SECURITY ON CLOUD COMPUTING AVAILABILITY ISSUE AND ITS COUNTER MEASURES

JAYACHANDRAN. J
Asst. Prof.
CSE Department,
Sri Sairam Institute of Technology, Chennai, India

Abstract: Cloud computing is an emerging technology. It provides storage, resources and services such as Virtual Machine(VM) on user demand basis. The main issue in cloud computing is security. In this research paper we address the availability issues in Cloud Computing . The main aim of this paper is to recommend the appropriate solution against DDoS attack and this paper also compares the different solutions provided by many researchers against DDoS (Denial of Service) attack in Cloud Environment.

Keywords: Cloud Security, Availability issues, DDoS Attack, Virtual Machine

---

1. INTRODUCTION

Cloud computing is a emerging technology that provides shared computer processing resources and data to computers and other devices on demand. It provides storage, computer resources, services and networking that user can make use of it. User have to pay for using cloud and they can specify their requirements. Cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data. Cloud Providers: Amazon Web Services, Microsoft Azure, IBM, Google Cloud platform and Oracle Cloud.

1.1 CLOUD ARCHITECTURE

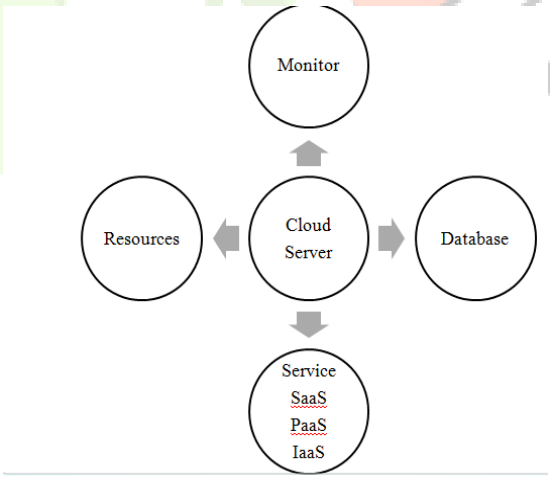

Fig:1 Cloud Computing Architecture

1.1.1SERVICES OF CLOUD COMPUTING

1.1.2. Software-as-a-Service (SaaS):

Application are accessible from various client device via web browser no need to control Infrastructure including OS, network, server,etc., where the cloud provider owns the application, server, storage operating system (OS) and infrastructure and you use the application remotely. Through a thin client interface such as Web browser.Providers: Google Docs, Mobile me and Salesforce.com.

1.1.3.Platform-as-a-Service (PaaS):

User has control over the Deployed application and application hosting environment configuration. The provider owns the OS and infrastructure, and you own the application. In PaaS the user cannot not control the cloud infrastructure including server, storage, OS, network but has control over the provided application. Providers: Microsoft Azure, Force.com and Google AppEngine

1.1.4.Infrastructure-as-a-Service (IaaS):

User has control over storage , OS , Deployed application and limited control of select networking component.the provider owns just the infrastructure and you own both the OS and the application. Provide the user with the capability of processing, storage, network and other computing resources and allow the user to deploy and run software. Providers: Amazon S3, Sun's Cloud and Google Compute Engine.

2. CLOUD COMPUTING SECURITY

Cloud computing security or, more simply, cloud security it describes the broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and,more broadly, information security.

2.1 DATA SECURITY IN CLOUD COMPUTING:

2.1.1.Confidentiality:

Data confidentiality deals with the user's data content should be secured the it should not be accessed by illegal user's. Only authorized person only can access data other should not get information of the data.E.g.: Data sharing, Data search, Data computation, without the leakage of the data contents to CSPs or other illegal users.

2.1.2.Integrity:

Data integrity describes the owner's data should be maintained and assuring the accuracy and completeness of data. A data owner always expects that the data in a cloud can be stored correctly and trustworthily.

2.1.3.Availability:

Data availability is giving authorization to the owner to access the data andresoures . The cloud data should not be shared with other user's. The main issue in data availability is DDOS Attack(Distributed Denial of Service).

3. Cloud Computing Availability Issue- DDOS (Distributed Denial Of Service)[11]

DDoS attack is almost same as Denial of Service (DoS) attack, but the impact of DDoS attacks are massive. In DoS attack, the attacker uses one system to attack the server (One-To-One mapping). DDoS is implemented with several compromised systems which are useful to send malicious traffic to the target server (Many-To-One mapping). DDoS is the biggest threat of availability in cloud computing.DDoS stands for "Distributed Denial of Service." A DDoS attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.

3.1 Types of DoS Attack:

3.1.1.Smurf Attack:

In this attack, the attacker sends a large number of Internet Control Message Protocol (ICMP) echo requests to the server. The victim server will be flooded with broad cast addresses since the sender IP address is the broad cast IP address.

3.1.2.PING of Death attack:

A ping of death involves sending a malicious ping to a computer. The pin is generally of 32 bytes in size. The attacker sends a packet with a size greater than the limit of the IP protocol 65,535. Handling an oversized packet affects the victim's machine inside the cloud environment and its resources. Many operating systems had problems of what to do when they received an oversized packet, so crashed, or rebooted. Many new variants of ping of death include jolt, sPING, ICMP bug, IceNewk, Ping o' Death.

3.1.3.Buffer overflow Attack:

The attacker sends an executable code to the targeted system in order to create buffer overflow attack . In such way, the victim's machine will be controlled by the attacker. As a result, the attacker can use the infected machine to perform cloud based DDoS attack.

3.1.4.SYN Flood Attack:

The SYN Flood attack happens when the attacker machine sends a flood of TCP/SYN packets with a fake IP address. In a TCP/IP handshaking process, each of these packets is treated like connection request. So the server sends back a TCP/SYN_ACK packet and waits for a packet in response from the sender IP address. Since the sender IP is a fake, the response to the ACK packet never comes. As a result, it causes to half-open connections. These half-open connections saturate the number of connections to the server so that it avoids responding to the legitimate requests.

3.1.5.IP Spoofing attack:

Internet Protocol (IP) spoofing attack occurs when the attacker modifies the headers of source IP field either by a legitimate IP address or by an unreachable IP address. When this happens, the cloud server will be misguided to the legitimate client and in turn it affects the genuine user or the server will be unable to complete the task to the unreachable IP address, which affects server resources. Preventing this type of attack is difficult due to the fake IP address of the source IP.

4. COUNTER MEASURES OF DDOS ATTACK:

4.1.Two Tier CAPTCHA

The Captcha shows alphanumeric images and it also display some query user has to type the valid code according to the query.Use of this two tier captcha ,it is not easy identify the pattern because the system using random queries so it is not easy task to identify the input for the computer.It contains random queries so very difficult to hack user system.method has been developed to distinguish human users and computer programs from each other by the same fact that human user have to provide a data after solving the query associated with CAPTCHA. The query must be very difficult for computers to solve and relatively easy for humans.

Ex: 1. Please provide only digit's shows in image.

2. Please provide the counting number of character shown in image.

Fig:2 Two Tier Captcha

4.2.Network Egress and Ingress Filtering

NEIF installed at the ISP's edge router and plays as a dual role in shielding DDoS attacks. As a first role, the goal of ingress filtering is to discover and prevent the ddos attacks launched from its customer.Ingress filtering is process of discarding the unwanted packets which is being send to the victim.Ingress filtering can ensure an ISP's network do not participate in flooding DDoS attacks.Ingress filtering is the filtering of any IP packets with untrusted source addresses before they enter and affect the system.Egress filtering is used to protect ISP's customers from being attacked.Network filtering can operate either on traffic aggregates or on individual flows.Egress filtering is user to filter the networks outbound traffic.The traffic can be filtered by routers and firewalls but these strategies will leave the DDoS. Egress filtering can be able to detect and prevent DDoS attacks.Egress filtering is used to monitor and potentially restricting the flow of information outbound from one network to another.The egress filtering is used to prevent packets with invalid or incorrect address leaving from the system.

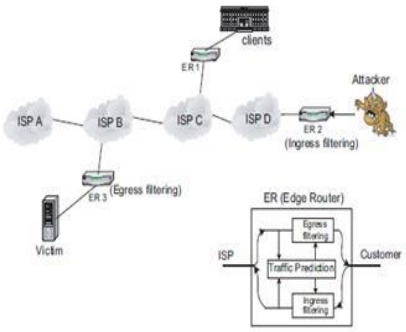

Fig:3 Egress and ingress filter

4.3.Time Based Port Hopping

The port hopping mechanism used to detect the DoS/DDoS flooding Attack.The proposed system is to change the server's port numbers dynamically as a function of time In this scheme, time is divided into discrete slots Si, where i={0,1,2..},each of duration T. The port number is unchanged for a specific communication session.In this mechanism, different port numbers are used in different time slots for the same service.Pi->Port number Si->server in time k-> cryptographic key between the server and the client and f->pseudo-random number generator. Pi=f(i, k).When a client needs to communicate with the server, it will determine the server's current port number **Pi** using the shared secret key **k** and the time slot number **i**. When the server receives packets that carry "invalid" port numbers, they can be easily detected and filtered off .The server does not monitor the contents of the packet and no need to determine the packet is malicious.

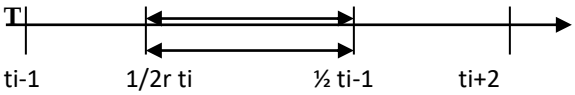

Fig:4 Time based port hopping

The packet transmission may takes place near the boundary of time slots.There occurs synchronization errors between the server and client, the two ports are used at the boundaries of time slot. L->overlapping time factor. This parameter deals with two issues sync error and transmission delay between the server and client.Let *ti* be the start of time slot *i* and *Pi* the associated port number. Then *Pi* is defined to be valid from time ($ti - l/2\ \tau$) to ($ti+1+ l/2\ \tau$) (see the above figure(e)).If L=0,a port number is valid with in a specific slot. The major issue in this system, If attacker knows about this scheme, they can give request by giving random port numbers so many packets may contain correct port number. Hence there occurs DoS. The higher probability that the attacker will be able to guess the correct port number.

Solutions	Features And Advantages	Downside
Two Tier Captcha [5]	This application works as the user has to type the valid captcha based on the query which been displayed. The application will block the attacker at the authentication phase	If there is a complex queries very difficult to answer for the user. Producing random queries is a difficult task.
Egress and Ingress Filtering [6]	Ingress filter block the unwanted packets which is been sent to the victim system. Engress filter never allows the networks outbound traffic .	This techniques are overhead and complexity.
Port Hopping [7]	This method works between client and the server it produces random number of keys which provide different port number to the client.	The attacker will be able to guess the port number by giving random port request to the server.

Table 1: Comparison of Counter measures for DDoS attack

5. CONCLUSION

The aim of this paper is to produce the appropriate solution for the DDoS attack in Cloud Computing environment. A deep study has been made, this paper compares the various work of the researchers and throws the light on the downside. In this research paper we recommend "The two-tier CAPTCHA" as the best solution as it blocks the attacker at the authentication phase and prevent the attacket to access the user system or server.

REFERENCES

[1]https://en.wikipedia.org/wiki/Cloud_computing
[2]https://en.wikipedia.org/wiki/Cloud_computing_security
[3]https://www.fortinet.com/solutions/enterprise-midsize-business/cloud-security.html
[4]https://en.wikipedia.org/wiki/DOS
[5] Poonam Yadav and Sujata, " Security issues in cloud computing solution of DDOS and Introducing Two-Tier CAPTCHA ", International journal on cloud services and cloud architecture(IJCCSA) ,Vol-3, No-3, June-2013, PP: 12
[6] Prince Gupta(Prof), Jayant Shekhar
“Analysis Of DDOS Attacks And Solutions For Cloud Computing Environment.”, International Journal of Research Review In Engineering Science and Technology(IJRREST) Vol-4,Issue-1,April-2015, PP: 4
[7] T.Siva and E.S.Phalguna Krishna.
“Controlling Various Network Based ADOS Attacks In Cloud Computing Environment: By Using Port Hopping Technique”, International Journal of Research Review In Engineering Science and Technology(IJRREST) Vol-4,Issue-1,April-2015.
[8]http://whatis.techtarget.com/definition/ingress-filtering. [9]http://whatis.techtarget.com/definition/egress-filtering.
[10]http://www.dummies.com/programming/networking/cisco/network-firewalls-ingress-and-egress-filtering/
[11] Nagaraju kilari and Dr. R. Sridaran
“An Overview Of DDOS Attaks In Cloud Environment”, International Journal Of Advanced Networking Applicatoins(JIANA)
ISSN No: 0975-0290