A Survey of Intrusion Detection System for Denial of Service Attack in Cloud

Shalki Sharma
Dept. of Computer Technology and application
NITTTR, Bhopal.

Anshul Gupta
Department of Information Technology
MPSTME, NMIMS.

Sanjay Agrawal, PhD
Dept. of Computer Technology and application
NITTTR, Bhopal.

ABSTRACT

Cloud computing provides its user a lot of advantages but this technology has quite a bit of flaws as well. One of main flaw in cloud is the security present in the cloud. There are various threats, attacks and security issues that pertain in cloud. Among all the attacks DoS is a crucial one. The main aim of this attack is to bring down the services and resources and thus effecting everyone who is accessing the resource. This paper discusses about the Denial of Service attack or DoS attack in cloud environment and what are the various detection methods which have been proposed for the same.

Keyword

Cloud Computing; Denial of Service; Intrusion Detection.

1. INTRODUCTION

The world of cloud computing is growing day by day. In the world of computing, cloud computing is growing fast as third party storage servers. There are a lot of definitions of cloud which have been provided by many people. But in a simple way we can define cloud computing as a combination of "virtualization" and "automation". By virtualization we simple mean that anything that is not physical. Everything from simple software to a complex hardware infrastructure can be virtualized these days. There are various advantages of using virtualization and one of the main benefits of using virtualization is that one does not require a fully fledged set up and accessibility is very easy as well in cloud. Automation provides user with three most important things. These are 1) self-service 2) infinite scale 3) utility based services.

So from the above we can now define cloud computing as "the combination of virtualization and automation to provide users with an easy access and infinite scale at low cost." Cloud has five basic characteristics defined by NIST [1]. These are:

1. Cloud provides on demand self service.

2. Cloud gives a broader network access.

3. Cloud provides resource pooling by combining many service provider's resource to serve as many customers.

4. Cloud provides rapid elasticity.

5. Cloud gives us measured services.

There are various benefits of using cloud over a traditional approach. Cloud helps to reduce the cost; it provides global accessibility, unlimited storage capacity, improved performance and many more advantages but apart from providing a lot of benefits there are various issues which are associated with cloud. One of the major issues associated with cloud is the security associated with the cloud. As we know in cloud every user has access to the data residing in the cloud so security of data is a major concern.

Apart from the data security there are several threats like man-in-the-middle, spoofing/sniffing, account or service hijacking etc. These threats aims to make the services of cloud weaker and sometimes even bring down them down.

1.1 Various services provided by Cloud

There are basically three types of services which are provided by Cloud Service Provider.

*1.1.1 Software as a Service or SaaS***:** SaaS provides clients to use softwares or applications which are residing on cloud directly on their machines. These applications or softwares run on a distant machine which is in the cloud by means of internet [1] [2].

1.1.2 Platform as a Service or PaaS: In PaaS the whole underlying architecture i.e. operating system, hardware is provided and the user develops his own software or any application [1] [2].

1.1.3 Infrastructure as a Service or IaaS: Infrastructure as a service provides only with the hardware and the networks and operating system has to be installed by the user [1] [2].

1.2 Cloud Computing deployments models

There are basically four deployment models present in cloud [1][14]:

1.2.1 Public Cloud: This is a kind of deployment model where all the services and resources are provided to the users over the internet. All the resources are managed by the cloud service provide and are available to everyone.

1.2.2 Private Cloud: In private cloud the whole infrastructure is owned and managed by a private organization.

This kind of model is exclusively made for a single organization having multiple users.

1.2.3 Hybrid Cloud: Hybrid cloud is a combination of public and private cloud. It uses private cloud as a foundation in combination with the strategic use of public cloud services.

1.2.4 Community Cloud: Community cloud is made especially for a community of users that share the same concerns.

The rest of the paper is described as below. Section II discusses about various threats and vulnerabilities which are present in cloud. Section III discusses about Denial of service attack. Section IV describes what all are the various techniques used for detection of denial of service attack in cloud. Finally we conclude the paper with section V.

2. CLOUD SECURITY: VULNERABILITIES AND THREATS

Cloud security is major area of concern when dealing with a cloud. There are various security issues or threats which are related with cloud. Keiko Hashizume et al. [3] gave a description about the

various threats and vulnerabilities which are present in a cloud. All the services provided by the cloud saas, paas, iaas have their level of security issues. As known saas and paas lie on top of iaas so any security defect in iaas will directly affect saas and paas and so is possible in the reverse case. Each cloud service provider provides the user with its own level of security resulting in inconsistent combination of security models. This also creates confusion between the service providers when any attacks happen.

2.1 Vulnerabilities in cloud

Cloud uses many technologies like virtualization, web browsers, web services etc. Any vulnerability in these technologies will affect the cloud also. There are a lot of vulnerabilities in a cloud environment. Keiko Hashizume et al. [1] discussed what all are the vulnerabilities present in a cloud. Following table provides a overview of the vulnerabilities [1], [2].

Vulnerability	Description
Vulnerabilities pertaining with data.	Information about where the data is residing is not known to the user. Data may reside in a different country with a different law and data cannot be deleted completely [3].
Virtual Machine Vulnerabilities	Allocation and deallocation of resources in VMs can lead to a vulnerability. Sometime migration of a VM from one server to another is also responsible for this.[3]
Vulnerability in Hypervisors	Hypervisors complex coding and their flexible configuration to meet any organizations need.[3]
Vulnerability in Network	Virtual machines share their virtual bridges for networking.[3]

Table 1 Vulnerabilities in cloud

2.2 Threats in cloud

According to the report by CSA i.e. Cloud Security Alliance [2], there are seven security threats which are present in cloud which cover all the threats like DdoS, sniffing, man in the middle attack etc. and classify which service model is affected by it.

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure interfaces and APIs.
3. Malicious insider.
4. Shared technology issues.
5. Data loss and leakage.
6. Account or service hijacking
7. Unknown Risk profile

Security threats in a cloud environment are no different from network security threats. Threats like DoS, sniffing, spoofing, data scavenging etc. persist in cloud also. All these affect the working of any cloud and also of the users. Threats like denial of service make the resource unavailable to the legitimate user by making illegitimate user use or occupy the resource. Attack like data leakage happens when data gets into bad hands while it is being transferred or stored [3].

There are a lot of threats which are present in cloud. This paper tends to discuss Denial-of-Service attacks in cloud and also various detection methods proposed for the same.

3. DENIAL OF SERVICE ATTACK

Denial-of-Service or DoS is a kind of attack in which a resource is made unavailable to the intended user. So attacks with respect to resource unavailability can be said to a DoS attack. The main aim of such type of attack is to exhaust the CPU resources and make legitimate user void of the resources. "Primary victims" are resources which are under attack and "Secondary victims" are those which generate these attacks [4] [5].

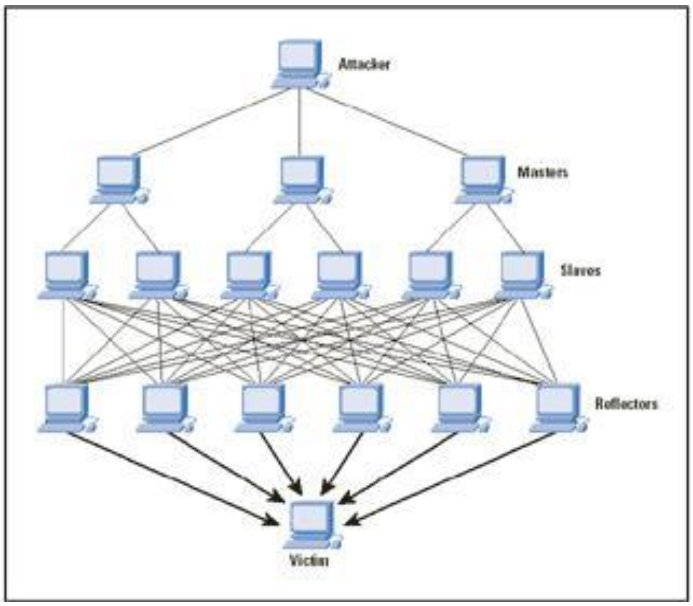

Figure 1 Denial of Service Attack [14]

A distributed denial of service attack or DdoS is a DoS attack but here multiple systems are used for generating this attack. Master, Slave and Victim are the main components of this type of attack. Master is one who generates the attack, slave provides a platform for the attack and victim is the one on which the attack is done. Figure 1 [14] gives a description of typical DoS scenario.

4. RELATED WORK AND TECHNIQUES.

The following section discusses what are various techniques used for the detection of Dos in a cloud environment.

4.1 Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network.

The authors, Ruiping Lua and Kin Choong Yow, in this paper proposed a novel approach for DDoS attacks which uses an intelligent fast-flux swarm network. They have used the Intelligent Water Drop algorithm for distributed and parallel optimization. To maintain connectivity between swarm nodes, clients, and servers fast-flux technique is used. Fast-flux networks allow building a transparent service, allowing minimum modifications in the existing cloud services (e.g. HTTP, SMTP)[6].

The authors here have used the concept of swarm in the following two ways:

• Fast-flux technique in domain name servers

• Organization of swarm.

Fast-flux hosting allows a fully qualified domain name to have many IP addresses assigned to it. IWD is highly resistant to the sudden network changes and performs partial optimization depending on the parameters it sense. In the proposed approach, a layer is added for communication purpose. All incoming coordinates and forwards the requests to the designated server. The server's response is sent back to the swarm, which forwards it to the requesting client [6]. The clients reach the server by using a fully qualified domain name.

4.2 A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks

The author, E.Anitha et al. [7] proposed a new technique for detection of DDoS attack using a packet marking approach. In the proposed method HX-DoS attacks are checked against cloudweb services to discriminate between the legitimate and illegitimate messages. This is done with the help of rule set based detection, called CLASSIE. Modulo marking method is used for avoiding the spoof attack. Reconstruct and Drop method is used on the victim side to drop the packets and make decision. The above technique improves the reduction of false positive rate and the detection and filtering of DDoS attacks is improved.

4.3 A Cooperative Intrusion Detection System Framework for Cloud Computing Networks

Chi-Chun Lo et al. [8] proposed a cooperative intrusion detection system for dos attack in cloud. The proposed system is Distributed IDS and uses cooperative defense for each cloud environment by the IDSs. IDS are provided to each cloud region and any IDS who is suffering from an attack sends out alert to the other IDS which are defined in the block table. The IDS exchange their alerts and a judgment criterion is defined to find the trustworthiness of the alerts. If the attack or alert is a new one then it is added in block table and thus an early detection of attack from the victim IDS makes it possible for other IDS to prevent the same attack. The IDS has four components within it-intrusion detection, alert clustering and threshold computation and comparison, intrusion response and blocking, and cooperative operation. Along with this each IDS has three modules: block, communication, and cooperation modules. Intrusion detection is used for collecting packets and analyzing them. If the packet is listed in the block table the system drops it and if not the packet is forwarded to the next component. Alert clustering and threshold comparison identifies the level of packet is send from the intrusion detection. These are divided into three type 1-serious, 2-moderate and 3-slight. Intrusion response and blocking is present in each IDS and is used to for blocking bad packets and sending an alert to all the other IDSs. Communication and block modules are used to alert other IDSs and to drop the packets if they are above the threshold. Cooperative operation is present in each IDS and is used to receive alerts from other IDS. The advantage of this system is that it prevents the whole system from single point failure.

4.4 Detecting Web based DDoS Attack using Map-Reduce operations in Cloud Computing Environment

Junho Choi et al. [9] proposed a method combining HTTP GET flooding within DDOS attacks and Map-Reduce for fast detection of attack in cloud. The proposed method assures the availability of the target system for authentic and reliable system which is based on HTTP GET flooding. In the proposed approach the IP with Ddos attack is send challenging values and connection is provided in normal way. At the same time another IP is filtered. TCP connections are checked for confirming the HTTP GET request. Input values so generated by the packet analysis for detection of Ddos attack are send to map-reduce for statistical analysis. With increasing congestion the proposed method is found to be better than Snort detection as the processing time is found out to be less then Snort.

4.5 Securing Cloud Computing Environment Against DDoS Attacks

Bansidhar Joshi et al. [4] is using Cloud Trace Back(CTB) model for detecting DDoS attacks employing back propagation neural network. The system handles DDoS attack in a good manner. Main architectural idea behind CTB is the use of SOA method to Trace Back methodology, for finding out the true source of a DDoS. Deterministic Packet Marking approach is used by CTB. In the proposed work the CTB uses FDPM by incorporating the CTM i.e. cloud trace back mark within the CTB header in the web service message. Thus every request is first send to the CTB header for marking and the sender's address is removed which increases the security. If in case there has been an attack then the victim can recover and reconstruct the CTM tag which reveals the source of the attack. The above approach introduces the use of a back propagation neutral network which is called as Cloud Protector. Cloud Protector is trained to detect and filter attack traffic. The system detects most of the attacks in a very short span of time and can successfully trace back 75-81% of the attacks.

4.6 Analysis and Detection of DoS Attacks in Cloud Computing by Using QSE Algorithm

Pallavali Radha Krishna Reddy et al. [10] proposed a technique for detection of DoS attack in Cloud by making use of Quantum Swarm Evolutionary Algorithm. The authors used quantum inspired particle swarm optimization for analyzing and detecting the Dos attack in cloud. The proposed system was divided into three steps-basic feature selections for individual records, QSE working nature and decision making. Anomaly based detection technique is used for decision making because it finds any type of dos attack without having any knowledge about the attacker. The whole technique is divided into two sub-phases namely training and testing. In the training phase normal traffic is captured QSE algorithm is implemented in this phase for

generating normal traffic profile. In the testing phase QSE module for detection is used for detecting abnormal traffic. The observed outcomes were compared with QEA algorithm and QSE was found to be better than QEA.

4.7 Controlling High Bandwidth Aggregates in the Network

Ratul Mahajan et al. [11] proposes a technique called Pushback which is a combination of two techniques: aggregate congestion control (ACC) and pushback. In the proposed technique two mechanisms are proposed related to ACC-local ACC consisting of identification algorithm for finding out the aggregate causing the congestion and control algorithm for reducing the effect of this ACC. The second mechanism is pushback which allows router to request their adjacent upstream router to rate limit the specified aggregate. Local ACC is used for detecting crowding at the router level and creates an attack signature that can be converted into a router filter. The signature describes a high bandwidth aggregate, a subset of network traffic, and local ACC finds out an apt rate limit for the aggregate. Pushback proliferate this rate limit to the intervening upstream neighbors contributing to the highest amount of traffic. The above method works best against flooding-based attacks because they are treated as congestion phenomena.

5. CONCLUSION AND FUTURE WORK

As the field of cloud is growing so is the security issues related to it. Security attacks like Denial of Service attack, IP spoofing, Man in the Middle affects the overall efficiency of the cloud. One of the most serious threats to cloud security comes from Denial of Service or DoS attack. The main motive behind Denial of Sevice attack is to make the intended resource unavailable to the users and to disrupt the services provided by the resource. A lot of research has been going on in this field and several IDS have been proposed to solve this problem. This survey report examines various IDS which have been proposed for finding denial of service attack in cloud. Bansidhar Joshi [4] proposed the use of Cloud Trace Back to find the source of the attacks and introduced Cloud protector by using back propagation neural network to filter and detect these types of attacks. The use of neural network can be taken into account for other IDS system for detection of DoS attack. This paper presents recent research for finding DoS attack by use of Swarm Intelligence. Ruiping Lua [6] proposed the use of fast-flux swarm network for finding these types of attacks. Methodology adapted by Pallavali Radha Krishna Reddy and Samia Bouzefrane [10] can further be extended by using a more effective advanced quantum computing technologies.

6. REFERENCES

[1] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[2] Alliance, C. "Security guidance for critical areas of focus in cloud computing v3. 0."*Cloud Security Alliance* (2011).

[3] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing."Journal of Internet Services and Applications 4.1 (2013): 1-13.

[4] Joshi, Bansidhar, A. Santhana Vijayan, and Bineet Kumar Joshi. "Securing cloud computing environment against DDoS attacks." *Computer Communication and Informatics (ICCCI), 2012 International Conference on*. IEEE, 2012.

[5] Kumar, Naresh, and Shalini Sharma. "Study of intrusion detection system for DDoS attacks in cloud computing." Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on. IEEE, 2013.

[6] Lua, Ruiping, and Kin Choong Yow. "Mitigating ddos attacks with transparent and intelligent fast-flux swarm network." *Network, IEEE* 25.4 (2011): 28-33.

[7] Anitha, E., and S. Malliga. "A packet marking approach to protect cloud environment against DDoS attacks." *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*. IEEE, 2013.

[8] Lo, Chi-Chun, Chun-Chieh Huang, and Joy Ku. "A cooperative intrusion detection system framework for cloud computing networks." *Parallel processing workshops (ICPPW), 2010 39th international conference on*. IEEE, 2010.

[9] Choi, Junho, et al. "Detecting web based DDoS attack using MapReduce operations in cloud computing environment." Journal *of Internet Services and Information Security* 3.3/4 (2013): 28-37.

[10] Reddy, Pallavali Radha Krishna, and Samia Bouzefrane. "Analysis and Detection of DoS Attacks in Cloud Computing by Using QSE Algorithm." *High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS), 2014 IEEE Intl Conf on*. IEEE, 2014.

[11] Mahajan, Ratul, et al. "Controlling high bandwidth aggregates in the network."*ACM SIGCOMM Computer Communication Review* 32.3 (2002): 62-73.

[12] Top Threats Working Group. "The notorious nine: cloud computing top threats in 2013." *Cloud Security Alliance* (2013).

[13] What is cloud? Computing as a service over the Internet: http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html

[14] A denial of service (DoS) attack. http://hacksguide.blogspot.in/2009/06/denial-of-service-dos-attacks.html