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

AN INVESTIGATION OF THE IMPACT ON DOS ATTACKSAND SLOW DDOS ON TRANSFER HTTP CLOUD ENVIRONMENT

Daralslam Abdalrhim Hassan Ali*[1], Khalid Hamid Bilal Abdalla[2], ZeinabMahmoud Omer[3] and Afaf Mustafa Elhassan[4]

[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.
[4]Department of Telecommunication Systems, University of Science and Technology, Sudan.

Article Received on 15/04/2022 **Article Revised on 05/05/2022** **Article Accepted on 25/05/2022**

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

ABSTRACT

Cloud computing has brought many benefits to the IT industry, and it can reduce cost and facilitate business growth especially for startup companies that do not have enough financial resources to build their own IT infrastructure. One of the main reasons why companies are reluctant to use cloud services is the security issues that cloud computing technology suffers from. This paper contains the concept of cloud computing, reviews security vulnerabilities in cloud computing according to security standards, explains denial of service attacks in the cloud and will focus on HTTP DOS attack. HTTP slow rate attacks were chosen because of their ingenuity and also their disastrous impact. There is some research on the different way a web server or web service can be protected fromslow HTTP attacks, but there is a lack of research on the impact of an attack on a cloud computingvirtual environment or whether or not such an attack has a cross impact on the virtual machine. This study investigates the impact of a slow HTTP attack on the cloud virtualization environmentand will analyze the direct and indirect impact of these attacks. To analyze slow HTTP attacks, using the opnet program to analyze the impact of the attack, the attacks are initiated by measuring object response time, page response time, sending and receiving traffic (bytes/sec), sound (jitter (sec), MOS value, packet Delay) Cloud Computing

QoS Assessment.

KEYWORDS: Denial of Service (DoS), Distributed Denial of Service (DDoS), Slow HTTP DOS,Cloud computing, Vulnerabilities, DOS on cloud.

INTRODUCTION

DDoS: DDoS stands for Distributed Denial of Service Referred to as a DDoS Distributed Denialof Service. A DDoS attack is to flood a website with requests within a short period of time, with the goal of disrupting the website. The reseller means that these attacks come from multiple and different sites at the same time, compared to a DoS that comes from just one site.

Definition of a slow DDoS attack: A slow-deploying DDoS attack is an attack that sends legitimate HTTP POST headers to a web server. In these headers, the text sizes of the message that will be followed are specified correctly. The text of the message is sent at a slow speed. For example, one byte every two minutes.

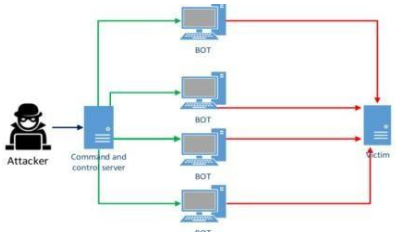

Figure 1.a: DDOS attack architecture.[7]

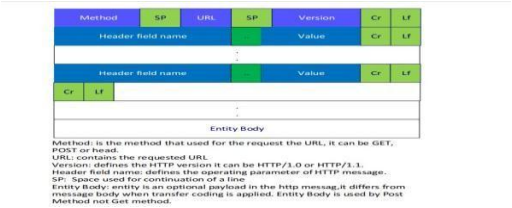

Figure 1.b: HTTP request message.[7]

Cloud computing concept

Cloud computing provides computing services, servers, storage, database, networking, software, analytics, etc…… through internet services. In return, companies charge their customers a fee based on cloud usage which can be time based or based on the resources customers use.[1]

Cloud service models

Software as a Service (SaaS) is a software licensing model in which access to the Software isprovided on a subscription basis, with the Software located on external.

Servers rather than on-premise servers. For example, customers use a provider application that runs on a cloud, and this application can be network servers, an operating system, or an individual Application. In this model, the customer has no control over the underlying cloud infrastructure.

Platform as a Service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud based applications to complex cloud-enabled enterprise applications. PaaS gives developers the ability to develop and deploy applications on the development platform provided by a cloud service provider (CSP).

Developers can access these services online.

Developers are responsible for managing the published application and configuring the development interface. PaaS provides the programming language, application framework, and databases. Google App Engine, Force.com, and Red hat Open Shift are examples of PaaS.

Infrastructure as a Service (IaaS): It is a type of cloud computing service that provides on-demand, on-demand, on demand computing, storage, and networking resources on a pay-as-you- go basis. IaaS is one of four types of cloud services, along with software as a service (SaaS), platform as a service (PaaS), and server less. (IaaS) provides processing, storage, networking, virtual machines (VMs), and other core computing resources on a pay-per-use basis. Clients can run any random program i.e. Operating Systems (OS). The IaaS client does not manage the underlying cloud hardware but rather controls the components provided by the cloud. The customer can access the IaaS through the Internet. Amazon Web Services (AWS) and Google Cloud Platform are examples of IaaS. Cloud computing facilitates the process of scaling a business, especially in the field of information technology, while reducing the cost of infrastructure. Using the capabilities of cloud computing, we can extend IT functionality with existing environments. Despite all the advantages of using the cloud, there are still security challenges facing the cloud.

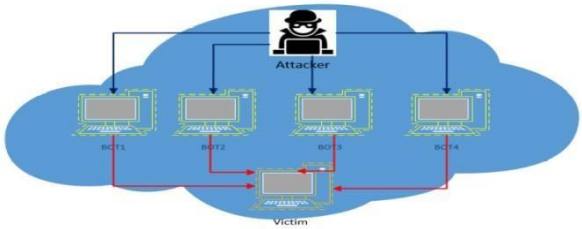

Figure 2: Cloud internal DDOS architecture.[7]

In February 2015, Anthem Inc. a world-renowned health insurance company, was hit by a DDoS attack resulting in the information breach of more than 80 million users. In 2012, Dropbox was attacked by worms and 68 million users were hacked. Wellknown companies like Dropbox and Anthem Inc. are exposed to this kind of attacks and data breaches, so it reminds us that security in cloud computing has become one of the most researched fields. Security are challenges one of the main problems that slow down the growth of cloud computing. The CSA has created broad standards for cloud security and become a standard catalog of best practices for securing cloud computing. CSA has issued more than 12 Cloud Security Rules which are.[2]

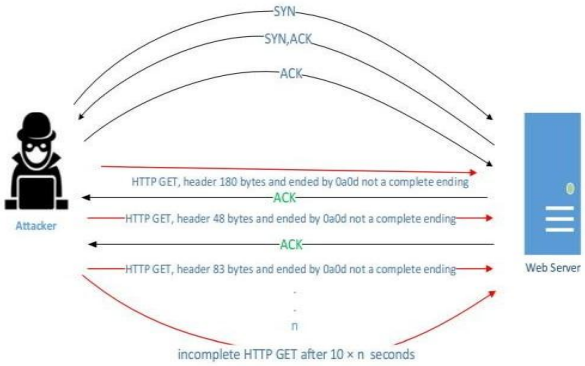

Figure 3: Slow header attack architecture.[7]

Data breaches

Weak identity, Credential, and access management. Insecure API. System and application vulnerabilities. Account Hijacking. Malicious insider. Advanced Persistent threats (APTs). Dataloss. Insufficient Due Diligence. Abuse and Nefarious Use of Cloud services. Denial of service. Shared technology issues.

Signs of a slow DDoS attack

Slow DDoS attacks are sending HTTP requests that target thread-based web servers, sending data very slowly, but not slowly enough for the server to time out. Since the server keeps the

connection open in anticipation of additional data, the original users are prevented from accessing the server. The servers seem to have a large number of clients connected but the actual processing time will be very low. Slow attacks are dangerous: why are they dangerous?

Since Slow Post DDoS attacks do not require extensive bandwidth, as is required with brute force DDoS attacks, they can be difficult to distinguish from normal traffic. Since these types of application layer DDoS attacks do not require a large amount of resources, they can be instigatedfrom a single computer, making them very easy to operate and difficult to mitigate. Can a slow deployment attack be prevented or mitigated and how?

Since traditional methods for detecting this type of attack will not stop a slow DDoS attack, oneway is to raise server quality. The idea is that the more connections available on a server, the lesslikely there is an attack on that server. In many cases, the attacker will simply scale the attack to try and increase the increased capacity of the server.

Another approach is reverse proxy-based protection, which will intercept slow DDoS attacks before reaching the server.

While there are no measures that completely eliminate the threat of Slow Post DDoS attacks, there are measures that can be taken: Set tighter URL limits for each resource. Set connection timeout based on average connections from legitimate clients. Set a minimum incoming data rate, and drop any connections slower than this rate. Consider adding more DDoS protection measuressuch as event-driven software load balancers, hardware load balancers to implement late binding, and intrusion detection/prevention systems to drop connections that match suspicious behavior patterns gleaned from log files.

Common technological weaknesses CSPs offer their services by sharing hardware, platform, or software. Users, a redeploy able PaaS architecture, or multi-client applications such as SaaS. This can cause common technological vulnerabilities. A misconfiguration or a vulnerability can compromise the entire CSP cloud.[2]

To reduce or prevent common vulnerabilities in shared technology, CSA proposes that CSPs implement multi-factor authentication for each host, using Host based Intrusion Detection System (HIDS) and implement Network-based Intrusion Detection System (NIDS) on the intranet, using hash methods in Cloud network and constantly restore shared resources.[3,2] A VM attack is anexample of a common technology vulnerability.

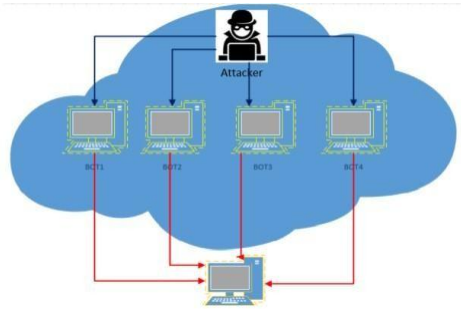

Figure 4: Cloud External DDOS architecture.[7]

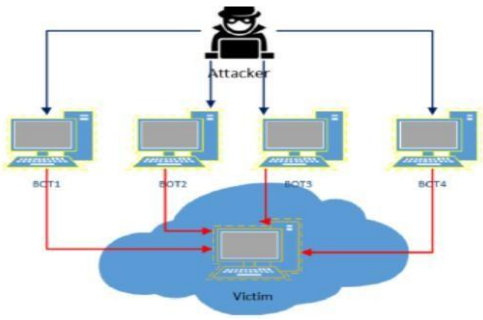

Figure 5: External-based DDOS on cloud architecture.[7]

Objectives

Show different types of slow HTTP attacks.

Main objectives

Lazy HTTP attack specification analysis. The direct analysis of a slow HTTP attack (SlowLoris) on the CPU. Network load.

Measurement of indirect coefficients of attack, network load, and web server performance.

Methodology

This paper follows the experimental research method. Since the goal is to implement DDoS attacks on Cloud computing generated by Cloud computing devices, there are three main stages: network design, implementation of the attack DDoS. In the second stage, the network performance was measured before and after the attacks and the extent of the impact on the network was determined as in Figure 6.

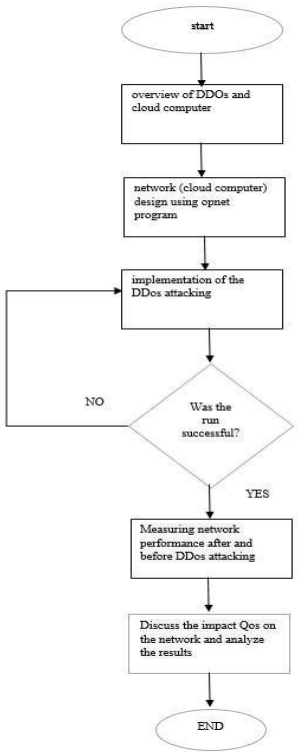

Figure 6: Methodology of work.

Related Works

In,[4] the authors provide an overview of DOS and DDOS that are implemented in the cloud. They also give an overview of the tools that can be used to launch the attack, such as LOIC, XOIC, and HULK. Moreover, they categorize the different types of defense mechanisms against attacks. DDOS.

In.[5] the first part they provide a comprehensive analysis of slow HTTP attacks and in the second part they present an attack detection method using Markov chains and queuing system. Chapter 3 of this thesis contains a similar analysis and implementation of the slow http attack butthe author of this thesis made a deep analysis of packets and explained where the attack occurredfor the captured packets.

In,[6] the authors review the functionality of slow HTTP attacks and then suggest an anomaly detection systemThe probability distribution was established in the training and testing phases. The training stage creates a normal profile of complete and incomplete HTTP requests, since it isknown that during slow HTTP attacks the percentage of incomplete HTTP requests increases, thenthe proposed method compares the measurement result of the normal profile and detects the slowHTTP attack.

Most of this research work was done on slow HTTP attacks and analysis of the impact of the attack on the web server application.

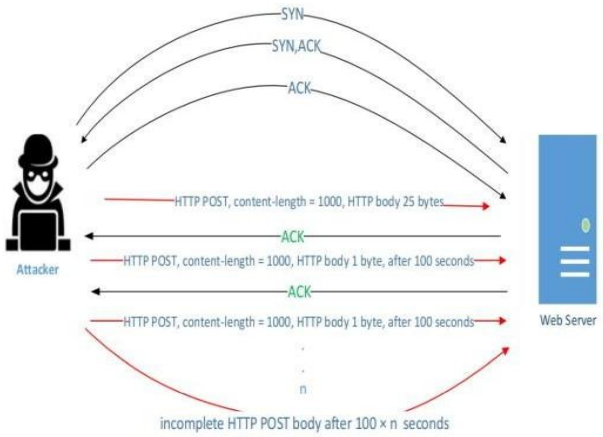

Figure 7: HTTP slow body attack architecture.

General setup for the experiment

1. We discussed the effect of a slow HTTP attack, now using two modes, No DDOS Mode and No DDOS Mode. Figure 4. Depicts the architecture of the attack method and Figure 5 .llustrates the architecture of the slow HTTP DDOS. Details of the servers used for this experimental work are on the table1 and table 2.

Table 1: Details of the servers.

Statics	Data
Number of connections	1000
HTTP request type	GET
Content-Length header value	4096
Interval between follow up data	10 seconds
Connection per second	200
Timeout for probe connection	3 seconds
Test duration	240 seconds

Table 2 Machines' specifications.

Machine	CPU	RAM	OS
Measurement machine	**Intel (R) Pentium, 4 CPU 2.80 GHZ**	**4 GB**	**Ubuntu 14.04.3 LTS**
Attacking machine	**Intel(R) Core(T M) 2, dual CPU E7400, 2.80 GHZ**	**8 GB**	**Ubuntu 14.04.3 LTS**
Coordinator machine	**Intel(R) Core(T M), i7- 2630QM, 2 GHZ**	**8 GB**	**Windows 10 pro**
VM server	**Intel Xeon Quad Core -8 cores 2.4 GHZ**	**8 GB**	**Ubuntu 14.04.3 LTS**
VM 1	**Intel(R) Xeon(R), X3430, 2.4 GHZ**	**514MB**	**Debi an GNU/Linux 7.1 (wheezy)**

2. Designed Cloud Environment on opnet

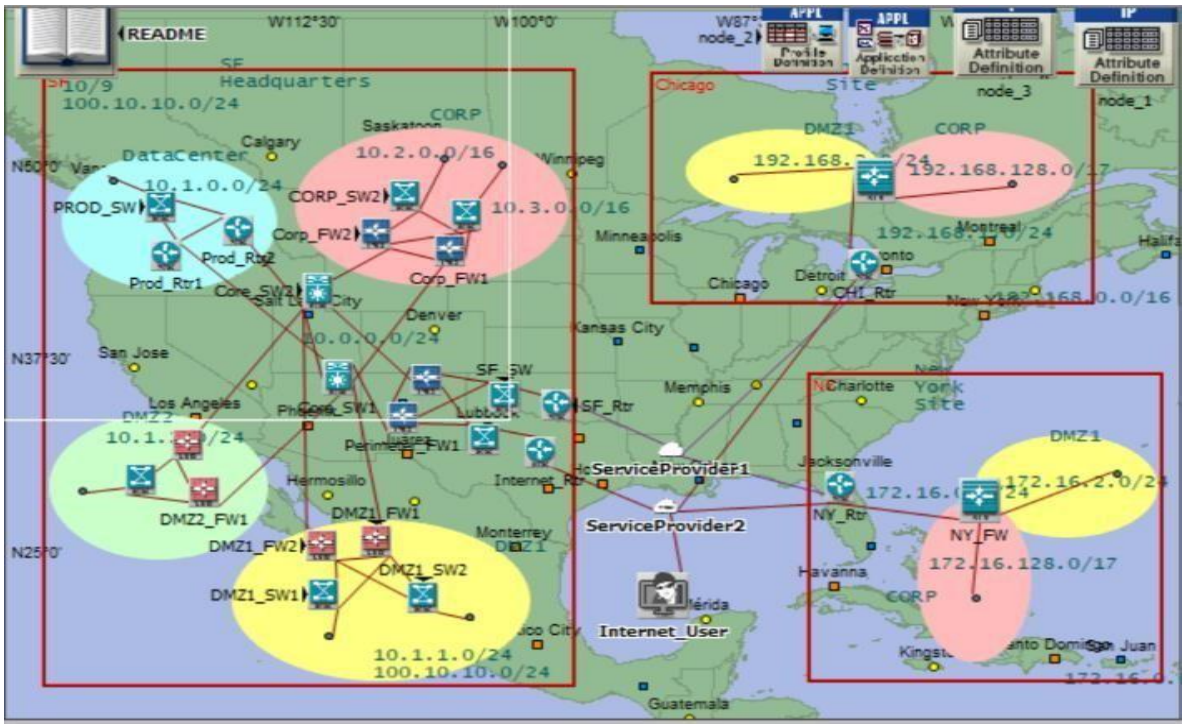

Figure 8: designed Cloud Environment.

RESULT

Analysis of the impact of the Slow Loris attack on the victim network In this section, we measure and analyze the impact of the Slow Loris DOS and DDOS on the simulation environment opnet. The measurement tests are taken while there is no attack means the network is stable and the measurement are repeated while network is under DOS and DDOS attack.

Table 3: HTTP.Object Response Time.

Statistic	scenario1DES- 1: HTTP.Object Response Time (seconds)	Scenario2after ddos attack-DES-1: HTTP. Object Response Time (seconds)
simplemean	0.06291170 4	0.001028968

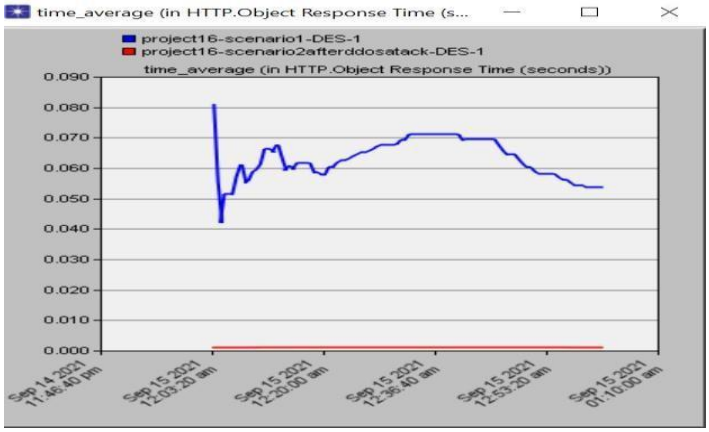

Figure 9(a): HTTP. Object Response Time (seconds) mean.

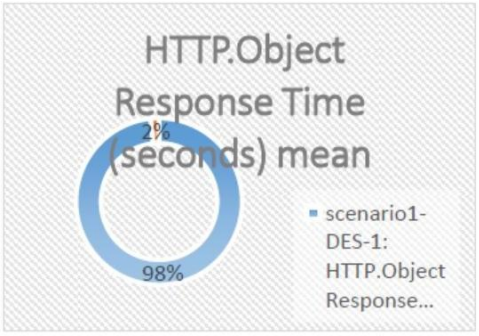

Figure 9(b): HTTP. Object Response Time.

Table 4: HTTP. Response Time.

Statistic	scenario1DES-1: HTTP.Page Response Time (seconds)	scenario2DES-1: HTTP.Page Response Time (seconds)
HTTP.Page Response Time (seconds)mean	0.25379598	0.002836413

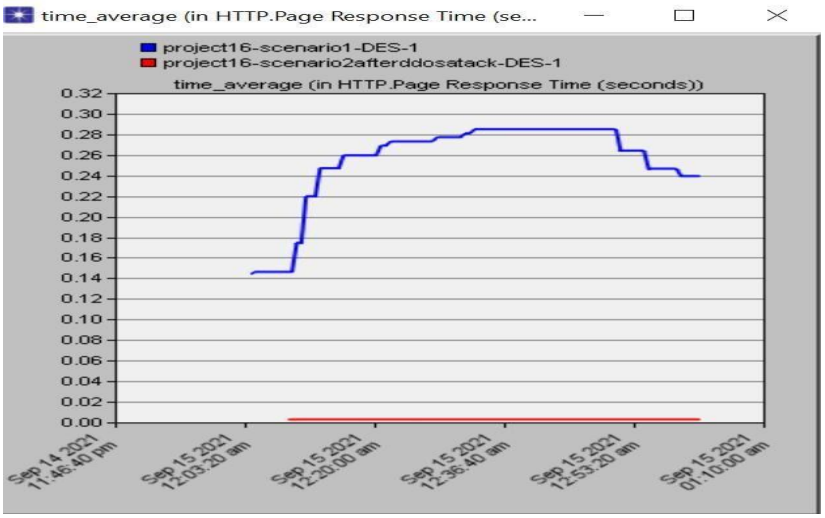

Figure10 (a): HTTP. Page Response Time (seconds).

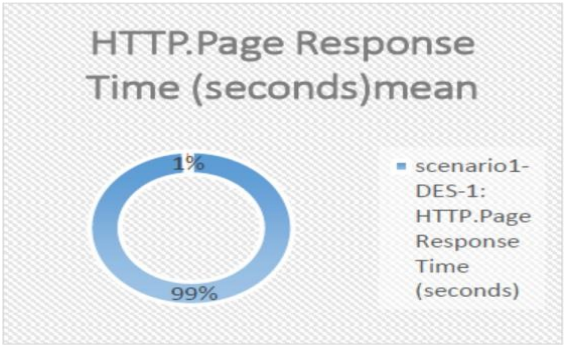

Figure 10(b): HTTP. Page Response Time (seconds)

Table 5: HTTP. Traffic Received /Sent (packets/sec)

statistic	Scenario 1DES-1: HTTP. Traffic Received (packet s/se c)	Scenario 1DES-1: HTTP. Traffic Sent (packets/sec)	scenario2after ddos attack- DES-1: HTTP. Traffic Received (packet s/sec)	Scenario 2after ddos attack- DES-1: HTTP. Traffic Sent (packet s/sec)	less packets on scenario1
HTTP. Traffic Sent (packets/sec)mean	0.1 374 751 69	0.1 385 506 21	0.0281 77567	0.0281 77567	0.0 010 754 53

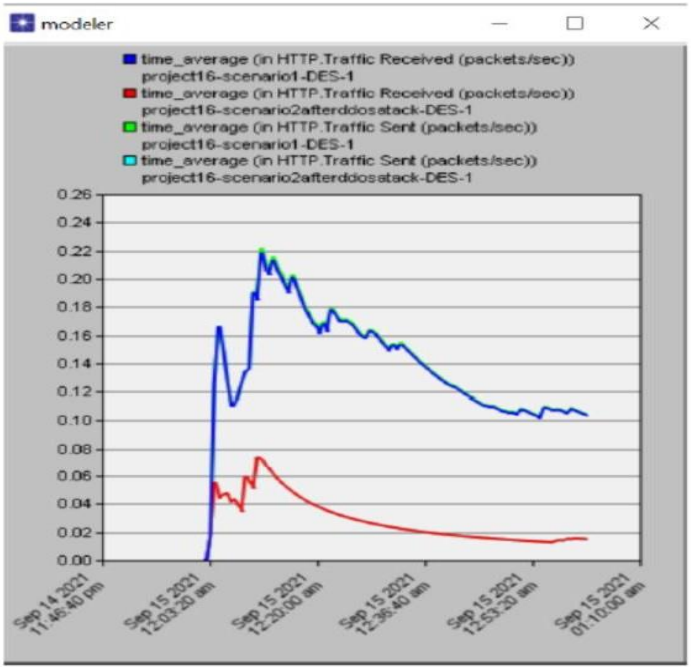

Figure 11(a): HTTP. Traffic Received /Sent (packets/sec).

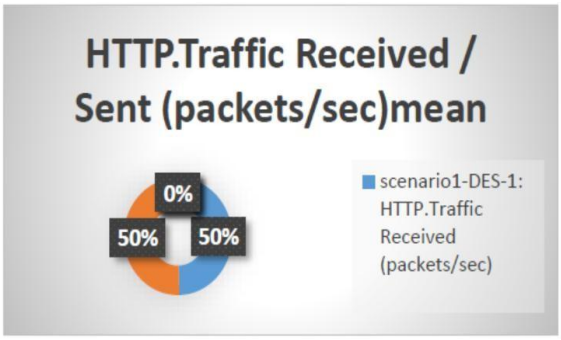

Figure 11(b): HTTP .Traffic Received /Sent (packets/sec).

Table 6: Voice. Jitter.

statistic	scenario1DES-1: Voice. Jitter (sec)	scenario2DES-1: Voice. Jitter (sec)
Voice. Jitter (sec)mean	-3.88E-08	0

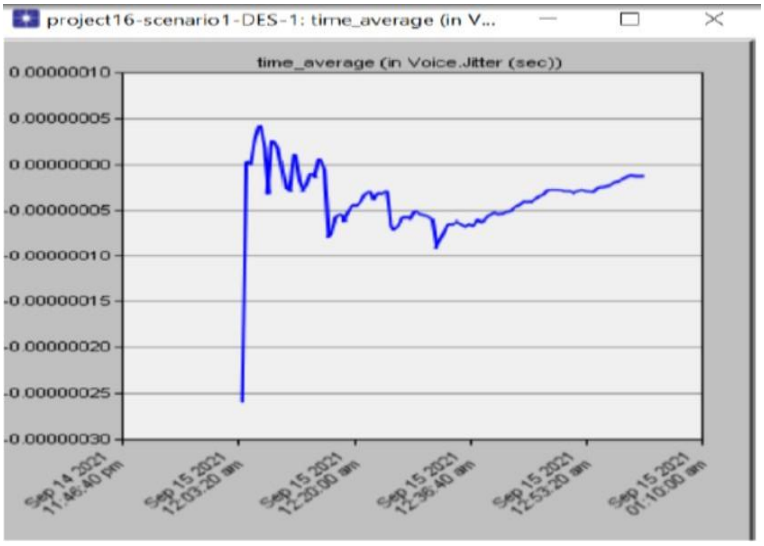

Figure 12: (a) Voice. Jitter (sec).

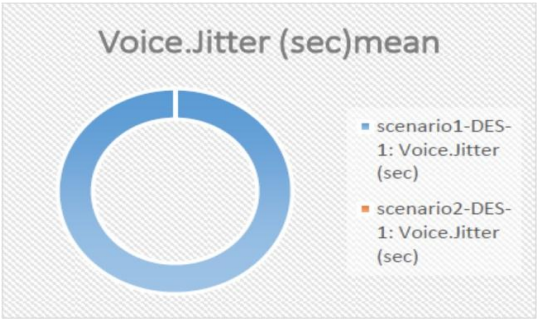

Figure: 12(b) Voice. Jitter (sec).

Table 7: Voice. MOS.

statistic	scenario1DES-1: Voice .MOS Value	scenario2DES-1: Voice .MOS Value
Voice.MOS Value mean	3.487632925	0
standard deviation	0.000464492	0

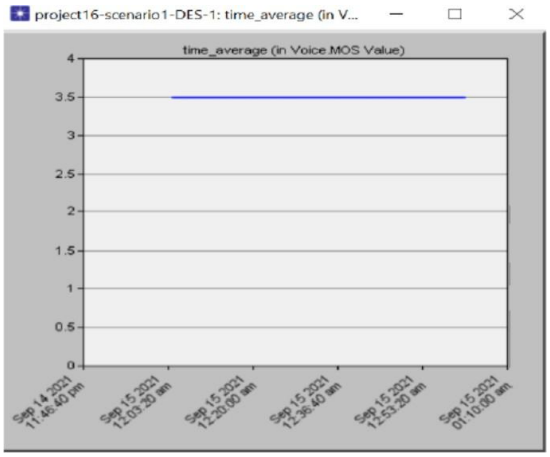

Figure: 13(a) Voice. MOS Value (Scenario 2 has no result).

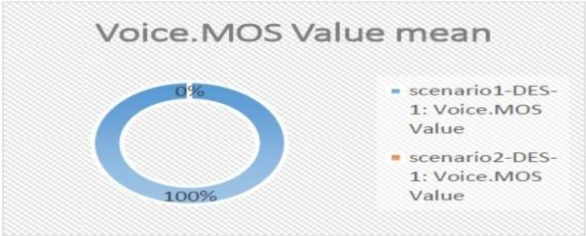

Figure: 13 (b) Voice. MOS Value.

Table 8: Voice Packet Delay Variation.

statistic	scenario1DES-1:Voice. Packet Delay Variation	scenario2DES-1:Voice .Packet Delay Variation
Voice .PacketDelay Variation mean	2.02E-08	0

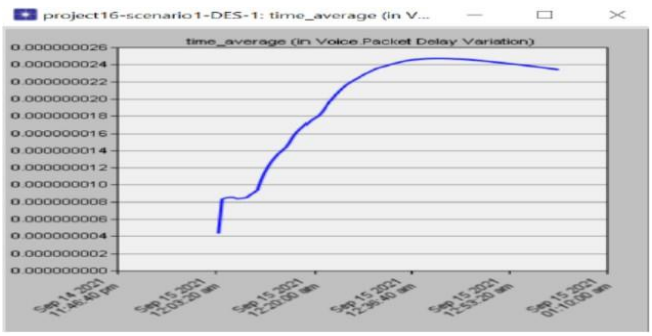

Figure 14 (a): Voice. Packet Delay Variation (Scenario 2 has no result).

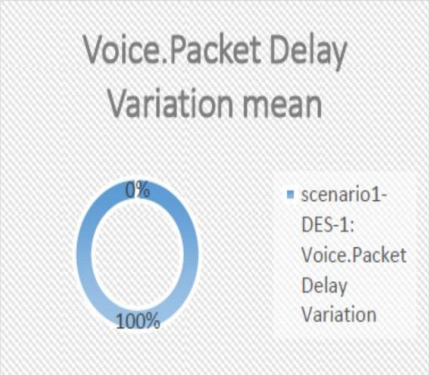

Figure 14 (b): Voice. Packet Delay Variation.

Conclusion and Future WorkConclusion

The goal for paper is to find out how much Slow Loris attack which is not resource costly for the attacker can put stress on the and consequently on the neighbors. The results of measurementstaken from scenario1 were compared, and the exact effect of DOS and DDOS on voice transmission quality, http coefficients and network load were compared.

Future Work

We have run HTTP Slow header attacks against a virtual machine on a virtual environment which is an ideal environment to work with. Testing the impact of slow HTTP attacks on an opnetcan be considered an ideal work, so you should try this work on a real environment 1 such as Microsoft Hyper-V, KVM or VMware ESXi installed directly on top of the machine, as a future work also we recommend solving the problem of DDoS using QOS**.**

REFERENCES

1. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Network. Computer. App., 2011; 34(1): 1–11.
2. Cloud security Alliance, "Cloud Computing Top Threats in The Treacherous 12,"Cloud Secure. alliance, no. February, 2016; 1–35.
3. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," J. Network. Computer. Appl., 2013; 36(1): 42–57.
4. B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment," Neural Computing and Applications, 2016; 1–28.
5. A. L. Carlsson, A. E. Duravkin, "Analysis Of Realization And Method Of Detecting Lowintensity Http-Attacks. Part 2. Method of Detecting Slow Http ATTACKS,"

http://pt.journal.kh.ua/, 2014; 1: 96–100.

6. N. Tripathi, N. Hubballi, and Y. Singh, "How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection," 11th Int. Conf. Availability, Reliab. Secur., 2016; 454–463.
7. E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnetbased Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," Int. J. Comput. Appl., 2012; 49(7): 24–32.
8. P. Revathi, "Flow and rank correlation based detection against Distributed Reflection Denialof Service attack," 2014 Int. Conf. Recent Trends Inf. Technol., 2014; 1–6.
9. J. Yeh, H. Hsiao, and A. Pang, "Migrant Attack: A Multi-resource DoS Attack on Cloud Virtual Machine Migration Schemes," Inf. Secur. (AsiaJCIS), 2016.
10. S. Alarifi and S. D. Wolthusen, "Mitigation of cloud-internal denial of service attacks," Proc. - IEEE 8th Int. Symp. Serv. Oriented Syst. Eng. SOSE, 2014; 478–483.
11. F. Abazari, "Exploring the Effects of Virtual Machine Placement on the Transmission of Infections in Cloud, 2014; 278–282.
12. K. Anusha, N. Tulasiram, and S. B. S. Mary, "Detection of economic denial of sustainability using time spent on a web page in cloud," IEEE Int. Conf. Cloud Comput. Emerg. Mark. CCEM, 2013.
13. F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, and A. Castiglione, "Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures," J. Supercomput., 2015; 71(5): 1620– 1641.
14. T. Siva, E. S. P. Krishna, S. Vidyanikethan, and C. Dist, "Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, 2013; 4: 2099–2104.
15. David Holmes, "Mitigating DDoS Attacks with F5 Technology," [Online], 2013.
16. Available:https://f5.com/resources/whitepapers/mitigating-ddos-attacks-with-f5technology. [Accessed: 26-Apr-2017].
17. Ws-attacks.org, "XML External Entity DOS - WS-Attacks," Ws-attacks.org. [Online]. Available: http://www.wsattacks.org/XML_External_Entity_DOS. [Accessed: 26-Apr-2017], 2015.
18. "What is BPEL (Business Process Execution Language)? - Definition from WhatIs.com." [Online]. Available: http://searchmicroservices.techtarget.com/definition/BPEL-Business-Process-ExecutionLanguage. [Accessed: 26-Apr-2017].
19. WS-Attacks, "BPEL Instantiation Flooding - WS-Attacks. [Online]. Available:

http://www.wsattacks.org/BPEL_Instantiation_Flooding. [Accessed: 26-Apr-2017], 2015.

20. Ws-attacks.org, "BPEL Indirect Flooding - WS-Attacks. [Online]. Available: http://www.wsattacks.org/BPEL_Indirect_Flooding.[Accessed: 26-Apr-2017], 2015.
21. C. Mainka, J. Somorovsky, and J. Schwenk, "Penetration Testing Tool for Web Services Security," IEEE Eighth World Congr. Serv., 2012; 163–170.
22. A. Chonka and J. Abawajy, "Detecting and mitigating HX-DoS attacks against cloud web services," Proc. 15th Int. Conf. Network-Based Inf. Syst. NBIS, 2012; 429–434.
23. T. R. Sree and S. M. S. Bhanu, "HADM: detection of HTTP GET flooding attacks by using Analytical hierarchical process and Dempster-Shafer theory with MapReduce," Secur. Commun.Networks, 2016; 9(17): 4341–4357.