DDOS Attacks in Cloud Computing and its Preventions

U M Shahil, Deekshitha,Nuzha Anam M, Mustafa Basthikodi
Bearys Institute of technology
Mangalore,India

Abstract **- Cloud Computing is a popular phrase that is shorthand for applications that were developed to be rich Internet applications that run on the Internet (or "Cloud"). Cloud computing enables tasks to be assigned to a combination of software and services over a network. This network of servers is the cloud. Cloud computing can help businesses transform their existing server infrastructures into dynamic environments, expanding and reducing server capacity depending on their requirements. As it provides services to customers, so same way time it provides facility to attackers. They are several types of threats that attacks the Cloud Computing and Distributed Denial of Service (DDoS) threat is the most prominent attacks in this area of computing This paper provides a wide survey on various DDOS attacks and its preventions, By using neif and Honeypot techniques it helps in preventing DDOS attacks from cloud computing.**

Keywords **: Cloud Computing Environment ,DDOS Attacks, Prevention : Neif and Honeypot Techniques.**

I. INTRODUCTION

Cloud Computing is the use of software and hardware to deliver service over the internet. Cloud computing is the use of various services, such as software development platforms, servers, storage and software, over the internet[7], often referred to as the "cloud.". User just needs a browser with internet connectivity to avail the many cloud services. Most widely used now a days popular cloud services are Gmail, Facebook, Dropbox etc are all can be accessed through browser having internet connectivity anywhere through laptop, cell phones or tablet etc with any modes of mobility. 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 fig

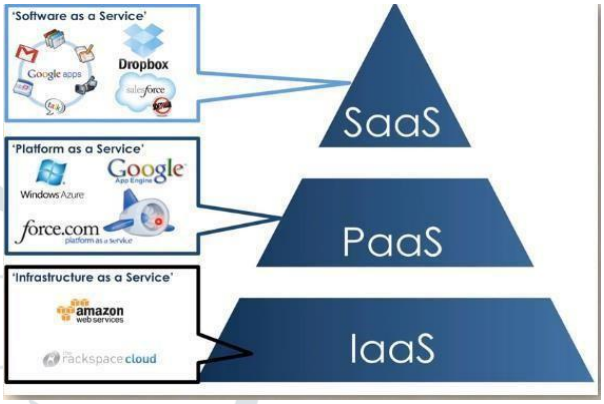


Figure:1 cloud service models.

Where IAAS allows users to access fundamental resources such as Physical machines, virtual machines ,virtual networks and storage, while PAAS provides runtime environment for applications, development and deployment tools etc ,Also. SAAS enables the users to access software applications to end users, where he leases you the applications or software to use which is owned by the owner. One of the major advantage of cloud computing is that cloud infrastructure and its maintenance will be taken care by the third party or cloud service provider on their own cost. But still most of the cloud computing prone security attacks and lose their data[1]. As cloud computing avail many services to users, same features can also be threat cloud computing. there are several threats and DDOS(Distributed Denial of service) attack is one of them, A distributed denial of service attack results in a temporary or long-term non availability of a service to its intended users by the way of either crashing a service resulting in complete non-availability or by flooding a server with fraudulent requests there by slowing down the delivery of service to real users. The purpose Denial of Service attack is to make the network resources such as internet, Web services and applications unavailable to the genuine users for a certain period of time [2]. A Distributed Denial of Service (DDoS) attack is a synchronized threat which is performed by compromising less important systems to launch an attack against a target system or network [6]. On February 9, 2000 there are more number of DDOS attacks are performed against various websites such as against Yahoo.com, Amazon, eBay.com, E*Trade, Buy.com FBI and more websites fell wounded to DDOS attacks resulting in a huge

amount of damage and difficulty. so it is necessary to take steps to prevent DDOS attack in Cloud environment .This paper proposes two techniques to prevent from DDOS attacks one is neif techniques Network Egress and Ingress Filtering (NEIF), which can be implemented at ISPs' edge routers, to avoid a DDOS attacks in Cloud. With NEIF technique, an Internet Service Provider (ISP) can easily protect their clients against a DDOS attack (egress Filtering), but also protect their networks from participating in spreading DDOS attacks (ingress filtering). An other is Honeypot Techniques which is a sort of a trap, can be used to interact with potential attackers to deflect, detect or prevent such attacks and ensure continuous availability of service. hence it is necessary to defend and mitigate a DDOS attack to minimize the damages to Cloud environment.

II. UNDERSTANDING A DDOS ATTACK

DDOS attack is the most prominent security attacks in the cloud computing, which is the largest which can impact on cloud services. DDOS attack is almost same as DOS Attack, but the impact of ddos are massive. DDOS is Implemented with several compromised systems here is the wing leader who is the attacker, would develop malware program and sends the malware program to various computer in the form of email ,or any other website .As they go through the website or open such email attachments ,the malware will be installed on their computers and will be infected without even owner knowing ,so their computer can be recruited in an arm y of other infected computers to perform ddos attacks , an army of infected computers are called botnets.This can result in either temporary interruption in service by means of overwhelming the server with several requests or a permanent one that causes the server to crash.

III. TYPES OF DDOS ATTACKS

1)**Smurf attack**: Forged ICMP packets are sent to the destination server which responds with ICMP reply packets thereby flooding the server with fake requests and denying service to real users.

2) **UDP Flood Attack**: This happens when the attacker sends a forged UDP packet to a port which responds with a destination unreachable ICMP response. This floods the system if several UDP packets are sent

3) **TCP/SYN Flood Attack**: The target server is sent TCP packets with unreachable addresses. The server wastes all its time and resources in determining the right destination causing denial of service to others.

4) **Teardrop Attack**: Here, jumbled overlapping TCP/IP fragments are sent to the victim server which can crash the system due to difficulty in reassembling the overlapping fragments

.5)**Ping of Death Attack**: In this case, the destination server is sent an ICMP packet much larger than it expected size. The victim server is unable to reassemble the packet and crashes as a results.

IV. FACTORS AFFECTING DDOS ATTACKS

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 [5]. The following are the opportunities for the attackers to use attack to ols easily to launch attack:

1. **Internet security is highly interdependent** The launch of DDoS attack depends upon the global internet security.
2. **Limited Internet resources** be consumed by a sufficient number of users.

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.

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.

V. DDOS ATTACK SCENARIO IN CLOUD

Distributed computing gives an on-request utility registering model where assets are accessible on "pay-asyou-go" premise. . The cloud worldview gives tremendous chances and advantages to buyers and a similar arrangement of highlights are accessible and might be helpful for DDoS aggressors. Specifically, the cloud supplier is a "Infrastructure as a service (IaaS)" supplier, who arrangements VMs on-request. Then again, a specialist organization is a cloud purchaser who has put the web administration as a VM in the foundation cloud given by the cloud supplier. Figure 1 portrays a commonplace distributed computing condition with an extensive number of servers running VMs. An ordinary assault situation is as appeared in Figure 2. A framework cloud will have numerous servers equipped for running VMs in multioccupant virtualized conditions . Aggressors altogether plant bots and trojans on traded off machines over the Internet and target web administrations with Distributed Denial of Service assaults. An assailant who designs a DDoS assault would send enough phony solicitations to accomplish "Denial of Service". Nonetheless, this assault would produce overwhelming asset use on the unfortunate casualty server. also, subsequently VM gets over-burden. Over-burden VM

might be given some more assets or moved to a higher asset limit server or might be bolstered by another occurrence began another server. In the event that there is no relief framework set up, this procedure will continue including the assets. This circumstance may last till specialist co-op can pay or cloud specialist organization devours every one of the assets. At long last, it will prompt "Administration Denial". Thusly, this prompts on-request asset charging, and subsequently monetary misfortunes well beyond the arranged spending plan may happen. One inconsequential arrangement is to run VMs on fixed or static asset profile where the SLA does not have any arrangement for extra assets on interest. For this situation, the DDoS will legitimately result "Trying to claim ignorance of Service" and all the appealing highlights of the cloud will assaults where a botnet controller coordinates countless malware driven bots to dispatch the assault. We show legitimately unmistakable assault impacts just as assault impacts which are not straightforwardly obvious or turned out to be noticeable post-assault. Direct assault impacts incorporate administration personal time, financial misfortunes because of the vacation, auto-scaling driven asset/monetary misfortunes, business and income misfortunes, and the vacation and related consequences for administrations which are subject to the injured individual administration. There are various roundabout impacts to the cloud DDoS attacks. Assault moderation costs, vitality utilization costs, notoriety and brand picture misfortunes, accidental losses to the cloud segments and the impacts because of ongoing smoke-screening assaults. Notoriety and brand picture misfortunes may not be all around evaluated and might be treated as long haul misfortunes [10]. Accidental losses incorporate aberrant DDoS attacks, expansion relocations and scaling, and the vitality utilization impacts as given in .

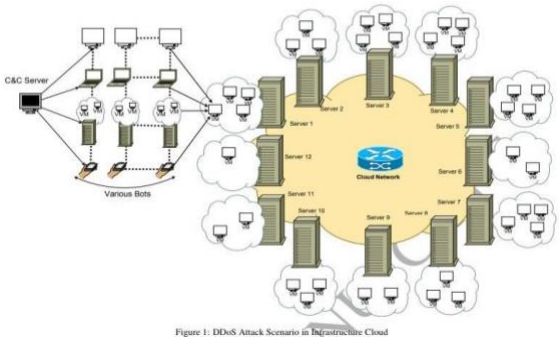


Figure 1: DDoS Attack Scenario in Infrastructure Cloud

Figure 2:DDOS ATTACK SCENARIO IN CLOUD

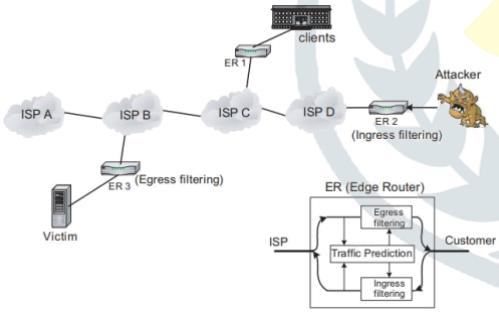
VI. PREVENTION OF DDOS ATTACKS IN CLOUD COMPUTING

Many observers have stated that there are currently no successful defences against a distributed denial of service attack, but there are numerous safety measures that a host or network can perform to increase the security of network and neighbouring networks, DDoS prevention in the cloud is a master dynamic measure, where presumed assailants' solicitations are separated or dropped before these solicitations begin influencing the server. Aversion strategies don't have any "nearness of assault" state thusly, which is generally accessible to the assault recognition and relief techniques. In this way, anticipation techniques are connected to all clients whether real or ill-conceived. A large portion of these techniques are tried against their ease of use, which acquires an overhead for the server just as real customers. we here further classified two techniques: NIEF(Network egress and ingress filtering)technique and Honeypot techniques

1)NEIF Techniques

NEIF installed at the ISPs' edge routers 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 customers. Actually, the ingress filtering has already been extensively deploying to avoid source IP spoofing by discarding packets which have a source address which is not allocated to that customer. Our proposed ingress filtering can be a supplement of the existing one. Ingress filtering can ensure an ISP's network do not participate in flooding DDoS attacks. Ingress filtering requires the understanding between Internet Service Providers (ISP's) so it takes more amount of time to implement at all ISP's. [4]Egress filtering is used to protect ISP's customers from being attacked. Note that single egress filtering cannot avoid major flooding attack that may damage the Internet infrastructure directly. However, if most ISPs have already deployed ingress filtering, egress filtering can work well. However, a main obstacle to execute flow-level filtering is that it is infeasible to exactly compute all flows. Additionally keeping a counter costs more for each flow, since it grows linearly with the number of flows even with state-of-the-art sampling technique such as Cisco Net Flow. Egress filtering is used to filter the networks outbound traffic. Why is this significant? Either through malicious intent or simple misconfiguration of a network, sites can flood the Internet with bogus packets. On February, 2000 the sites are hacked exclusively to send bogus packets to other servers on the network. Traditionally, the traffic can be filtered by routers and firewalls but these strategies will leave the Distributed Denial of Service (DDOS). Egress filtering can be able to detect and prevent the Distributed Denial of Service (DDOS) attacks. DDOS attacks can be controlled by implementing egress filtering at the networks. This paper briefly converse the benefits of egress filtering, gives examples for what common DDOS tools it can block, and directs the reader to sites with specific details on how to execute this filtering at the site. The egress filtering is used to prevent packets with invalid or incorrect address leaving form the system. These invalid packets may be originate from a misconfigured router in network or, more dangerously, from a compromised system hosting one of the many DDOS

tools available. Egress filtering usually occurs at the edge of a network, at the firewalls and border routers. At no time should the network send out any packets with addresses not legally assigned to you – to do so means either firewall may be misconfigured to show the world how internal address space, or worse, that you are the home of one or more DDOS attack agents. There should be very little effect or loss of functionality to the network when implementing egress filtering – all justifiable traffic requires is in legal addresses, so blocking anything else will only break things that should not be sent in the first place! The firewalls and routers struggle to prevent the traffic, when the site has been already compromised.. Similar to egress filtering, Ingress filtering is the filtering of "any IP packets with untrusted source addresses before they enters and affect the system" This can be implemented at ISP level where it can be cleanly hold the packets coming through their many networks. Unfortunately, for some of the larger ISP's like AT&T and sprintlink.net, they connect such a huge quantity of networks that filtering for legal addresses is tremendously complicated. Ingress filtering has its limitations– for large ISP's, other companies with different addresses may be using their backbone. To prevent those addresses from going through the network would be its own form of denial of service attack. Keeping track of the many genuine addresses that can go through a large ISP is next to impossible – it is better to have security as close to the source as possible, encouraging each site to perform their own egress filtering. The architecture of the NIEF and



Edge routers at ISP's are shown in figure below

FIGURE 3: NEIF ARCHITECTURE

2) Honeypot Techniques:

Since distributed denial of service attacks can be potentially harmful to a target server, Since it is defensive approach it's essential to effectively detect and reduce such attacks. Although absolute prevention of attacks is difficult, several techniques have been proposed to counter DDoS attacks. The two main techniques that deal with DDoS attacks involve mitigation of attacks and identification of the attack source [4]. Honeypots can be effectively used in both of these cases. Fig.4 illustrates the design of a basic honeypot There are several ways in which a honeypot can be defined. In simplest terms, a honeypot can be defined as a trap for an attacker that mimics some or all activities of a real system and records the activities of the attack source [3]. Honeypots can be used in a flexible manner at the server side to not only detect such attacks but to also protect the user's critical data and record possible malicious activities so as to track the attacker. Honeypots can be broadly classified into two categories namely low interaction and high interaction honeypots [3]. High interaction honeypots imitate most services of real production systems and host a variety of tasks. They provide more security and are hard to detect but are relatively expensive to maintain. On the other hand, low interaction honeypots simulate services that are frequently requested by attackers. They consume fewer resources and can be easily maintained . Both types of honeypots can be implemented as virtual machines and hosted on a single physical server .

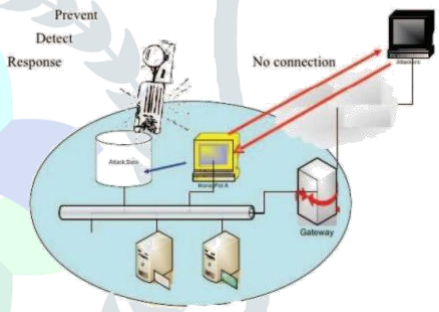


Figure4:Basic Honeypot Design COMPARITIVE STUDY

	HONEYPOT TECHNIQUE	NEIF TECHNIQUE
Deployment	Server side	Edge routers
Objective	Attack detection and prevention	Attack prevention
Advantage	It can take attack and attackers and give information about them if needed	Handle network traffic such as secured increased visibility of network traffic and increase control over network
Disadvantage	Cannot replace security mechanism	Increased overhead and complexity
Remarks	A honeypot , works by fooling attackers into believing it is a legitimate system, they attack the system without knowing that they are being observed completely	NEIF installed at the internet server providers(ISP's) edge routers and play a dual role in shielding DDOS Attacks.

CONCLUSION

No doubt cloud computing technology proved to be very helpful to many industries and individual consumers, but also prone security threats and DDOS Attack is one of them. This paper deals

with Distributed denial of service (DDOS) attacks are dangerous and can potentially render the production site unusable either by flooding the server network with thousands of malicious requests or crashing the server by exploiting the vulnerabilities in its software. This paper also concludes by preventing two strategy techniques (NEIF) network egress and ingress filtering, and honeypot technique where neif helps in preventing the DDOS attack from the cloud, whereas honeypots also helps in capturing attacks and attackers as well by recording his activities. As there is risks in each field , further refinement can be done in each techniques.

REFERENCES

[1] Ruchi mehta , Institute Of Technology, "**Distributed Denial of service Attacks on cloud environment"**, Ijarcs,may-june 2017.

[2] R. Sridaran , Marwadi Education Foundation's Group of Institutions**, "An Overview of DDoS Attacks in Cloud environment"**, Research gate.net,november,2014.

[3] Rashmi V.Deshmukh, Kailas K. Devadkar, Sarder Patel Institute Technology, University Mumbai,India, "**Understanding DDOS Attack and Its Effect in Cloud Environment"**,Sciencedirect.com,2015.

[4] J.RAMESHBABU, *B.SAM BALAJI, *R.WESLEY DANIEL,**K.MALATHI ," **A PREVENTION OF DDOS ATTACKS IN CLOUD USING NEIF TECHNIQUES",** International Journal of Scientific and Research Publications, Volume 4, Issue 4, April 2014

[5] Manoja ,Computer Science and Engineering, VFSTR University, AP , Nazma Sultana Sk, Information Technology VFSTR University , AP , Deevi Radha Rani, Computer Science and Engineering, VFSTR University, AP ,India "**Prevention of DDoS Attacks in Cloud Environment"**,IEEE,2017

[6] DDOS Attack ,Types of DDOS Attacks, prevention,https://www.incapsula.com/ddos/ddosattacks.html

[7] what is DDOS Attack, https://www.cloudflare.com/enin/learning/ddos/what -is-a-ddos- attack

[8] Gaurav Somani, Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buyya, **DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions, , Computer Communications** (2017).

[9] Rahul Reddy Nadikattu. 2016 THE EMERGING ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY. International Journal of Creative Research Thoughts. 4, 4 ,906-911.

[10] Sikender Mohsienuddin Mohammad, "DEVOPS AUTOMATION AND AGILE METHODOLOGY ", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.946-949, August-2017, Available at :http://www.ijcrt.org/papers/IJCRT1133441.pdf

[11] **A Cloud Computing Overview,Research and Reviews,** Journal of Global Research in Computer Science,(2018).

[12] Rahul Reddy Nadikattu. 2017. The Supremacy of Artificial intelligence and Neural Networks. International Journal of Creative Research Thoughts, Volume 5, Issue 1, 950-954.

[13] Sikender Mohsienuddin Mohammad, "IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf

[14] Aamir, M. and Arif, M., "Study and performance evaluation on recent DDoS trends of attack & defense", International Journal of Information Technology and Computer Science, 2013, pp. 54–65.