International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 7, July - 2013

Framework Of Security Mechanism In Cloud Computing By Denial Of Service Bandwidth Allowance Parameters

Mr. Venkateswarlu Maninti, Fahmida Begum, B. Manjula, M. N. P. Swetha Priya

[1]*Asst. Professor, Dept. of IT, Fishermen Training Institute, Salalah, Sultante of Oman,*
[2]*Asso.Professor, Dept. of MCA, Dr. K.V Subba Reddy college of MCA, Kurnool.(Dt),A.P,*
[3]*Asst.Professor, Dept. of CSE, AVR & SVR College of Engineering, Nandyal, Kurnool (Dt.,), A.P,*
[4]*Asst. Professor,Dept.of CSE, R.G.M College of Engineering and Technology, Nandyal, Kurnool (Dt.,), A.P.*

Abstract

One of the major challenging issues in cloud is to provide security in a cloud server from various unexpected attempts. Cloud computing has given a good freedom for normal user for using of cloud services with low cost or free of cost charges through third party server. Therefore cloud computing has a good chance of becoming a most widely used technology. There will be many challenges to face the cloud to be useful for the normal user or third party business team for trusting of vital information from a cloud server. These challenges become tie into developing trusted security measures in the cloud. One of developing an important aspect of security obstacles is how to well defend against either a Denial-of-Service (DOS) or Distributed Denial-of-Service (DDOS) attacks from a cloud server or virtual cloud server. Existing DOS attacks are serious and nothing new; but many strategies have been proposed and for the purpose of testing against with DOS attacks on any public or private networks. We observed that none are able to completely prevent DOS attacks. Due to this reason, we search for an effective solution to keep data available users who need it. Hence, the main contribution of the work is to propose a methodology in this paper and it has the capability of provide a quality of security services in case of said Denial-of-Service attacks.

Keywords- *Cloud computing; Denial of service; Bandwidth*

1.Introduction

Cloud computing [1] has been provide services provisioning (SaaS) infrastructure, (PaaS) infrastructure with less maintenance cost and data. Cloud computing has basically provide three layers for their services i.e system layer, the platform layer and application layer. For the three layers, cloud computing offers three service s namely Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. PaaS model facilitates to users by providing platforms on which applications can be designed, developed and run. IaaS delivers infrastructure services to users by maintaining large infrastructures like hosting servers in various remote places, managing networks remotely and other resources for clients. SaaS has makes user as a free of installation and running software services on their own machines. Many leading cloud service providers such as Salesforce.com, Google and Amazon web services extend their services for storage, application and computation on pay as rental basis instead of purchase. Cloud computing has been supports distributed service paradigm on multi-domain and multi-users administrative infrastructure; therefore, it is more prone to security threats and attacks. Currently the most emerging problem solving issues in organizations is that cloud security. Despite of its distributed nature, cloud environment has capable of solving high intrusion prospects and also suspect of security infringements. In large organizations we place the required important data into the cloud with limited free of storage service for cloud provider, if it is require for large storage and we can also use large storage on rent bases. But control of the data by various providers is also becomes challenging issue in either DOS or in DDOS for providing of challenges of security like data integrity, confidentiality and availability.

In cloud computing, the different types of clouds (private, public, and hybrid) are designed depends on organization need. Virtualization is another emerging concept in cloud computing for the purpose of resolving concerned cloud issues such as fault tolerance, security issues, and scalability. Both cloud and grid computing are the most important in various vulnerable targets for intruder's attacks in distributed environment. For such kind of environments, the technique of Intrusion Detection System (IDS) [4] can be used to enhance the security measures by reading a systematic examination of logs, and theirs configurations in network traffic.

Cloud data, cloud applications and their services non-availability can be imposed through Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks and both cloud service provider and users become incapable to provide or receive cloud services from remote servers [3]. Therefore, for such type of attacks Intrusion Detection System (IDS) can be considered as a strong defensive mechanism.

IJERT

Due to the above said reasons, we concentrated for how to avoid Denial of Service (DOS) attacks in the proposed approach. For making of supervision, an entity is integrated into a cloud server for monitoring of ratio for available bandwidth is being used by user. For finding of maximum available bandwidth of the server, we focus another entity DOSBAD (Denial-of-Service-Bandwidth-Allowance-Device) that will periodically send a series of packets within the cloud (router-to-router). First, we send two large packets to create a queue at the switch between the routers, and then secondly, we send two small packets. The total time to transfer these packets will be calculated as the time at which packet 1 is sent subtracted from the time at which packet 2 is received. Based on the time for the receiver to receive the packets, DOSBAD has been calculating the bandwidth available between two routers. It will also monitor for how much of bandwidth is used at each router.

A Denial of Service (DoS) attack is nothing but any attack that overwhelms a website [10,11, and 12], the content will be normally provided by website to be no longer available to regular visitors. Distributed Denial of Service (DDoS) attacks are purely traffic content based attacks that are originating from large number technical sources which are usually compromised workstations.

Total incoming packets along with the amount of acknowledgement packets that are sent back out are measured. Basically the number of packets received should match the number of acknowledgement packets and this is indicating that the router is not overwhelmed with the number of incoming packets.

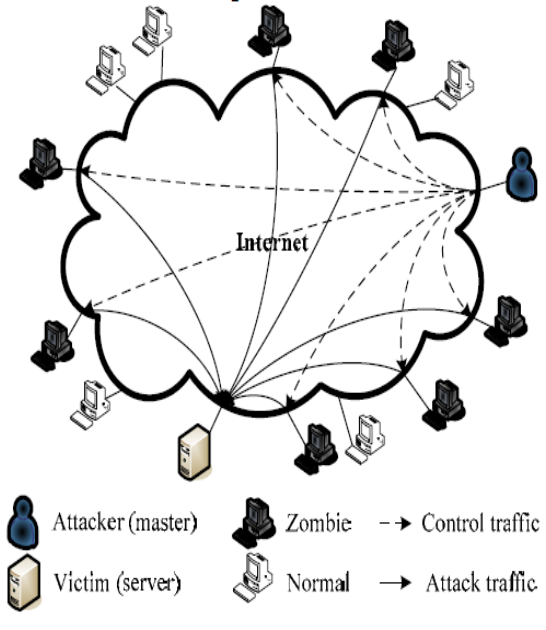

Figure 1: Attack Network (BotNet)

Effective of Denial of Service attacks are depends on current used resources, so we have to estimate that how much resources are committed before an attack. We think that all the resources involved including (but not limited to) hardware and software application limitations, network and bandwidth limits. When bandwidth limit may be close to being reached, then it indicates that either there is an abnormal thing in an activity across the network (i.e. a flash crowd), or there will be possible for any malicious activity is being attempted. At this point, DOSBAD may return addresses on incoming packets at the overwhelmed points and then it send out a ping to those addresses. Suppose DOSBAD does not receive a proper response that may indicate an attack of DOS. Finally, DOSBAD send signals to the corresponding router for dropping of incoming packets from that respective address. Another beneficial feature of cloud manager may use DOSBAD with automatic change of address for the attacked router. With this change of effect, the attacker tries again from a different attacking address, but he is unable to find that router again.

DOSBAD maintains and keeps all addresses of senders for incoming packets within specified time interval. DOSBAD observes that which address have the most incoming packets and we can be store the signature of incoming packets. Distributed denial of service attacks are originating actually from a number of computers usually called as workstations. These workstations are known as 'zombies', across a widely distributed attack network which is called as a 'botnet'. This is shown in Fig. 1. Many of modern Denial of Service attacks are Distributed Denial of Service attacks, but it is certainly not true for all denials of service which is experienced by websites. Suppose the users are experiencing difficulty in getting to the website content, it should not be assumed that the site is under a DDoS attack. Hence, it is required for paramount to do proper analysis of attack traffic when a site becomes unable to perform its normal function. All signatures of various packets that are coming from zombies in a DOS attack can be used to detect that a whether the DOS attack is occurring or not.

Some important strategies such as the various types of site mirroring are implemented as the required operating procedure whether the site is under attack or not.

This discussion of the paper is described as follows: Section II provides related work along with literature survey. Section III describes the diagrammatic view of DOSBAD and DOSBAD structural concept. Section IV describes the proposed approach of security in cloud computing.

2. Related Work

The clouds have been sees no borders in an internet because it is global in scope but respect only established

IJERT

communication paths. People can also access from everywhere for different expected services. Globalization of any computing assets may be the main contribution so that the cloud has made to update. With reference of this reason, the cloud is the criteria of many combinational complex geopolitical issues. Every cloud vendor has to satisfy deliver cloud services to a global market[6]. For example, there will be full-blown applications, support customer services, filtering services and storage services, etc. IT practitioners have also learned to contend with different cloud-based technology services out of necessity things as important business needs dictated and focuses. Cloud computing vendors or suppliers are already available in many cloud points for offering packages of required client products and client-supported services as a single entry point into the cloud area.

Cloud computing has becomes much more be evolved as collection of services[7] which begins to think that what today modern IT always require interms of different kinds of infrastructure, this means that clouds were increase capacity into to their infrastructure dynamically, without investing or paying instant large amount of money in the purchase of new infrastructure Cloud computing can also be viewed as a resource available as a service for virtual server points. Inr Amazon's S3 Storage Service, data storage service is designed and it is available for use across the Internet (i.e., the cloud) for cloud clients [4]. SaaS is another type of cloud computing service that delivers applications to cloud clinets through a internet browser using a multiuser architecture. Platform-as-a-Service (PaaS) is another variation of SaaS. Sometimes it is referred to simply as web services in the cloud, PaaS is very closely to SaaS but it delivers a platform for running of various applications. Grid computing is similar to cloud computing in some aspects but still it is most often confused with cloud computing. Grid computing is in the form of distributed computing that implements a well known virtual supercomputer made up of a cluster of networked computers acting. Many cloud computing emerging technology deployments today are mostly powered by grid computing designs and its implementations and these are billed like utilities for use of rent based services.

Authors of [1] refers about the types of things are expected in the future of cloud computing such as infrastructures, platforms, and software being offered as services. Clouds have some internal characteristics that describe their type, such as "internal" or "external/hosted", and "private", "public", or "hybrid". Because, cloud as either private cloud or public cloud or hybrid cloud. In private cloud, only the organization people can be accessed. Every people can be accessed and use their basic service if it is public cloud.

Cloud is both the hardware and software based structure.

The three classes of utility computing, which is what Cloud users purchase from providers, are defined by three different abstraction levels for resources provided to Cloud users. For low-level abstraction the user has more flexibility with what kinds of applications they want to program but limit the scalability of the application is very limited (it's hard to change the limits on the application if the demand for it suddenly skyrockets above the set limit). For high-level abstraction the user can make things that are much more scalable but not very flexible for general computing since the user cannot control the low-level hardware. Mid-level abstractions provide some aspects of the previous two classes.General-purpose computing and multiple programming languages are available (low-level) and the libraries help provide limited scalability (high-level). Each of these classes have different models for how they provide computations, storage, and networking to users. For now, none of the three classes have proven to be the most useful out of the three. Each of them is ideal for certain situations. Software licensing can becomes a problem because a cloud user may purchase a service and not able to use that service on other computers for self service to other users. Another critical thing is making services out of components or systems, which can be described by different valuable properties such as reusability, substitutability, extensibility, scalability, customizability, composability, reliability, availability, and security. Cloud developers, who are well configured and maintained the frame work of cloud technology, other service authors, who develop templates for required services, valuable service experts are most decidable man power during the stages of cloud implementation. The challenging research issues of cloud computing are getting feedback on cloud workflows, collecting data , storing data, and preventing provenance valuable information, optimum use of cloud service components, extendable service portability, and cloud computing security issues. Authors of [9] describes some specific privacy issues with respect to cloud computing. The main contribution requirements are defined such as minimize the user's data stored on the cloud, protection on data stored on the cloud, limiting the purposes the data and the people may access the controlled data[8].

Authors [11] research work describes that it is very difficult to track down possible bugs in a program that can be used by malicious. In that instance, we observed that denial-of-service attack is initiated. Denial of service (DoS) attacks has always become a major threat to current cloud computer networks.

DoS attacks are to be appeared as illegal actions. Cloud companies have might use DoS attacks to knock off their competitors in the market for ultimate increase of business needs in cloud marketing. All known DoS attacks in the cloud network may conquer the target by exhausting its cloud resources, such as bandwidth, application/service buffer, CPU cycles, etc. Spoofing techniques [5] define how

IJERT

the attacker chooses the spoofed source address in its attack packets. Spoofing attackers can choose one of the three approaches as depicted in Fig. 2.

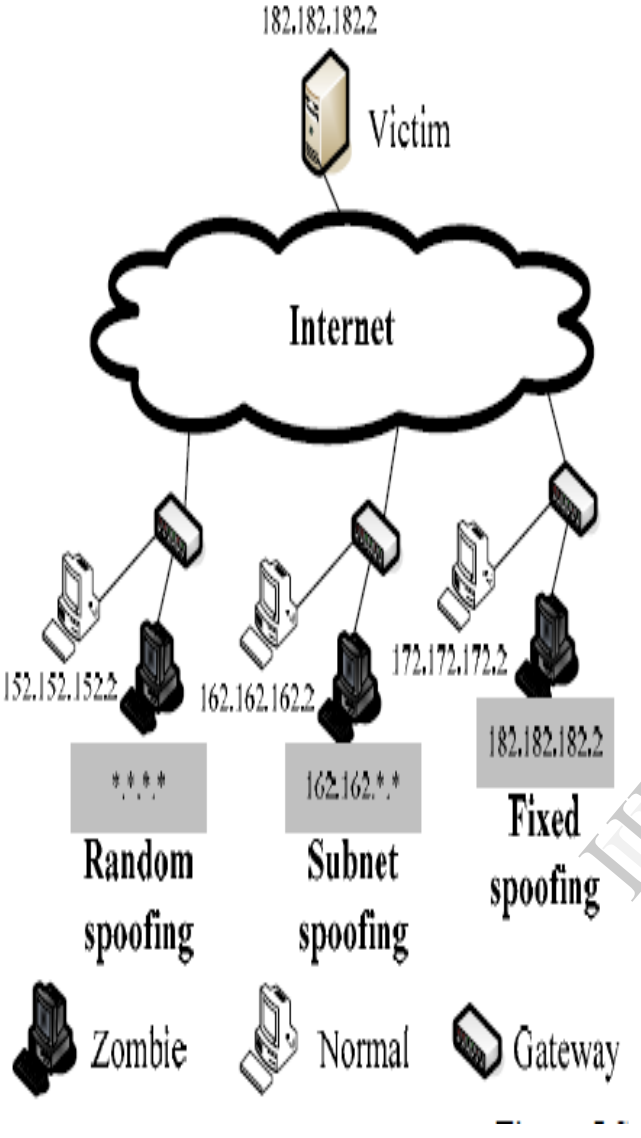

Figure 2: Source Address Spoofing

Known individual attackers can also be exploring his vulnerability, break or crash into target servers for the purpose of brings down cloud services. Finding errors using software to send it random input data to check the resulting output does not always find all these errors, as demonstrated by an experiment in this article. A solution of this paper is to offers a new approach for exploring behavior of various security programs by MACE [2] (Model-inference-Assisted Concolic Exploration). Basically, MACE is inference based algorithm have inference idea of Mealy machine for generating a path to get to that state that is the shortest possible path. Few of limitations of MACE are discussed: It cannot be guaranteed that MACE found ever possible vulnerability, and it was not able to go at kernel level.

With the internet, intrusion attacks are gained sophistication over the time. In beginning, attackers are needed to have a respective in-depth knowledge of computer network cloud system.

III.Architecture of DOSBAD

DOSBAD is frequently measures the available bandwidth along the various paths of the network between routers. A series of 1500 byte packets are passed along the desired path for creating a queue at the router. Two 64 byte packets are sent for down the path. The formula for available bandwidth is as follows:

Available bandwidth = C * (1-((d0-tp)/dl))

Where ‘C’ is the maximum bandwidth of the path, ‘d0’ is the time gap, ‘tp’ is the time to transmit the second packet, and ‘dl’ is the time gap between sending each of the 64byte packets. The proposed architecture model shown as follows.

The packets usually send along the narrowest path in terms of bandwidth in the network, because that is the considered as most vulnerable area in the cloud network. We repeat the process of packet sending once for every second, a trend can be observed and it will be drawn. All incoming packets are going to be encrypted at particular instant, and then DOSBAD cannot check the packets for looking of validity from the content itself. DOSBAD must use packet signature for authentication purpose on the packets which are coming from the suspicious addresses. DOSBAD have store a list of signatures.

DOSBAD is to stores each instance of network traffic will be either to or from a host within the cloud network. At the time of detection of low available bandwidth by DOSBAD, usually DOSBAD can be check dynamic organized data table, checking of various instances of the same source address or destination address. For simple example, we assume there are various instances of the IP address 129.210.5.6 sending packets to the destination within the network of 124.216.78.3. We observed that an acknowledgement is sent out for the first instance of cloud network traffic, and that the other instances from this source IP address is not sent an acknowledgement. It means that 129.210.5.6 is the most likely suspect in launching of DOS attack.

IJERT

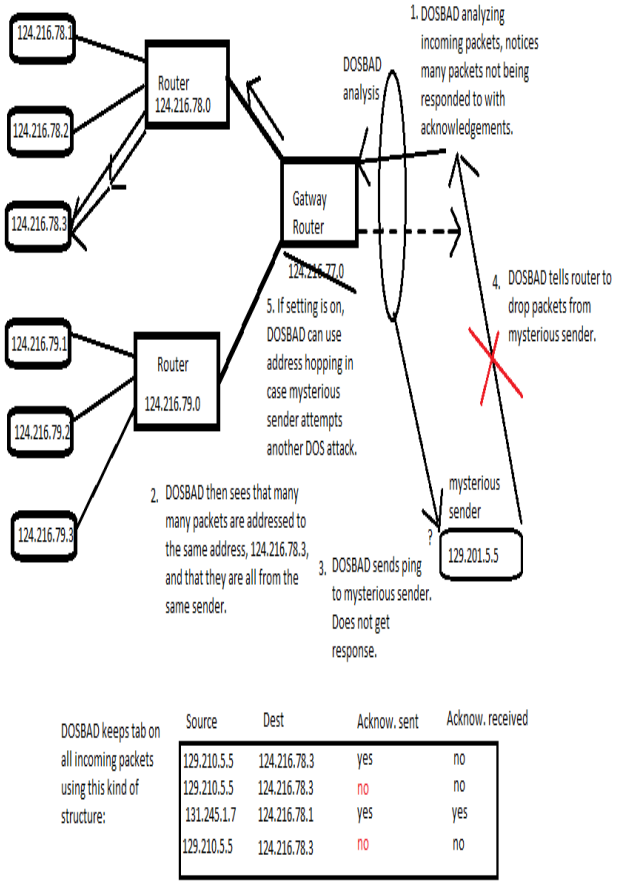

Figure 3: Architecture of DOSBAD

Source (32 bits)	Destination (32 bits)	Acknowledgement Sent (0 for no, 1 for yes) (1 bit)	Acknowledgement Received (0 or 1) (1 bit)	Duration in milliseconds (up to 1 second) (10 bits)
129.210.5.6	124.216.78.3	0	0	301
129.210.5.6	124.216.78.3	0	0	498
131.245.1.7	124.216.78.1	1	1	543
129.210.5.6	124.216.78.3	1	0	782

DOSBAD informs that many packets are being sent to 124.216.78.3. But DOSBAD will also still informs that unreturned acknowledgements things, even in the case of all the source IP addresses are be different. This could indicate a distributed DOS attack against the cloud network. Because of that is not so simple to just dropping the packets from a specific source IP address, so that we see that the DOSBAD will have to check for a 1 on the acknowledgement sent bit with a 0 on the acknowledgement received bit. This will be ensures that DOSBAD is always dealing with one of the specified zombies which is discussed earlier section since they would not be return the acknowledgement.

IV. Implementation on DOSBAD and Its Results Discussion

In this proposed work, the implementation is attempted for the purpose of simulating DOSBAD. Simulations of DOSBAD software analyzing various packets, and which is converting them to understandable organized data tables. It then checks organized data tables with user generated attacks. The implemetation details are represented in the following Fig. 4.

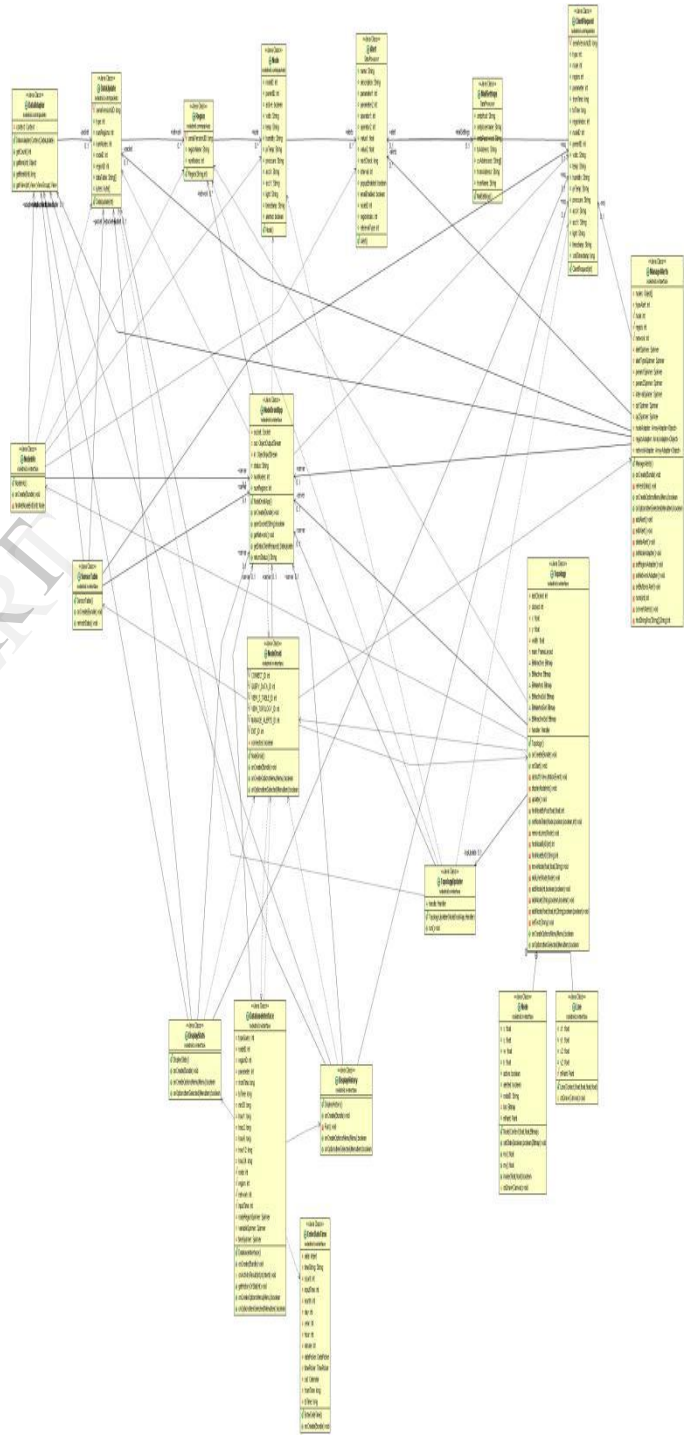

Figure 4: Implementation of DOSBAD

IJERT

Fig.4. shows the classes and methods used in DOSBAD implementation. We use Java object input and output streams for supporting the simulated actions of DOSBAD objects. We successfully initiate and open both streams, but we get a class loader exception when we tried to transmit packets across nodes.

. To accomplish this we have used the following specifications:-

- Windows 7
- Java & Swings

During programming, we have implemented model architecture, namely, view controller (MVC-2) architecture and assume that view is accessible to number of users with playing the action of client side machine, we have a java class called ProtectedServerThread which is acting as a server, in the experiment we are use and accessing packets from the server.

Two type of experiments were implemented and for each experiment we had been tried to follow the same architecture design, also we design a cloud attack and at the same time we tried to find response time of the system in the stage of attack. In the first experiment, DOSBAD does works as a Monitor, DOSBAD have java objects which can be seen as different virtual machines. The thread which is basically acting as protected server in DOSBAD, we would be referring this thread is called as "Thread Server". In this experiment we also track the response time and transaction time. The architecture is a model view controller (MVC), MVC pattern is implemented in java with the object orientation. Hence, architecture point of view, the DOSBAD java based instances will be initiates as a powerful network service which are running on cloud infrastructures for business need inorder to avoid attacks.

In the experiment 2, DOSBAD is acted as a monitor and in this experiment we have projecting various multiple threads which are considered as basic events. In this second experiment we are trying to calculating the response time for multiple events happening at the time of conceptually gives the same environment when a server is under attack.

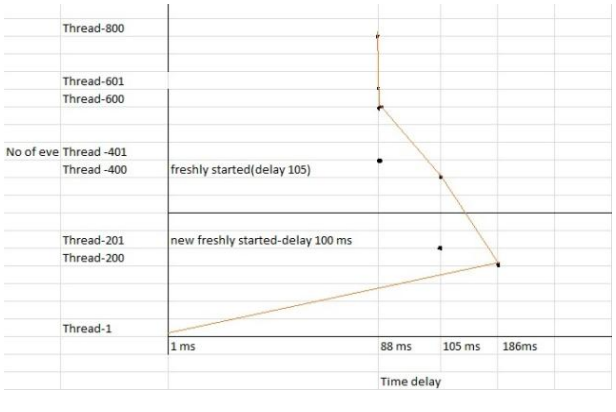

Figure 5: Response Time Delay

Firstly it verifies the available bandwidth. We also defined threshold bandwidth for our testing purpose. This value may be changed based conditions of environment in the cloud network.

The response time delay for each event is shown in the graph Fig. 5.The graph is clearly shows and drawn between number of events and time delay to get the response from the server with respect to each event.

Mathetical analysis for the experiment is as follows:

Assumption

Ab-Available bandwidth
Number of Threads are X;
Eu- End user
Tb=Time before execution
Ta =time after execution,
Tt= transaction time
D= delay

When$\mathrm{Ab} < Tb$ then Eu is valid. If $\mathrm{Ab} > Tb$ then Eu is invalid.

Transaction time for each thread $Tt = Ta - Tb$

Total delay D = transaction time for each event $\times$ number of events

Hence $D = \mathrm{X}(\mathrm{Ta} - \mathrm{Tb})$ or $\mathrm{D} = \mathrm{X} \times \mathrm{Tt}$ (millisecond)

Assuming number of threads = T
And time delay = t
Increase in thread= ΔT and in change in time = Δt [$\Delta\rightarrow$ difference]
From the graph we can substitute the value of ΔT = Thread1 to Thread200 = number of thread is 200
Hence $\Delta\mathrm{T} = 200$
The response time for 200 threads is 1ms to 186ms
$\therefore \Delta\mathrm{T} = (186 - 1) = 185ms$

$$\therefore \frac{increase\ \ in\ threads}{change\ \ in\ time} = \frac{\Delta\mathrm{T}}{\Delta\mathrm{t}} = \frac{200}{185}$$

Hence to derive the equation we can write

$$\frac{dT}{dt} = \frac{200}{185} = 1.08$$

Therefore there will be always time delay will be occurred in the case of the attack.

Fig.6. shows the transaction time by the server under the attack. This graph is to drawn for considering the server is under attacking situation, the java program dynamically creates 100 requests and for each request goes to the server for collecting the file and it return to the cloud end user. For each request the transaction time grows high. For Req -1 and 2 transactions time is 1 ms and for Req 3- Req-4 and the

IJERT

transaction time grows higher when we increase the request number.

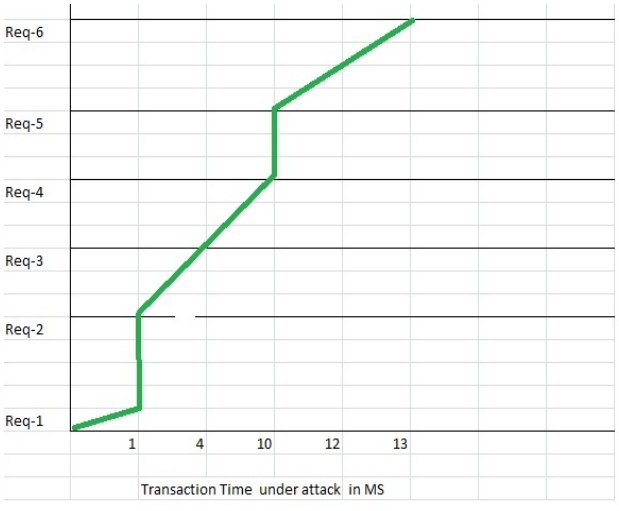

Figure 6

Therefore, we proven in the experiment 2 is that increasing number of request will always have growth and consequently there will be always possible for a time delay under the attacking cases.

V. Conclusionand Future work

The proposed protocol namely, DOSBAD is used to avoid Denial of Service (DOS) attacks in cloud servers and provide quality of security mechanisms. There is scope for integrating DOSBAD into a cloud server and this integrated mechanism can be used to monitor that what ratio of available bandwidth is being used.

This protocol can be extended by improving for its implementation in its actual cloud servers. Different DOS or DDOS attacks can also simulated to make sure that it can be handle multiple attacks scenarios in cloud networks.

IJERT

References:

[1] MA Vouk - Cloud Computing – Issues, Research, and Implementations, Journal of Computing and Information Technology, 2004.

[2] Chia Yuan Cho, DomagojBabic, PongsinPoosankam, Kevin Zhijie Chen, Dawn Song and Edward XueJun Wu, "MACE: Model-inference-Assisted Concolic Exploration for Protocol and Vulnerability Discovery", To appear in Proceedings of the 20th USENIX Security Symposium, (USENIX Security'11)

[3] Jansen, W.A.; Cloud Hooks: Security and Privacy Issues in Cloud Computing System Sciences (HICSS), 2011 44th Hawaii International Conference.

[4] Jinpeng Wei Xiaolan Zhang Glenn AmmonsVasanthBalaPengNing, Managing Security of Virtual Machine Images in a Cloud Environment,CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security

[5] Andreas Berl, ErolGelenbe, Marco Di Girolamo, Giovanni Giuliani, Hermann De Meer, Minh Quan Dang, and Kostas Pentikousis, Energy-Efficient Cloud Computing, Incorporating Special Issue: Architecture/OS Support for Embedded Multi-Core Systems, 2009.

[6] Cong Wang; Qian Wang; KuiRen; Wenjing Lou; Ensuring Data Storage Security in Cloud Computing, Quality of Service, 2009. IWQoS. 17th International Workshop

[7] Cong Wang; Qian Wang; KuiRen; WenjingLou , Improved Verifiability Scheme for Data Storage in Cloud Computing, Wuhan University Journal of Natural Sciences 2011.

[8] Wei Xu , EepBhatkar , R. Sekar, Practical Dynamic Taint Analysis for Countering Input Validation Attacks on Web Applications, 15th USENIX Security Symposium (Vancouver, BC, Canada, August 2006).

[9] Liang Yan, ChunmingRong and Gansen Zhao, Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography, Cloud Computing Lecture Notes in Computer Science, 2009.

[10] Anthony D.Wood, John A. Stankovic,Denial of service in Sensor network, University of Virginia.

[11] Christos Douligeris and AikateriniMitrokotsa, DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION University of Piraeus, Piraeus, Greece.

[12] Ming Luo, Tao Peng, Christopher Leckie, CPU-based DoS Attacks Against SIP Servers,The university of Melbourne

Author Profiles :

1). Mr. Venkateswarlu Maninti has received Master's Degree from Jawaharlal Nehru Technological Univeristy, Anantapur, AP (India). He is currently Lecturer in Information Technology, Fishermen Training Institute, Salalah, Sultante of Oman. He served different levels as a Lecturer at SGPR Govt. Polytechnic, Kurnool, AP (India), Asst. Professor, Associate Professor and Head of the Department of Computer Science and Engineering of Dr. K.V. Subba Reddy College of Engineering for Women, Kurnool, AP (India). His research interest includes Denial of Services in Cloud Computing and Cloud Storate, Grid Computing Network and Wireless Networks & Database applications. He has published 5 peer-reviewed national journal papers, 2 International journal papers. Published IEEE publications and organized national conferences / workshops and also having Microsoft Certification and IBM certification etc..
e-mail: venkateshjournals@gmail.com.

2). Fahmida Begum did his MCA from Osmania University, and pursuing Ph.D from MJPRU , U. P. Her interested areas are mobile computing and cloud computing . I have 9 years experience of Teaching in various colleges. At present she is working as an Associate Professor in Dr. K.V Subba Reddy college of MCA, Kurnool.(Dt).

3]. Manjula Baipireddy working as Asst.prof in CSE Dept. AVRSVR college,she Completed M.Tech from KLC,Vijayawada. Her Research interests in areas are Network Security, image processing, Mobile computing and wireless networks. Mail id:manjula530@gmail.com.

4].Ms.M.N.P.Swetha Priya completed B.Tech(CSE) in 2003 and M.Tech(CS)in 2007 from RGMCET, Nandyal.I have 5 years of experience in teaching. I have published papers both at national and international level in Image processing and an international journal in Networks. My areas of Interest for research include Image Processing ,Data warehousing and Data mining, Computer Networks. I also attended number of workshops related to technical and non-technical. Right now I am working as Assistant Professor in the Department of Computer Science and Engineering at Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Kurnool (Dt.,), A.P. niru_shweta@yahoo.co.in

IJERT