Distributed Denial of Service Attacks in Cloud Computing

Hesham Abusaimeh
Associate Professor in Computer Science
Middle East University, Amman, 11831 Jordan

***Abstract*—The Cloud Computing attacks have been increased since the expanded use of the cloud computing. One of the famous attacks that targets the cloud computing is the distributed denial of service (DDoS) attack. The common features and component of the cloud structure make it more reachable from this kind of attack. The DDOS is targeting the large number of devices connected in any cloud service provider based on its scalability and reliability features that make the cloud available from anywhere and anytime. This attack mainly generate a large number of malicious packets to make the targeted server busy dealing with these huge number of packets. There many techniques to defend the DDOS attack in the regular networks, while in the cloud computing this task is more complicated regarding the various characteristics of the cloud that make the defending process not an easy task. This paper will investigate most of the method used in detecting and preventing and then recover from the DDoS in the cloud computing environment.**

Keywords—Cloud; cloud computing; DoS attacks; DDoS attacks; DDoS prevention; DDoS mitigation

I. Introduction

Cloud computing features include availability at any time, network access, resource pooling, flexibility, and measured service. Availability means that cloud users can access and can manage their computing resources anytime, anywhere. Pooled resources mean Cloud users can use them from a range of computing resources if they need more resources to add to their existing cloud. Flexibility means that services can increase in size more or less. Moreover, the cloud user will only pay for their cloud resources.

Cybersecurity researchers are considering the attacks performed on the cloud as these attacks affect the budget, resource management, and quality of service they are providing. We provide a comprehensive classification of solutions to classify DDoS attack solutions, and to provide a comprehensive discussion of important measures to evaluate different solutions.

Many companies have adopted cloud computing due to its various features like on-demand service, wide network access, resource pooling, fast flexibility, and measured services. These features allow companies to look after their business operations, while the Cloud Service Provider (CSP) is managing the computing resources. Cloud model contoured to reduce business costs by making the installation of hardware and software updates and ensuring computing resources at the cloud service providers' side.

This paper is looking to provide information about DDoS attacks over the cloud environment. We also will try to distinguish between the types of various DDoS attacks, exploring and classifying the various contributions in this field. For this purpose, we prepared a detailed classification of these studies to assist to understand this survey.

A. DOS vs DDoS Attacks

When developing services on the cloud, safety must be taken into account critically. Some of the aspects that pose a challenge for cloud computing are:

Identity Authentication Authorization Confidentiality Integrity Isolation Availability

In a DDoS attack, hosts, such as robots or zombies, maybe a virtual machine, PC, or laptop. They have a remote-control feature. The use of a large number of hosts in an attack is called DDoS. More annoying DDoS than DoS. A group, hundreds of thousands of robots known as a botnet. The DDoS attack targets connection bandwidth and resources such as buffers, network protocols, or application processing logic.

II. Background

In this section, we will try to highlight the purpose or motivations behind some of the common DDoS attacks. However, many different categories can be identified to characterize the motivations behind DDoS attacks; the following is a summary of the purpose or motivations behind DDoS attacks.

- Financial or criminal benefit: This is classified as a motivation, and considers the most dangerous attack as the attackers try to get financial benefit by performing their attacks.
- Revenge: This type is classified as a motivation, as some frustrated individuals perform some of the attacks as payment of some injustice perceived.
- Ideological belief: Attackers performing this attack are motivated by their ideological beliefs.
- Intellectual challenge: Attackers perform DDoS attacks as a way to show off the capabilities and what they can harm as self-arrogant.
- Cyberwarfare: some well-trained military people or some of what is called terrorist individuals or organizations make this type of attack.

- Script Kiddies: New enthusiastic attackers who are trying some of the new tools on the Internet. They could use a bot-master that manages a network of bots or becomes part of Botnet that is involved in the attack.
- Hacktivists: They are recruited through social networking sites. They fight for the cause gives them a sense of purpose.
- Labor issue: The competitors may play a dirty game. You can launch DDoS attacks easily to the point of stop web services for competitors, by making use of the services of the attack Botnet provider. Botnet provider has fields to fill the target, and then a single click can be thousands of nodes begin to flood server's competition.
- Thrill attacks: Where the attacker so only to feel a sense of pride in this achievement.

Extortion or Ransom: Criminals who are willing to do anything malicious in exchange for money [1].

III. Types of DDoS Attacks

In this section, an analysis of the basic functioning of the DDoS attacks will be covered, and list the main types of DDoS attacks and provide a brief description of each type of attacks as the following.

- Direct Flood Attacks: Indirect flood attacks, an attack transfers a single package directly from its computer to the victim's site. It is the simplest type of DDoS attack.
- Remote Controlled Network Attacks: In these attacks instead of individual attackers like direct flood attacks, an attacker breaches a series of computers and places an application or proxy on computers.
- Flooding Attacks: These attacks generate the source of the IP packet source address with the victim's IP address and send it to an intermediate host whenever there is a response from the intermediate host; it is sent to the victim's destination address, and the victim is dumped [2].
- Worms: We can distinguish between a worm and a virus in the fact that the virus needs human intervention to inject a computer that the worm does not need. Worms can greatly disrupt the normal operation of the Internet.
- Viruses: Viruses have had a major impact on network providers. To structure a large zombie network, viruses are oftentimes used. In 1983 and 1984, serious Internet viruses included Melessia (1999), Love letter (2000), Nimda (2001 - a bunch of worms and viruses)[3].
- Fragmentation Attacks: Fragmentation Attacks have occurred on the firewalls of Cisco checkpoints and routers from Cisco and Windows PCs.
- Network infrastructure: Attacks targeting the network infrastructure can affect all Internet operations. Mostly, these types of attacks can create regional or global networks outside or slow down. A warning signal was sent to the root name server operators to reinforce the robustness of their infrastructure.
- Protocol violation attacks: In protocol violation attacks, the attacker originally sends packets. Attacks that generally use invalid or reserved IP protocols are protocol breach attacks. Protocol (255) is reserved, and protocols (135-254) are not allocated according to the specified online powers [4].
- Buffer Overflow Attack: where in this attack a large data is sent to the targeted buffer in a certain machine, and the size of this data is larger than the buffer size, which cause to save the data on a different buffer and remove the needed data, exist on that buffer.
- Email Bombing: where the inbox of a certain victim has been attacked with lots of emails.
- Ping of Death: the ping command is used to send a huge amount of data in the same packet while the received computer cannot accept and process this size of the data, which will slow the processing on this machine and reduce the connection between that computer and any other server.
- Smurf Attack: the ICMP protocol is used in this attack to obtain the same IP of the targeted machine and send back all the responses to the source machine with a larger bandwidth than the network bandwidth which is originally used.
- Synchronisation Flood: the attacker takes the advantage of the TCP protocol of starting the synchronisation process, which reserve a server for further data that should be sent after the synchronisation packets. While the attacker aim is to keep the server, busy with many Synchronisation packet and do not send any actual data after that.
- GET Flooding: the attacker in this attack generate many request packets using the HTTP protocol to a certain server that becomes busy with many GET messages from that client, and the server will also wait for the confirmation of these request, which never respond [5].
- Reflection Attacks: the attacker here use the UDP protocol to send many requests after spoofing the victim IP address [5].
- Amplification Attack: In this attack generating a large number of packets to target a victim website and use the DNS request after spoofing the source IP, address [5].

IV. Methodology

We conducted a set of literature by conducting a comprehensive search on previous papers and surveys and collecting a large number of papers related to the topic. The study results from the last papers we used. We believe that the contributions contained in this survey are comprehensive and include a list of all-important contributions in the field to date. In this paper, cloud security problems and some security mechanisms focus on eliminating and emphasizing them. Despite the need to reinforce existing security measures to provide more security in the cloud environment.

V. Related Work

Andrew Carlina (2017) a number of low load systems have been specifically proposed for WBANS. Based on a review of these modern methods, it is clear that the cloud model presents new security vulnerabilities. However, he began to monitor new cloud-based systems themselves to defend against widespread DDoS attacks. This enables systems to adopt scalability features to enhance the cloud for all parties. It is also necessary to think about safety models in terms of protecting individual clients and their services as well as the cloud as a whole, he said. To develop an effective defence system, aspects of these research systems must be combined to protect from a wide range of attacks. A number of these devices use VMs as system administration units. This allows these systems to take advantage of the flexibility and scalability of the cloud model to provide a more effective attack response and help reduce system bottlenecks [6].

It was concluded that there are two main research methods that must be followed. First, the hack tries to hack VMs to launch The DDoS attacks against a target outside the cloud. Although this may seem like a simplified solution for outbound systems, it is not a widely adopted solution by CSPs as it adds to their overheads, although indirectly jam their infrastructure. Second, developing more traditional cloud infiltration defence mechanisms target of the attack is the cloud or any part in the cloud itself.

Tasnuva Mahjabin (2017) in his survey, he provided a comprehensive and systematic analysis of DDoS attacks. It summarizes different types of attacks, filtering techniques, and methods for detecting attacks. However, his survey was an easy way to get the idea of DDoS attacks in which to systematically understand and analyse these attacks. Since his survey included recent attacks and recent researches against these attacks, it shows the current state of the attacks. It provides some discussions about DDoS attacks on unconventional systems such as clouds, smart grids, smart homes, CPS systems, and Internet of Things systems. As his study extracts an understanding of the search for DDoS attacks, it is important to understand the mechanisms for categorizing DDoS attacks in this survey. The author looks to analyse all the sorting of those attacks and provide an easy-to-understand classification mechanism.

Gaurav Somani (2017) in his survey provides a detailed survey on the DDoS attacks and its defence mechanisms on the cloud-computing environment. It has been demonstrated through discussion that a DDoS attack is the primary form of a DDoS attack in the cloud [7].

There is a number of solutions to DDOS attack such as attack detection and attacks mitigation. Among these solutions, a few contributions target specific cloud features such as allocating resources to demand resources reconfiguration employ SDNs. We also provide a broad list of performance metrics for these solution categories for assessment and comparison.

Seth Djane Kotey et al. (2016) concluded that with the increase in size, sophistication, and scale of modern DDoS attacks, further research is important to come up with very strong defences to fight these attacks.

Some DDoS defence types are discussed in this survey. They classified defence mechanisms according to their main functions: detection, tracking, and mitigation. They also discussed their strengths and weaknesses. It has been discovered that most solutions conflict with scalability and may not be able to perform well in the real world, due to the increasing size of attack and traffic robots involved in recent attacks. Most of the current solutions also added some additional computing and additional expenses to the network, which will have an impact on the network, and some of them may slow down, in a real scenario with large amounts of attack traffic [8].

A comparison was made between the different mechanisms; however, not all solutions had results for the criteria they have used in the comparison. For such mechanisms, it will be tested to determine their actual performance based on the metrics chosen by them. Overall, most of the defensive solutions reviewed were performing reasonably well.

Zargar et al. (2014) also provided an evaluation of the DDoS and OSI layer deployment mechanisms and defence system-based mechanisms: source-based, networked, and hybrid (hybrid) mechanisms. They also discussed the advantages, advantages, and disadvantages of defence mechanisms based on on-site deployment. In addition, the authors classified defence systems according to the time they start the process (before the attack or during the attack or after the attack). Then compared the performance of the defence mechanisms in accordance with the classifications they used. Following is a summary of the features, advantages, and disadvantages of defence mechanisms against DDoS flood attacks at the network/transport-level based on their deployment location.

For the source-based, the detection and the response is done at the source hosts directly and the pros of this is that it aims to detect and to respond to the attack traffic at the source before to wastes lots of resources, and the cons is that the sources are distributed at different domains, hence it is hard for each source or detect bad filter each attack in an accurate way, besides it is difficult to differentiate DDoS attacks at the source, since the traffic volume is low, as it is not clear who would pay for these services [9].

For the destination-based, the detection and response tools are installed on the victims hosts, they are easy to set up and cheaper compared to other tools in detecting DDoS attacks as they can access to aggregated traffic near the destination sources, but they cannot accurately detect and respond to attacks before it reaches to the victim and can waste resources while the attack is on its wait to the victim.

For the Network-based, the detection in response tools are deployed ate the network itself, one of its advantages is that it detects and responds to the attacks at the network and try to be closer to the attack source as it can, although some of its disadvantages is it needs high storage and the overhead that happens on the routers is difficult to detect because of lack of aggregated traffic destined for the victims.

In the hybrid model, the detection and the response tools are deployed at various locations; detections usually occurs at the victim side and the network, and the response usually takes place at the source and upstream routers near the source, the advantage of this Hybrid approach is that it is more robust against DDoS attacks and many resources can be used to stop the attacks, the disadvantages of this approach is the complexity and the overhead because of the communication that happens between many distributed components all over the internet.

VI. DDoS Protective Controls

In the survey conducted by Ahmed Bakr et al. (2019) prevention techniques are proactive, unlike detection and recovery that are reactive. Preventive controls must contain or eliminate the effects of a DDoS attack, and some techniques used to achieve this, following we will list some of these control and their techniques [10].

- Moving Target Defence (MTD): The Idea is rather than using layered defence by building static walls around your IT assets; it is working on making the attack surface dynamic.
- Completely Automated Public Turing Test (CAPTCHA): CAPTCHA is considered the most widely used prevention control by web applications. The shield can be used to protect web applications from malicious programs like Bots [11].
- EDoS-Shield Mitigation: This approach relies on implementing a front-end virtual firewall that maintains white and blacklists for IP addresses.
- sPoW (self-verifying Proof of Work): This approach relies on implementing a front-end virtual firewall that maintains white and blacklists for IP addresses.
- DNS based techniques: By blocking these malicious namespaces through ISP or web filtering agents, it will help with preventing launching bots to perform DDoS attacks [12].

As discussed previously, detection accuracy might be higher on the victim side but not powerful; victims cannot stand the large volume of DDoS traffic. Stopping attacks on the source can be the best option to respond, but it is very difficult since the amount of traffic in the sources is not important to distinguish the project from the harmful traffic. Moreover, side damage is high in midway networks due to insufficient memory and CPU cycles to determine traffic. Therefore, the central mechanisms in which all defence components (i.e. prevention, detection, and response) are deployed on the same site, are not practical against DDoS flood attacks.

VII. Defense against DDoS Attacks

Cloud Computing is now more targeted from the attackers by the DoS attacks. Solutions are being figured to deal with such risky attacks. Generally, guarding against DDoS attacks can be classified into three main categories: preventing attacks, detecting attacks, and responding to attacks as shown in Fig. 1 [13].

The cloud pool of resources will be blocked from the user access when a DoS attack is detected. In addition, even without detecting DoS attack the prevention scenario can also stop the user from accessing the cloud resources. The prevention techniques may install different protection components on all the cloud sites such as the user system, the network controllers, the internet routers, and track the attacker site [14].

Furthermore, the security prevention and detection methods can be placed on the VM of the cloud services, which includes all the hosted operating system installed. While this process will have some characteristics impact on the cloud service such as limited the processing capacity, reduce the network access, reduce the outsourcing dependency, limit the enhancement of the available protocols used in the cloud, reduce the network bandwidth with extra overhead protocols, and increase the power consumption of these units attached to the cloud services [17].

Since mitigating DDoS attacks is challenging, efforts should be increased to prevent these attacks from happening. Most of the cloud service providers establish a set of procedures to treat all the rules and actions that would be used by the customers as a policy requirement. These procedures are mandatory to follow the participation in the cloud service activities used. Table I shows an example of how the procedures are linked to the DDoS attack.

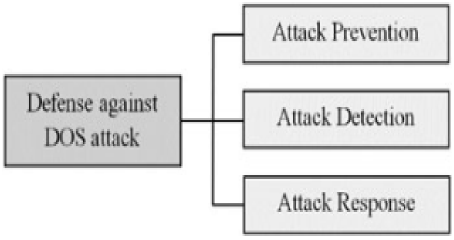

Fig. 1. Defense Type Against DoS Attack.

TABLE I. PROCEDURES TO DEAL WITH THE DDOS ATTACK [13]

DDoS attack	Procedure
Before the DDoS attack	To prevent DDoS attack the customer should use a firewall and prevent any unauthorized access and use proxies to connect to the hosts on the cloud pool.
During the DDoS attack	Stop most of the administrators' access to the network services and reduce the traffic on the cloud hosts.
After the DDoS attack	A team of administrator should act on recovering all the services and track the down services. In addition to document the type of the attack and the reason behind the attack and update the policy to prevent it in the future.

There are also other classifications of the DDoS attacks on the cloud and the detection or prevention techniques used for these types of attacks as summarized below [14].

1) Virtual machines level attacks: this kind of attack targeted the hypervisor layer in the virtual machines, and it needs an advanced cloud protection system is used that track the hosted virtual machines inside the hypervisor.

2) Resources Attack: this attack consumes all of the targeted system's resources by many pieces of data packet send and received from the attacker Screen OS.

3) BGP Prefix Hijacking: This kind of attack happens by flooding many announcement about fake IP addresses related to fake systems to attract certain users.

4) Port Scanning: this attack target the default and the unprotected ports like HTTP that are always open to provide web services; this can be prevented by, securing ports with encryption and using firewalls.

VIII. DDoS Attacks on SDN Overview

DDoS is increasing in the cloud computing environments due to the features of the cloud. With recent developments in Software Defined Networking (SDN), the SDN-based cloud provides is now a new opportunity to defeat DDoS attacks in cloud computing environments [15]. However, there is a contradictory relationship between SDN and DDoS attacks as shown in the different types in Table II. On the one hand SDN capabilities including existing traffic analysis software on the central control vision of the World Wide Web and the dynamic update for re-routing, make it easy to detect and respond to DDoS attacks. On the other hand, the SDN security itself remains to be addressed, and potential vulnerabilities in the DDoS system exist across SDN platforms.

In the following table Qiao Yan, F. Richard Yu published in their survey called "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges" lists a comparison of DDOS attacks defence mechanisms using SDN [16].

TABLE II. Types of DDoS Attack on SDN

Types	SDN capabilities exploited	Description of the solution
Source-based Mechanisms Using SDN	Programmability	The programmable home network using the routing switches compatible with Open Flow and NOX as a controller detects security issues in SOHO.
	Traffic analysis	Discover the access point, which is a converter that supports Open Flow is whereby the console Open Flow controller, malware by analysing traffic in real-time.
	Traffic analysis, dynamic rules updating and global views.	Suggests VALVE that uses Open Flow protocol to resolve the problem of validating the source address with a view to improving the global SAVI solution.
Network-based Mechanisms Using SDN	Traffic analysis and centralized control	Use statistical information in the flow table to classify traffic as normal or harmful to self-organizing maps.
	Traffic analysis and dynamic rules updating	A novel content-oriented networking architecture (CONA) can react to DDoS attacks by the use of accountability and content-aware supervision.
	Programmability	And displays FRESCO, which is in the same application Open Flow limit. It can provide programming inspired by clicking frame.
	Abstraction ability	An agent-based framework, Agnos, has been introduced to build collaborative SDNs that extend beyond enterprise networks and built on the abstraction provided by SDN.
	Programmability and dynamic rules updating	An efficient memory system is proposed for distributed and collaborative monitoring of each stream called DCM. DCM uses Bloom filters to represent the monitoring rules and to install a custom and dynamic monitoring tool at the switch data level.
	Global views and centralized control	Abstraction suggests full of resources and the provision of anti-DDoS and alignment with the network operations to provide, manage and control the protection of DDoS as a service within the system of environmental Open Flow.
Destination-based Mechanisms Using SDN	Dynamic rules updating	It analyses the theoretical quantitative relationship between the probability that flow is successfully tracking number again jump level, and the probability of sampling independently, and the package number that includes the flow of the attack.
	Global views and centralized control	It was built Net Sight, which is an extendable platform that captures the history of packages and applications can retrieve from the date of packets are concise and flexible packages of interest.

IX. Conclusion

Attacks on the Cloud Computing components and software become a daily issue especially after the wide use of it in various applications. The demand to have a stable cloud services with high availability to be offered for all the kind of device PCs, Laptops, and mobile is an urgent issue. The DDoS attack is one of the simplest and high redundant attack in the Cloud Computing environment where it has different types that attack different cloud computing resources. The Distributed resources and the multi virtual platforms inside these distributed resources are the main vulnerability in the cloud computing services. This paper discussed the most kinds of the DDoS attacks that targeted the pool of resources in the cloud computing and give the most defending procedures that is used to prevent, detect and recover the tracks of the DDoS attack and its damage. This damage may cause to stop the cloud service and may consume losing the data stored in the cloud without any backup or replica. The main way to protect the cloud is to define a policy for using the cloud resources and make rules based on the statistics threshold of the previous use of that service.

Acknowledgment

The author is grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

References

[1] Ryan K.L. Ko, Kim-Kwang Raymond Choo, “Cloud Security Ecosystem”, Elsevier,pp.1-14, 2015

[2] Taghavi Zargar, S., “Towards Coordinated, Network-Wide Traffic Monitoring for Early Detection of DDoS Flooding Attacks”, University of Pittsburgh, June 2014.

[3] Somani, G., Singh Gaur, M., Snaghi, D., and Conti, M., “DDoS attacks in cloud computing”, the international Journal of Computer and Telecommunications Networking, Vol. 109, November 2016.

[4] Ludiora, S., Abiona, O., Oluwatope, A., et al., “A user identity management protocol for cloud computing paradigm”, International Journal of Communication, Network, and System Science, Vol. 4, Issue 3, pp. 152–163, 2015.

[5] Han, J., &Kamber, M. (2018), “Data mining: Concepts and techniques (2ed Ed.)”, Beijing: China Machine Press. DDoS Attacks and Impacts on Various Cloud Computing Component, 2018.

[6] Hammoudeh, M., Aldabbas, O., “Intrusion Detection and Countermeasure of Virtual Cloud Systems - State of the Art and Current Challenges”, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 6, 2015.

[7] Kalkan, K., Gur, G., and Alagoz, F., (2016), “Filtering-Based Defense Mechanisms Against DDoS Attacks: A Survey”, IEEE Systems Journal PP(99):1-13 · September 2016.

[8] Masdari, M., Jalali, M. (2016), “A survey and taxonomy of DoS attacks in cloud computing”, Security and Communication Networks, 13 July 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1539.

[9] Malomo, O., Rawat, D., and Garuba, M. (2017), “A Survey on Recent Advances in Cloud Computing Security”, Journal of Next Generation Information Technology, Vol. 9, No. 1, March 2018.

[10] Bakr, A., Abd El-Aziz, A., and Hefny, H. (2019), “A Survey on Mitigation Techniques against DDoS Attacks on Cloud Computing Architecture”, International Journal of Advanced Science and Technology, Vol.28, No. 12, 2019.

[11] Aldaej, A., “Information Security and Distributed Denial of Service Attacks : A Survey”, the 2017 International Conference on Electrical and Computing Technologies and Application (ICECTA), UAE, November 2017.

[12] Zargar S., Joshi, J., and Tipper D., (2014), “A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks”, IEEE communications surveys & tutorials, Vol. 15, No. 4, 2013.

[13] Alsowail S., Sqalli, M., Abu Amara, M., Baig, Z., and Salah, K., “An Experimental Evluation of the EDoS-Shield Mitigation Technique for Securing the Cloud”. Arabian Journal for Science and Engineering, Vol. 41, No. 12, pp.5037– 5047, May 2016.

[14] Ubale, T., and Jain, A. K., “Survey on DDoS Attack Techniques and Solutions in Software-Defined Network”, Springer International Publishing, 2020.

[15] Yan, Q., Yu, F.R., Gong, Q., Li, J., “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges”, IEEE Communications Surveys and Tutorials, Vol. 18, Issue 1, 2016.

[16] El-Sofany, H., El-Seoud, S., and Taj-Eddin, I., “Case Study of the Impact of Denial of Service Attacks in Cloud Applications”, Journal of Communications, Vol. 14, No. 2, February 2019.

[17] Abusaimeh, H. and Yang, S.H., “Reducing the transmission and reception powers in the AODV”, Proceedings of the 2009 IEEE International Conference on Networking, Sensing and Control, ICNSC 2009, pp. 60-65, 2009.