A SURVEY ON PREVENTING DDOS ATTACK IN CLOUD ENVIRONMENT

Karthik Sekaran[1], **Karunakaran G**[2], **Charanya R**[3]

Abstract— Cloud computing is an evolutionary technology, which is a lead topic in IT Industry at today's trend. The reason behind this development is flexibility for the users to make use of the service from anywhere else to access the data more secure from a private environment. But there are some issues in this technique in which there is some lack of security for the data in cloud. Where there is a data, there will a security breach by the attackers. Nowadays more number of people are willing to make us of cloud environment today. Meanwhile, attackers change their attitude by perform attack in cloud bases. The most common attack is Distributed Denial of Service, which can be done by any sort of attackers without any need of more technical skills. More tools are available to perform this sort of attacks which will make the server not to provide service to anyone and keep on getting the server down for a longer time until they stop the attack. Some tools are available in market which is often used by the sophisticated attackers because these tools having the ability to send a more number of threads (spoofed requests) to server for a certain period of time, which will exhaust the service availability provided by the server and makes the resource in the server unavailable for certain period of time for the legitimate users. In fore coming topics we are going to explore some security issues and its prevention mechanisms in detail.

Key Terms—Cloud computing, DDoS attacks, Flooding attacks, mitigation.

I. INTRODUCTION

Cloud Computing is an internet based environment in which the data stored in the cloud center is done via networks. Data which needs to be placed in the cloud area needs to be uploaded from the client's system to cloud server. Login based security will be given for authentication process. Data in the cloud is encrypted for data security purpose. After the data is uploaded, the file can be re progressed to the client from anywhere else using the authentication scheme. On February 9, 2000 most of the corporate websites like EBay, E-Trade, Yahoo and Federal Bureau of Investigation (FBI) websites are damaged by a huge DDoS attack. Hence it is necessary to prevent and mitigate the web servers from DDoS attack to ensure data security on cloud environment by the service provider.

A. Cloud Computing:

Cloud Computing is simply like a data warehouse which is not available in the client's system. The storage medium will be somewhere else in an area from which we can access our previously stored data via some authentication mechanisms in which no other persons can access the data. Because of the reason of its simplicity and flexibility more number of users are make use of cloud services. Many cloud service providers allows the client to make use of the system to some extend without cost of money. This makes cloud computing technology as a most emerging storage mechanism among the clients across the world.

Cloud computing mainly consists of three layers:

i. Software as a service

First and Topmost layer. The services of Cloud are accessed by the client system. Reduces the workload while installing and running the product in clients system also maintenance [3].

ii. Platform as a service

Acts as a centric layer. A Cloud platform involves in changing settings and configuration of server as per increase and decrease in the demand [3].

iii. Infrastructure as a service

It is the bottom layer of cloud Infrastructure [1]. The basic function of this layer is to provide IT infrastructure through Virtualization. It is a concept of breaking or separating hardware components that is measured by means of CPU or other elements [3].

B. DDoS ATTACK:

Previously Denial of Service is the technique which is often used by the attackers to make the data source unavailable for the legal users. But it is not efficiently perform the damages to the victim environment. So attackers find a new way called DDoS attack in which more number of slave systems interconnected with one master system which will command the slave systems to perform attack on a specific victim system. At a time more number of service requests is reached to the server. The server can't be able to handle such a huge sort of

Manuscript received March, 2014.
First Author name, *Karthik Sekaran, SITE,VIT University, Vellore,India,*

Second Author name, *Karaunakaran.G, SITE,VIT University,Vellore,India,*
Third Author name, *SITE,VIT University,Vellore,India,,*

requests so it won't able to provide service for the other legitimate users. Nowadays botnets comes into an extend to perform these sort of attack instead master-slave architectures. DDoS attack is dangerous because not only financial and gaming organizations gets suffer under these sort of attacks, also they targets the mission critical business applications in which peoples are normally relies on such as email messaging, money transfers, banking sectors, ATM transactions etc. These attacks makes the peoples liable among those organizations. Thus sophisticated attackers make use of this opportunity to make a huge changes in economy of that environmental factors. Rapid development in cloud computing, makes these attackers are motivated to concentrate on cloud data security mechanisms to break and steal data from that environment. DDoS is used as a key factor to perform attack on cloud area which will results in an effective way for the attackers.

C. GENERAL ATTACKS:

i) Tsunami SYN Flood Attack:

A normal SYN Packet is bounded about 40-60 bytes per packet. This type of attack departs from the typical make up of SYN packet by transmitting large packet size which make more complex and defeat many security algorithms. This SYN-Flood is different in which its characterized as approximate of 1000 bytes per packet in size and the attack can hit an entire network ranges. Attacks with these dimensions to make them quickly consume bandwidth and thus far even these modest timed attacks were witnessed experienced pulses of about 4-5 Gbps in attack traffic. This new type of attack has the ability to saturate the internet pipe of its victim faster than most attack types we have witnessed beforehand [4].

ii) ICMP Flooding Attack:

Similar to other sort of flooding attacks, this type of attack is done by delivering huge pack of ICMP threats. The goal is to deliver a huge packets to victim, results in slower down the network connectivity strength and disconnect at a point of time due to timeout signals.

iii) Volumetric Attacks:

These attacks are performed to consume a large amount of bandwidth of the victim organization. These type of attacks is falling under two categories. One is done within the target service and other thing is done in between target service. Mostly this attacks is reasonable for creating congestion between network traffic.

iv. Application Layer Attacks:

One of the most effective attack is fall under this category of performing attacks in application layer. This will be more effective and it can be done under a low traffic rate and very difficult to defect and mitigate. Sophisticated attackers are make use of this attack because of its effective results and undetectable for a while.

Application Layer Attacks Types:

Common Application-Layer DDoS Attack Types , HTTP Flood Attacks.

1. Common Application-Layer DDoS Attack [18]:
It is categorized into four types. [11,12]

Type 1: Request-Flooding Attacks:

This type of attack occurs when a heavy legitimate application-layer requests like HTTP are sent to server to exhaust or overwhelm its session resources. [9,19]

Type 2: Asymmetric Attacks:

Motivation is to reduce the efficiency of server and finally makes the server down. This is possible when a normal request consumes huge server resources like disk space, CPU performance results in redundancy of resource utilization on server.

Type 3: Repeated One-Shot Attacks:

When a high workload request across many TCP sessions is sent to the server, with the target of degrading the service of the server [19].

Type 4: Application-Exploit Attacks:

This attack targets the vulnerabilities in applications by causing a fault in a server's operating system or applications and allow the attacker to gain control of the application, system or network. Scripting vulnerabilities, buffer overflows, cookie poisoning, hidden field manipulation, cross-site scripting and Structured Query Language (SQL) injection are the examples of these attacks [12,19].

2. HTTP Flood Attacks.

Type 1: HTTP Malformed Attacks*:*

Creates service unavailability problems by sending illegitimate HTTP packets to the server [19].

Type 2: HTTP Request Attacks:

These attacks are often performed with different types of legitimate HTTP requests which are sent to web servers in an attempt to flood them by consuming the server resources [14,19].

Type 3: HTTP Idle Attacks :

When HTTP connections are opened and left idle without actually sending a complete HTTP request by an attack [19].

II. EXISTING SYSTEM:

A. Intrusion Prevention System and Firewalls:

Traditional way of securing the cloud environment, basically they won't mitigate to defend against security issues. These devices are mainly focuses on defending once for each connection and not at higher bandwidth. This will suffers legitimate users a lot. At the same time, Firewall and IPS are only a stateful devices, in which they are suitable only for normal connections which maintains a state table of some thousands of active connections in which every incoming data is compared with state table connection, checks whether the connection is valid or

not. If a flooding attack is done with some millions of sessions, then it will exhaust the connection table at once. Therefore it is said that both IPS and firewall is only for handle some thousands of connections and only to check for active connection and categorize among legitimate users and attackers. But they are no longer relied because they can't manage huge amount of connectivity and fail to stop packets from non-legitimate users. They won't be able to differentiate between DDoS packets and normal packets. At the same time, they are not intended to defend the cloud against attacks, only to check whether the packet arrival is from legitimate users or attacker.

B. TVA Scheme:

The impact of packet floods is limited, so that even if other hosts gets affected, two hosts can communicate between them[15].

III. DEFENSE MECHANISMS AGAINST DDoS ATTACKS IN CLOUD ENVIRONMENT:

A. Defending Against Distributed Denial of Service Attack with VMM:

The main objective of Virtual Machine Monitor is to monitor and compute the current resource availability on server and compares with the given value which is considered as a threshold from which we can able to find the existence of attacks. After detecting an attack this method lively transforms the OS and specific applications into an isolated place which also is a virtual machine. The advantages of this method is that without stopping OS performing makes the system able to escape from this kind of attack [15,20].

B. Cloud Trace Back Model and Cloud Protector:

This model is focuses on Trace Back our application module to find DDoS attack source. The new introduction in this scheme to perform back propagation neural network which is called as Cloud Protector, to detect and filter traffic Techniques for mitigating EDoS attacks. [16]

Cloud Trace Back (CTB) objective is to apply a SOA approach to Trace Back methodology, in order to identify the true source of a DDoS. CTB is based upon Deterministic Packet Marking (DPM) algorithm. DPM marks the ID field and reserved flag within the IP header. As each incoming packet enters an edge ingress router it is marked, outgoing packets are usually ignored. The marked packets will remain unchanged for as long as the packet traverses the network [16,22].

Cloud Protector is to detect and filter out DDoS packets. Threshold Logic Unit (TLU) which adds incoming data into stack to see if they are above the threshold or not. It has three different units.

i. Dataset for training and testing:

Depending on the accuracy of the training data, the performance will be enhanced. Also neural network depend on training data [16,22].

ii. Pre-processing Dataset:

Input to the developed system is given only when the dataset is pre-processed. It consists of numerical and symbolic values and it is converted to numeric form. This modified dataset is ready to be used as training and testing of neural network [16].

iii. Determining NN model:

A comparison is made for many cases and optimum is selected to get the optimum number of hidden layers and their neutrons and there is no more existence of a mathematical approach to done the optimum number [16].

C. Confidence-Based Filtering (CBF)method Analysis

This method is deployed by Chen et al. .It is mentioned as attack and non-attack period. A normal profile is created by capturing and analyzing legitimate packets according to the attribute pairs present inside TCP and IP header. CBF score and Confidence are computed in attack period. Confidence is a frequency of single and pair attribute in packet. Each discarding threshold is compared with CBF score at attack period. Reason is that, it is not based on severity of the attack. At the same time the performance of CBF is depends on the attack environment and it works efficiently at heavy data traffic rates [20].

D. A Filter Tree Approach to Protect Cloud against XML and HTTP DDoS Attacks:

This approach was proposed to protect the cloud environment against HTTP and XML DDoS Attacks. Defender of this scheme is mainly consists of three steps between client and server and defend attack before reaches the cloud[20]. IP address is used to recognize and trace back the attackers Virtual Machines. Cloud Defender comes under five steps given as sensor filtering, Hop count filtering, Internet Protocol Frequency Divergence Filter, Confirm legitimate user IP Filter and Double Signature Filter [17][20].

IV.CONCLUSION:

Since cloud computing meets a rapid development, it faces more number of security flaws mainly DDoS attacks on cloud environments. Botnets facilitates attackers to perform the attack more effective at acceptable costs. Moreover, most of the organizations migrated themselves from LAN or other topological network to cloud bases. This is a key activity which enhances development of cloud computing. As a result, more number of security issues arises. As we discussed earlier about some security mechanisms, which will helps us to improve data security and accessibility controls in cloud. Sophisticated attackers improve their method of attacks to some extend and having the ability to penetrate these mechanisms which will be outdated after some period of time. So it should be noticed that, whatever the security mechanisms which is used to prevent data

security, should be enhanced periodically to provide more reliability among organizations and users.

REFERENCES

[1] Stephen M. Specht, Ruby B. Lee," Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures". In Proceedings of the 17thInternational Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004.[2] http://www.in.idc.asia/ (accessed in Feb, 2013)
[3] Naresh kumar, Shalini Sharma,"Study of Intrusion Detection System for DDoS Attacks in CloudComputing".[4]http://blog.radware.com/security/2014/10/tsunami-syn-flood-attack (accessed in Mar, 2015)
[5] Gulshan Shrivastava and Kavita Sharma, "The Detection & Defense of DoS & DDoS Attack. A Technical Overview" Proceeding of ICC, 27-28 December 2010
[6] Niraj Suresh Katkamwar, Atharva Girish Puranik and Purva Deshpande, "Securing Cloud Servers against Flooding Based DDoS Attacks"
[7]http://www.DDoSattacks.biz/protection/firewalls-and-ipss-can-they-stop-DDoS-attacks/
[8] J. Ramesh Babu, B. Sam Balaji, R.Wesley Daniel. K. Malathi, "A Prevention of DDoS attacks in cloud using NEIF Techniques".
[9] FuiFui Wong and Cheng Xiang Tan, "A Survey of Trends in massive DDoS Attacks and Cloud-Based Mitigations".
[10] Arbor Networks, "The Growing Threat of Application-Layer DDoS Attacks," 2012.
[11] S. Ranjan, R. Swaminathan, M. Uysal, And E. Knightly, "DDoS-Resilient Scheduling To Counter Application Layer Attacks Under Imperfect Detection," In Infocom 2006. 25th IEEE International Conference on Computer Communications. Proceedings, 2006, Pp. 1-13.
[12] D. Watson, "Web Application Attacks," Network Security, Vol. 2007, Pp. 10-14, 10// 2007.
[13] Prolexic Technologies, "Prolexic Quarterly Global DDoS Attack Report Q1 2013," Florida2013.
[14] C. Linhart, A. Klein, R. Heled, And S. Orrin, "Http Request Smuggling," Computer Security Journal,Vol. 22, Pp. 13-26, 2006.
[15] Gopinath.V, Anand.C, "An Efficient Approach to Block DDoS Attacks Using Adaptive Selective Verification Protocol".
[16] I. Mettildha Mary, P.V.Kavitha, Priyadharshini M, Vigneshwer S Ramana, "Secure Cloud Computing Environment against DDOS and EDOS Attacks".
[17] Sara Farahmandian, Mazdak Zamani, Ahad Akbarabadi, Joobin Moghimi
Zadeh, Seyed Mostafa Mirhosseini, Sepiden Farahmandian", A Survey on Methods to Defend against DDoS Attack in Cloud Computing"
[18] Zhang, Yun Peng. "Design for the Application Layer of Network Security Solutions", Advanced Materials Research, 2014.
[19] http://www.airccse.org/.
[20] http://www.wseas.us/.
[21] Chonka, A.. "Cloud security defence to protect cloud computing against HTTP-DoS and XML DoS attacks", Journal of Network and Computer Applications, 201107
[22] Bansidhar Joshi. "Securing cloud computing environment against DDoS attacks", 2012 International Conference on Computer Communication and Informatics, 01/2012

