DDOS ATTACKS IN CLOUD: A SURVEY

C.Vinothini[1], P.Balasubramanie[2]
[1]Department of Computer Science & Engineering,
Dr.N.G.P Institute of technology, Coimbatore, India,
[2]Department of Computer Science & Engineering, Kongu Engineering College, Perundurai, India

Abstract

In today’s world, the internet is an essential one to access all the applications which are needed to use by the end users. Cloud computing is a mounting technology in the global since it is consuming less resources and high throughput. There is no need of additional knowledge, control and ownership to the users in the cloud environment. The user can access anything in the cloud from anywhere in the world through rental basis. Even though it is very fast to access, store and provide services to any end users, but still it has remained untouched to the attackers. Constantly, users of cloud services are in the fear of data loss and security challenges. The main dispute which is notified as DDOS attacks. A distributed denial of service (DDOS) attack is an attack which is performed by the malicious program from the attacker to the compromised machines called zombies to make a server or a network resource unavailable to users. This paper underlying a clear review on the cloud computing concepts as well as security issues inherent with DDOS attacks and its types.

Keywords: Cloud computing, DDoS, DDoS attacks.

I. INTRODUCTION

Cloud computing is originated from various accessible technologies like cluster computing, Grid computing, Utility computing and service oriented architectures [1]. In this regard, many companies can provide many services without any investment for infrastructure, software license and building large data centers. Cloud Computing is a combination of all the computing resources and services which is obtainable on the internet. Many eminent companies are available like Amazon, Google, Yahoo, IBM to provide the cloud services for the customers. [2]

Cloud services are user friendly just to satisfy the customer needs. Each users' data is stored in the cloud. Some of the popular services in the cloud are Facebook, Gmail, one drive, Dropbox, google drive. These services can be used by anyone through the proper internet connectivity. But still some difficulties are there for the customer who has to trust on third parties for its sensitive (private) data.

The main concern in the cloud computing is the security and attacks which are happening in the environment when we offered services to the customer needs. There are some security threats which doesn’t target other attributes in the security like integrity or confidentiality but rather only focus on availability. This is called as Denial of services.

Distributed Denial of service (DDoS) is one of the type of DOS attack where the number of compromised systems are injected with any malicious program like Trojan and makes the target victim ‘s to be down or crashed entirely. Fig 1 shows that targeted system of a DDoS attack and all other compromised systems are controlled by the attacker through some commands. DOS attack is totally different from DDoS attacks.

DoS attack, only one computer is considered along with single internet connection to flood the victim‘s system or resources. The computers with this attack are distributed around the world and it is known as a botnet or zombies.[4][7]

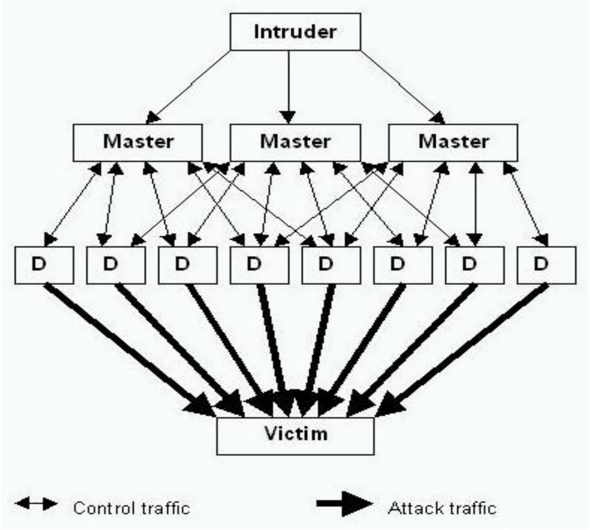

Fig 1: General diagram for DDOS

There are four sections in this paper, In the first section we have discussed the overview of the cloud computing concepts, second section we will be discussing Evolution of DDoS, a third section will be based on the types of the attacks, fourth section describes the conclusion of the attack.

II. EVOLUTION OF DDOS ATTACKS

The Internet is globally-connected network.The internet was designed to work for the user's functionality and not in the focus of security at that time. Theoretically, any computer machines can be connected to the Internet and can access any resources in the online. so DDOS attacks is not limited to single machines or group of individuals in the commercial organizations. The evolution of DDOS attacks should be as follows:

In November 1988, Robert Morris released the worm called Self replicating computer program which later spreads to hundreds of computers through the influence of the internet.It was detected easily due to more consumption of resources.

In 1996, DDOS attack was occurring in which it affected all the commercial institution's operations. Due to this attack, it caused a huge loss.This attack is called as Panic Attack. The attack was happened by a large number of SYN packets were sent from the attackers to make the server to respond to customer requests [9][10].By that time, US community Emergency Response Team Provided essential measures for fake address protection.

In February 2000, Yahoo, Ebay, Dell, CNN and Amazon were affected due to DDOS attack by which servers are overloaded from different types of communications where the systems are shut down completely. Mafiaboy's Rivolta are made the yahoo to be shut down for an hour. TFN2 is a tool for launching distributed attacks and also to control the encryption communication protocols [9][10].

In July 2001, the worm code red occurred. It was self replicating and it could affect the other systems automatically.Initially the target of the attacker is White House Website ((198.137.240.91)) and later it expanded to government websites too.

In october 2002,DDOS attacks on root nameservers which are distributed to target one or more root servers out of thirteen DNS root servers.Due to this threats and attacks, few root name servers are not reachable and many valid queries are unanswered.

In 2003, thousands of PC 's are infected by DDOS and faced the problem to send the data to the target system.From May 2007, Estonian governmental websites and other main websites which including the websites of the presidential palace and the Prime Minister's Office are affected by DDOS attacks.Estonia took the responsible for these attacks and tried to claim for Russia.

From July 2009, American governmental websites and other main websites including the White House, the Pentagon, and the Department of Defenceare affected from DDoS attacks from Zombies. 27 websites were attacked according to the report of statistics. In August 2009, all the social medias like Facebook, Twitter, and YouTube were affected by DDOS attacks.[9][10]

In October 2010, DDOS attack were launched on financial institutions such as Swiss Bank PostFinance and PayPal. .[9][10] In 2012, Bank of America, Citibank, and HSBC, were attacked because of lack of service availabilty.

In March 2013, DNS reflection attack principle was used to launch the traffic attack with the peak traffic rate standing at 300 GbpsIn March 2015, DDoS attacks was suffered in Github. China's largest search engine Baidu was hijacked and used to redirect to Github. .[9][10]Its traffic was fully based on the visitor in the search engine.

In 10th Aug 2015, Hacker used DDoS and stole 2.4 million personal data from Carphone Warehouse, UK.

III. SPECIFIC DDOS ATTACKS ON CLOUD

These are the method which is used for denial of service attacks

Smurf Attacks:

It involves the attacker to send the large amount of Internet control message protocol(ICMP) echo request from spoofed IP address of victim and sent to broadcast address. ICMP responses are forwarded to victim. The victim machine will be busy with broadcast address. Fig 2 shows the general diagram of the smurf attacks to make the target system to be slow down.

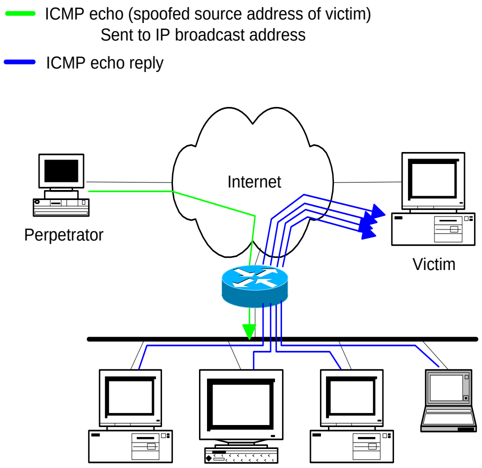
ICMP echo (spoofed source address of victim)
Sent to IP broadcast address
ICMP echo reply
Internet
Perpetrator
Victim

Fig 2 Smurf Attacks

Ping of Death

Ping of death involves sending a malicious ping with the size of 32 bytes. Fig 3 shows it is quite difficult when the attacker tries to send a packet with a size greater than the limit of the IP protocol 65,535. Oversized packet makes the victim machine to be affected because operating system faced the problem of what to do, when an oversized packet received. Many new variants of ping of death include jolt, Sping, ICMP bug, Icenewk, Ping o' Death c address.

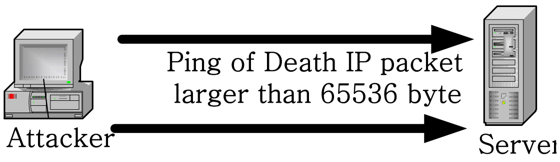

Fig 3 : Ping of Death

Buffer overflow attack

The buffer overflow attack is an attack which is mainly used to disable the network servers. It occurs when a process or program tries to store the data into the buffer. The term buffer means temporary data storage area. Buffer Size should be predetermined so it can store only limited capacity of the data and extra information are to be stored in adjacent buffers or overwriting in the buffer which had already.[7] The buffer overflow attack is a very common type of security attack on data integrity. The extra data may contain executable code which is designed to send new instructions to affect the targeted system.[5]

Syn/TCP Flood

The SYN/TCP Flood is one of the type of DDOS attacks which is exploiting TCP three way handshake to allocate server resources to make the system to be unresponsive. This attack happened when an attacker sends SYN/TCP packets from the spoofing IP address. [11]In normal three way handshake, each TCP packets are treated as connection request. After receiver receives the packet and then send back the ACK packet to the client side and waits for the response. But in SYN flood, malicious client never sent back ACK packets.[7] As an alternative client program sends the multiple SYN requests to all the server ports. The server will down when request in the queue is overloaded. It is also known as half open attacks. Fig 4 shows the attacker sends the SYN packets from a fake IP address.[6]

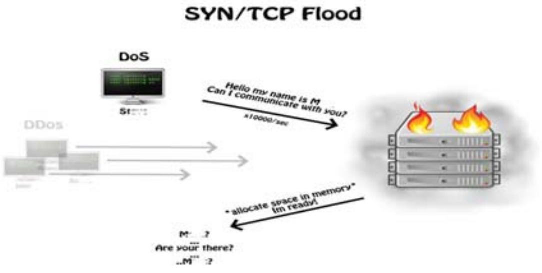

Fig 4: SYN/TCP flood

UDP Flood

Normally, UDP is a connectionless network protocol in which the data and requests are allowed to send to a server without a need of acknowledgement or response. An attacker sends a large number of UDP packets with a fake IP address to the random ports on the targeted system to launch the UDP flood. This attack consumes the network resources, available bandwidth , draining the network and no longer respond to legitimate user. Fig 5 illustrates the UDP Flood Attacks by sending the UDP packets to the spoofed IP address to the destination ports

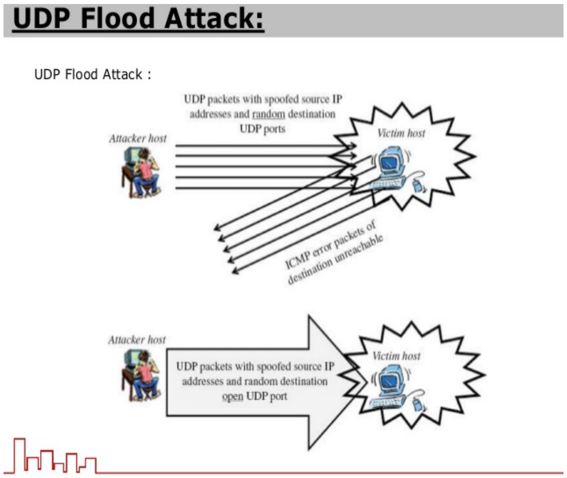
UDP Flood Attack:
UDP Flood Attack :
UDP packets with spoofed source IP addresses and random destination UDP ports
Attacker host
Victim host
ICMP error packets of destination unreachable
Attacker host
UDP packets with spoofed source IP addresses and random destination open UDP port
Victim host

Fig 5: UDP Flood Attack

DNS Amplification Attacks

DNS amplification attacks are organized when the attacker instructs bots to send DNS queries with a spoofed IP address to a server. This Attack is happened by using thousands of DNS servers can direct gigabits of data per second to against the target system when the actual bots are used to invisible the victim. Fig 6 illustrates the amplified DNS Response from the spoofed IP Address request.

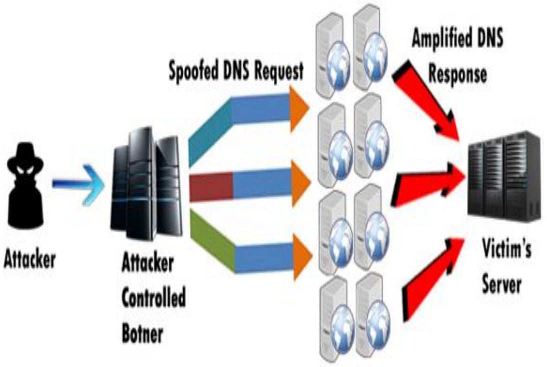

Fig 6 DNS Amplification Attacks

Teardrop attack

A teardrop attack is a denial of service attack that involves to sending the fragment packets to a target machine. The target machine receiving the packets, but can't reassemble the code due to a bug in the fragmentation and also it can overlap each other and crashing the victim machine. This generally happens in the older operating systems like Windows 95, Windows 3.1 x ,Windows NT.

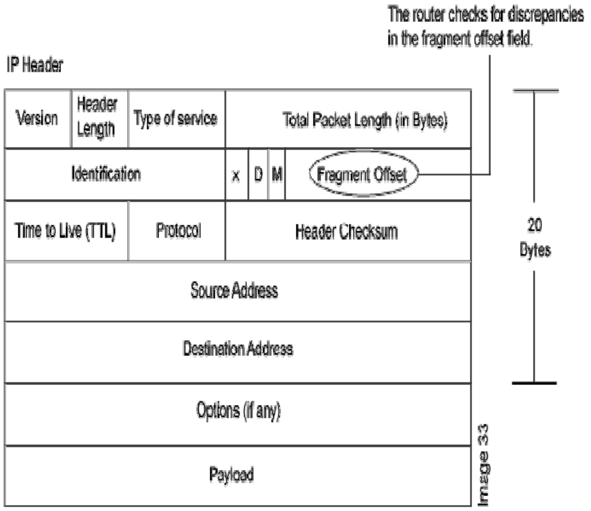

Fig 7 Teardrop Attack Example

Above fig 7 illustrates the IP header which operates the network layer . IP header, there is a field called fragment offset which indicates the starting position and the data contained in the fragmented Packet relative to the data in the original packet. If offset value and size of one fragmented packets differs then packets overlap. When this happens, a server is unable to reassemble the packets which lead to DDOS Condition.

IV. CONCLUSION

Cloud computing is an emerging technology in the industry since it provides elasticity and demand resource provisioning. Therefore the DDOS attack is major threat based on the availability of the services.[3] DDOS attack is launched at a specific well organized, distributed zombies and remotely controlled computers are sending huge amount of traffic to the victim.The attacker finally gets the target system to be down or crashes completely because of some malicious program like Trojan, worms, or backdoor's.[4] DDOS security efforts initially are not sufficient to tackle the situations. The main significance of this paper to be surveyed general concepts of cloud and also a clear review of the specific DDOS attacks

REFERENCES

[1] Madarapu Naresh Kumar, P Sujatha, Vamshi Kalva, Rohit Nagori, Anil Kumar Katukojwala and Mukesh kumar: Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing using In-Cloud Scrubber Service, 2012 Fourth International Conference on

Computational Intelligence and Communication Networks

[2]"Luit Infotech: What is Cloud Computing", Download,pp1http://www.luitinfotech.com/kc/ what-is-cloud-computing.pdf (accessed in Feb 2013)

[3]Sara Qaisar, "Cloud Compuitng: Network Security Threats And Countermeasures"Interdisciplinary Journal of Contemporary Research In Bussiness, Vol 3, No 9,pp-1323-1329, January 2012.

[4] Bansidhar Joshi, A. SanthanaVijayan and Bineet Kumar Joshi: Securing Cloud Computing Environment against DDoS Attacks (ICCCI-2012) Jan10-12, 2012.

[5] Chandini M Patel and Viral H Borisagar: Survey on taxonomy of DDoS attacks with impact and mitigation techniques, IJERT, ISSN: 2278-0181, Vo. 1Issue 9, NOV2012.

[6] AnLei and Zhu Youchan: The Solution of DDOS attack based on Multi-agent, 978-1-4244-803571101$26.00 © 2010 IEEE.

[7]Nagaraju kilari and Dr. R. Sridaran: An Overview of DDoS Attacks in Cloud Environment, ISSN No. : 0975-0290

[8]A.M. Lonea, D.E. Popescu, H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment, International Journal of Computing and communication , ISSN 1841-9836 8(1):70-78, February, 2013.

[9]http://www.cybersecurity.my/data/content_files/13/72.pdf

[10]https://nsfocusglobal.com/how-ddos-attacks-have-evolved-in-the-last-two-dec

[11]S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mosse, and T. Znati, "Proactive Server Roaming for Mitigating Denial-of-Service Attacks," in Proceedings of the 1st International Conference on International Technology: Research and Education (ITRE'03), pp. 286-290, Aug. 2003

[12]Internet World Stats, Internet User Statistics – The Big Picture: World Internet Users and Population Stats, http://www.internetworldstats.com/stats.html

[13] Bansidhar Joshi,A. Santhana Vijayan,Bineet Kumar Joshi, "Securing Cloud Computing Environment Against DDoS Attacks, International Conference on Computer ,Communication and informatics, Jan 212,2012,Coimbatore,India.

[14] Navdeep Singh, Abhinav Hans, Kapil Kumar and Mohit Pal Singh Birdi ,"Comprehensive Study of Various Techniques for Detecting DDoS Attacks in Cloud Environment" Vol. 8, No. 3, (2015), pp.119-126