EDoS-Shield - A Mitigation Technique against EDoSAttacks in Cloud Computing

Amita
Lovely Professional University
Jalandhar-Delhi G.T. Road,
National Highway 1, Phagwara,
Punjab 144411

***Abstract*- Cloud Computing is a collection of resources that are available for 24 hours as well as it can accessible from anywhere through browser software all over the world. Cloud term define as a "virtual collection of computing resources". We can define the cloud computing term means different things to different people. Cloud computing is internet based computing in which cloud service provider are charged to client on the basis of usage of cloud service and network resources. The DDoS attacks are performed typically by the gathering of programmers so as to accomplish some specific objective. The programmers may point the DDoS strategy to hurt the system reliance and asset accessibility of some specific online administration supplier, which may hurt the monetary undertakings of the specific firm. These attacks are called EDoS attacks .The EDOS attack is a new breed of attack specifically targets the cloud environment. EDOS Attack does not objective to exhaust the victim bandwidth ,the main aim is to put a huge financial burden on victim through consumption of victim metered (pay as you go) bandwidth. In this Paper, we propose a solution,to mitigate the Economic Denial of sustainability attack in Cloud Computing Environment.The experimental results have shown the effectiveness of the proposed model. The proposed model has been found efficient to protect the EDoS attack on the cloud platform simulations.**

Keywords-Cloud Computing;EDoS;Mitigation;

I. INTRODUCTION

Cloud computing in which a huge number of resources are dynamically allocated to the applications with aim of to offer the services to a maximum number of clients, we can expand or release our servers in size or accessibility but without spending costs in news infrastructure, training new personnel or licensing new software due to cloud computing, clients can lease these resources from an cloud provider as an outsourced service instead of investment on actual physical servers, storage and network equipment. Cloud computing is internet based Computing in which cloud service provider are charged to client on the basis of usage of cloud service and network resources. Moreover, cloud allows the clients to maximize and minimize the number of requested resources as needed due to elasticity facility. Furthermore, In cloud models, users do not require to pay hardware and software maintenance cost .

But sometimes, a new type of attack is possible in cloud,which is called Economic Denial of Sustainability,it cause a new type of problem in cloud environment.DDoS attack can be transformed into EDOS attack in an Cloud environment. This Attack has been referred to EDoS while it is termed as Fraudulent Resource of Consumption Attack. It uses the cloud resources without paying to cloud service provider.It works in different manner as compare to DDoS attack. For example, legitimate user demand a resources from cloud and starts using it,after sometimes unauthorized person using the services from legitimate user id. Cloud service provider allocates more resources to user according to request which is received by user. In this situation, Cloud would not be able to check that request for resources is coming from legitimate user or unauthorized person and he thinks that user want to extend services that he provided.

In this Paper, we propose a mitigation techniqueagainst EDoS attack in Cloud Computing. This is achieved by forwarding the request to the neighbor request to node X in our proposed architecture. Node X has to determine the location, Packet size, Payload information of the requests node then it allows them to join the Cloud server application.If payload information is found same in two packet of a single communication stream, it is marked as possible attacker.If the number of same packets found in a huge quantity, then the sender node is marked as the EDoS attacker and the information is provided to all of the nodes in the cluster.All nodes are updated to block the attacker node and stop receiving the packets from the attacker node.Thus,It mitigating the EDoS attack in cloud environment.

In SectionII, we discuss the related works. Section III presents theproposed architecture. simulation results and analysis are discussed in Sections IV . Finally, the conclusion and the future work arepresented in Section V.

II. RELATED WORK

One technique to solve the EDoS attack on the Network level, explores the security Framework for EDOS Attack protection,which is clarified in two components ,one with a genuine User and another with an attacker .on basis of public key cryptography,Client solve the puzzle and sends to puzzle server and check the user is genuine or not.The current methodology is not suitable to totally taking out the EDOS Attack. It is still required a enhance component to dispense with the Edos Attack from the Cloud.

Another technique that came into existence to solve the EDoS Attack which was based on Graphic Turing Test (GTT) and Crypto Puzzles are two sort of tests Graphic Turing Test (GTT) and Crypto Puzzles ,such tests are done to verify the authenticity of the source in this proposal .In such a schema, just checking two packets that are coming from any source instead of testing all packets in order to overcome delay (end-to-end) .Moreover, we perform these two types of tests in which one verifies the client and other one check the packet. The drawback of this schema is that these tests are performed on every incoming request which causes time delay.

In[4],Proposed, EDoS mitigation Technique in which In-Cloud Scrubber Service is Used in order to generate a puzzle as well as to check the legitimacy of the user with the objective to provide the cloud service to legitimate user. Cloud-service is switched between normal and suspected modes, it depend on server and network bandwidth.During the normal mode,the incoming requests will be immediately directed to cloud-service and otherwise it will be directed to In-Cloud Scrubber Service for verification process during the suspected mode. The limitation of this technique is that Client-puzzles provide weak access guarantees to customer/users.

In [5],Virtual firewalls(VF) and verifier cloud nodes(V-nodes) are used in proposed DDoS-EDoS Shield mitigating the EDoS in a cloud computing environment.Virtual firewall hold the IP address in white list or black list based on the incoming packets coming from authenticate user or attacker. Another component of this proposed system is the verifier nodes(V-Nodes),it has to verify the requests by using the Turing tests Such as UNIQUE QUESTION TESTING at application level .Second task of the V-node have to update the lists that is used by the virtual firewall(VF). The limitation of this scheme is that if requests are generated from compromised machines, it will fail at verification stage.

Sqalli[1] Proposed a technique to solve the EDoS attack on network level,it basis on Turning test which it uses CAPTCHA to verify that request is coming from genuine user or attacker.If request is coming from attacker side, it is not added into the white listand firewall block the request.The limitation of this technique is that test is performed on every incoming request.

AI-Haidari[7],this technique was based on time to live(TTL) value and V-node. When the first time user registers into cloud,it request goes to v-node and TTL (time to live) value is recorded with the respect to IP-address. When user requests,it is checked at v-node with ip-address. If both values are match then requester/ user is added to white list and request pass to virtual firewall. Otherwise, request is blocked by firewall. A V-Nodehas to verify requests at theapplication level using graphic Turing tests [27], such asCAPTCHA or RECAPTCHA. The limitation of this technique is that if attacker attacks from within the network, then TTL value will be same for attacker or legitimate user.

III. PROPOSED ARCHITECTURE

In this section present a proposed architecture to detect and mitigate the EDoS attack in cloud computing environment.This scheme detect and mitigate the effect of an EDoS attack against on demand services benefit of the cloud.It allows theCloud computing enables the users to use its resources without any interaction between of one another and also its provider. As a result, there is no need of human interaction ,thus it improves efficiency and saving the cost for user as well as its provider.Here we propose a technique to solve the EDoS attack using node.

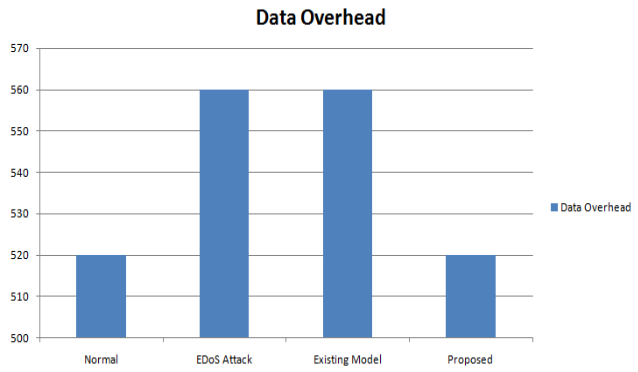
when any neighbor node X1 send the request to neighbor node X, then Node X checks the location of requested node , determine the location of that node and check the legitimacy of the node with the objective to provide the cloud service to that node X1. The second task of Node X determines the Packet stream (it is transfer of packet at a steady high speed rate) and size of packet. If packet size of every packet remains same, then it checks the data which is contain within packet(Payload information). If Payload information is found to be same in two packet of a single communication stream ,then it is marked as possible attacker. If the number of same packets that are coming from a single communication stream that is found to be in a large number or increase a certain limit, then it is considered as an attacker node.Further more,incoming packets will be blocked of that node and all nodes are updated to block the attacker node and stop receiving the packets from attacker node.

3.1 Algorithm:

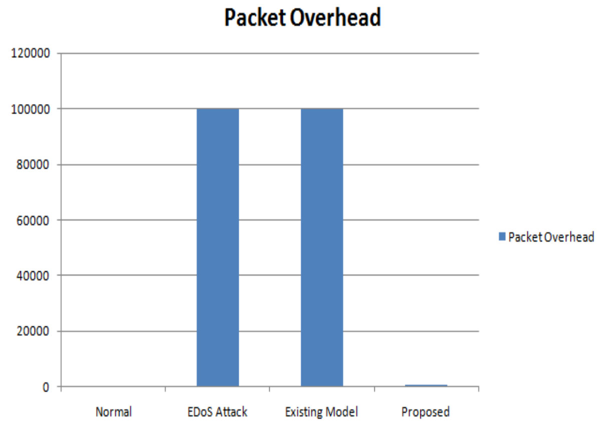
1. Node A sends the request to the neighbor request to node B.
2. Node B verifies the location of node A, and also allow it to join the Cloud server application.
3. Node B examines the packet stream, its size and payload information.
4. If packet size remains same for every packet, itverifies the payload information. If payload information is found same in two packet of a single communication stream, it is marked as possible attacker.
5. If the number of same packets increase a certain limit, the sender node is marked as the EDoS attacker and the information is provided to all of the nodes in the cluster.
6. All nodes are updated to block the attacker node and stop receiving the packets from attacker node.

IV.SIMULATION AND ANALYSIS

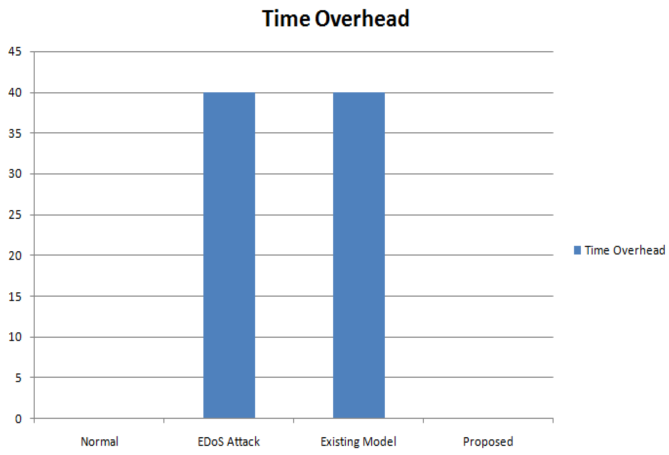
In this section,we present the simulation results to illustrate how our proposed scheme mitigate an EDoS attack against the cloud .



The figure suggests that the Data overhead in both cases (Normal &proposed)scheme are equal as well as minimal as compared to EDoS attack and Existing model.



Simulation result is shown In fig. 2 In existing model and EDoS attack ,Packet overhead are equal while in Proposed Scheme is almost negligible.



Simulation result is shown In fig 3.Packet overhead in existing model andEDoS attack are equal in both the cases but it is much higher than in proposed model.

It is evident that it takes time to identify the packets, who is sending or to determine the location. When we using this proposed approach, some attack packets can still enter in cloud environment, but there is difficult for attacker to inject the attack packet into the system. If it is happens, identification will be perform to check the location of the node.

V.CONCLUSION

Cloud computing is most extensively used technology which offers a wide range of benefits and services. Therefore,its security is also most important.EDoS attack is a new breed of DDoS attack which is only cloud specific attack owing to its presence only exist in cloud . Existing model of security are not able to completely remove the EDoS attack in the cloud.We have proposed a scheme based on node which can detect and mitigate the effect of EDoSattack which offers a fair control on those resources that are accessed by end-users. By analyzing the results obtained from the simulation of proposed mechanismshow that it is an effective approach in terms of the finish time,data overhead and time overhead. First, our proposed mechanism reduces extremely theoverhead It efficiently distinguish from the legitimate user or attacker and when the access of cloud resources is controlled ,effect of EDoS attack is minimal .

It is better scheme to protect the cloud from EDoS attack.

VI.REFERENCES

[1] Mohammed H.Sqalli Fahd AlHaidariKhaledSalah ,"EDOS-Shield – A Two-Steps Mitigation Technique against EDOS Attacks in Cloud Computing ",Fourth IEEE International Conference on Utility and Cloud Computing.

[2] Vivinsandar ,S And Shenai S,2012 "Economical Denial of Sustainability(EDOS) in Cloud Services using HTTP and XMl based DDOS attacks, International Journal of Computing Applications41(20),pp 11-16

[3] WaelAlosaimi and Khahd Al-Begain ,"A New Method to Mitigate the Impacts of Economical Denial of Sustainability Attacks Against the Cloud", ISBN (2013) PGnet

[4] MadarapuNaresh Kumar, P.Sijatha, VamshiKalva, RohitNagori ,Anil Kumar KatuKojwala(2012)," Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing using In-Cloud scrubber Service ",Fourth IEEE International Conference on Computing Intelligence and Communication Networks

[5] Mettildha Mary , P.V Kavitha, Priyadharshini M, Vigneshwar S Ramana,"Secure Cloud Computing Environment against DDoS and EdosAttacks",International Journal of Computing Science and Information Technologies 5(2),pp 1803-1807

[6] MohitKumar,Nirmal Roberts," A Technique to Reduce the Economic Denial of Sustainability (EDoS) attack

[7] Sqalli,MohammedH.Fahd AI-haidari and khaledSalah."EnhancedEDoS-Shield for MitigatingEDoS Attacks originating from IP Spoofed Address.In ,2012 IEEE 11th International Conference on Trust ,Security and Privacy in Computing and Communication IEEE,PP,1167-1174.

[8] KaziZunnurhain and Susan V.vrbsy,"Security Attacks and Solutions in Cloud".

[9] Soon HinKhor and Aki Nakao,spow:On-demand Cloud-based eddos mitigation mechanism.In In proc.of the fifth workshop on hot topics in system dependability,2009.