Prevention of DDoS & EDOS using Hybrid Filtering Technique in a Cloud Environment

Shruti Wadhwa\(^1\) and Dr. Poonam Saini\(^2\) Dr. C. Ramakrishna\(^3\)
\(^1\)Computer Science Department, NITTTR, Chandigarh. shrutiwadhwa99@gmail.com
\(^2\)Computer Science Department, PEC, Chandigarh. nit.sainipoonam@gmail.com
\(^3\)Computer Science Department, NITTTR, Chandigarh. rkc_97@yahoo.com

Abstract
Cloud Computing is a heterogeneous distributed environment which provide resources on pay per use scale as service through internet. The data stored in cloud needs to be secured from the attackers as it is remotely kept. However, security is one of major challenge in cloud. In recent years, DDoS is the major attacks in cloud on the catalog of cloud attacks. EDoS is the latest type of threat to the cloud infrastructure. The purpose is to consume cloud resources although the price of services is pay off by the valid customer. The key intention of DDoS attack bring down the specific service by draining server’s resources whereas EDoS’s objective is to create an economical unsustainability in the cloud resources for the object and causes financial consequences by exhausting resources and leading to a heavy bill. Therefore, a new approach is proposed for the mitigation of the DDoS & EDoS attack which consist VF (virtual Firewall) as key component which discards the attack traffic before billing is triggered.

Key Words: DoS, DDoS, EDoS, Cloud Computing, Ingress and Egress filtering

1 Introduction

383
Cloud computing is a new IT delivery model, which enables users to store and access data according to their needs irrespective of time and place. It would be the rebellion in the IT Company, which also signifies various development trends. The idea behind cloud computing is reducing the workload from user's computer to cloud making use of simple internet connection. It allows IT industries to focus on doing what they actually want without spending money on infrastructure and wasting time in arranging them [1] [2]. Farzad Sabahi [3] provide the various issues of security and availability in cloud computing and suggest some obtainable solution for them. Cloud is vulnerable to various attacks being Malware injection, Metadata spoofing, DNS and DDoS attacks, Cross-site scripting, SQL injection, and Wrapping Attack. The main aim of DDoS is to harm a target either for individual reasons, material gain, or to gain popularity. A special kind of DDoS attack which is specific to only cloud infrastructure. This is called Economic Denial of Sustainability (EDoS). The main aim of EDoS is to make cloud resources carefully untenable for the victim, EDoS attack take place just beyond the average movement threshold and beneath the threshold of DDoS attack [4].

**Distributed Denial of Service Attack.** Distributed Denial of Service (DDoS) may be explained as an aim to create a network or machine resources inaccessible to legitimate users. This attack restrains the availability of resources. The widely popular DDoS attacks on eBay, Amazon, Yahoo, and numerous popular websites in February 2000 exposed weakness of still fine equipped network and massive Internet users [5]. DDoS harms are likely to grow to be more ruthless in future in comparison to other attacks as there be short of valuable solutions to protect these attacks. Behind major DDoS attacks are botnets and they make use of flooding to block the availability of the resources of benign user [6]. The straightforward logic structures and small memory size of DDoS attacking programs makes them comparatively simple to employ and hide [7]. Therefore it is very important to protect data and prevent attacks like DDoS [8].

**Economic Denial of Sustainability:** An EDoS attack is a distinctive type of DDoS attack that sets a target on the pay-as-you-go model of the cloud. This type of attack harms the cloud’s auto scaling feature. An attacker creates malicious requests of HTTP for web application and the CSP (Cloud Service Provider) measures the design mechanically to deal with those requests for which the cost is incurred by a cloud consumer. Its outcome is maintainable drop in the client’s budget. Moreover, the spiteful HTTP traffic imitates to be real and thus go undetected. The security devices to provide protection from DDoS attack are not valid to against EDoS attack because EDoS attack is executed over a long time span [9]. Cloud Computing adopts the utility model in which customers pay...
converted the problem of DDoS attack into cloud specific economic one identified as EDoS attack. The purpose of this attack is to dispossess the regular users of cloud from their lasting economic sustainability. The objective of an EDoS is to create economical unsustainability in the cloud resources for the object, while the objective of DDoS attack is to damage or block the services of cloud. DDoS attacks are accomplished in a short span of time on the other hand EDoS attacks are more delicate and accomplished in a long span of time. EDoS attack takes place above the usual activity threshold and beneath the threshold of DDoS attack [9].
2 Related Work

Darwish, M et al. [10] have discussed about the various cloud based DDoS attacks and its defenses. The paper gives an DDoS overview initially mentioning the arrival of DDoS attack with different DDoS attacks like IP Spoofing, Syn flooding, smurf, buffer overflow land attack which existed those days. In this, the defense mechanisms are even explained corresponding to their attacks. DDoS attacks are currently a major threat against the cloud services. Defense mechanisms are not always effective, but combining different mechanisms to build hybrid defense mechanisms with different layered security of cloud is always recommended. It is recommended to investigate the effects of these different DDoS attacks on cloud and their remedies provided.

Zakarya et al. [11] have discussed about DDoS Verification and attack packet dropping algorithm in cloud computing. This paper discussed a new solution for DDoS attack confirmation and attack packet reducing for cloud computing. The algorithm confirms the attack flow, if it occurs, if not the flow is discarded. The packet drop algorithm was implemented in routers. The algorithm itself gets activated dropping the packets down thus successfully defending the DDoS attack in cloud based environment. On DDoS detection at the edge router the flow is shifted to subsequent adjacent router where the flow is checked and dropped using the packet drop algorithm. If not, then the packets are thrown to the target node or system on its own way. This technique is implemented on the routers that are far near the source so that the attack can't be reached to destination and could be detected and prevented earlier. The scheme is proactive in nature.

Malathi et al. [12] have discussed the challenges of DDoS attack and its impact on cloud computing environment. The paper discusses a network egress and ingress filtering called NEIF method which is used as a defensive method to conquer DDoS attack. In this technique the objective of the ingress filtering is to determine and prevent the DDoS attacks. The NEIF technique can be implemented at internet service provider's edge routers which can improve the throughput under various deployment models and also can be implemented with less complexity.

3 Proposed Prevention Technique

**Detection:** The common type and easiest way of DoS attack includes flooding of communication requests to the target resource. This overloading of requests blocks the resource from replying to valid traffic, or can significantly slow its response that it effectively becomes rendered unavailable. So, it’s beneficial to establish the analyzer of network traffic which helps to identify the beginning of the attacks by the parameter values which will allow in time. Before the direct start of attack, bots steadily raise a flow of packets on system. Consequently, it become necessary to continuous observes the router associated to the external network. On the basis of advanced mathematical model, the choice of quantity and the size of routing domains are defined. For the idea of maintain of highest
account which changes the network topology. Therefore a novel model of routing is developed at the cost of the amount of failure attacks in service of resources of routing will permit increasing effectiveness of information transfer in the networks. Hence it becomes essential to take into account the situation of feasibility of parameter values of network transmission capacity and computing resources. It is convenient to decide the parameters which regulate the number of the packets being transferred on each communication link individually and overall number of the packets transferred during the update of routing tables. And the total volume of traffic is determined by the model and is calculated by (1) [13].

\[ V = \frac{T_{sys}}{\Delta t_{sys}} \sum_{i=1}^{N} P[iQ] \]  

Where \( \Delta t_{sys} \) – time of one clock period of system, \( Q_j \) – amount of information, transferred for one clock period on each certain canal, \( N \) – Quantity of nodes on the computer networks, \( P_j \) – the degree of a node is compromised, \( T_{sys} \) – time during which in case of topology change of a network nodes distribute messages of message on restoration of routes.

**Prevention:** For the prevention of DDoS attack, Phase 1 is Ingress and Egress Filtering for Mitigation DDoS in which there are many DDoS detection methods which can be implemented in cloud: DDoS detection stress substantial resources and time for a server to carry out a variety of detection technique when they experience DDoS attack. DDoS can carried out in different forms, and in practice, there are different detection methods which exist like the detection methods which is based on IP spoofing, low rate attacks, packet score, hop count, and many more. As mentioned before, we only concentrate on how to prevent DDoS attacks in cloud environment. Filtering is carried out in this phase to distinguish between legitimate user and the attacker. Packet filtering is the process of allowing or blocking packets at a network interface on the basis of source and destination addresses. In this phase, two filtering techniques can be used which are Ingress filtering and Egress filtering. Ingress filtering is an inbound filtering and a system of confirming that inbound packets received at a network is from the same source of computer that they are claiming to be from earlier to permitting the entry (or ingress). Egress Filtering is an outbound filtering mechanism. It blocks the traffic with an IP address that has an invalid source. This keeps a DoS attack utilizing the spoofing of IP address from initiating on the internal network. The filter must permit traffic to go outside your network only by a source IP address. The key objective of egress filtering is to make sure that traffic that is not wanted or that is destructive does not go outside of a particular network. For instance, In a university campus network, a firewall might be used to prevent students from sending malware or copyrighted material outside from any of the computer systems within that network. It may also be used within an organization’s network to permit only some particular servers or computers to send the data outside of that network. For instance, this safety measure can prevent employee from using business computers for excessive personal communications or casual Web surfing. The Phase 2 is IP based Validation Rule in which Whitelist is used which is a list that includes the ip address of the legitimate user of the network which avails the service of the cloud.
4 Simulation and Result
For simulation, a virtual lab is created in virtualbox in which ownCloud server is used as cloud server and some legitimate clients are made in virtual lab which accessing the cloud services and for performing the DDoS attack, three virtual attacker machines are prepared. First attacker machine is windows machine in which DDoS tools are installed like Slowloris, Faster DDoS Attack for performing the DDoS attack. Second attacker machine is Ubuntu machine, we made a shell script by combining many tool scripts as it is not possible to perform attack using single tool onto the cloud server. And third is Kali Linux machine in which metasploit is used for performing TCP SYN flood attack. The Faster DDoS Attack tool is used for performing the DDoS attack by providing the cloud server ip address (primary) and other details (secondary) through which the flood of packets is send to the cloud server. The second attacker machine is ubuntu 14.04. In this attacker machine we made script by combining the three scripts of DDoS attack. Goldeneye, Hulk and Slowloris scripts are collectively combined and they run parallelly after providing the destination address for performing DDoS attack. Third and last attacker machine is Kali linux, metasploit framework is used for performing TCP SYN Flood DDoS attack. During DDoS attack, legitimate clients are not able to access the services and various parameters are checked for evaluating the performance of the cloud server in normal scenario, attack scenario and in prevention scenario. Detection of the attack can also be done using netstat on owncloud server which shows the number of packets sent and the ip address of the source. If number of packets is exceeded from specific threshold which is calculated by equation 1 and when the legitimate client is not able to access the cloud services then we can say server is under DDoS attack. When the amount of SYN requests raise above the server threshold, it falls without establishing proper connection. From proposed method, a threshold limit of traffic is set up that the server would be able to resist. The most suitable characteristic of this method is that the technical administrator is able to decide how much traffic to permits inside the network. The traffic rate relies on the company size, the traffic it can resist and processing capacity of the server. We have applied these rules on linux firewall iptables to incoming and outgoing traffic in a particular interface. And the network traffic which follows these conditions is transmitted and rest is dropped. Any single filtering does not provide fully protection from attack. Therefore, hybrid of the techniques gives a better defense mechanism. Here both the IP based and the Ingress Egress filters are used together provides the network an better solution. Performance of the proposed technique can be determined by evaluating Bandwidth, Server response time, download time and mean request time which can be shown in figure 1,2,3,4.
EDoS Prevention

This hindrance technique is a proactive approach which helps the genuine client to access the resources without being activated by the attacker on billing mechanism. The basic idea for the prevention of EDoS attack is to use Virtual Firewall whose function is to perform real time traffic analysis and also keeps a log file of packet which passes through it. In Virtual firewall, ingress and egress packet pattern matching rules and whitelist/blacklist is used which help to get rid of the attack traffic earlier than billing is triggered. The key idea is to confirm that request coming from the genuine user not from the attacker. It always checks the packets at the entry point of the cloud. Ingress and Egress filtering is used for the protection of IP spoofing. Therefore, it will also protect the cloud environment from the IP spoofing attacks. And in proposed method, end to end delay is reduced as the packets after successful request by the VF would be promoted directly to protected service of cloud. And for the evaluation of the performance of the proposed mitigation mechanism for EDoS attack parameters included are allocation of resources and response time. Although the EDoS attack is primarily directing the cloud adopter, the cost associated with the computing resources is also evaluated. The proposed prevention technique for EDoS is represented by figure 5.
6 Conclusion and Future Work

In this research, the problem of DDoS attack and EDoS attack and prevention of DDoS attack and EDoS attack is discussed in order to reduce the effect of DDoS attack and EDoS attack in cloud environment. Filtering is carried out to distinguish between legitimate user and the attacker. Thus, hybrid filtering techniques can be used with IP based validation rule which helps to prevent DDoS and EDoS attack in cloud environment. The implementation of the proposed approach of DDoS attack is done in virtual lab environment. The proposed method can be adopted by most of the providers as it proves to be efficient and saves the network components from permanent denial of service. The finest mark of this method is that the technical administrator is able to determine the amount of traffic to let inside the network. This prevention mechanism works well for small network and it can be executed with less complexity and it is transparent so that it can be easily accepted by the Service Provider. In future, the proposed mechanism is implemented on cloudsim for EDoS attack.

References
