A Prevention of DDoS Attack in Cloud Computing

[1] Hetal.N.Joshi, [2] Priyanka Sharma
[1] Student M.Tech(Cyber Security), [2] Professor (IT)
[1,2]Department of Information Technology
[1,2]RakshaShakti University, Gujarat-Ahmedabad, India.

ABSTRACT

Cloud computing is one of the emerging technologies in which a huge amount of storage, data and services are available over the internet. The main advantage of cloud computing environment is the users have to pay only for what they use. Cloud services are distributed in nature so they can be sharable by millions of users [1]. Because of this, the cloud environment has numerous security challenges. Distributed Denial of Service (DDoS) is most prominent security attack in cloud computing. DDOS is the largest threat which can impact on the availability of cloud services since it has multi-tenant architecture. This paper highlights various DDoS attacks and its countermeasures [3].

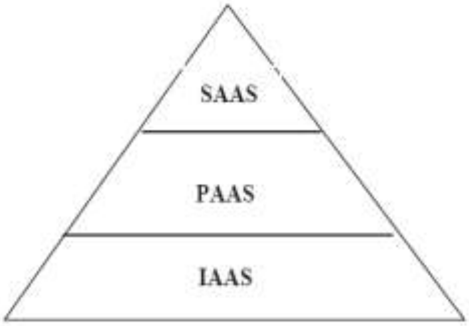
Keywords - Cloud computing, Cloud models, DDoS attacks, network, security, Factors, Ddos Threats, Vulnerabilities, flooding, counter methods,

INTRODUCTION

Cloud computing is evolved from various existing technologies like Grid computing, Utility computing and service oriented architectures. With the use of cloud, many companies can scale up without having to invest large amount in new infrastructure, software license and building large data centers [10].

Cloud computing is very useful to make use of hardware, software and to provide services to end users. A cloud computing structure depends on three main services: Infrastructure as a service (IAAS), Software as a service (SAAS) and Platform as a service (PAAS) as shown in figure [6]:

Fig: 1



IAAS allows users to access physical resources such as networks and storage, while PAAS provides access to the various platforms and operating system. SAAS enables the users to access software application [4].

The architectural design of cloud computing provides number of benefits to the users and at the same time it also imposes challenges like security, performance, data integrity and cost etc. Out of these, security is the major concern for a cloud. One of these security challenges is how to handle with DDoS attacks which is a key factor for the reputation of any company. DDoS attack is a major threat since the main characteristic of cloud is resource sharing at host level, browser level, network level and server level [8].

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). The two main objectives of DDoS attacks are to overwhelm the server resources (CPU time, Network bandwidth) so that the genuine users are cannot access the Server and second objective is to hide the identity of malicious users (attackers) [5].

LITRACURE REVIEW

This section will investigate Denial of Service attacks. It will show the history of these attacks and current evolvements, starting from the simple “ping–of–death” packet and leading towards amplification attacks. It will evaluate the current research in this area and examine the gaps in literature. This section will be mostly focused on the theory behind DoS attacks, detection methods and mitigation techniques; however some commonly used hacker tools will also be described. In addition to this, the section will describe the indications of the new DoS amplification attack and the several metrics used in the literature to evaluate Denial of Service attacks. When computers were first created, there were very little concerns regarding their security. The key focus was to protect them against physical damage. This then evolved to a situation where computers and computer networks were mostly used by academics and large companies (Leiner et al., 1997). There was little need for security as everything was considered to be one large experiment. Security concerns started after several incidents occurred. One of the most famous incident includes the computer software Creeper (Szor, 2005), created by Bob Thomas, which is considered to be the first computer virus. Creeper was taking large amounts of computer resources from the DEC PDP–10 systems, which resulted in a need to remove this software. The solution came from the same author, which was called Reaper and this was the first known anti–virus (Szor, 2005). This and other incidents led engineers and administrators to think about secure design of their systems and measures that would mitigate these security risks. Nowadays, internet connections are present everywhere thus threats towards computer services have increased rapidly. One of the most growing IT security threats are Denial of Service attacks. Some claim that 30% of all hacker attacks in 2012 are Denial of Service attacks (Passeri, 2012).

Factors affecting DDoS attack

One of the main reasons that make the DDOS attacks widespread and easy in the cloud is the availability of attacking tools and the powerfulness of these tools to generate huge volumes of attacking traffic. The following are the opportunities for the attackers to use attack tools easily to launch attack [9]:

1. **Internet security is highly interdependent**
   The launch of DDoS attack depends upon the global internet security [7].

2. **Limited Internet resources**
   Each Internet host has limited resources that can be consumed by a sufficient number of users [4].

3. **Control is distributed**
   Due to privacy concerns of the Internet, sometimes it is nearly impossible to investigate the cross network behavior and to deploy certain global security mechanism [10].

4. **Multipath routing**
   This causes authentication process difficult and hence it may leads to unauthorized activities. Intermediate router forwards IP packet from source to destination without knowledge about the IP packet whether it is genuine or not [12].

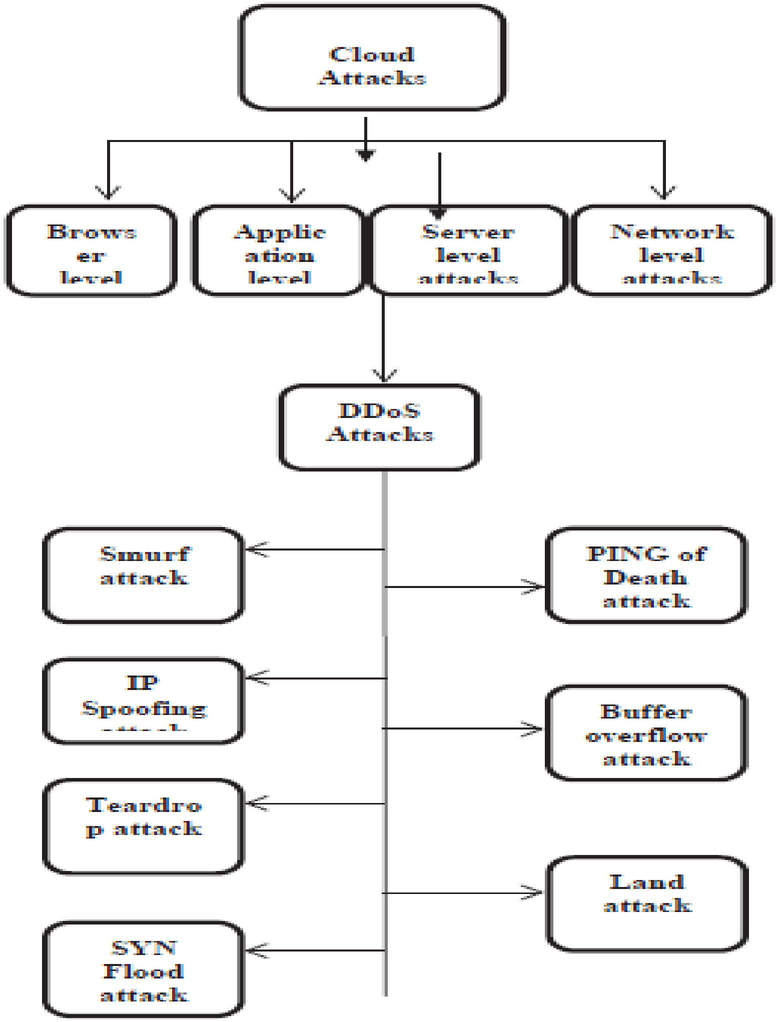
DDoS as the Main Threats to Cloud Computing

DDOS attack is a large scale coordinated attack on the availability of service of a target system or network bandwidth. There are various DDoS attacks to disrupt the cloud services. Among these attacks, ICMP (ping) flood where the attackers consumes bandwidth that use ICMP packets, ping of death attack in which the attackers sends multiple malicious pings to a cloud resources (servers), HTTP GET Flood, attackers send huge flood of requests to the cloud servers and consume all the resources and the smurf attack where the attackers use ICMP echo request packet to generate the denial of service attack [7].

In a DDoS attack, the attackers attempt to temporarily interrupt or suspend the services of a website so that it is unavailable to the users. Akamai’s Fourth Quarter, 2012 State of the Internet Report has stated that a total of 768 DDoS attacks were reported in 2012. Over a third (269 or 35%) of the attacks targeted companies in the Commerce sector, 164 attacks (22%) targeted Media and Entertainment companies, 155 attacks (20%) targeted Enterprise companies that include financial services, 110 attacks (14%) targeted High Tech companies, and 70 attacks (9%) targeted Public Sector agencies [3].

On February 9, 2000 major DDoS attacks were waged against Yahoo.com, eBay, Amazon, E*Trade, ZDnet, Buy.com FBI and several other websites fell victim to DDoS attacks resulting in substantial damage and inconvenience.

In 2004, series of DDoS attacks against variety of companies providing anti-spam services. These attacks caused companies to shut down their services. These attacks have cost targeted companies or organizations losses in revenues, customer satisfaction and brand equity. Figure 2 shows various DDoS attacks in cloud environment [9].



DDoS attack includes different types of attacks. Descriptions of those attacks in the cloud system are presented in the following sections [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 [4].

The Smurf attack is caused by following steps:

1. Attacker sends packets to a network device that supports broadcast addressing technique e.g. Network amplifier. The return address in these packets are forged or spoofed with victim's address [4].

2. ICMP_ECHO_RESPONSE packets are sent by the network amplifier to all the systems in the broadcast IP address range. 3. An ICMP_ECHO_REPLY message from all the systems in the range reaches the victim [5].

(2) 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 [10].

(3) Teardrop attack

In a network transmission, IP packets are broken down into smaller chunks and each fragment will have the original IP packet's header that will be useful to re assemble at the destination host. When the TCP/IP stack is overlapped with IP fragments, the re assembling will be a very difficult and sometimes it can quickly fail. To avoid this attack, most of networks use firewalls which can block tear drop packets in return since this makes it disregard all broken packets. Of course, if you throw a ton of Teardrop busted packets at a system, it can still crash many other variants such as Targa, SynDrop, Boink, Nestea Bonk, TearDrop2 and NewTearare available to accomplish this kind of attack [7].

(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 [9].

(5) PING of Death attack

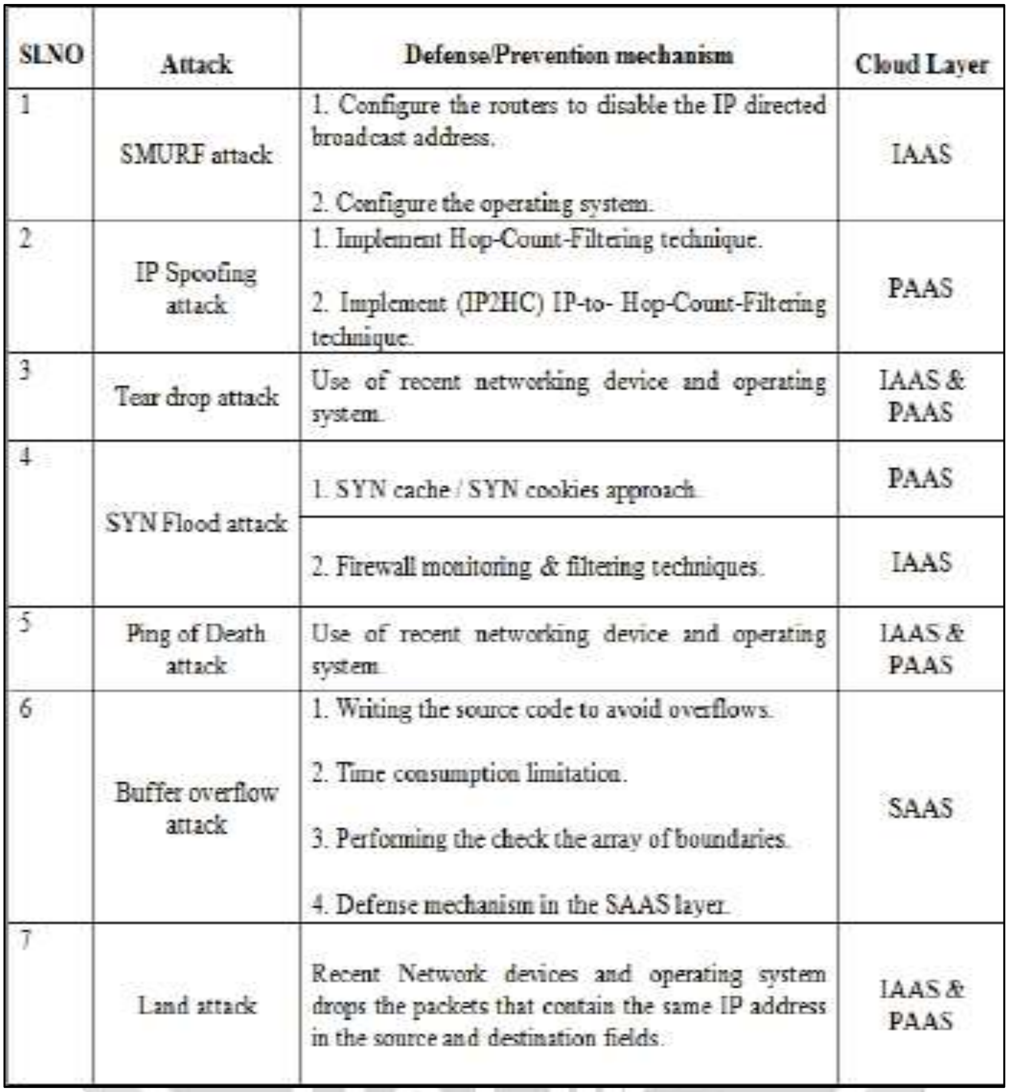
A ping of death involves sending a malicious ping to a computer. The pin is generally of 32 bytes in size. The attacker sends a packet with a size greater than the limit of the IP protocol 65,535. Handling an oversized packet affects the victim's machine inside the cloud environment and its resources. 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 [13].

(6) 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 [12].

(7) LAND attack

It is similar to ping attack where it uses “land.c” program to send the modified TCP/SYN packets with the victim's IP address in both source and destination IP fields [2]. As a result, the machine itself sends the requests and crashes. DDoS attacks are highly distributed, offensive assaults on services, hosts and infrastructure of the Internet. The following table shows the effective mitigation/ defense countermeasures to various DDoS attacks [11].



SLNO	Attack	Defense/Prevention mechanism	Cloud Layer
1	SMURF attack	1. Configure the routers to disable the IP directed broadcast address. 2. Configure the operating system.	IAAS
2	IP Spoofing attack	1. Implement Hop-Count-Filtering technique. 2. Implement (IP2HC) IP-to- Hop-Count-Filtering technique.	PAAS
3	Tear drop attack	Use of recent networking device and operating system.	IAAS & PAAS
4	SYN Flood attack	1. SYN cache / SYN cookies approach.	PAAS
		2. Firewall monitoring & filtering techniques.	IAAS
5	Ping of Death attack	Use of recent networking device and operating system.	IAAS & PAAS
6	Buffer overflow attack	1. Writing the source code to avoid overflows. 2. Time consumption limitation. 3. Performing the check the array of boundaries. 4. Defense mechanism in the SAAS layer.	SAAS
7	Land attack	Recent Network devices and operating system drops the packets that contain the same IP address in the source and destination fields.	IAAS & PAAS

CONCLUSION

DDoS attacks are major threats against the availability of cloud services. Defense/prevention mechanisms to protect against DDoS attacks are not always effective on their own. Combining different mechanisms (load balancing, throttling and Honey pots) to build hybrid defense mechanisms, in particular with different cloud computing layers, is highly recommended. In this paper, various DDoS attacks have been presented. We also highlighted the defense mechanism to counter attack different types DDoS attacks in the cloud environment.

REFERENCES

[1] J. Nazario, “DDoS attack evolution,” Network Security, vol. 2008, no. 7, pp. 7–10, 2008.

[2] P. G. Neumann, “Inside Risks: denial-of-service attacks,” Commun. ACM, vol. 43, no. 4, p. 136, Apr. 2000.

[3] D. Dittrich, J. Mirkovic, P. Reiher, and S. Dietrich, Internet Denial of Service: Attack and Defense Mechanisms. Pearson Education, 2004.

[4] C. M. Patel and V. H. Borisagar, “Survey On Taxonomy Of Ddos Attacks With Impact And Mitigation Techniques,” International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 9, pp. 1–8, 2012.

[5] H. Wang, C. Jin, and K. G. Shin, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering,” IEEE/ACM Transactions on Networking, vol. 15, no. 1, pp. 40–53, Feb. 2007.

[6] J. M. Gonzalez, M. Anwar, and J. B. D. Joshi, “A trust-based approach against IP-spoofing attacks,” 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 63–70, Jul. 2011.

[7] M. Kumar, A. Panwar, and A. Jain, “An Analysis of TCP SYN Flooding Attack and Defense Mechanism,” International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 5, pp. 1–6, 2012.

[8] J. Lemon, “Resisting SYN flood DoS attacks with a SYN cache,” in Proceedings of the BSD Conference 2002 on BSD Conference, 2002, p. 10.

[9] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, “Analysis of a denial of service attack on TCP,” Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097), pp. 208–223, 1997.

[10] D. Fu and F. Shi, “Buffer Overflow Exploit and Defensive Techniques,” 2012 Fourth International Conference on Multimedia Information Networking and Security, pp. 87–90, Nov. 2012.

[11] L. F. Capretz and F. Ahmed, “Why do we need personality diversity in software engineering?,” ACM SIGSOFT Software Engineering Notes, vol. 35, no. 2, pp. 1–11, Mar. 2010.

[12] A. Keshariya and N. Foukia, “DDoS Defense Mechanisms: A New Taxonomy,” in Data Privacy Management and Autonomous Spontaneous Security SE - 17, vol. 5939, J. Garcia-Alfaro, G. Navarro- Arribas, N. Cuppens-Boulahia, and Y. Roudier, Eds. Springer Berlin Heidelberg, 2010, pp. 222–236.

[13] S. M. Specht and R. B. Lee, “Distributed denial of service Taxonomies of attacks, tools, and countermeasures,” in Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004, pp. 543–550.