International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 4 Issue 12, December-2015

Distributed Denial of Service (DDOS) Attacks in Cloud Computing: A Survey

Neha Gupta[1], Rajet Veshin[2], Rajneesh Sharma[3]

[1,2,3]Department of Information Technology, Model Institute of Engineering and Technology, Jammu, J&K, India

ABSTRACT

Cloud computing is the use of computing resources (hardware & software) that delivered as service over internet. For sensitivity or security of data, existing solutions usually apply cryptographic methods by using encryption and decryption keys and giving these keys to only authorized users. But when we apply these methods to real cloud the problem of simultaneously achieving fine-grainedness, scalability and data confidentiality of access control actually still remains unsolved. In the cloud computing, the prevalence and sophistication of DoS and DDoS on the internet are rapidly increasing. Service providers are under mounting pressure to prevent, monitor and mitigate DoS/DDoS attacks directed towards their customers. Attacks that are seen every day on the internet in the cloud computing include Zombie attack, phishing attack, DoS and DDoS attack, man-in-middle attack, service injection attack, metadata spoofing attack. These attacks can cause damage and wide spread out gages when directed at a service provider's infrastructure. The monitoring and mitigation of these attacks is a crucial part of a service providers operation. In this paper we have studied cloud computing, attacks (mainly DDoS attacks) on cloud computing and techniques to cover these attacks. Further we have tried to explain the pros and cons of different techniques and its impact on real world cloud.

Keywords: **Security, legitimate, mitigation, zombie, overwhelming, network**.

I. INTRODUCTION

In cloud computing, the word cloud represents the metaphor "the internet" and the phrase cloud computing "means a type of internet based computing" where different services such as servers, storage and application are delivered to an organizations, computers and devices through the internet. Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software [1]. National Institute of Standards and Technology NIST [2] defines Cloud computing as a "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction".

The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are the most common but fatal type of attack on cloud service providers (CSPs) which are working hard to prevent, monitor and mitigate these types of attacks as the frequency of these types of attacks have risen sharply in the last few years. DDoS are directed at service provider's infrastructure can be very damaging. In cloud computing, the DoS or DDoS attack is when a machine or network resources unavailable to its intended users. DDoS attacks are sent by two or more persons or bots. DDoS attacks are sent by one person or system. In this paper we have discussed the most common types of DoS/DDoS attacks seen on the internet and ways that service providers can prevent or mitigate damages from the attack threats. The monitoring of DoS/DDoS and black hole filtering became mandatory as entry for service providers to sell the service of internet in the financial industry. The financial industry is easily susceptible to DoS/DDoS attacks as millions of consumers move to electronic bill payments, purchases and On-line banking.

Therefore in this paper we are analyzing and observing the main techniques and further classifying DoS attacks as logic attacks and resource exhaustion flooding attacks. We will evaluate various logic attacks based on their effect on the network infrastructure and critical network services (DNS, BGP, RADIUS etc.) as logic attacks significantly reduce performance causes the server's or network resources to be consumed to the point where the service is no longer responding. We have studied flooding attacks by their amplification factor. The amplification factor is the amount each source packet is multiplied by before reaching the victim. For e.g. – In a direct flooding attack, for each source packet transmitted by the attacker, one packet is received at the victim's site.

In the section II we will analyze the basic functioning of DDoS attacks, further in Section III we analyze various existing techniques to handle DDoS attacks and in Section IV we have put the future work required on DDoS techniques.

II. DISTRIBUTED DENIAL OF SERVICE (DDOS)- OVERVIEW

Direct Flooding Attacks: In the Direct flooding attacks, there is an attacking which transfers one packet directly from his computer to the victim's site. So, it is simplest case of DoS attack. Large number of tools is available to allow these types of attacks for a variety of protocols including ICMP, UDP & TCP. Some examples of common tools are stream 2, synhose, synsend. The amplification factor of Direct Flooding attack is 1 to 1.

Remote Controlled Network Attacks: In these attacks instead of single attacker like direct flooding attacks, there is an attacker that compromising a series of computers and placing an applications or agent on the computers. Out of all these compromising computers, the computers then listen for commands from a central control computer. We can do compromising of computers either by manually or automatically through a worm or virus. The attacker could use the packet header fields to determine what command to run and which IP address to attack. Cdoor.c is a working example of this [3].

Reflective Flooding Attacks: These attacks forge the source address of IP packets with the IP address of the victim's and send them to an intermediate host whenever there is a reply of intermediatehost; it is sent to the victim's destination address, flooding the victim. The amplification factor of Reflective flooding attack can be three to several hundred depending on the type of protocol used andthe application and configuration involved. In these attacks, the flood packets are actually sent from intermediate servers, so it can be difficult to trace the original attacker.

1. **Worms:** We can distinguish worm from virus in the fact that a virus has a need of human intervention to inject a computerwhere a worm does not. Worms can significantly disrupt the normal operation of the internet. Worm propagation technology has advanced significantly in the past several years [4, 5].

2. **Viruses:** Viruses have had a significant impact on network providers. To build a large zombie networks, the viruses are often used. In 1983 and 1984 the original research on viruses has taken place but only much later would they have a significant impact on internet operations. Significant internet viruses include Melessia (1999), Love letter (2000), Nimda(2001-a combination of worm and virus) and so big (2003).

3. **Protocol Violation Attacks:** In the protocol violation attacks, the attacker is sending packets in a manner not originally intended. The attacks which generally use IP protocols that are not valid or are reserved are considered as Protocol Violation Attacks. Protocol 255 is reserved and protocols 135-254 are unassigned according to the internet assigned numbers authority (IANA)[6].

4. **Fragmentation Attacks:** Fragmentation attacks have occurred against check points firewalls, cisco routers and window computers [7].

5. **Network Infrastructures:** The attacks which directed at Network Infrastructure can affect the overall operations of the internet. Mostly, these kinds of attacks can create regional or global network out gages or slowdowns. It sent a warning signal to the root name server's operators to fortify the robustness of their infrastructure [8]. We can classify the traffic on network elements into the data plane, control plane and management plane. When the packets are forwarded from the router to another destination, it considered as data plane. Control plane as the name indicates simply contains the simply routing protocols that allow the new network to function properly. The management plane gives the tools and protocols addresses used to manage the network elements.

Zombies in DoS: Zombies are the types of innocent hosts through which an attacker tries to flood the victim by sending requests with the help of internet.

PROCEDURE (MAKING OF A ZOMBIE IN DOS):

In the cloud, Zombies are innocent hosts the requests for virtual machines (VMs) are accessible by each user through the internet. An attacker can flood a large number of services with the help of zombies. When this attack happens, it interrupts the expected behavior of cloud affecting the availability of cloud services. After having large number of requests, the cloud may be overloaded to serve a number of requests and hence exhausted which can cause Denial of Service (DoS) or Distributed Denial of Service (DDoS) to the servers. The services affected by zombie attack are SaaS, PaaS, IaaS.Denial of service attack against BitBucket.org, a code hosting site, caused an outage of over 19 hours of downtime during an apparent denial of service attack on the Amazon Cloud infrastructure [9].Usually, zombies the innocent hosts are taken over by exploiting program bugs left by the programmers. After takeover of a zombie, its intrusion done by sending harmless looking code or data which contains malicious codeSuch as Trojan horse to the

vulnerable candidate. When host is taken over and made a zombie, the harmless looking code or data which contains hidden malicious code will run as background process that performs the actual attack.
(The problem of DoS will become worse as more home systems come online and remain connected on cable modems).

Effects of zombie:

1) It affects service availability.

2) May create an account for false service usage.

III. TECHNIQUES TO PREVENT DDOS

We can have two types of techniques (general techniques and filtering techniques) to present DDoS. We can see in Figure 1 the total number of DDoS defending techniques used in cloud computing. Since each virtual machine may or may not use same or different type of filtering techniques as each datacenter in cloud consists of different virtual machines of different configuration.

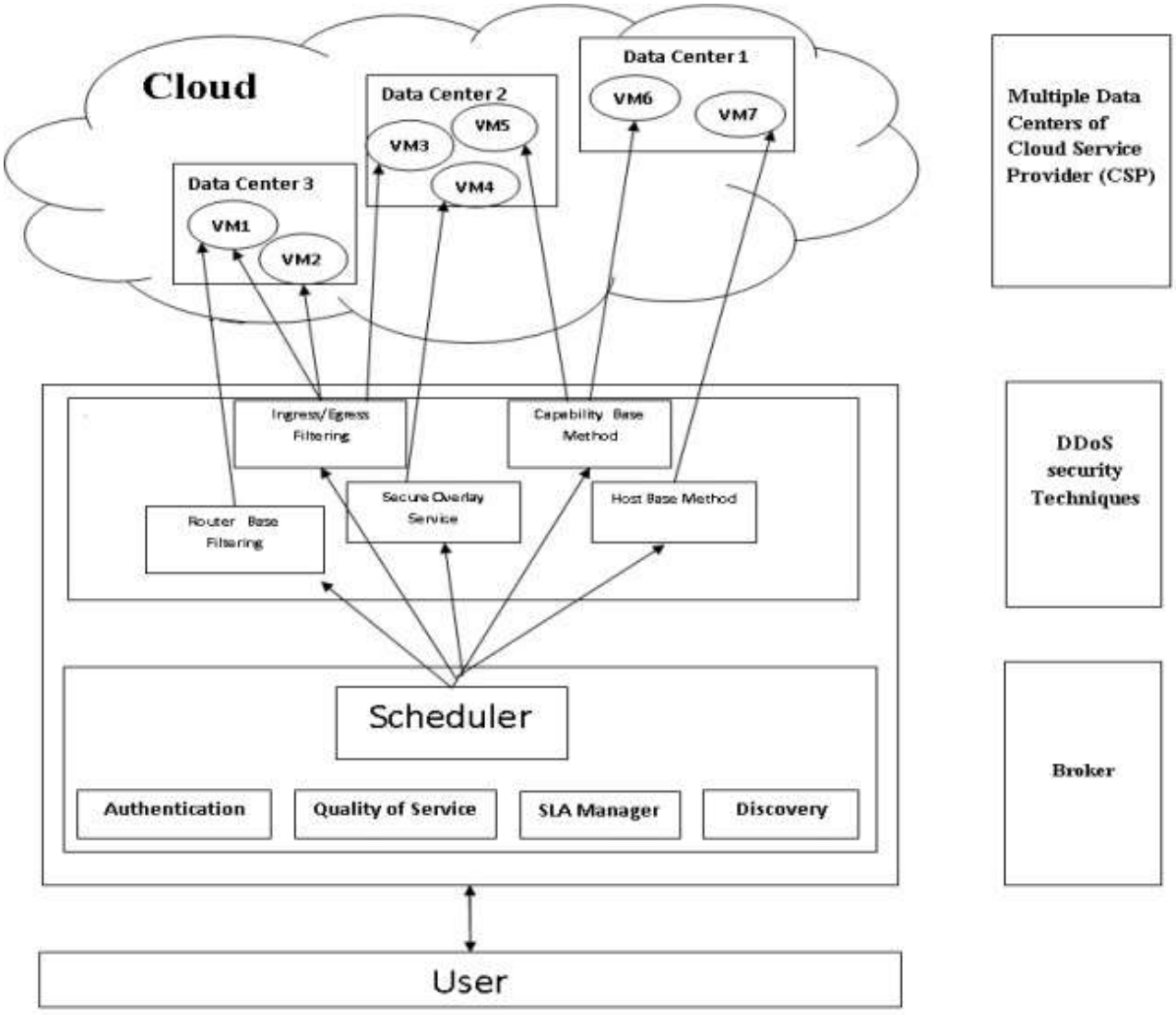

Figure 1: Schematic view of DDOS preventive techniques

In table 1 we have summarized the various techniques used for DDOS prevention

Table 1: DDOS Prevention Technique

General	
Disabling unused service	[10]
Install latest security patches	[10]
Disabling IP broadcast	[11]
Firewalls	[12,13]
Global defense architecture	[10]
IP Hopping	[10]
Filtering Techniques	
Ingress/Egress Filtering	[14,15]
Router based Filtering	[16]
History based Filtering	[17]
Capability based Method	[18]
Secure Overlay Service	[19]

General Techniques: These are some common preventive measures [10] i.e. system protection, replication should follow so they do not become part of DDoS attack.

1. **Disabling unused services**: In this technique, we just disable the unused services. If we have less applications and open ports in hosts, then there is less chance to exploit vulnerability by attackers. Therefore, there are network services which are not required or totally unused services we can prevent DDoS attacks. E.g. UDP echo, character generation services [10].

2. **Install latest security patches**: At present, there are so many DDoS attacks which exploit vulnerabilities in target system. We can prevent the re-exploitation of vulnerabilities in the target system by removing the known security holes by installing all the relevant latest security patches [10].

3. **Disabling IP Broadcast**: The Disabling IP Broadcast technique is useful to defense attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks will be successful only if host computers and all the neighboring networks disable IP broadcast [11].

4. **Firewalls**: The technique of firewalls can prevent users by launching simple flooding type attacks from machines behind the firewall. Firewalls are simply used to allow or deny protocols, ports or IP addresses. Firewalls can't prevent some complex attack because they can't distinguish good traffic from DoS attack traffic [12, 13].

5. **Global Defense Infrastructure**: We can prevent global deployable defense infrastructure can prevent from many DDoSattacks by installing filtering rules in the routers of the internet, such type of global defense architecture is possible only in theory because the internet is administered by various autonomous system[10].

6. **IP hopping**: If we change the location or IP address of the active server proactively within a pool of homogenous servers, we can prevent DDoS attack. We can invalidate the IP address of victim's computer by changing it with a new one. If the IP addresses change is completed, it will be informed to all internet routers and edge routers will drop the attacking packets. We can make computer vulnerable by using this action because the attacker can launch the attack at the new IP addresses[10]. On the other hand, if we add domain name service tracing function to the DDoS attack tools, this technique will become useless.

Filtering Techniques: It includes ingress filtering, egress filtering router based packet filtering, history based IP filtering, SAVE protocol etc.

1. **Ingress/Egress filtering**: It was proposed by Ferguson et al. [14]. Ingress filtering is a type of restrictive mechanism which is used to drop traffic, if addresses that do not match a domain prefix connected to the ingress router. Egress filtering ensures that only assigned or allocated IP address space leaves the network. The knowledge of expected IP addresses at a particular port is a key requirement for Ingress\Egress filtering. We can build this knowledge by using the technique known as reverse path filtering [15]. This technique works as follows. Generally, a router always knows the reachability of networks via any of its interfaces. It is possible to check whether the return path to that address would flow out the same interfaces as the packet arrived upon, by looking up source addresses of the incoming traffic. If they do, these packets are allowed otherwise they are dropped.

2. **Router based filtering**: This technique of filtering was proposed by Park & Lee [16]. It is based on the principle that there is only a limited set of source addresses for each link is the core of the internet from which traffic on the link could have originated. It is the extension of ingress filtering and for filtering out spoofed IP packets, there is a usage of route information. It is assumed that the source address has been spoofed, if an unexpected source address appears in an IP packet, so the packet should be filter. In RPF whenever we have to filter traffic with spoofed source addresses, we have to use information about the BGP routing technology. The result of simulation shows us that only a significant fraction of spoofed IP addresses can be filtered, if RPF is implemented in at least 18% of Ass in the internet because of this we have limitations in this scheme. The main limitation relates to the implementation of RPF in practice. The second limitation is that RPF may drop legitimate packets if there has recently been a route change. The third limitation is that RPF relies on valid messages to configure the filter.
3. **History based filtering**: Normally, in the normal operation the set of source IP addresses which we see tends to remain stable. In DoS attacks, most of source IP addresses have not been source before. Peng et al. relies on the above idea and use IP address database (IAD) to keep frequent source IP addresses. We will have to drop the packet, if the source address of a packet is not in IAD, during an attack. For the searching of IP in IAD, the hash based/Bloom filter techniques are used. This scheme does not need the cooperation of the whole internet community; hence scheme is robust [17]. When the attacks come from real IP addresses, this history based packet filtering scheme becomes ineffective. To keep track of IP addresses, it requires an offline database. Therefore, cost of storage and information sharing is very high.
4. **Capability based method**: Whenever we have to control the traffic directed towards itself, capability based mechanisms are used which provides destination. Firstly router sends request packets to its destination. Router marks are added to request packet while passing through the router. There is no need for destination to grant permission from the source to send. If permission is granted then destination returns the capabilities, if not then it doesn't supply the capabilities in the returned packet. In the last, this technique helps us to control the traffic according to its own policy. Thereby reducing the chances of DDoS attack, as packets without capabilities are treated as legacy and dropped at the router when congestion happens [18].
5. **Secure overlay Service (SoS):** It was proposed by Keromytis et al. [19] defines an architecture called Secure Secure overlay Service (SoS) to secure the communication between the confirmed users and Secure victim. Secure overlay Access Point (SoAP) is used to verify all the traffic from a source point. SoS addresses the problemof how to guarantee the communication between legitimate users and a victim during DoS attacks. The power of SoS is based on the number of distribution level of SoAPS.

In table 2 we can compare and see the benefits/limitations of various filtering techniques

Table 2.

Types of techniques	**Benefits**	**Limitations**
Ingress/Egress Filtering	Works efficiently by preventing IP spoofing.	Requirement of global development.
Router based Filtering	Usage of static routing.	Cannot work properly with dynamic routing.
History based Filtering	It works according to priority in case of any congestion or attack. It can work properly without the co-operation of whole internet community.	If the attack takes place from real IP addresses, this technique will become ineffective. Fully works according to the information collected.
Capability based method	Whenever there is congestion, it provides a way or destination to control the traffic.	It is quite complex for high computations.
Secure overlay service	For predefined source nodes, it works well for communication.	It is not applicable to web servers. Requirement of new routing protocols .

CONCLUSION AND FUTURE WORK

With the evolution of cloud computing all the service providers in the industry are moving towards cloud for its elasticity and on demand resource provisioning. However DDoS attack on these services is creating a panic and traditional security efforts are not sufficient enough to tackle the situations. In this paper we discussed various techniques to undertake security measures and observed that each technique has its own limitation. In the future work we suggest that a comprehensive measure should be required to build a shield against DDoS. The security measure should be capable to identify the difference between genuine requests and DDoS packets. It has the power to identify and neutralize various attacks well within in time.

REFERENCES

[1]. What cloud computing really means. InfoWorld. http://www.infoworld.com/d/cloud-computing/What-cloud-computing-really-means-031? Page=00
[2]. Mell P, Grance T (2011)Thenist definition of cloud computing (draft). http://csrc.nist.gov/publications/drafts/800–145/Draft-SP-800-145_cloud-definition.pdf
[3]. [PHE01] FX ofPheneolit. “cdoor.c, packet coded backdoor, version 1.3.” 13 June2000. 19 Aug. 2003. <http://www.phenoelit.de/stuff/cd00r.c>.[PHE01] FX of Pheneolit. “cdoor.c, packet coded backdoor, version 1.3.” 13 June2000.
[4]. 19 Aug. 2003. <http://www.phenoelit.de/stuff/cd00r.c>.
[5]. Moore, David, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, andNicholas weaver. “The Spread of the Sapphire/Slammer Worm.” 2003. Cooperative Association for Internet Data Analysis (CAIDA). 14July2003http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html
[6]. “Protocol Numbers.” 13 Jan. 2003. Internet Assigned Numbers Authority. 17 Aug. 2003. <http://www.iana.org/assignments/protocol-numbers>[IPF01]
[7]. “FW-1 IP Fragmentation vulnerability (remote DoS).” 6 June 2000. Beyond Security. 17 Aug. 2003. <http://www.securiteam.com/securitynews/5NP010A1YI.html>.
[8]. Vixie, Paul, Gerry Sneeringer, and Mark Schleifer. “Events of 21-Oct -2002.”18 Aug. 2003. <http://f.root-servers.org/october21.txt>.
[9]. Metz C (2009) Ddos attack rains down on Amazon cloud. http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/
[10]. . X. Geng, A.B. Whinston, Defeating Distributed Denial of Service attacks, IEEE IT Professional 2 (4) (2000) 36–42.
[11]. Felix Lau, Rubin H. Stuart, Smith H. Michael, and et al., "Distributed Denial of Service Attacks," in Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, Vol.3, pp.2275-2280, 2000.
[12]. R. Oppliger,”Internet Security: firewall and beyond,” Communications of the ACM, Volume 40, Issue 5, pp. 92-102, 1997.
[13]. McAfee, “Personal Firewall”. Available at: http://www.mcafee.com/ myapps/ firewall/ov_firewall.asp.
[14]. P. Ferguson, and D. Senie, “Network ingress filtering: Defeating denial of ser-vice attacks which employ IP source address spoofing,” RFC 2267, the Internet Engineering Task Force (IETF), 1998.
[15]. Baker, F. “Requirements for IP version 4 routers,” RFC 1812, Internet Engineering Task Force (IETF).Go online to www.ietf.org.
[16]. K. Park, and H. Lee, “On the effectiveness of router-based packet filtering for distributed DoS attack prevention in power-law Internets," Proceedings of the ACM SIGCOMM Conference, 2001, pp. 15-26, 2001.
[17]. T. Peng, C. Leckie, K. Ramamohanarao, “Protection from Distributed Denial of Service attack using history-based IP filtering,” in Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, USA, Volume 1, pp. 482-486, 2003.
[18]. T. Anderson, T. Roscoe, D. Wetherall, “Preventing Internet Denial-of-Service with Capabilities,” In ACM SIGCOMM Computer Communication Review, Volume 34, issue 1, January 2004, pp. 39-44
[19]. A.D.Keromytis, V. Misra, and D. Rubenstein, “SOS: Secure Overlay Services,” in the Proceedings of. ACM SIGCOMM, pp. 61-72, 2002.