khattab S, Melhem R, Mossé D, Znati T. Honeypot back-propagation for mitigating spoofing distributed denial-of-service attacks. In *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*, IEEE, 2006; 8.
140. Das VV. Honeypot scheme for distributed denial-of-service. In *Advanced Computer Control*, *2009. ICACC '09. International Conference on*. 2009.
141. Zargar ST, Takabi H, Joshi JB. DCDIDP: a distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments. In *Collaborative Computing*: *Networking*, *Applications and Worksharing* (*CollaborateCom*), *2011 7th International Conference on*. IEEE, 2011.
142. Upma Goyal GB, Mehmi S. A dual mechanism for defeating DDoS attacks in cloud computing model. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* 2013; **2**(3): 34–39.
143. Lonea AM, Popescu DE, Tianfield H. Detecting DDoS attacks in cloud computing environment. *International Journal of Computers Communications & Control* 2013; **8**(1): 70–78.
144. Bul'ajoul W, James A, Pannu M. Improving network intrusion detection system performance through quality of service configuration and parallel technology. *Journal of Computer and System Sciences* 2015; **81**(6): 981–999.