International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 7, ISSN No. 2455-2143, Pages 185-188
Published Online May - June 2016 in IJEAST (http://www.ijeast.com)

A NUCLEIC FILTER TO DEFEND THE DDoS ATTACKS IN CLOUD COMPUTING ENVIRONMENT

Mr. Oinam David Singh
M.Tech (CSE)
Subharti Institute of Technology & Engineering
Meerut, India

Dr. Jayant Shekhar
Principal
Subharti Institute of Technology & Engineering
Meerut, India

Abstract— **Distributed Denial of Service was widely publicized when Yahoo was attacked in the year 2000. We were motivated to write this research paper from this incident. Distributed Denial of Service attack is characterized by an explicit attempt by an attacker to an attempt network resource unavailable to the legitimate users. Towards the Cloud Computing, flooding attempt will be targeted towards the data center. In this paper, we propose 'Nucleic Filter' a defending mechanism as a solution to monitor the incoming request towards the data center. Security is must towards the data center in Cloud computing environment since the concept of virtualization is applied.**

Keywords— **Cloud Computing, DDoS, Attacks, Cloud War, Nucleic Filter**

I. INTRODUCTION

Cloud computing is relatively a new hype that communicates the use of information technology services and resources that are provided on a service basis. NIST (National Institute of Standards and Technology, USA) definition [1] of Cloud Computing is: *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable that can rapidly be provisioned and released with minimal management effort or service provider interaction."*

Cloud model is a new technology of traditional data centre with the inclusion of advanced features to provide services in a shared environment on virtualized systems with essential five characteristics, three service models and four deployment models. Initially Cloud services began with extracting out the infrastructure layer to a shared data centre environment, followed by platform and applications.

Confidentiality, integrity, and availability are known as CIA triad of information security are the backbone of cloud software assurance. According to the author of [2], proposed CIA-triad extension as the IAS-octave, which further includes Accountability, Auditability, Authenticity, Non-repudiation and Privacy to CIA-triad

Distributed Denial of Service attack is characterized by an explicit attempt by an attacker to an attempt network resource unavailable to the legitimate users. It interrupts or suspends services of a host connected to the internet either temporarily or indefinitely. A denial of service attack includes [3]

a. Sending flooding packets to the server
b. Teardrop attack
c. Executing malwares
d. Application level flood

The goal of this work-in-progress paper is to propose a Nucleic filter to make as an idiosyncratic filter in order to defend the DDoS attacks over the cloud computing environment. The very most recent DDoS attack is the attacker hijack the particular cloud and send the flooding message to the data center to reach the threshold of the server.

II. DEPLOYMENT MODELS

In a Cloud services, four deployment models are usually discussed, namely public, private, community and hybrid cloud.[4] Fig 1 below illustrates Cloud Deployment Models.

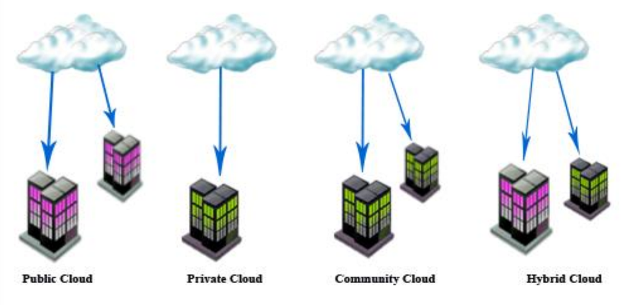

Fig. 1. Cloud Deployment Models

A. Public Cloud –

In Public Cloud model, service provider makes resources, like applications and storage, accessible over the public network like Internet.

B. Private Cloud –

The Private cloud infrastructure has all the features of public cloud but confine in a single organization.

C. Hybrid Cloud –

The integration of both private and public cloud form the hybrid cloud service deployment model.

D. Community Cloud –

Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group, which requires a central cloud computing facility, utilize this shared cloud resource.

III. SERVICE MODELS

Cloud Computing associates mainly with three different service models: *Software-as-a-Service (SaaS), Platform-as-a-Service PaaS),* and *Infrastructure-as-a-Service (IaaS).* [3] Fig 2 below illustrates Cloud Service Models.

End User
SaaS
Application Developer
PaaS
Network Architect
IaaS

Fig. 2. Cloud Service Models

A. SaaS –

In Public Cloud model, service provider makes resources, like applications

B. PaaS –

In Public Cloud model, service provider makes resources, like applications platform is use to perform the experiment.

C. IaaS –

Infrastructure as a Service shares Internet infrastructure, such as servers, storage, networks, and operating systems.

IV. DDoS ATTACK TYPES

The major protocols that are used in DDoS are HTTP, TCP, UDP, ICMP, IP etc. DDoS attack types are categorised as below.

1. Application Layer Attacks –

In Application Layer attacks, attacker targets to server overflow by sending a large number of requests. HTTP floods, slow attacks and DNS query flood attacks are the common attack vectors of this layer attacks. [5] Fig 3 shows Incapsula mitigates a massive DNS flood, peaking at over 25Mpps

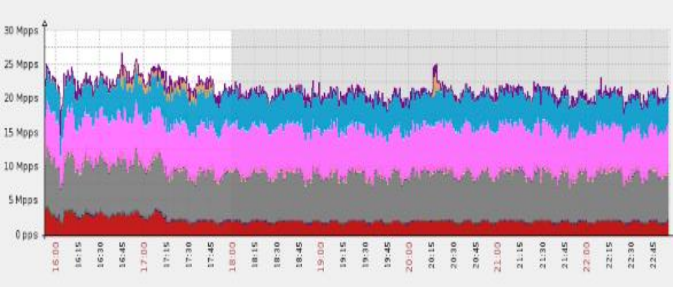

Fig 3. Incapsula mitigates a massive DNS flood, peaking at over 25Mpps (million packets per second).[5]

2. Transport and Network Layer Attacks –

In OSI model, these layers are represented as layer 3 and 4. The main protocols are TCP and UDP. Attackers target to flood the network interface in order to exhaust the resources and deny to response the legitimate traffic. [6]

3. Smurf Attack –

Attacker sending a huge number of ICMP echo traffic to asset of IP broadcast addresses where the echo packets are specified with source address of victim. [7]
IP network will accept ICMP echo requests and an echo reply to the source address. [8]

4. SYN Flood Attack –

It is also known as TCP SYN attack. It is focussed on exploiting TCP three-way handshake. When server initially receive the request, send back SYN/ACK and wait for client final ACK. In this attack, attacker will send a barrage of initial request without sending the client ACK, leaving the server to wait. As server has limited buffer, initial request will make server overflow and unable to process new connection. [9]

5. UDP Flood Attack –

In this attack, attacker uses UDP which is connectionless networking protocol. A huge number of UDP packets are sent, victim will be forced into sending ICMP packets which are not even reached to clients. In this attack, flooding takes place due to ICMP packets instead of UDP packets.

V. CLOUD WAR

When a Provider that host the server, it includes the high availability of computational resources. DDoS attacks which are common to exhaust resource cloud since attacker may use cloud to send flooding message. The attacker may hijack the particular cloud and initiate a particular message and send continuous message until the server overflow. Such attack includes two or more cloud as shown in Fig 4. [10]

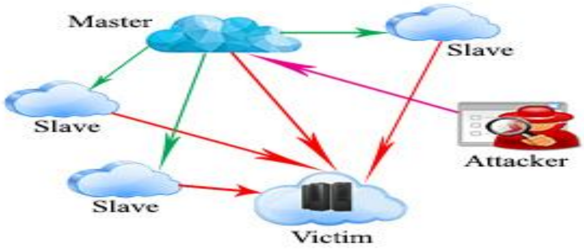

Fig. 4. Cloud War

Attacker send the instruction to the Master and Master sends the instructions to the slaves. Master and slaves attack the target victim.

VI. YAHOO ATTACK

The surprise attack on Yahoo that took place in the year 2000, February 7, down the server for more than three hours. Yahoo attack was based on Smurf attack combining with Tribe Flood Network Technique. Yahoo was receiving more than one gigabit per second of data request at the peak of attack. [11]
The magnitude of attack was unexpected and not prepared to defend. Yahoo believed that the Internet Service Provider could easily defend any of the DoS attack with the bandwidth provided to the end users. Yahoo were not aware of a large number of DDoS attack from many servers and network across the internet.

VII. NUCLEIC FILTER

There are a numerous number of End Users and it is not so possible to provide security towards the users. The security protocol must be imposed towards the data center.

Our Designed Nucleic Filter is extracted from the idea of nucleus of an atom from Chemistry. The nucleus of an atom comprises of protons and neutrons but the properties of chemistry are not followed. To design this filter, we analyze with the existing paper and proceed with the working process as below.

1) Analysis of a few recent publication –

According to author, [12] proposed a multilevel thrust filtration defending mechanism against DDoS attacks, but the major drawback is flagging to legitimate user as malicious user takes place when legitimate traffic occurs.

According to author, [13] discussed about Anti-Dos but failed to detect the types of DDoS attack and remain unconsidered spoofing kind of passive attack.

According to author, [14] proposed DDoS detection Scheme based on Over Court Gateways. This mechanism detects the legitimate user and migrates to a separate channel but could not classify the impersonating passive DDoS attack.

2) Proposed architecture of nucleic filter scheme to defend the DDoS attacks –

A Nucleic Filter is designed in such a way that it is internally segmented. Each segmented filter contains the nucleus which is consisting of numerous numbers of proton and neutron. Fig 5 illustrates the designed architecture of Nucleic Filter to defend the DDoS attacks. The red balls indicate the proton and green ball indicates the neutron

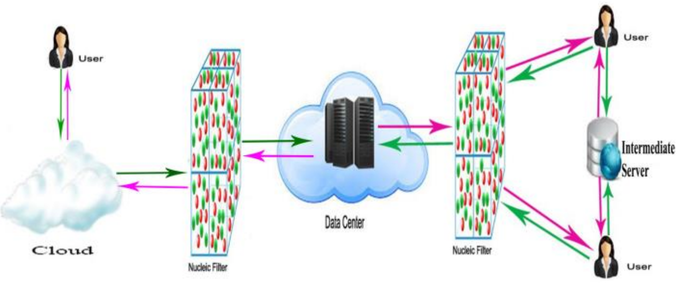

Fig 5: Architecture of Nucleic Filter scheme to defend DDoS attacks

Note: Green arrow: request and Pink arrow: response

When User likes to use resources from data center, initially, log in id and password will be sent to intermediate server. IS (Intermediate Server which act as look-up server) response as valid and hence user can connect with data center passing through the filter else user will be marked as invalid User. IS is maintained by CSP which holds information about the Users which and hence no third party is required for the user to request the resources from Data Center. For the valid user, Nucleic Filter validates digital signature and generates particular Key and Time. Request is passed to Data Center.

When request is from User to Data center

At Filter, monitor request rate, type and size

If (appropriate)

Validates digital signature and generates particular Key and Time

(Service Allow)

Else

Block all such request with neutron and destroy those blocked request by protons

If one neutron marks as inappropriate request, warn all the neutrons of such request as inappropriate to block.

When the request is from the cloud to data center, follow the same procedure at filter as above.

When legitimate traffic occurs from legitimate users, Block temporary all the incoming request and prompt the users, request in queue.

Using SJF (Shortest Job First) Algorithm for those queue requests, process the request.

Flagging a legitimate user as malicious can be resolved.

VIII. CONCLUSION

In this work-in-progress paper, we discussed Distributed Denial of Service attack on internet for the past many years. As Cloud computing is a new hype, many users, organizations will look forward for virtualization. In the lacking of security features, market will crash.

DDoS is a common method to exhaust resources. So it is necessary to deploy detection method and destroy such attacks. Each request must be viewed either flooding attempt or legitimate users.

Our Proposed solution is neither host based nor router based. We aim to work in future experimentally and apply this filter towards DNS amplification attacks.

IX. REFERENCES

[1] Peter Mell, Tim Grance (2011, Sept.) “*The NIST definition of Cloud Computing*”, *v.* 800, no 145
Available:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] Cherdantseva, Y.; Hilton, J., "A Reference Model of Information Assurance & Security," Availability, Reliability and Security (ARES), 2013 Eighth International Conference on , vol., no., pp.546-555, 2-6 Sept. 2013 doi: 10.1109/ARES.2013.72

[3] BARFORD, P., KLINE, J., PLONKA, D., AND RON, A. A Signal Analysis of Network Traffic Anomalies. In Proc. Of ACM/USENIX IMW (2002).

[4] Krutz, Ronald L., and Russell Dean Vines. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing,” New Delhi, India: Wiley, 2010. Reprint 2013, pp. 37–49

[5] https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

[6] https://www.cloudflare.com/lp/ddos/?_bt=95962033332&_bk=ddos%20attack&_bm=e&_bn=g&gclid=CMzWl9vIgs0CFdcRaAodGFsCDQ

[7] Daemon9, Infinity, and Route, “IP-spoofing demystified: trust-relationship exploitation,” Phrack Mag., June 1996, http://www.fc.net/phrack/files/p48/p48-14.html

[8] S. Bellovin, Ed., “The ICMP traceback message,” Network Working Group Internet Draft, Mar. 2000, http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt.

[9] Cisco Systems, Inc., “Defining strategies to protect againstTCP SYN denial of service attacks,” July 1999,
http://www.cisco.com/warp/public/707/4.html.

[10] Nils Gruschka and Meiko Jensen “Attack Surfaces: A Taxonomy for Attacks on Cloud Computing”, 3rd International Conference on Cloud Computing, 2010, pp 276-279

[11] A. Harrison, “The denial-of-service aftermath,” Feb. 2000,
http://www.cnn.com/2000/TECH/computing/02/14/dos.aftermath.idg/index.html.

[12] Iyengar, N.Ch.S.N., Ganapathy, G., Mogan Kumar, P.C and Abraham, A. (2014) ‘A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment’, Int. J. Grid and Utility Computing, Vol. 5, No. 4, pp.236–248.

[13] Chen, S., Ling, Y., Chow, R. and Xia, Y. (2007) ‘AID: a global anti-DoS service’, *Computer Networks*, 2007, pp.4252–4269.

[14] Du, P. and Nakao, A. (2010b) ‘OverCourt: DDoS mitigation through credit-based traffic segregation and path migration’, *Computer Communications*, Vol. 33, No. 18, pp.2164–2175.