DDoS Attacks and Impacts on Various Cloud Computing Components

Fadi SHAAR*, Ahmet EFE**‡

* Computer Engineering, Faculty of Natural Sciences, Yıldırım Beyazıt University Ankara/Turkey

** Ankara Development Agency, Internal Auditing Executive, 1322 Cadde No:11 Çankaya Ankara/Turkey

‡ Corresponding Author; Address: Tel: +90 312 3100300/172, Fax: +90 312 3093407, e-mail: icsiacag@gmail.com

Abstract- Cloud computing is the subject of the era and is the current keen domain of interest of organizations due to its promising opportunities and catastrophic impacts on availability, confidentiality and integrity. On the other hand, moving to cloud computing paradigm, new security mechanisms and defense frameworks are being developed against all threats and malicious network attacks that threaten the service availability of cloud computing for continuity of public and private services. Considering the increasing usage of cloud services by government bodies poses an emerging threat to e-government and e-governance structures and continuity of public services of national and local government bodies. IoT, industry 4.0, smart cities and novel artificial intelligence (AI) applications that require devices to be connected in ever present cloud platforms, provide an increasing wide range of potential zombie armies to be used in Distributed Denial of Service (DDoS) attacks which are amongst the most critical attacks under cloud computing environment. In this survey, we discuss in detail the classification of DDoS attacks threatening the cloud computing components and make analysis and assessments on the emerging usage of cloud infrastructures that poses both advantages and risks. We assert that considering various kinds of DDoS attack tools, proactive capabilities, virtual connecting infrastructures and innovative methods which are being developed by attackers very rapidly for compromising and halting cloud systems, it is of crucial importance for cyber security strategies of both national, central and local government bodies to consider pertinent pre-emptive countermeasures periodically and revise their cyber strategies and action plans dynamically.

Keywords- Cloud Computing; Service availability; DDoS; Malicious network attacks, E-government Security.

1. Introduction

E-government undoubtedly makes citizens' lives comfortable and communications easier by its positive effects on increasing efficiency, economy and effectiveness of bureaucracy for the people and providing better communication channels for politicians. Moreover, e-government permits greater access to information, improves public services, and promotes democratic processes. For these reasons there is a dramatic shift to technology usage and a transition to a "paperless government" which is constantly increasing towards a widespread usage of cloud components and services. The ever increasing usage of electronic technologies and applications in government services has played a significant role in citizen satisfaction and budget minimization. Even though the transition to digital governance has great advantages for the quality of government services it is accompanied with many security threats. One of the major threats and hardest security problems e-government faces are the denial of service (DoS) attacks. DoS attacks have already taken some of the most popular e-

government sites off-line for several hours causing enormous losses and repair costs [1].

Currently, cloud computing is considered to be the newest computing paradigm that offers numerous flexible and consistent services using virtualization technology that is used in the next generation of the data centers. Not only private companies and individuals but also government departments are trying to increase service availability through cloud computing infrastructure. Cloud computing by means of its capacity, resilience and cost minimization that provides the capability to share resources in a pervasive and transparent way, also it has the ability to perform procedures that meet different needs. Moreover, cloud computing offers on-demand services to the users and can have the ability to access common infrastructure. (NIST) which is the National Institute of Standards and Technology, identifies five fundamental specifications of cloud computing as on-demand self-service, broad network, access resource pooling, measured service, and rapid elasticity [2]. It also defines that the cloud offers services in four different deployment models (hybrid and community, private, public). It states that cloud providers provide the services in three service models namely infrastructure as a service (IaaS), platforms as a service (PaaS), and Software as a service (SaaS), and it is on the period of development to provide everything as a service (XaaS) [2]. [16, Fig. 1] shows cloud service models together with cloud deployment models, and the fundamental characteristics of this environment.

Due to its capabilities and cost effectiveness, cloud computing has been attracting the attention of many academic entities as well as many organizations [4]. High availability in cloud computing is essential. The availability in the cloud requires the use of cloud resources and services by authoritative users, based on their demands [5]. However, threats related to data confidentiality and service availability can threaten the cloud environment due to its resource multi-tenancy and sharing features [4]. The impacts of the non-availability of services and resources in the cloud are calamitous; and this can lead to a partial or even total failure of delivering the required service [5].

One of the biggest security attacks that threaten the service availability in cloud computing environment is Distributed Denial of Service (DDoS) attack. This attack blocks the legitimate users of cloud from reaching the services or resources offered by the cloud providers [6]. This is accomplished by exhausting the computing resources of the server by flooding the network bandwidth, which eventually leads to the non-availability of cloud services or resources, thereby, resulting to massive financial loss [7]. According to the recent Arbor Networks security report, the proportion seeing of DDoS attacks targeting services related to cloud computing has grown up from 19 percent two years ago, to reach up to 33 percent up to this year [20]. We can conclude from this report and from many other security reports and academic articles that, the problem of DDoS attacks targeting cloud services availability is still an open research problem and needs to be highlighted and studied more by researchers. This survey paper explores the taxonomy of DDoS attacks in general and also highlights the classification of this attack targeted the components of cloud computing. It explains the main categories of DDoS attack and discusses the weaknesses or vulnerabilities which are used to fire each kind of the attack. Also, it categorizes the DDoS attacks according to the targeted cloud components. Furthermore, it describes in details the recent trends and reports about DDoS. As far as we know, a very few proposed papers have explored in detail the DDoS attack targeting the cloud computing components, and this survey paper is one of the papers that covers this issue in detail. Conducting this survey is quite essential for defining the latest DDoS attacks that are threatening the cloud components and designing new defense mechanisms and tools to defend against this kind of threat.

Both public and private organizations should be aware of the risks arising from online service interruptions and use a comprehensive risk management model integrated with security and business processes such as COBIT-5. Moving to cloud and having attentions of hackers requires a holistic approach to business operations and governance alongside with security, risks and internal control structure [37].

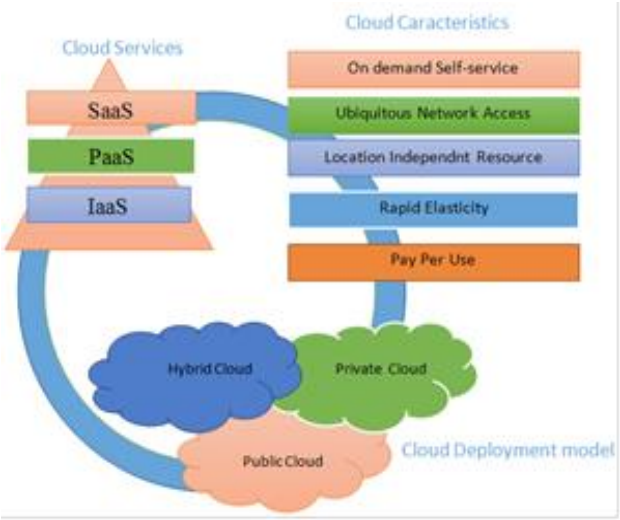

Fig. 1. Cloud deployment models, Characteristics, and infrastructures

Source: Somani et al, 2017

2. Methodology

This survey has been done after performing a systematic literature review including a collection of more than 40 of indexing papers and recent reports related to the area. A subclass of the collection is resulted after performing our initial scan. Then the papers we used in this survey are resulted after conducting our second deep scan and also we used it for the taxonomy preparation. We consider that the listed contributions in this survey are comprehensive and include almost all the crucial contributions in the emerging field up to date.

This survey divided into several sections. We provide an overview of DDoS attack in section 2. Section 3 describes in details the recent trends and reports about DDoS. The remainder of this survey discusses the classification of DDoS attacks and presents DDoS attacks on the cloud computing components then ends up with the concluding comments and future research directions. Table 1 below lists the abbreviations and acronyms that are most used in this survey.

Table 1. The abbreviations and acronyms

Acronym	**Description**
DoS	Denial of service
DDoS	Distributed denial of service
EDoS	Economic denial of service
IoT	Internet of Things
PaaS	Platform as a service
SaaS	Software as a service
IaaS	Infrastructure as a service
XaaS	Everything as a service
C&C	Control and Command
SLA	Service level agreement
EMEA	Europe, Middle East, Africa
APAC	Asian Pacific American Coalition
Mbps	Megabit per second
Gbps	Gigabit per second
Tbps	Terabit per second
CCTV	Closed circuit TV
DNS	Domain Name Server
SOA	Service oriented architecture
VM	Virtual Machine
VMM	Virtual Machine Monitor
XML	Extensible Markup Language

We consider the contributions in this study as the following:

- Conducting this survey is very important to define what are the latest DDoS attacks threatening the availability of this services provided by the cloud computing providers; and identifying how various components of cloud computing are affected by this attack.
- We also introduce a detailed taxonomy and survey of up-to-date DDoS attacks in cloud computing components for a uniform verification and comparison among various attacks.
- This survey provide up-to-date statistics and trends related to DDoS threat collected from different we known security reports and resources such as ArborNetwork, Kaspersky security Lab, Cisco, and Akamai.
- This information provided by this survey would support researchers in the future to design new defense mechanisms against DDoS attacks on cloud computing and e-government domains.

3. The Overview of DDoS Threat

Nowadays countless economic impacts and losses to the victim party are caused by one of the most common cyber-attack methods which are Denial of service (DoS) attack. In network and computer security, generally the expression denial of service is used to indicate to an attack intended to damage or saturate the computer resources or network resources, with intent of making the legitimate users no longer be able to use the provided services [6, 8]. Such an attack is typically achieved by overwhelming the targeted resource or machine with extra and unnecessary requests in an attempt to prevent all or some legitimate requests from being fulfilled which will lead to system overloading [8, 9]. Sometimes when we try to get access to a website, we see that the server hosting this website is inaccessible due to overload and we notice an error message. This happens when the number of requests processed by a server surpasses its maximum capacity. The most popular method of DoS attack is named as DDoS the Distributed DoS which is officially known as a coordinated attack because it has the ability to cause more serious effects rapidly and easily. Simply, DDoS attacks use thousands of infected host machines (zombies) to launch disrupts assault operations at a large scale by attacking the target network devices or web applications with information requests that flood the server [10]. A typical setup of DDoS attack showed in Figure 2 below.

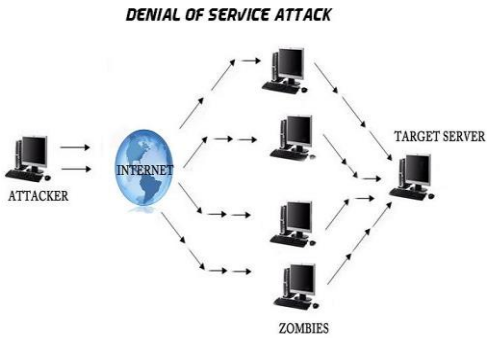

Fig. 2. A typical setup of a DDoS attack.

DDoS attacks are launched either by compromised distributed hosts acts as botnets or by distributed attackers and the machine engaged in the attack can be either network routers or smartphones or computers. Across geographies and using a Trojan virus, the attacker infects and exploits open-to-attack systems, to be as compromised machines. By planting this Trojan codes on these machines, hackers can easily and quickly build their legion of zombies [7, 9, 10]. This Trojan virus which is a small application enables the attackers to get remote access of the user systems without their knowledge for control and commands capabilities in an attempt to attack the intended target servers. These are called Bots or Zombies. These infected bots or systems in turn further infect and compromise others then working as a group acts as Botnets [11]. These zombie hosts or slaves are recruited unwittingly from the millions of vulnerable computers that accessing the Internet through high bandwidth connections. With enough participation of zombie hosts in the attack, the volume and the effects of DDoS attack can be astonishing. Thus, the higher the impact of DDoS attacks, the higher the chances of targeted server being unavailable and the higher the resources being wasted.

3.1.*Recent Trends*

DDoS remains as a serious threat that would lead to business lose or even discontinuance to various groups of users including government services, manufacturing, and retailers, health care data support, logistics, and cloud service providers. DDoS is not only breaking down the targeted servers 'performance but it also preventing legitimate users from accessing the subscribed services and using the basic need of server's availability. The growth of DDoS mitigation solutions in the cloud and the adoption of cloud and are two important points complement each other [7].

3.2.*The Effects of DDoS Attacks in/from Cloud Computing*

After cloud inception in 2007, enterprises took few years to start adopting the cloud infrastructure, and now many organizations are partly or entirely transformed their IT infrastructure into cloud (3, 4, 7). In case of cloud computing system, DDOS attack consider to be much more serious, more difficult and even more complicated because cloud computing uses virtualization, distributed server, the use of sharing resources and multi tenancy are some of the reasons that make DDoS attacks to be highly destructive in the environment of cloud computing [12, 13].

Cloud computing system has new vulnerabilities since it consists of new protocols, components, and concepts that allow the attackers to take advantage of this kind of vulnerabilities to perform new DDoS attacks [14, 15, 16]. Moreover, the key difference between DDoS attacks using the conventional networks and DDoS attacks that use the environment of federated cloud computing is shown in [40, Fig. 3]. We can see clearly in Figure 3 that all zombie hosts participated in the attack of DDoS might be a cloud. For instance, the victim and the botnet themselves might be a cloud, or the Command and Control servers (C&C servers) also might be a cloud. Thus, even the attacker might be a cloud due to their high CPU efficiency. In this case, the attackers will have the ability to have more accessible resources to preceding their attacks. Thus, by using clouds the attackers will make DDoS attacks' prevention, handling, and detection more difficult and more complicated. Generally, when the target of the DDoS attacker is a cloud, flooding the gateway of the Internet of the cloud infrastructure is the first aim of the attacker. Though, if the attackers failed to saturate it, then they will try to flood the servers of the cloud. DDoS attack will cause extremely large effect on availability in Cloud computing services which can lead to violation of the agreement between the client and the cloud service provider which is called Service Level Agreement (SLA) [10, 17]. Now using the innovative "DDoS as a Service" tools is making it easier for attackers to launch these effective and developed attacks.

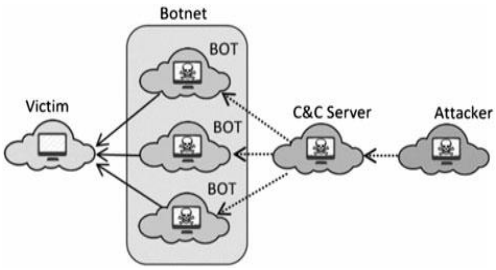

Fig. 3. A typical DDoS attack using cloud computing

Denial of service attacks are studied and measured in the market by several security solutions providers [7]. There are a few other reports which study about the rise and the impact of DDoS attacks in the cloud. According to Q1 report of 2015 [18], it has been proven that DDoS attackers was expected to have a major changing in target; shifting from using traditional servers to the use of cloud-based services. As per this report [19], in Q1, 2015 cloud services were most of the DDoS attack targets. Also, as it is shown in [20, Fig. 4] below, the proportion seeing of DDoS attacks targeting services related to cloud computing has grown up from 19 percent two years ago, to reach up to 33 percent up to 2017 [20]. The first example of DDoS attacks targeting cloud providers is the Lizard Squad planned attacks on Sony gaming servers and Microsoft. Likewise, in early 2015 and using a large DDoS attack, Rackspace servers and Amazon EC2 servers the cloud service providers were also attacked [7, 21].

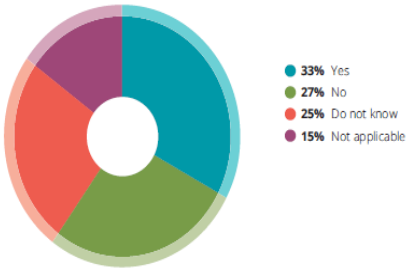

Fig. 4. Attacks targeting cloud service

Furthermore, the economic sides of DDoS attacks are challenging. For instance, in March 2015, a heavy DDoS attack targeted Greatfire.org website which belongs to Chinese Censorship watchdog which is an activist group that monitors Chinese web blocks. This attack cost the company a cost of $30,000 daily on Amazon EC2 cloud [7, 22]. According to the report in [23], the average economic loses by a DDoS attacks is up to 444,000 USD. Another fundamental character to ponder is the DDoS's target servers. Most of DDoS attacks targeted towards media and entertainment industries that are mostly hosted in the cloud. In detail, the report concerning different statistics is covered in [24]. There are some other reports by Arbor Networks [25], which show that there is an additional dangerous attack that has been started showing its impact parallel to a DDoS attack. This attack is known as Smoke screening attack which is termed very dangerous attack that is used to plan data or information breach behind a DDoS. While the whole staff is distracted in preventing or mitigating from the present DDoS attack, the attacker may plan to do other attacks to harm the target. According to this report by

Neustar [26], around 50% of the organizations have been afflicted by the "Smoke screening" attack while they were only preventing or mitigating DDoS. Another major issue is the repetition of the attack, and 90% of the targeted industries and companies have suffered from repetitive attacks leading to huge business damages.

3.3. *DDoS Attack Landscape*

Main security violations have become so popular that they barely surprise anybody anymore. Cisco predicts that by 2020, a much more developed 17 million DDoS attacks annually will happen. According to the huge increasing volume of DDoS attacks and the growth trends being noticed, Cisco believes that DDoS attacks are the greatest serious cyber security attacks toward all the organizations all over the world. With the advent of quantum computing opportunities that provides millions of times more CPU of a single core computation speed, DDoS attack will become more widespread and effective. They also believe that the sizes of peak attack are increasing dramatically [27]. The biggest attacks in 2013, 2014, 2015 and 2016 were 300, 400, 500 and 600 Gbit/sec respectively [8, 24, 28, and 29]. It believes that a whale of such a DDoS attack can swallow 10 percent of a country's overall Internet traffic. These large DDoS attacks consider being exceptional cases, but even the number of smaller attacks is also rising, which increase and concentrate the threat to businesses. 2015 year's 6.6 million attacks grew to 8.4 million 2016 year, more than doubling to 17.4 million in 2020, the firm said [27]. Unfortunately, it seems that in 2017 year, DDoS attacks will get worse before they get better. [26, Fig. 5] shows the worldwide distribution of DDoS attack. This worldwide distribution of DDoS attack study is conducted by Neuster in the summer of 2016. The purpose of this research study was to find out how distributed denials of service (DDoS) attacks are affecting the world, and what safety measures they're taking to alleviate the threat. The findings of this study show that DDoS attack still has international staying power and has a chilling impact on all areas of business.

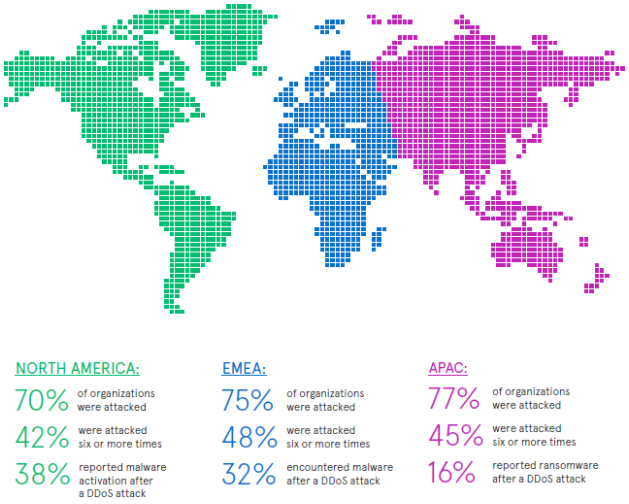

Fig. 5. Worldwide distribution DDoS attack

[20, Fig. 6] and [24, Fig. 7] show that the number and size of DDoS attacks have been growing. Through November, there was an average of 414,985 DDoS incidents per month globally in 2016, according to network security company Arbor Networks, up from 283,303 monthly in 2014, a 46% increase [20, 24]. As for the size of DDoS attack, it is clear in [19, Fig. 6] that the size dramatically increased between 2005 and 2016. It shows that the bandwidth size of DDoS attack on 2016 arrive to more than 350 Gbps and the number of requests increases to more than 350 Mbps. According to Akamai report on 2016 [29], there are two factors that driving the increase in the size of volumetric DDoS attacks:

• The growing in the traffic-generating capacity of large botnets, deriving from both the computing power of every connected device as well as an increasing number of connected devices. Every year, not only botnets are increasing in size, but individual bots are also growing and becoming more powerful as the cost of bandwidth decreases and the speed of computers increases.

• The continuous discovery of new attack vectors such as NTP (Network Time Protocol) and DNS (Domain Name Server) reflection. Reflection-style techniques exploit vulnerabilities in existing Internet services to produce much larger attacks than otherwise possible. For example, DNS reflection generates 28x to 54x amplification in attack size, while NTP reflection generates 556.9x amplification.

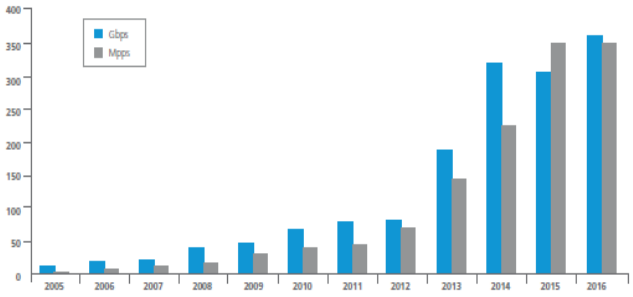

Fig. 6. Growth in DDoS Attack sizes

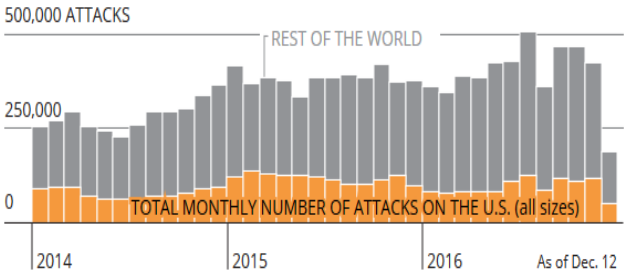

Fig.7. Growth in DDoS Attack sizes

Many people are now asking the question, were the 2016 DDoS attacks just test runs drills or warm-up for even bigger attacks that would paralyze large parts of the Internet? The possibility certainly exists; is it possible? Yes, it is, by all accounts and based on the recent directions in the cyber threat landscape, 2016 was one for the record books in terms of cyber security calamities. Botnets were generally consisting of endpoint systems (laptops, servers, and PCs) but the demand for connected homes, industry 4.0, smart cities, IoT, SCADA systems, security systems, and other non-profit devices formed a new infrastructure or platform for hackers wishing to expand their bot volumes. These connected devices are usually misconfigured by users and usually have low security in the first place. So, for remote communications by smart device apps and leaving the default access credentials open through firewalls; all these vulnerabilities give the attackers a big opportunity to penetrate the devices and perform their attack [24].

A new report delivered by ForeScout Technologies [30] illustrated how easy it is to compromise home IoT devices, particularly security cameras. These compromised devices are being used by the attackers to create the Mirai botnet. Mirai botnet code is an evil portion of malware that influences a widespread group of zombies mainly formed by the Internet of Things (IoT) compromised devices such as closed circuit TV (CCTV) cameras, which in in the past years were not actually taken into consideration to be a mean of such an attack by many security expert devices [31]. With the existence of such botnet tool like Mirai, the vast attack area will extend to include the millions of insecure Internet of Things (IoT) devices distributed across the globe, and consequently more sophisticated DDoS hackers will increase. Such huge and sophisticated attacks would be enough to far devastating impact the Internet's availability in major regions, states or countries that are geographically distributed. ISPs themselves could be disabled by such a big attack. As a result, in the DDoS attack landscape, we may perhaps see new broken records with this extensively effective utilized DDoS attack, and it is probable will be extended in size to reach tens of Terabits per second in the nearest future. Attackers can now have access to 100,000 IoT-based Mirai nodes for about $7,500 [32]. This IoT botnet business is booming, currently with over 6.4 billion IoT devices connected and by 2020 it is expected to be 20 billion (IoT) online devices [33]. [26, Fig. 8] below indicates that 38% of the organizations that adopted IoT "we hit with DDoS attacks greater than 10 Gbps" they said.

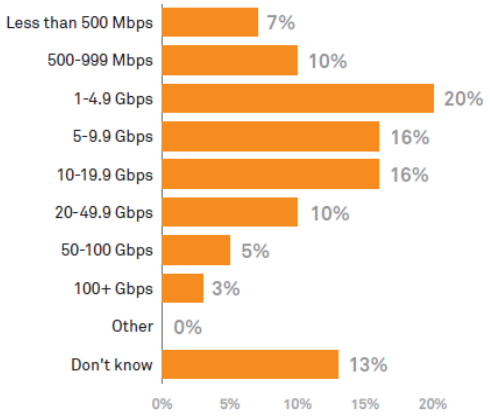

Fig. 8. 38% of the organizations that adopted IoT we hit with DDoS attacks greater than 10 Gbps.

DDoS is relatively inexpensive and very disruptive. The attack on security journalist Brian Krebs's blog site that happened on 20 September of 2016 was one of the huge DDoS attack ever launched [32]. This attack hardly affected his anti-

DDoS service providers' resources. At that time, the attack reached a record bandwidth of 620 Gbps and lasted for about 24 hours. This attack was launched completely via Mirai IoT botnet. In this specific state, it is believed that the original botnet was controlled and created by a single individual so the only cost to launch it was the time, and the cost to Krebs was just a day of being offline [34]. The one who suffer from DDoS Krebs is not only Krebs. The attacks that happened against companies that depending on the Internet like Dyn, which caused the inaccessibility of Netflix, Twitter, Reddit, the Guardian, Github, CNN, Spotify, Etsy, and many others, the cost is much higher. Losses and damages in economics can reach multi- millions of dollars [32]. It was on 21 of Oct, 2016, where various main websites that are hosted by the American domain name service provider Dyn temporarily shut down and suffered outages. When a massive, 1.2 Tbps distributed denial of service (DDoS) attack targeted the company that monitors several Domain Name Servers that serve American domains which is called Dyn (now it is part of Oracle) the Domain Name Service provider. The volume of this attack was about two times as big as the massive attack that stunned a single website, Krebs on Security, last month (that was 620 gigabit per second). This enormous DDoS attack temporarily shut down several of household-name websites, including, but not limited to Netflix, Wired, Twitter, The New York Times, Air BnB, Spotify and Reddit. That attack it was just a wake-up call and it was one of several massive attacks, record-breaking DDoS attacks that overwhelmed the Internet in 2016. Recently the British security scholar Kevin Beaumont stated that a groups of huge cyber-attacks using the Mirai DDoS botnet periodically broken down all Internet access across all the country of Liberia [35, 36]. With the note that, Liberia has only one Internet cable, set up in 2011, which means that for Internet access there is only a single point of failure. "The attacks are enormously worrying because the attackers used a Mirai tool that has enough capacity to extremely impact systems in a nation state," Beaumont wrote [36]. An employee that was working at a mobile service provider of Liberia said that the attacks were badly affected his business. He also said, "Our business has been targeted frequently and it's killing our revenue". Kevin Beaumont said that it seems that the attacks which targeted Liberian telecom operators who is the co-owner of the single Internet cable of Liberia, were being used to test denial of service techniques [35]. The attacks reached a record bandwidth of more than 500 Gbps; Beaumont said it seems that the Mirai botnet is controlled by the same actor who attacked the managed DNS provider Dyn on October 21, disabling websites across the U.S. This means that a site that costs generates millions of dollars in revenue and several thousands of dollars to maintain and set up can be disabled for a few hundred dollars, making it an extremely cost-efficient attack. With a high accessibility, resilient control infrastructure, and a low cost, it is confirmed that DDoS is not going to be disappeared, and as Cisco predicts that by 2020, a much more developed 17 million DDoS attacks annually will happen. Therefore, companies that are depending on their web presence for income need to highly consider their DDoS tactic to comprehend how they are going to protect themselves to stay afloat.

4. Taxonomy of DDoS Attacks

In the world of computing, diversity of DDoS attacks are growing very fast. The taxonomy of the DDoS can be categorized depends on their varied characteristics. The main categories of DDoS attacks fall into two categories including resource based attacks and bandwidth based attacks. Each of these types either causes an exhausting to the entire bandwidth or overwhelming all the network's resources that's been targeted. After doing a long comprehensive survey about DDoS types, we come up with the DDoS classification that is shown in the Figure 9 below. These types of DDoS attacks showed in the Figure 9 below are described in detail in the following section.

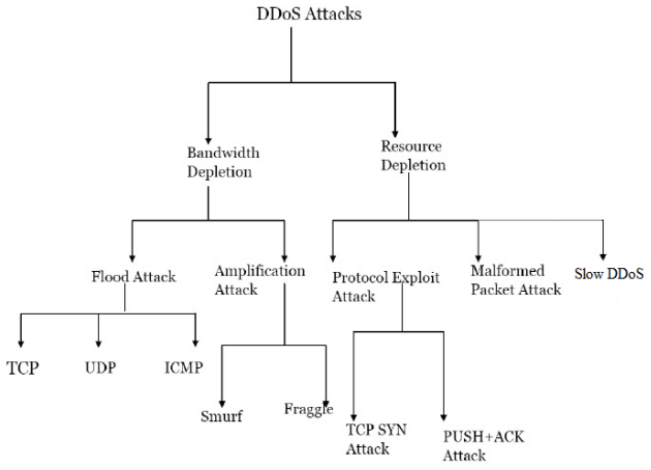

Fig. 9. Classification of DDoS attacks

4.1.*Bandwidth Depletion*

4.1.1. *Flooding DDoS Attacks*

In this kind of attack, which is also called volume-based attack, the victim is flooded with high stream traffic by the attacker to deny traffic that is described to be authentic to reach the system of the victim [10]. Different protocols are used in the flooding attacks to flood the victim such as TCP, UDP and ICMP [4]. SYN flood is one kind of flooding attack which uses TCP connection sequence as adverse effect. In this case, the attacker launches the SYN request which then needs to be responded with SYN-ACK, but the attacker does not answer the ACK request, and keeps overloading the target with SYN requests, this cause the resource or session and queuing overflow and leakage and cause denial of service at the end [11, 38, 39]. Internet Control Message Protocol (ICMP) is look like UDP. The attacker continuously and as fast as possible sends ICMP ping packets to the victim without expecting any reply. This generates queue at the server side which is the victim that leads to bandwidth congestion. So the server would not be able to handle the requests and may leads to server shutdown. Some Flooding attacks perform more complicated attacks by means of amplification and reflection mechanisms, which have highly destructive impacts on the targeted user and are difficult to deal with [38].

4.1.2. *Reflection-Based DDoS Attacks*

One more technique that is also used by the DDoS attackers is the reflection technique. In this kind of attack, the attacker use servers that are described to be uncompromised to send unwanted traffic to the targeted victim which leads to overwhelming the bandwidth of the victim's network [38]. This technique allows the attacker to remain undetected by sending the traffic indirectly to the targeted victim by the help of uncompromised servers. Moreover, all the packets used in the attack contain the victim's IP address as an origin address field of the packet of the IP address. As soon as the uncompromised servers receive these requests from the attacker, then they send the reply to the targeted node (victim), instead of sending it to the real source of these infected packets [6]. A more sophisticated type of reflection-based attack is called Distributed reflective DoS (DRDoS) attack as showed in [40, Fig. 10] below. Here, the attacker monitors the slave and master botnets and guide them to saturate the victim with an infected packets using of the reflector node [39]. The attackers can use botnets to prevent detection and to perform more affective attacks. An example of well-known DRDoS attack is the Smurf attack [38]. DDoS smurf attack preformed using ICMP ECHO REQUEST and REPLY packets. In this attack, the attacker directs packets contains ICMP REQUEST to be amplified using network broadcasting. These packets have a spoofed return IP address of the victim. So, each system replies this request by sending ICMP ECHO REPLY packets to the target. As a result, it will cause bandwidth consumption. Another attack which is called Fraggle attack that is alike with Smurf attack. In this attack the attacker uses UDP ECHO packets to perform DDoS Fraggle attack [41].

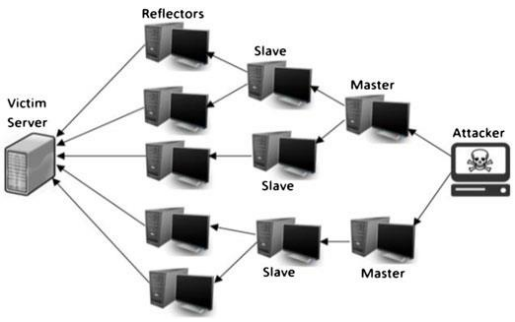

Fig. 10. Distributed reflective denial-of-service attack.

4.1.3. *Amplification-Based DDoS Attacks*

This attack is described to be the high destructive form of reflective attacks. Here, the volumes of the reflected traffic forwarded to the targeted victim are being increased by using the inherent nature of some network protocols. In this attack, the attacker uses the reflector servers so the size of the applied reflector servers responses by generating a traffic with a size that is more than the size of the request traffic message published by the attacker. Thus, traffic that will arrive to the target is magnified by a server called the reflector. Thus, this will bring down the target's bandwidth and resources [42]. This gives the chance to the attackers to perform more powerful attacks and only using a small size of botnets. For example, when a query packet is received by this server, it replies with one or more than one packet where the new size of the reflected packets is larger than the size of original received packets. Furthermore, the attackers in the amplification attacks may take the advantage of using the protocols that are based on UDP protocol to perform DDoS attacks, since UDP protocol has a lack of mechanisms such as handshake mechanisms that used to validate the origin node [12, 21]. Therefore, the amplification attacks allow the attackers to have the ability to send more unwanted traffic to the targeted victim; which means that this attack is more dangerous than reflexive attack. [43, Fig. 11] below describes the architecture of this attack.

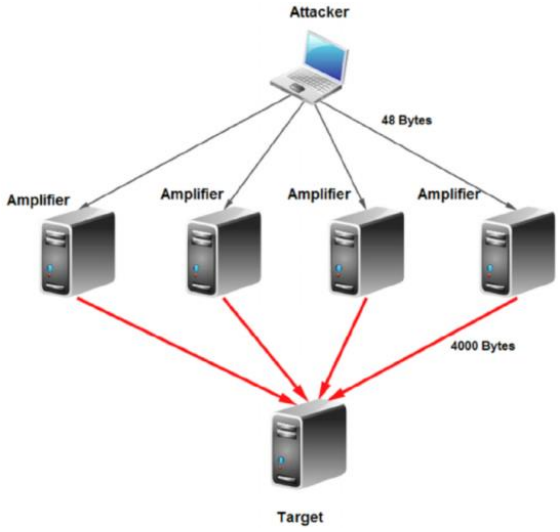

Fig. 11. Architecture of amplification-based DDoS attack

4.2.*Resource Depletion*

4.2.1. *Protocol Vulnerability DDoS Attack*

It is also called semantic attacks. These kinds of attacks exploit some identified protocol vulnerabilities like implementation flaws or design that is used to change the information forwarded to or from a certain target and cause inappropriate behaviors [44]. Specific steps of the protocol may generate the desire for DoS attacks based on the design of this protocol. Additionally, although the protocol might be secured and designed very well, putting it on with other protocols might cause bad circumstances [45]. The ping of death attack is an example of this kind of attack. DDoS TCP SYN attack is also an example of protocol vulnerability attack. It performed by sending fake TCP SYN request to victim server and exploiting the three-way handshake between sender and receiver [41]. With spoofed source IP address and by using many zombies attacker to send large amount of TCP SYN requests to the targeted victim. After receiving these packets, the server in the victim side will send ACK+SYN replies. Thus, the server will run out of resources and processor when a large number of SYN request is being received. Moreover, the agents may send PUSH+ACK TCP packets to the victim server. When the victim server found that packets it indicates that all the data in the TCP buffer should be unloaded. Then, it sends the acknowledgment when completed. At the end, the server cannot process that much amount of data sent by agents and the system will go down [38].

4.2.2. *Malformed Packet DDoS Attacks*

The term malformed packet denotes that the packet covered with pernicious data or information. Usually, in such kind of attack, the attackers depends on sending this wrapped data formed as packets to the targeted victim to flood and saturate its resources [21]. Many protocols can be used by attacker to launch this malformed packet attack. For instance, malformed packet attacks that targeted IP protocol. This kind of attacks can be performed and categorized into two different attacks [12]. In the case of IP address attack, same destination and source IP address are utilized to wrap the packet which creates chaos and confusing the operating system of victim and may rapidly slow it down and smash it. However, in IP packet

options attacks, the attackers use the optional field (the quality of service bits) that exists in each of IP packets to carry additional information and form a malformed packet. For example, assigning one for all the bits related to the quality of service, may lead to handling the packet by the victim takes additional time and as a result it slows down the target's system which may lead to crash it [12, 21]. When the attack uses more than one zombie, victim systems will be more vulnerable.

4.2.3. Slow DDoS Attack

It is called also Slowloris. This attack considered to be the recent development of DoS threats. Matching between both the old DoS flooding based attacks and the Slow DoS attacks (SDA), we can conclude that Slow Dos attacks are primarily distinguished by utilizing a few of network bandwidth [47]. Slow DoS attack usually works at the layer of application. This kind of attack is used to allowing one web server to bring down another server, without having an effect on any other ports or services on the target network. That's why it is considered highly-targeted attack. it performs this by keep creating an open connections as many as possible with the targeted web server and keep these connections open for as long as possible [28]. It achieves that by generating connections and sending only a partial request to the target server [38]. For example, Slowloris constantly directs more HTTP headers, but always do not complete it. This eventually overflows the maximum concurrent connection pool. As a result, this causes a denial of further connections from authentic clients as shown in Figure 12 below.

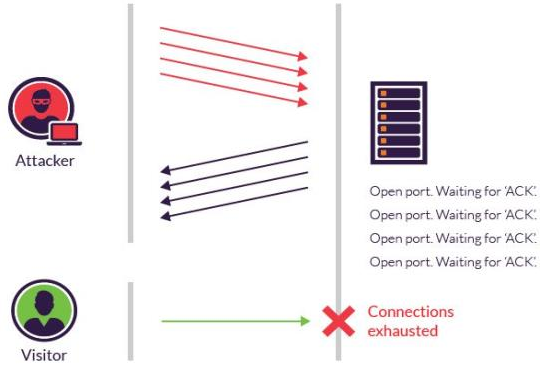

Fig.12. an example of Slow DoS attacks.

5. DDoS Attacks on the Cloud Computing Components

Cloud computing mainly involves several new technologies such as virtualization and SOA, which are susceptible to numerous external and internal security issues especially, targeted the public clouds [48]. In cloud environment, it is possible for DDoS attacks to be categorized depend on the origin of the attack as external Distributed Denial of Service attacks and internal Distributed Denial-of Service attacks.

External Distributed Denial of Service attacks: where an external botnet attackers have the ability to successfully send and load a Trojan horse that covers a thousand or hundreds of VMs running in a cloud. This compromised VMs or botnet can be used to be as a source of any further attacks toward external victims [49].

Internal Distributed Denial of Service attacks: These kinds of attacks are more dangerous than External DDoS attacks. It is possible to lead to disrupting the infrastructure of the cloud completely [49]. Normally, in this attack, the internal botnet attackers targeting a group of virtual machines working on the same cloud. [49, Fig 13] shows an examples of Internal and External DDoS attacks towards cloud infrastructure.

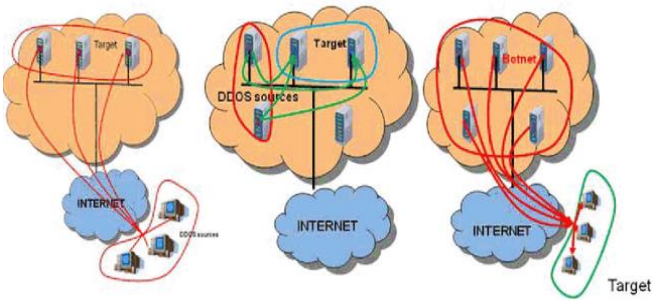

Fig. 13. Internal and external DDoS towards cloud infrastructure

Thus, it is possible to a cloud to be as the source of many external and internal DDoS threats when the cloud has significant security vulnerabilities especially in public clouds. The remainder of this part defines these kinds of DDoS attacks in detail. Figure 14 shows the taxonomy of popular DoS attacks targeted the components of cloud computing environment.

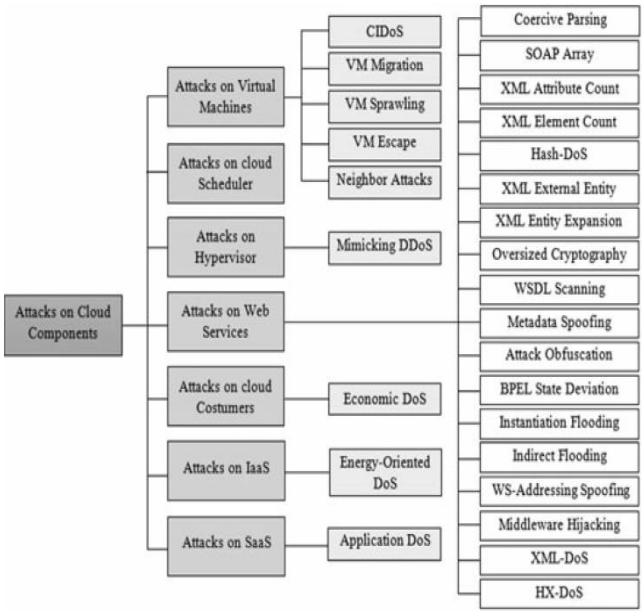

Fig. 14. Classification of the denial-of-service attacks targeted the components of cloud computing environment.

5.1. Attacks against Virtual Machines

The technology of virtualization provides many characteristics in isolation, sharing, and managing of the cloud resources. Thus, it is considered to be the essential technology for cloud's infrastructure [50]. Using virtualization, numerous VMs can be hosted on a single machine [51]. Also, several virtual machines can be shrunk, composed, moved, or automatically expanded based on changing on the demand. Figure 15 shows the diagram of hosted virtualization. The hypervisor or Virtual Machine Monitor (VMM) is the software layer that is responsible for maintaining the isolation between the VMs in addition to managing and creating them [52].

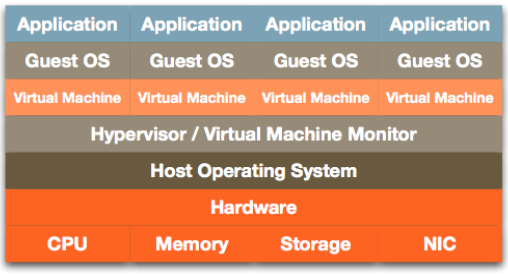

Fig. 15. Hosted Virtualization.

Hypervisor should also detect any malicious actions or behaviors, by monitoring the applications and operating systems related to the guest [53]. The cyber security threats in the physical system are similar to the security threats that could threaten VM environment. Normally, the security threats in a virtual environment can be performed amongst several items [54]: Between the VMs and their host, Between the VMs, Guest-to-guest attack, VM monitor from the host, External modification of a VM, VM monitor from another VM, and External modification of a hypervisor. Actually, we need security methods in each Virtual Machine (VM), since the operating system (OS) of the guest can access the network [55]. In the clouds environment, there are Some DoS threats are performed by exploiting some features in the VM such as misusing some migration features and degrading the ability of service provider to fulfill the requirements of the agreement between the clients and the cloud provider in the form of service level agreement (SLA). Moreover, the migration between the VMs improves the power saving percentage in the data centers of the cloud environment. It also provides an efficient utilization to the physical resources used in the data center. Typically, in case one of the cloud's servers is overloaded, then the VMs hosted in this server can be migrated to other servers that are lightly loaded. Additionally, for power saving, and when some servers in the cloud are underused, their hosted Virtual Machines can be conjoined into less numbers of servers. Nevertheless, VM migration operation is actually a costly process since the state of a certain VM is transmitted from one server to another [56].

5.1.1. *Virtual Machine Migration Attack*

This kind of attack is done by increasing the exhaustion of the VMs's resources conducted by the malicious attackers. This attack leads to degrading the cloud's performance and causes many costly migrations of Virtual Machine from one host to another [57]. When a DDoS attack overloaded a physical server in the cloud, unfortunately the migration process of Virtual Machine not only does not mitigate the issue, but also it might break down the system's status [58].

5.1.2. *Cloud-Internal DoS Attack*

This attack is classified as Internal Distributed Denial of Service attack since it is a cloud-specific attack. The attackers in this kind of attack consist

of several malicious VMs hosted on the same physical server (host) in a cloud. Thus, the attackers try to attack their host on the same cloud [59]. These malicious VMs use different protocol and converting channels strategy to coordinate with each other. By launching this attack, the attackers overwhelm the host's capacity so the host will not be able to deal with the load, by increasing their resource usage. Since the behavior of the attackers during the attack is look like the usual workload of a highly busy server, this kind of attack is difficult to detect.

5.1.3. *Virtual Machine Sprawling Attack*

In the virtual environment, the management strategy of VM is very crucial, where unsuitable VM management procedure can lead to this kind of attack which is called Virtual Machine sprawling attack. In this case, constantly there will be an increasing of the number of Virtual Machines, even though some of them do not back from sleep or even some of them are idle [60]. Thus, the bad VMs management strategies can lead to create more vulnerabilities and entry points for attackers to launch their attack and overwhelm the cloud resources [61].

5.1.4. *Neighbor Attack*

Neighbor attack considers one of the possible DoS attacks directed toward the system of cloud virtualization, which is caused by inappropriate vulnerabilities and configurations in the hypervisor. In this attack and in the same physical machine (host) the virtual machines can attack each other where each VM causes greatest workload to other neighboring VM. This DoS attack may cause destructive effects on the hosted servers. Thus, it can affect the total performance of cloud infrastructure [62]. Neighbor attacks between virtual machines are showed in [52, Fig. 15] below.

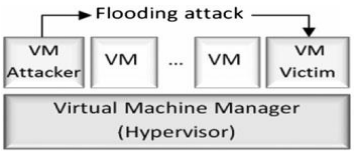

Fig. 15. Virtual Machines' Neighbor attack.

Virtual Machine Escape Attack

The attackers in this attack use a malicious application to be executed in a VM. In this case, this infected VM will have the ability totally to avoid or ignore the hypervisor and gain access to the physical server that hosts the infected VM. When it gets access to the system of the host, it also gets from the infected VM all the escapes and root privileges such as the access rights and privileges. This causes paralysis of the host security system. Though, we can protect the host from this kind of attacks, by appropriately setting the configurations related to the interactions between the host and the guest [54].

5.2. Attacks on Hypervisor

In this kind of attacks, a customer of a cloud can install a malicious guest OS by leasing a guest VM. Then, by installing this malicious OS the attackers are ready to attack the hypervisor through getting access to the neighboring VMs's memory contents and changing the source code of the hypervisor [63].

The attackers of DDoS can conceal their attacks in the Mimicking DDoS Attacks, by imitating authentic traffic to avoid detection [64]. DoS attack detection methods can be swindled by DDoS attackers when the attackers have the ability to mimic the traffic patterns of the network using monitoring systems that can detect the network traffic patterns. Yet, differentiating between the imitating DDoS attacks and the high stream of traffic caused by legitimate users still an open challenge.

5.3. *Attacks On Cloud Customers Or EDoS Attack*

Service Level Agreement (SLA) is considered to be the contract between the clients and the cloud service provider. It means that SLA includes the services offered by the cloud provider and also includes the level of these provided services that are required by the user [17]. One of the ever serious attacks targeted both the cloud providers and the cloud customers are called Economic DoS (EDoS) where the attackers sends numerous phony requests to the providers of the cloud services. The workload on the cloud will be increased and that will lead to increase the bill of the customer. This kind of attack relies on the resources affordability,

configuration of the server, and the availability of the cloud customers [65, 66]. EDoS attacks are so critical to SLA, because meeting the SLA; it means that to provide a formal assurance of the availability of the service to the targeted user, the cloud service providers have to allocate more resources, which leads to extra cost for the attacked user to pay [67].

5.4.*Attacks On Cloud Scheduler*

The Hypervisor or the monitor of virtual machines has the ability to administer several VMs. The scheduler of this virtual machine monitor may be accessible and exposed to be attacked by some malicious actions of the VMs. Thus, this possibly will lead to inaccurate or unfair scheduling of VMs. For instance, an open-source Virtual Machine Monitor (VMM) Xen is used for both the ×86 and ×64 platforms. This VMs monitor utilizes a mechanism for VMs scheduling that might be unsuccessful in calculating the CPU usage that belongs to some VMs that behaved poorly. In [55], Fangfei et al. proposed in his paper that in Amazon's Elastic Compute Cloud service (EC2), there is a vulnerability that permits customers with a malicious behavior to get improved service at the loss of others. They have also discovered that the applications that take advantage of this issue, have the ability to use the CPU core up to 98% of a CPU power, disregarding of the VMs's competition between each other. In order to resolve this issue, Amazon Elastic Compute Cloud service utilizes a copy of patched Xen [68].

6. Software As a Service DDoS Attacks

Generally, Distributed Denial of Service attacks that targeted applications mainly focus on the software as a service (SaaS) clouds. They take advantage of defects or faults in the applications to deny legitimate clients from accessing to the different services provided by victim (targeted cloud service provider). This kind of attack is difficult to trace it back, that's why the current solutions for security monitoring may not have the ability to detect it. Usually, these kinds of attacks utilize protocols such as HTTPS or HTTP and use proxy servers to blur the source of the attack [69].

5.5.Infrastructure As a Service DDoS Attacks

Cloud infrastructures including the data centers can be extremely affected by DDoS attacks. Currently, there is a new form of DDoS attack that is described as Energy-oriented attack that has very bad impact to the cloud infrastructures. The attackers in this attack are trying to do some malicious actions that lead to overwhelm the victim as much as possible with a huge amount of workload. Thus, the targeted victim continuously will be fully busy serving the malicious actions caused by the attackers. In consequence of this attack, there will be extra consuming and wasting the energy of the cloud data center. This in turn leads to increasing the costs of the penalty on the cloud providers because of the extra gas emissions come from the over utilization of the cloud data centers [70].

5.6.DDoS Attacks On Web Services

Web service as a definition is a standardized way of communicating between two devices connected with each other by a network. It also utilizes a standardized Extensible Markup Language (XML) to encode all the messages and communications that may occur between the connected devices for a purpose of exchanging data. For example, Simple Object Access Protocol is actually an XMl based protocol (SOAP) used for data exchanging purposes. Generally, there are many DoS attacks that conducted against web services and in this part we briefly define the popular DoS attacks that performed against web services which are as the following:

• Attack of Coercive parsing: This kind of attack consider being one of the simplest attacks where the attackers try to attack the web service to exhaust its system resources [71]. They only send an SOAP message and they include in the SOAP body huge number of opening tags. It means that, a very extremely nested XML document is directed by the attacker towards the attacked web server or service. In this attack, this may lead to a high CPU usage in addition to causing error in the memory when the parser trying to process this malicious XML document [71]. Figure 16 presents an example of an infected XML document used in this kind of DDoS attack.

```
<soapenv:Envelope xmlns:soapenv="..." xmlns: soapenc:"...">
<soapenv:Body>
 <x>
   <x>
     <x>
       <x>
         <x>
             <!-- Continued for as long as wanted by the attacker -->
```

Fig. 16. An example of an infected XML document used in Coercive parsing attack

• SOAP array attack: In this kind of attack the web service is imposed by the attackers to send huge SOAP messages [72]. Figure 17 shows an example of an XML document used in SOAP array attack.

```
<soapenv:Envelope xmlns:soapenv="..." xmlns: soapenc:"...">
<soapenv:Body>
<ns1:FunctionWithArrayInput xmlns:ns1="...">
<DataSet xsi:type="soapenc:Array"
soapenc:arrayType="xsd:string[1000000]">
<item xsi:type="xsd:string">Data1</item>
<item xsi:type="xsd:string">Data2</item>
<item xsi:type="xsd:string">Data3</item>
</DataSet>
</ns1:FunctionWithArrayInput>
</soapenv:Body>
</soapenv:Envelope>
```

Fig. 17. An example of an XML document used in SOAP array attack

• The Attack of XML attribute count: This type of attack is similar to Coercive parsing attack where the body of SOAP message includes huge number of attributes that will be directed to the server.

• The attack of XML element count: In this attack, several non-nested elements will be included in the body of SOAP messages that will be sent the server [71].

• Hash collision attack (Hash DoS): By forwarding one huge POST message that is fully loaded with several types of variables. Then, to process this huge message, the sever needs to use some hashing mechanisms to handle this message [73]. As a result, this operation consumes the processing power of the server and it could take an hour for the server to finish processing this single request. That is what is called a hash denial-of-service (DoS) attack.

• The attack of XML external entity: It imposes the server to analyze and parse a very big external entity document that is well-defined in a set of markup declaration called Document Type Definition (DTD) [74].

• XML entity expansion: This kind of attack is also called “XML bombing”. This attack performed by exploiting one of the XML’s capabilities which is called an XML nesting capability [75].

• Oversized cryptography: In this attack a big amount of the numerically signed or encoded parts of SOAP message is attached in the message by the attackers [76].

•Web Services Description Language (WSDL) scanning: WSDL defined as a document that has an XML format and used to characterizing the services of the network. It is also used to determine the parameters used for linking specific methods. So, the information provided by this document contains critical information, which gives a big chance to the attackers to perform other attacks [77].

• Metadata spoofing: in this attack, the attackers have the ability to be aimed to redesign the metadata description of the web service [78].

• Attack obfuscation: The attackers have the ability to utilize the encryption of an XML document to hide the content of the message from being message content from being detected by the IDS or the firewall. These encoded XML document can be utilized to perform other kinds of attacks like coercive parsing attack, XML injection attack, or oversize payload attack [79].

• The attack of Business Process Execution Language (BPEL) state deviation: BPEL engine have the ability to supply the web service with the endpoints, which can accept every probable incoming request message. A single process of BPEL engine may have several instances working simultaneously. Due to the fact that these endpoints that used for communications are available for any connections arriving at whatever time. Therefore, a malicious Web Service attacker might attack these unlocked endpoints. So, the attackers have the ability to send a huge amount of messages that are not associated with any current process instances [80]. Consequently, by processing such an invalid messages sent by the

attackers, the resources that are related to the computational process of the BPEL engine will be overloaded.

• Instantiation flooding attack: In this attack, a new instance of the BPEL procedure will be formed for each time a new message or request arrives. Then, the instructions that are existed in the description document of the process will be executed. Thus, the attackers have the ability to attack the BPEL engine through transferring a huge amount of requests messages to the process of BPEL [80].

• Indirect flooding: The concept of this attack is to utilize the BPEL engine in-between as an intermediary for an attack on a system targeted backwards the BPEL engine. Think of a process of BPEL that continually invokes a Web Service provided by the system that the attackers intend to attack. By saturating the BPEL engine's process with contaminated messages by the attackers, the BPEL engine will suffer from a massive workload itself. And at the same time, this simply will lead to similarly weighty workload on the side of the system targeted by the attackers. Consequently, if the system targeted indirectly by the attackers is not as strong and robust as the BPEL engine, it will result in a Denial-of-Service of the targeted system [81].

• Web Service (WS)-addressing spoofing: The attackers in this kind of attack send the requests of SOAP messages to the targeted server. These messages contain the header of WS-addressing. Thus, in this case, the server distributes the response of SOAP for a various endpoints that can be utilized to overflow another web service [82].

• The attack of Middleware hijacking: This kind of attack is similar to attack of WS-addressing spoofing, except that it directs the endpoint URL of the attackers to a system that is already exist. Then, at the specified URL a real service will be run by the attackers. Thus, the server of the web service will continually try to response to the requests that had been sent by the attackers [71].

• XML-based denial-of-service attacks: This attack indicates that the saturating XML messages will be sent by the attackers to the web service in order to saturate all the resources of the server side. In other words, the DX DoS attack consider to be the distributed form of the X DoS attack, that utilizes several hosts to perform the attack [83]. Often, in this kind of attack, the content of the message is contaminated to crash and saturate the web server. Due to the parsing process of these messages and since the design of XML documents is complex, even a small distorted message of XML can waste a huge number of server resources [74].

• The attacks of HX-DoS: Generally, the web services on the cloud work using XML and HTTP protocols for example SOAP. One of the serious attacks targeting the service provider of the cloud is the HX-DoS attack. This attack performs using two protocols the HTTP and the XML protocol [84]. HX-DoS attack is utilized to saturate the channel of communication of the cloud providers by using messages that are composed of both HTTP and XML messages. In fact, the illegal messages composed by the attackers should be differentiate in order to identify the issue of HX-DoS attacks against the web services cloud providers [85].

6. Cloud DDoS Detection Techniques

As DoS attacks turn out to be more popular against the cloud computing environment, a more prominent need is required to provide solutions to put an end and control such critical threats. Several DDoS protection techniques have been proposed since the commencement of the attack in 1999, when a DDoS tool called Trinoo was setup on roughly 227 hosts to crash a single PC in the University of Minnesota [86]. DDoS mitigation techniques are meant to avoid DoS attacks to happen or if nothing else relieve their impact. In general, protection against DoS threats can be partitioned into the three principle classes, which are attack prevention, attack detection, and attack response [87]. DDoS detection methods and frameworks have been examined and investigated a lot in the literature. That's why it needs a separate research study and it is beyond the scope of this survey. Briefly, we examined and listed some (Intrusion Detection Systems) IDSs that have been proposed recently to identify and prevent DDoS attacks in the clouds as shown in table 2 below.

Table 2. DDoS Detection Techniques in cloud environment

References	Detection / Mitigation	Detection Time	Year
Holistic DDoS Mitigation Using NFV, [88] 2017	Mitigation	Periodic	2017
Results: NFV (Network Functions Virtualization) and edge computing architectures are used to design a two-stage DDoS mitigation framework, which first scanning and analyzing the traffic and then decides what next-stage procedures are required for traffic flows. Its purpose is defending against all kinds of DDoS attacks.			
NIDSV: Network based Intrusion Detection and Counter-measure Excerption in Virtual Environment using AODV protocol. [95] 2017	Detection	Periodic	2017
Results: The main purpose of NIDSV system is to detect and monitor the traffic to capture the fishy process associated to alert. NIDSV uses Alert Correlational Graph (ACG) model to take attack anticipation and detection action.			
Distributed Denial of Services Attack Protection System with Genetic Algorithms on Hadoop Cluster Computing Framework, [94] 2015	Detection and Mitigation	Real time	2015
Results: This paper proposes a real-time, scalable traffic pattern analysis for protecting against DDoS attacks. This protection system developed based on genetic algorithm to prevent and detect DDoS attacks using the popular distributed processing infrastructure Hadoop.			
Design and Implementation of Cloud Security Defense System with Software Defined Networking Technologies, [93] 2016	Detection and Mitigation	Real time	2016
Results: is a real time Security Policy Decision System used in the cloud to detect the distributed denial of service (DDoS) attacks. This system designed based on OpenStack to create and combine multiple vIDS with multiple vFirewall to filter the packets sent by the attackers. In order to distribute the flow of packets to multiple vIDS, this detection system uses SDN technology to analyze and detect the attack packets and direct traffic to elsewhere.			
CAAMP: Completely Automated DDoS Attack Mitigation Platform in Hybrid Clouds, [92] 2016	Mitigation	Periodic	2016
Results: CAAMP is a Completely Automated DDoS Attack Mitigation Platform. This novel platform used on public cloud applications to mitigate DDoS attacks by utilizing the capabilities of network function virtualization and software defined infrastructure techniques. When a fishy traffic is recognized, CAAMP installs on-the-fly a copy of the application's topology (which is called shark tank) on an isolated private cloud. Then it creates a virtual network to host that copy of application's topology. The controller of the Software defined networking (SDN) dynamically arranges the virtual switches to redirect the fishy traffic to the shark tank until final decision is made.			
FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers, [91] 2016	Detection and Mitigation	Real time	2016
Results: FlowTrApp is a software defined networking (SDN) framework used for DDoS sensitive cloud and data-center applications. It achieves DDoS mitigation and detection using some bound information on two per flow based traffic parameters. The algorithm of FlowTrApp is based on taking incoming flow with a legitimate sample of traffic as an input and it classifies a traffic flow based on this information as either legitimate traffic or attack traffic. It attempts to distinguish the ranging of attack traffic from long lived to short lived attacks and from low rate to high rate using an SDN engine. If the flow is found not lying in the bounds of legitimate traffic pattern, it will install the mitigation actions against it.			
A Hadoop Based Analysis and Detection Model for IP Spoofing Typed DDoS Attack, [90] 2016	Detection	Periodic	2016
Results: This paper proposed an efficient and robust model for detecting of DDoS attack on cloud services. It focused on calculating the number of abnormal packets using two inbound and outbound rules, by designing a Hadoop based Periodic TCP/UDP flow statistics framework to work as an abnormal check mechanism. To evaluate the model, they made some experiments which showed that the detection model has strong characteristics in adaptability of different attack scale, sensitivity to attack traffic, and timeliness of detection.			
Mitigating HTTP Flooding Attacks with Meta-data Analysis, [89] 2015	Detection and Mitigation	Real time	2015
Results: This proposed DDoS protection system has the ability to serve the legitimate clients continuously even when the attacking line-rate raises up to 9 Gbps. An intelligent examination is first utilized for extracting the meta-data related to HTTP connection. Then, on the top of the meta-data, a big-data analyzing technique is applied on real time to match the IP addresses whose HTTP request frequency significantly exceeds the norm. These IP addresses are further aggregated in a form of blacklist, enabling load balancers and firewalls to apply the rules of rate-limiting in order to mitigate the attacks.			

7. Conclusion

A single-solution and one size fits all method unfortunately is ineffective to deter and prevent DDoS attacks, which are still the most common cybercrime threat. In addition to law and legislative precautions, technology also plays an essential role in preventing such threats. This can be done by optimizing protection measures that include prevention, detection, correction and reaction measures. All the possible administrative, legislative and technical solutions, if undertaken simultaneously will bring about a more expectant synergy in improving the protection of e-government information systems from DDoS-related cybercrimes [96].

Currently, cloud computing is considered to be the newest computing paradigm that offers numerous flexible and consistent services. It is also a fast growing technology and extensively recognized as the computing paradigm in all over the world through its characteristics such as large storage space, fast deployment and distribution, cost efficiency, and the availability for accessing to the system from anywhere and anytime. Increasing tendency of government services to make use of cloud services poses an emerging threat for e-government and e-governance applications. The bitter truth is that, in order to get benefit from this technology, it has to be visible on the unprotected internet networks. With this reality, cloud can be exposed to data confidentiality threats and unauthorized attacks would constantly look to attack the services provided by the cloud. Furthermore, availability of botnets and virtualization in the cloud systems poses another threat for effectiveness of DDoS attacks. The impacts of the non-availability of government services and resources in the cloud are calamitous; and this can lead to a partial or even total failure of delivering the required service.

This survey it is explained that main categories of DDoS attack and discusses the weaknesses or vulnerabilities which are used to fire each kind of the attack and it is categorized that the DDoS attacks according to the targeted cloud components. By analyzing and surveying several DDoS attacks, we have come to a fact that a DDoS attack has huge effects upon all internet community including cloud computing and other distributed systems. Considering criticality of e-government applications for national and local government bodies that uses cloud infrastructure, DDoS attacks can be number one threat giving major harms by cyber warriors and terroristic organizations.

As cloud computing develops day by day, at the same time DDoS attacks becomes more sophisticated to the degree that can lead to even overwhelm a cloud provider. With a high availability, resilient control infrastructure, and low cost, it is confirmed that DDoS is not going to be disappeared. As DDoS attacks are on growth in all developing technologies, we can anticipate in the future, that many vulnerabilities and security measures will also increase. On the other hand, adopting such a cutting edge technology like Quantum computing which is one of a handful solution of the next generation of computing power could be applied to solve cyber security issues. Such as looking for certain patterns in big data repository for intrusion detection purposes and more sophisticated forms of parallel computing that can prevent or mitigate possibly any sophisticated kind of DDoS attacks. To give an integrated picture about DDoS attacks targeting cloud computing environment, this survey can be extended to include all the antidotes, defense mechanisms and intrusion detection applications that had been used to deal with, detect, and prevent such kind of DDoS attacks. Furthermore, quantum computers can provide fertile and unchallengeable platforms for setting up DDoS attacks via Botnet VMs million times faster than single core traditional computer.

Following measures should be taken against DDoS attacks over e-government services:

- Integrating business objectives with security concerns and resources using a wisdom model [97, 98],
- Using a comprehensive framework such as COBIT-5 to have an integrated and holistic approach of both governance and management of business and IT services and measurable processes [99],
- Providing staff awareness and capability with pertinent training and required

Professional certifications such as CISM, CRISC and CSX.

- Monitoring internal network traffic and usage of server resources, such as Domain Name Server (DNS) and web server, to detect early traffic spikes and abnormal utilization of system resources.
- Logging security events and review alerts generated by security system, such as Intrusion Detection System (IDS) or Intrusion Prevention System (IPS), anti-malware solution, Internet gateway and firewall, to detect suspicious activities.
- Considering of segregating network so that critical and normal services can utilize different network connections.
- Increasing network's resilience against DDoS activity by implementing at least two links to the Internet via different ISPs.
- Considering adopting third-party security service for DDoS protection via content delivery network and distributed DNS service.
- Developing business contingency plan and conduct drill regularly on what actions should be carried out in the event of a DDoS attack.
- Reporting the case and seek advice from relevant organizations,
- Applying latest security updates and patches to computer and network devices to fix known security vulnerabilities timely.
- Adopting security solutions such as IDS/IPS, anti-malware solution, firewall, etc. for your computer and your network at the border.
- Setting up a demilitarized zone (DMZ) network for Internet facing servers and locating internal computing facilities behind firewalls.
- Configuring network devices properly by hardening security configurations to drop unnecessary network traffic. For example, blocking unnecessary ping traffic and request from unauthorized network port.
- Performing security risk assessments and audits regularly to ensure adequate security measures have been adopted.

References

[1]. H. Nemati, *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications*, New York: IGI Global, 2008, Ch.1.1.

[2]. P. Mell and T. Grance. "The NIST Definition of Cloud Computing". *National Institute of Standards and Technology (NIST) Special Publication*. Gaithersburg, MD. https://csrc.nist.gov/publications/detail/sp/800-145/final, 2011.

[3]. Z. Chiba, N.Abghour, K. Moussaid, and M. Rida, " A Survey of Intrusion Detection Systems for Cloud Computing Environment", *International Conference on Engineering & MIS (ICEMIS)* 2016; 1-13.

[4]. U. Oktay and O. K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing," *6th International Information Security & Cryptology Conference*, vol. 9, pp. 71–76, 2013.

[5]. J. Varia, "Best practices in architecting cloud applications in the AWS cloud", *Cloud Computing. Principles and Paradigms*, John Wiley & Sons, Inc. Jan 2011, pp. 459-490.

[6]. K. C. Okafor, J. A. Okoye, and G. Ononiwu, "Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective," *International Journal of Computer Applications*, vol. 138, no. 7, pp. 18–30, 2016.

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

[8]. H. Kaur and S. Behal, "Characterization and Comparison of Distributed Denial of Service Attack Tools," *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 1139–1145, 2015.

[9]. M. J. Hashmi, M. Saxena, and R. Saini, "Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System", *International Journal of Computer Science & Communication Networks*, vol. 2, no. 5, pp. 607–614.

[10]. A. Khadke and M. Madankar, "Review on Mitigation of Distributed Denial of Service (DDoS) Attacks in Cloud Computing.", *10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1-5, 2016.

[11]. K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, "A survey of distributed denial of service attack," *10th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, pp. 1-6, 2016.

[12]. B. Prabadevi, "Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey", *Networks, Computers and Communications, The 2014 International Symposium,* 2014.

[13]. O. Achbarou, M. Ahmed, and S. El Bouanani, "Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems", *International Journal of Interactive Multimedia and Artificial Intelligence,* pp. 61–64, 2017.

[14]. R. M. Jabir, S. Ismail, R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of Cloud Computing Attacks and Countermeasures," *Advanced Communication Technology (ICACT), 2016 18th International Conference,* pp. 117–123, 2016.

[15]. S. Singh, "Cloud computing attacks: a discussion with solutions". *Open Journal of Mobile Computing and Cloud Computing,* 2014.

[16]. B. Grobauer, T. Walloschek, and E. Stocker "Understanding cloud computing vulnerabilities". *Security & privacy, IEEE,* 9(2): 50–57, 2011.

[17]. S. VivinSandar, S. Shenai, "Economic denial of sustainability (EDoS) in cloud services using http and xml-based DDoS attacks". *International Journal of Computer Applications,* 41(20): 11–16, 2012.

[18]. A. Bhardwaj, G. Subrahmanyam, V. Avasthi, and H. G. Sastry, "Solutions for DDoS attacks on cloud" 2016 *6th International Conference - Cloud System and Big Data Engineering* (Confluence), Noida, pp. 163-167, 2016.

[19]. https://www.infosecurity-magazine.com/news/q1-2015-ddos-attacks-spike/, Security and technical news, "Q1 2015 DDoS attacks spike, targeting cloud", Latest Access Time for the website is 19 January 2018.

[20]. Arbor Networks, "10th Annual worldwide InfrastructureReport".http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf, 2014.

[21]. R. V Deshmukh and K. K. Devadkar, "Understanding DDoS Attack & Its Effect in Cloud Environment," *Procedia - Procedia Computer. Science.*, vol. 49, pp. 202–210, 2015.

[22]. https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/L, "Greatfire.org faces daily $30,0 0 0 bill from DDoS attack", Latest Access Time for the website is 22 January 2018.

[23]. Kaspersky Labs, "Global IT security risks survey 2014 -distributed denial of service (DDoS) attacks", https://media.kaspersky.com/en/B2BInternational-2014-Survey-DDoS-Summary-Report.pdf, 2014.

[24]. Arbor Networks, "11th Annual worldwide InfrastructureReport".https://www.arbornetworks.com/arbor-networks-11th-annual-worldwide-infrastructure-security-report-finds-relentless-threat-environment-driving-demand-for-managed-security-services-and-incident-response-support, 2016.

[25]. Arbor Networks, "Understanding the nature of DDoS attacks",https://www.arbornetworks.com/blog/asert/understanding-the-nature-of-ddos-attacks/, 2012.

[26]. Neustar News, "DDoS attacks and impact report finds unpredictable DDoSlandscape", https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddos-report.pdf , 2016.

[27]. Cisco, "The Zettabyte Era — Trends and Analysis – Cisco",https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html, 2016.

[28]. J. N. Ahamed, "A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment," *International Journal of Security and its Applications,* vol. 10, no. 8, pp. 277–294, 2016.

[29]. Akamai, "Akamai Cloud Security Solutions: Comparing Approaches for Web, DNS, and InfrastructureSecurity",https://www.akamai.com/es/es/multimedia/documents/content/comparing-approaches-for-web-dns-infrastructure-security-white-paper.pdf, 2016.

[30]. Forescout, "Forescout IoT enterprise risk report" https://www.forescout.com/wp-content/uploads/2016/10/ForeScout-IoT-Enterprise-Risk-Report.pdf, 2016.

[31]. https://www.helpnetsecurity.com/2016/10/31/extinguish-mirai-threat/, "Can we extinguish the Mirai threat", Latest access Time for the website is 22 January 2018.

[32]. https://blog.radware.com/security/2017/03/cost-of-ddos-attack-darknet/, "The cost of a DDoS attack on thedarknet", Latest Access Time for the website is 22 January 2018.

[33]. Cisco, "Fog Computing and Internet of Things: Extend the Cloud to Where the Things Are, A white paper," *Cisco Reports,* pp. 1-6, April 2015.

[34]. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, KrebsOnSecurity Hit With Record DDoS, Latest Access Time for the website is 22 January 2018.

[35]. http://www.telegraph.co.uk/technology/2016/11/04/unprecedented-cyber-attack-takes-liberias-entire-internet-down/ , "Unprecedented Cyber Attack Takes Liberia's Entire Internet Down", Latest Access Time for the website is 22 January 2018.

[36]. http://www.bbc.com/news/technology-37859678, "Hack attacks cutt internet access in Liberia", Latest Access Time for the website is 22 January 2018.

[37]. A. Efe, Risk Optimization as a Governance Goal of Regional Development Agencies in Turkey: An Analysis with COBIT-5 Framework, *International Journal of Education, Science and Technology,* 1 - 18, 2016.

[38]. F. Wong and C. Tan, "A survey of trends in massive DDoS attacks and cloud-based mitigations," *International Journal of Network Security & Its Applications (IJNSA),* vol. 6, no. 3, pp. 57-71, May 2014.

[39]. P. Revathi, "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.

[40]. M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Security and Communication Networks, John Wiley & Sons, Ltd*, no. July, pp. 3724–3751, 2016.

[41]. M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS Attacks and Defenses," *Information Society (i-Society), 2013 International Conference on IEEE*, pp. 67–71, 2013.

[42]. A. Colella, C. Colombini, "Amplification DDoS Attacks: Emerging Threats and Defense Strategies, in Availability, Reliability, and Security in Information Systems". *Springer*, 298–310, 2014.

[43]. B. Sieklik, R. Macfarlane, and W. J. Buchanan, "Evaluation of TFTP DDoS amplification attack," *Computers & Security Elsevier*, vol. 57, pp. 67–92, 2016.

[44]. K. Harrison and G. White, "A taxonomy of cyber events affecting communities". In System Sciences (HICSS), 2011 *44th Hawaii International Conference on. IEEE*, 2011.

[45]. V. Zlomislic, K. Fertalj, and V. Sruk, "Denial of service attacks: an overview. *In Information Systems and Technologies (CISTI), 2014 9th Iberian Conference on IEEE*, 2014.

[46]. S. Shafieian, M. Zulkernine and A. Haque, "CloudZombie: Launching and Detecting Slow-Read Distributed Denial of Service Attacks from the Cloud," *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Liverpool, pp. 1733-1740, 2015.

[47]. P. Farina, E. Cambiaso, G. Papaleo and M. Aiello, "Understanding DDoS Attacks from Mobile Devices," 2015 *3rd International Conference on Future Internet of Things and Cloud*, Rome, pp. 614-619, 2015.

[48]. M. Komu, M. Sethi, R. Mallavarapu, H. Oirola, R. Khan, and S. Tarkoma, "Secure Networking for Virtual Machines in the Cloud". *In CLUSTER Workshops*, 88–96, 2012.

[49]. J. Latanicki, P. Massonet, S. Naqvi, and B. Rochwerger, "Scalable Cloud Defenses for Detection, Analysis and and Mitigation of DDoS Attacks", *Towards the Future Internet G. Tselentis et al. (Eds.) IOS Press*, doi:10.3233/978-1-60750-539-6-127, 2010.

[50]. A. Bakshi, B. Yogesh, "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.

[51]. R. Shea, J. Liu, "Understanding the impact of denial-ofservice attacks on virtual machines". *In Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service. IEEE Press*, 2012.

[52]. J. Szefer, E, Keller, R. Lee, and J. Rexford, "Eliminating the hypervisor attack surface for a more secure cloud". *In proceedings of the 18th ACM conference on Computer and communications*, 401-412, 2011.

[53]. J. Szefer, R. Lee, "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.

[54]. J. S. Reuben. "A Survey on Virtual Machine Security", Vol. 2. *Helsinki University of Technology:* Helsinki, 36, 2007.

[55]. Z. Fangfei, M. Goel, P. Desnoyers, R. Sundaram, "Scheduler vulnerabilities and coordinated attacks in cloud computing". *Journal of Computer Security*, 21(4): 533–559, 2013.

[56]. M. Masdari, S. S. Nabavi, V. Ahmadi, "An overview of virtual machine placement schemes in cloud computing". *Journal of Network and Computer Applications*, 66: 106–127, 2016.

[57]. Y. Wang, J. Ma, D. Lu, X. Lu, L. Zhang, "From high availability to collapse: quantitative analysis of "Cloud-Droplet-Freezing" attack threats to virtual machine migration in cloud computing". *Cluster Computing*, 17(4): 1369–1381, 2014.

[58]. K. Lazri, S. Laniepce, H. Zheng, J. Ben-Othman, "AMAD: Resource Consumption Profile-Aware Attack Detection in IaaS Cloud". *In Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on. IEEE*, 379–386, 2014.

[59]. S. Alarifi, S. D. Wolthusen, "Mitigation of cloud-internal denial of service attacks". in Service Oriented System Engineering (SOSE), 2014 *IEEE 8th International Symposium on. IEEE*, 2014.

[60]. M. A. Zardari, L. T. Jung, and N. Zakaria, "A quantitative analysis of cloud users' satisfaction and data security in cloud models". *In Science and Information Conference (SAI)*, 2014. IEEE, 2014.

[61]. E. P. Krishna, E. Sandhya, and M. G. Karthik, "Managing DDoS attacks on virtual machines by segregated policy management". *Global Journal of Computer Science and Technology*, 14(6); 20–24, 2014.

[62]. M. N. Ismail, A. Aborujilah, S. Musa, and A. Shahzad, "New framework to detect and prevent denial of service attack in cloud computing environment". *International*

Journal of Computer Science and Security (IJCSS), 6(4): 226, 2012.

[63]. M. Kazim, R. Masood, M. A. Shibli, and A. G. Abbasi, "Security aspects of virtualization in cloud computing". *In IFIP International Conference on Computer Information Systems and Industrial Management, Springer*: Berlin Heidelberg, 229–240, 2013.

[64]. A. Chonka, J. Singh, and Z. Wanlei, "Chaos theory-based detection against network mimicking DDoS attacks". *Communications Letters, IEEE* 2009, 13(9): 717 719, 2009.

[65]. B. Saini and G. Somani, "Index Page-based EDoS Attacks in Infrastructure Cloud, in Recent Trends in Computer Networks and Distributed Systems Security", *Springer: Springer Berlin* Heidelberg, 382–395, 2014.

[66]. A. Koduru, T. Neelakantam, S. Saira Bhanu, "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.

[67]. M. Masdari, F. Salehi, M. Jalali, and M. Bidaki, "A Survey of PSO-Based Scheduling Algorithms in Cloud Computing". *Journal of Network and Systems Management*, 1–37, 2016.

[68]. M. Masdari et al. "Towards workflow scheduling in cloud computing: a comprehensive analysis". *Journal of Network and Computer Applications*, 66: 64–82, 2016.

[69]. T. Siva, E. S. P. Krishna, "Controlling various network-based ADoS attacks in cloud computing environment: by using port hopping technique". *International Journal of Engineering Trends and Technology* (IJETT), 4(5); 2099–2104, 2013.

[70]. F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, A. Castiglione, "Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures". *The Journal of Supercomputing*, 71(5): 1620–1641, 2015.

[71]. M. Jensen, N. Gruschka, R. Herkenhöner, "A survey of attacks on web services". *Computer Science-Research and Development*, 24(4): 185–197, 2009.

[72]. A. Falkenberg, C. Mainka, J. Somorovsky, and J. Schwenk, "A new approach towards DoS penetration testing on web services". *In Web Services (ICWS), 2013 IEEE 20th International Conference on. IEEE*, 491–498, 2013.

[73]. D. Holmes, "Mitigating DDoS attacks with F5 technology". *F5 Networks*, Inc, 2099–2104, 2013.

[74]. P. Siriwardena, "Security by Design in Advanced API Security". *Springer*, 11–31, 2014.

[75]. I. Siddavatam, J. Gadge, "Comprehensive test mechanism to detect attack on web services". *In Networks, 2008. ICON 2008. 16th IEEE International Conference on. IEEE*, 2008.

[76]. S. Tiwari, P. Singh, "Survey of potential attacks on webservices and web service compositions". *In Electronics Computer Technology (ICECT), 2011 3rd International Conference on. IEEE*, 2011.

[77]. P. Lindstrom, Attacking and defending web services. *Whitepaper*,https://www.cse.iitb.ac.in/~madhumita/seminar/web%20services/Attacking%20and%20Defending%20Web%20Services.pdf, 2004.

[78]. M. Younis, K. Kifayat, "Secure cloud computing for critical infrastructure: a survey". *Liverpool John Moores University*, United Kingdom, Tech. Rep, 2013.

[79]. A. Masood, "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*, 2013.

[80]. A. N. Gupta, D. P. S. Thilagam, "Attacks on web services need to secure XML on web". *Computer Science & Engineering*, 3(5): 1, *2013*.

[81]. M. Jensen, N. Gruschka, N. Luttenberger, "The impact of flooding attacks on network-based services*". In Availability, Reliability and Security*, 2008. *ARES 08. Third International Conference on. IEEE*, 2008.

[82]. C. Mainka, J. Somorovsky, J. Schwenk, "Penetration testing tool for web services security". *In Services (SERVICES), 2012 IEEE Eighth World Congress on. IEEE*, 2012.

[83]. A. Chonka, Y. Xiang, W. Zhou, A. Bonti, "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, 2011.

[84]. S. Farahmandian, M. Zamani, A. Akbarabadi, Y. Moghimi, S. M. Mirhosseini Zadeh, S. A. Farahmandian, "survey on methods to defend against DDoS attack in cloud computing". *System* 2013, 6(22): 26, 2013.

[85]. E, Anitha, S. Malliga, "A packet marking approach to protect cloud environment against DDoS attacks". *In Information Communication and Embedded Systems (ICICES), 2013 International Conference on. IEEE*, 2013.

[86]. M. Bhuyan, H. Kashyap, D. Bhattacharyya, J. Kalita, "Detecting distributed denial of service attacks: methods, tools and future directions," *The Computer Journal*, pp. 6-20, March 2013.

[87]. M. Alenezi, M. Reed, "Methodologies for detecting DoS/DDoS attacks against network servers". In ICSNC 2012, *The Seventh International Conference on Systems and Networks Communications.* 2012.

[88]. T. Alharbi, A. Aljuhani and H. Liu, "Holistic DDoS mitigation using NFV," 2017 *IEEE 7th Annual Computing and Communication Workshop and Conference* (CCWC), Las Vegas, NV, pp. 1-4, 2017.

[89]. D. Tang, A. Tang, E. Lee and L. Tao, "Mitigating HTTP Flooding Attacks with Meta-data Analysis," *2015 IEEE 17th International Conference on High Performance Computing and Communications*, New York, NY, pp. 1406-1411, 2015.

[90]. J. Zhang, P. Liu, J. He and Y. Zhang, "A Hadoop Based Analysis and Detection Model for IP Spoofing Typed DDoS Attack," *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, pp. 1976-1983, 2016.

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

[92]. N. Beigi-Mohammadi, C. Barna, M. Shtern, H. Khazaei and M. Litoiu, "CAAMP: Completely automated DDoS attack mitigation platform in hybrid clouds," *2016 12th International Conference on Network and Service Management (CNSM)*, Montreal, QC, pp. 136-143, 2016.

[93]. S. F. Lai, H. K. Su, W. H. Hsiao and K. J. Chen, "Design and implementation of cloud security defense system with software defined networking technologies," *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, pp. 292-297, 2016.

[94]. M. Mizukoshi and M. Munetomo, "Distributed denial of services attack protection system with genetic algorithms on Hadoop cluster computing framework," *2015 IEEE Congress on Evolutionary Computation (CEC)*, Sendai, pp. 1575-1580, 2015.

[95].]L. Ingle and G. K. Pakle, "NIDSV: Network based Intrusion Detection and counter-measure excerption in virtual environment using AODV protocol," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, pp. 1-6, 2016.

[96]. A. Y. Oktoberry, "The Role of The Law in Combating DDoS Attacks against e- Government A Comparative Analysis of The Substantive detection against network mimicking DDoS attacks". *Communications Letters, IEEE*, 13(9): 717 719, 2009.

[97]. A. Efe, A Model Proposal for Organizational Prudence and Wisdom within Governance of Business and Enterprise IT. *ISACA Journal*, 2017.

[98]. A. Efe, Unearthing and Enhancing Intelligence and Wisdom Within the COBIT 5 Governance of Information Model. *ISACA Journal*, 2016.

[99]. A. Efe, COBIT-5 Framework As A Model For The Regional Development Agencies. *International Journal Of Ebusiness And Egovernment Studies*, 33-43, 2013.