World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924

OVERVIEW OF PREVIOUS STUDIES OF DISTRIBUTED DENIAL OF SERVICE A (DDOS) SOLUTIONSON NETWORK QUALITY OF SERVICE (QOS)

Daralslam Abdalrhim Hassan Ali*[1], Khalid Hamid Bilal Abdalla[2] and Zeinab Mahmoud Omer[3]

[1]Department of Telecommunications, Faculty of Engineering, University of Bahri, Sudan.
[2]Department of Telecommunications, Faculty of Engineering University of Science and Technology, Sudan.
[3]Electrical and Electronic Engineering Department, University of BAHRI, Sudan.

Article Received on 08/04/2022 **Article Revised on 28/04/2022** **Article Accepted on 18/05/2022**

***Corresponding Author**
Daralslam Abdalrhim Hassan Ali
Department of Communication, Faculty of Engineering, University of BAHRI, Sudan.

ABSTRACT

The Internet has become a global communications network tool. Many platforms that support best effort traffic have evolved into a platform that now carries different types of traffic including those that include continuous media with Quality of Service (QoS) requirements. As more services are offered online, we face increased risks to their availability as malicious attacks on these online services continue to increase. Many networks have experienced denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks over recent years which have directly affected the quality of network services, thus violating the Service Level Agreement (SLA) between the customer and the Internet Service Provider (ISP). Hence, DoS or DDoS attacks are major threats to network quality of service. In this paper, some studies that explore techniques and solutions that have been used to thwart DoS and DDoS attacks and evaluate them in terms of their impact on the quality of service on the network for Internet services.

KEYWORDS: Network Security, IP Network, DDoS, Zombie Computers, Bots, Robots, Cloud Computing.

1- INTRODUCTION

The rapid development of the Internet over the past years has facilitated the increase in incidents of cyber-attacks. Internet users need quick access to information from every part of the network. Recently Distributed Denial of Service (DDoS) attacks have become a problem because they cause network unavailability to block services by taking over system resources of computers within the network until they stop working. In the cloud, users of computing servers can access many services without the burden of managing the cloud and their data can be accessed by many devices (such as sensors, smartphones, tablets, etc...).[1]

This type of network is more Vulnerable to attacks, which affects the quality of service. In such a situation, the user who has already started working in the system loses the connection and cannot finish his work. The user may not even be able to log out of the system, which they have to do on their behalf after the connection timeout is reached or when a broken connection is detected. DDoS attacks are a challenge for IT systems nowadays and must be eliminated. One solution could be a new Quality of Service (QoS) method that can work on all routers in the network. One such powerful and malicious attack is a Denial of Service (DoS) attack. Especially if such an attack is distributed. A distributed DoS attack (DDoS) is launched by a mechanism called a botnet through a network of computers that are controlled. The software controls computers and forspecific purposes, they are known as bots. Bots are small scripts that are designed to perform specific automated functions. Bots are used to control a botnet. Bots are associated with the concept of "Trojans" (for example, Zeus bot) and zombie computers created for purposes other than attacks.[2] Bots provide in large quantities computer power to create key tools for such activities as widespread delivery of spam, clicking fraud, spyware installation, spreading viruses and worms, and DDoS attacks (eg black power bot) DDoS attacks usually take advantage of weaknesses in the network layer, particularly, SYN, UDP, and Internet Control Message Protocol (ICMP) flooding. Such attacks encroach on the victim's network bandwidth and resources, making it easier to deny legitimate access.[3]

1.1 Defense DOS and DDOS

DOS and DDOS defenses are available in cloud computing cover different aspects, such as prevention, mitigation strategies and security (see table 1). The most important thing is to maintain availability for service providers, users and cloud infrastructure managers.

Difficult to defend against DOS and DDOS attacks. DOS or DDOS can be shut down by

selecting the source of the attack and then blocked. In most times, the attack benefits from a huge amount of robots.[3]

Table 1: Cloud Computing DoS (Denial-of-Service) and DDoS Defenses.[13]

		Techniques
Defense Strategy	Prevention	Service Level Agreement
	Attack Mitigation	Virtual Machine Monitor Intrusion Detection System IDS Firewall Detection Filter Limitation TraceBack
	Architecture	Trust Delegation Reputation Intrusion Detection System (IDS) Firewall Cryptography

1.2 Attacks and attackers

Address the types of attacks and types of attackers that pose a physical threat to cloud computing.

The different forms an attack can take. There are multiple ways involved in the cloud infrastructure and its environment itself.

In a DDoS attack, some host devices (VM, PC or laptops), which are also called "bots" or "zombies", can be remotely controlled. A group of such robots that are controlled by a main entity (attacker) are known as "bots".

Typical attackers are categorized into three categories, according to their location, motivation, or level of activity in the attack. External to internal, Internal to external, Internal to internal.

1.3 Virtual Machine Monitor (VMM).

VMM has more privileges than the guest OS. When under attack, the operating system and

all applications are moved to a new isolated entity. During the migration process, there is no outage for the user under attack because the applications are still running in both the original virtual machine and the new isolated virtual machine. Basically, the only difference with duplication is that the original virtual machine is destroyed when the migration is complete. This way, the attack will not have a greater impact on the user's applications. The difficulty is to correctly set the threshold value that indicates an attack. The advantage of this system is that the virtual machine can be migrated without interrupting the service which is a big advantage of this system. There is no need to migrate the entire virtual machine, just selected applications and operating system.[3]

2- Objectives

An overview of previous studies of Distributed denial of a(DDoS) solutions on network quality of service(QoS)

3- Understanding Cloud Computing Vulnerabilities.

Grobauer et al.[4] It detects vulnerabilities associated with cloud computing. Like,

(1) VM escape

(2) Cycle riding and abduction

(3) Insecure or obsolete encryption

(4) Unauthorized access to the management interface

(5) Internet Protocol vulnerabilities and

(6) Data recovery vulnerability. This paper identifies existing security standards that are not compatible with cloud infrastructures, so the study suggested developing new standards for more security. Although this study clarifies indicators of cloud security vulnerabilities, it does not provide solutions to solve them.

4- A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing

Gonzalez et al., in this paper, talked about.[5]

1- Defining, classifying, organizing and estimating security

2- Network configuration

3- Hosts and virtualization issues

4- Applications and services

5- Data security, storage and security management

6- Cloud computing access methods.

In addition, the authors present security concerns and solutions using pie charts in order to show the representation of each group with specific references. They determined that the security issues associated with virtualization are most seriously rated at 12%, but the search for solutions to this aspect is only 3%. So there is a lack of solutions. They suggest developing new VM isolation mechanisms, where proper isolation should be implemented between VMs to avoid attacks across VMs due to sharing of devices (CPU, storage, memory, etc.). They suggest developing firewalls to protect the provider's internal cloud infrastructure from insiders and outsiders, while enabling virtual machine isolation and accurate filtering of addresses and ports, thus preventing DoS and DDoS attacks.

5- Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing

Khurshid et al.[6]

Divide cloud computing security into three sections:

1- Security categories (cloud providers or cloud customers).

2- Security in service delivery models: SaaS, PaaS, IaaS.

3- Security dimensions.

The study presented the most important threats facing cloud computing and ways todetect attacks on cloud computing using machine learning techniques.

6- An analysis of security issues for cloud computing

Hashizum et al. in this paper, they talked about.[7]

1- Classification and analysis of a number of weaknesses

2- Threats, mechanisms and security standards

3- Data Security, Trust and Security Requirements for SaaS, PaaS and IaaS.

4- Cloud computing delivery models.

The paper reviewed the following threats:

1- Service theft.

2- Stolen data and DoS (and DDoS)

3- Problems related to virtual machines.

7- Cloud computing security: A survey. Computers

Khalil, I.M.; Khreishah.[8]

1- Security Standards.
2- Access Control.
3- Cloud Infrastructure.
4- Data.
5- Network.

Different solutions and procedures for Intrusion Detection (IDS) and Identity Management Systems (IMS) were compared.

8- Security in cloud computing: Opportunities and challenges

Ali.[9] Provide cloud security challenges at the level of communication (between customers and clouds, communications occur within cloud infrastructure), for virtual machines. The period discussed the different ways of security solutions.

9- Survey and taxonomy of DoS attacks in cloud computing

Made and others.[10] A study of types of service blocks displays with new attacks against virtual machines and Hypervisor programs in the cloud environment of computing environment. Authors Network Defense Network known and cloud computing against deprivation of service attacks.

10- Distributed denial of service (DDoS) resilience in cloud

Osanaiye et al.[11] DDOS scan attacks that target cloud computing. Section attacks at the application level and infrastructure level and presented different ways to conduct these attacks.

Cloud computing needs (wide range, direct access to cloud infrastructure, resource sharing etc.) to new and innovative solutions to protect both users.

Depending on the cloud model, security depends on the supplier or on the user. The cloud computing safety has become well documented. A survey achieves DOS and DDOS attacks targeting the availability of cloud computing. Provides paper types and attackers, DOS, DDOS, defense and evaluation.

11- Quality of Services Method as a DDoS Protection Tool

Lukasz Apiecionek.[12] this paper spoke about the quality of service methods and DDOSattack model. Some new QOS features are offered. According to the submitted features QOS

method can be used as a protection tool against DDOS attack. The capacity to implement the proposed quality of service features was tested to eliminate attacks. The results provided indicate that this method can be widely applied. The QOS method was offered to eliminate DDOS attacks with the information that proves that this use is possible in the real environment.

12- Design of trace back methods for tracking DoS attacks

Petropacis and others.[13] discussed efforts to secure user data in the cloud. Instead of storing information locally on the user's infrastructure, information is stored in the cloud and discussing the quality of network service.

13 – CONCLUSIONS

In this paper, a summary is presented of previous studies on the quality of service (QoS) method to eliminate DDoS attacks, most of these studies have shown that the use of this concept is possible in the real environment. The use of this concept is based on the cooperation of all ISPs. The effect of QoS method reduces DDoS attacks. He mentioned that the best solution is to apply this method to all routers and firewalls in the network.

In some studies, the new cloud computing model comes with known vulnerabilities, but also new types of attacks, due to the innovative way in which services areprovided to the user and due to the increasing success and adoption of cloud computing, by companies and individuals, it is clear that cloud computing provides Sufficient resistance to attacks.

These studies prove that many attacks still cause great harm to cloud computing, affecting various aspects of security (confidentiality, integrity, isolation, availability, etc...). Among those attacks, DoS and DDoS attacks are arguably the easiest and mostdestructive, yet there are still huge gaps to efficiently deal with those attacks. The studies provided some recent solutions: Some of them were easy to integrate into existing cloud infrastructures of cloud providers to prevent or reduce DoS and DDoS attacks. However, some solutions have not been able to detect all potential attacks or mitigate them completely. Others were more efficient, albeit more complex. In any case, there is no perfect solution.

For a CSP, this paper can help with knowledge of DoS and DDoS attack and defenses in defining Security Service Level Agreements (Security-SLAs).

Protecting against DDoS attacks is not easy, but it is essential to protect users and service

providers from hacker attacks, especially in situations where network resources are really required.

REFERENCES

1. Zissis, D.; Lekkas, D. Addressing cloud computing security issues.Future Gener. Comput. Syst., 2012; 28: 583–592.
2. H. R. Zeidanloo, A. A. Manaf, "Botnet command and control mechanisms," in the proc. of Second International Conference on Computer and Electrical Engineering, (ICCEE '09), 2009; 564-568.
3. C. Douligeris and D. N. Serpanos, "Network security: current status and future directions," Wiley-IEEE Press, 2007.
4. Grobauer, B.; Walloschek, T.; Stocker, E. Understanding Cloud Computing Vulnerabilities. Secur. Priv., IEEE,2011; 9: 50–57.
5. Gonzalez, N.; Miers, C.; Redigolo, F.; Carvalho, T.; Simplicio, M.; de Sousa, G.; Pourzandi, M. A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. In Proceedings of the, IEEEThird International Conference on Cloud Computing Technology and Science (CloudCom), Athens, Greece, 29 November–1 December, 2011; 231–238.
6. Khorshed, M.T.; Ali, A.S.; Wasimi, S.A. A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing. Future Gener.Comput. Syst, 2012; 28: 833–851.
7. Hashizume, K.; Rosado, D.; Fernandez-Medina, E.; Fernandez, E. An analysis of security issues for cloud computing. J. Int. Serv. Appl, 2013; 4: 5.
8. Khalil, I.M.; Khreishah, A.; Azeem, M. Cloud computing security: A survey.Computers, 2014; 3: 1–35.
9. Ali, M.; Khan, S.U.; Vasilakos, A.V. Security in cloud computing: Opportunities and challenges. Inf. Sci., 2015; 305: 357–383.
10. Masdari, M.; Jalali, M. A survey and taxonomy of DoS attacks in cloud computing. Secur. Commun. Netw., 2016; 9: 3724–3751; SCN-15-0746.R1.
11. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl, 2016; 67: 147–165.
12. Lukasz Apiecionek, Jacek M. Czerniak, and Wojciech T. Dobrosielski Casimir the Great University in Bydgoszcz, Institute of Technology ul. Chodkiewicza 30, 85- 064

Bydgoszcz, Poland {lapiecionek, jczerniak,wdobrosielski}@ukw.edu.pl, January 2014.

13. Priescu I, Nicolaescu S. Design of traceback methods for tracking DoS attacks. IEEE International Association ofComputer Science and Information Technology—SpringConference, April.