ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Detecting and Preventing the Sneaking of Data by Intruders

Karthikeyan.S, Gayathri.D

Asst. Professor, Dept. of C.S.E., Arunai Engineering College, Thiruvannamalai, India

M.E Student, Dept. of C.S.E., Arunai Engineering College, Thiruvannamalai, India

ABSTRACT: Cloud computing is a style of on-demand computing that provide common dispensation possessions and data to computer and other strategy on demand. cloud accumulate and practice their data in third-party data center. It enable ubiquitous, expedient, on-demand network right to use a common group of configurable compute resource that can be quickly provisioned and released with negligible executive effort. The present accessibility of lofty-capacity networks, low-cost processor and storage policy as well as the common adoption of hardware virtualization, service oriented architecture, and autonomic and service computing have led to a development in cloud computing. company can scale up as computing needs enlarge and then scale down again as load decrease. The purpose of cloud computing is to allocate user to take assistance from all of these technology, lacking the need for deep information about or proficiency with each one of them. Iaas model, the cloud client patch and maintain the operating systems and the function software. PaaS vendor offer a development situation to application developer. Platform as a Service (PaaS) patrons do not supervise the primary cloud infrastructure including system, server, operating system, but have manage over the deploy application and perhaps design setting for the application-hosting environment. Saas model, user gain admission to application software and databases. Cloud provider manages the infrastructure and platforms that lope the application. One drawback of SaaS model storing the users' data on the cloud provider's server. As a result , there might be a unofficial access to the data. DDOS attack is equivalent to a collection of people crowd the entry door and not leasing genuine parties enter into the shop or business, disorderly normal operations. Denial of Service attack is an challenge to formulate a machine or network resource unavailable to the planned user.

KEYWORDS: Cloud Donor, Bot net and Bot Controller, SIPDAS, Recognition Of Surreptitious Attack.

I. INTRODUCTION

Cloud is analogical to internet. cloud computing is an new paradigm that allow user to obtain cloud services and resources according to an pay by use, on –demand and self service , business model. cloud has provide three services Saas, Paas, Iaas .cloud computing introduces paas as a new enhanced model for delivering computing and storage service to end user. saas model makes user be bothered free of installing and running software services on its own machine .Iaas model deliver service to user by maintaining large infrastructure like hosting servers managing network and other resources for clients. cloud computing provide three basic abstraction layer i.e system layer(It is a VM abstraction of a server),platform layer(Virtualized os of the service)and Application layer(Includes Web application).Cloud User don't own the physical Infrastructure rather they rent the usage from the third party provider. They consume resource as a service and pay only for resource that they use. Service level agreement (SLA) regulate the cost that the cloud customer have to pay for the provided quality of service (QOS include Reliability, availability, maintainability) DOS attack aims to make a service unavailable to legitimate clients has become a severe threat to the internet security. DDOS attack has multiple attackers target multiple services that can affect deployed service chain. DDOS attack have been a major hazard to web application and Internet .DDOS attack aim at creating network congestion the application server by generating a large amount of traffic .DDOS attacks are typically carried out at the network layer. DDOS attack can be more effective than the traditional ones. Intrusion Detection System(IDS) are used to identify malicious activities and block the suspicious packet.IDS traces are a series of log data which is often unstructured and typically there is no relation information.IDS as a strong defensive mechanisms.IDS are host based, network based and distributed IDS.HIDS monitors specific host machine. NIDS identifies intrusion on key network points and distributed IDS (DIDS) operate both on host as well as network. Most of the method cannot concurrently realize.

- proficient recognition with a small number of false alarms.
- Real-time transfer of packets.

The last ten years, many efforts have been devoted to the detection of DDoS attacks in distributed systems. Protection avoidance mechanism regularly use approach based on rate controlling, time-window, worst-case and pattern matching method to separate between the nominal system operation and malicious behaviors. The attackers are aware of the presence of such protection mechanisms. This Paper offers a solution to detect DDOS attacks early and recognize the attack originating service to isolate it and protect other service in the service cloud. Service can detect DDOS attack by watching the number of message received from other services. SIPDAS (Slowly Increasing Polymorphism DDOS attack Strategy).Intruder uses SIPDAS attack strategy in DDOS perform attack..Using SIPDAS, Bot master perform attack through attacker bot. Attacker bot call URL (user request location) simultaneously requests the server, if the process continuous resource are unavailable to the user. Using SIPDAS mean slow down the performance of the server and also affecting the financial of customers.

II. RELATED WORK

Sophisticated DDoS attack is defined as that group of attacks, which are modified to hurt a specific weak point in the intention system design. In order to perform denial of service or just to considerably corrupt the performance. The term stealthy has been used to recognize sophisticated attacks that are explicitly designed to keep the hateful behaviours virtually imperceptible to the detection mechanisms. These attacks can be considerably harder to detect compared with more usual brute-force and flooding style attacks. The methods of initiation sophisticated attacks can be categorized into two classes: jobs arrival pattern-based and job-content-based .The earlier have been planned in order to achieve the worst-case complexity of lying on uncomplicated operations per submitted job, instead of the average case complexity of lying on. The jobs arrival pattern-based attacks develop the worst case traffic arrival pattern of requests that can be practical toward the reason system. In broad such difficult attacks are performed by transfer a low-rate traffic in arrange to be unnoticed by the DDoS detection mechanisms. In current years, variants of DoS attacks that use low-rate traffic have been planned, together with Shrew attacks (LDoS),decline of Quality attacks (RoQ), and Low-Rate DoS attacks against application servers. The expressions ‘stealthy DDoS’ mainly refers to Shrew attacks first introduced which was followed by a series of connected investigate. It refers to intermittent, pulsing, and low-rate attack traffic against the TCP protocol. This is obtained by transfer high rate but short-duration bursts, and repeating occasionally at slower RTO time-scales. RoQ attacks target the active operation of the review mechanisms widely adopted to make sure that the workload would be distributed across the system income to optimize the overall arrangement. By using a detailed attack pattern, RoQ induce stable oscillations between the overload and under load states, without behind the attack traffic. It is achieved by time the hit traffic and its amount in order to exploit the dynamics of the system. Specifically, LoRDAS attacks have no essential deviations in terms of network traffic volumes or traffic distribution with value to normal traffic. Due to its high similarity to legal network traffic and much lower initiation overhead than classic DDoS attack, this new beating type cannot be efficiently detect or prohibited by open network-based solution Therefore, in current years, the objective of DDoS attack has shift from arrangement to application server resources and actions Several LoRDAS assail model subsequently to application server have been intended. In exacting, they aim at keeping the package queue of the target application servers totally full of requests future from the attacker, so that any new incoming request sent by legitimate users is leftover.

2.1.Cloud Resources Provisioning:

Cloud providers propose services to rent working out and storage capacity, in a way as obvious as possible, giving the idea of ‘unlimited resource availability’. However, such resources are not free. Therefore, cloud providers allow clients to attain and configure correctly the system capacity, as well as to quickly renegotiate such capacity as their needs change, in direct that the clients can pay only for resources that they actually use. Several cloud provider recommend the ‘load balancing’ service for mechanically distributing the incoming application service needs across multiple instance, as well as the ‘auto scaling’ provision for enable consumers to closely follow the order curve for their application. The auto scaling ensures to facilitate the number of the application instance increases easily during the demand spikes (to maintain the constricted performance), and decreases repeatedly during the exact lull. For example, by using Amazon EC2 cloud services, the consumers can set a form to add new computational instances when the standard CPU utilization exceeds a fixed entry. Moreover, they can coordinate a cool-down stage in order to permit the application workload to steady before the auto scaling adds or removes the instances. It will show how this characteristic can be maliciously broken by a stealthy attack, which may slowly drain the resources provided by the cloud provider for ensure the SLA, and improve the costs incur by the cloud customer.

2.2. The mOSAIC Framework:

The mOSAIC project aimed at offer a simple way to expand and manage applications in a multi-cloud environment. It provides a structure composed of two main components: the cloud group and the software platform. The cloud agency act as a provisioning system, brokering resource from a grouping of cloud providers. The mOSAIC user develops the application on its local machine, and then it uses a local occurrence of the cloud agency in order to start-up the process of remote resource achievement and to deploy the Software Platform and the developed application. The Platform enables the execution of the developed application on the acquire cloud resource.A Java-based API is provided to extend software components in the form of Cloudlets. A mOSAIC application is a set of Cloudlets, which are unified through communication resource, such as queue or shared key value stores. The Cloudlets run on a committed operating system, named mOSAIC Operating System (mOS), which is a small Linux distribution. At runtime, the Software Platform obviously scales the Cloudlets instance on the acquire virtual machines (VM) on the base of the resource consumption (auto scaling). For example, when the Platform detect that a Cloudlet is burdened (e.g., it has too messages on the intercommunicating queues), it may choose to start a new Cloudlet occurrence. The Platform assumes such a result on the base of policies defined by the application developer. Finally, a load balancing mechanism repeatedly balances the application service requests among the instances.

III. PROPOSED SYSTEM

In this paper four modules are used to describe the system architecture. They are as follow

- **Cloud Donor**
- **Botnet and Botcontroller**
- **Slowly Increasing Polymorphic DDOS Attack Strategy**
- **Recognition Of Surreptitious Attack**

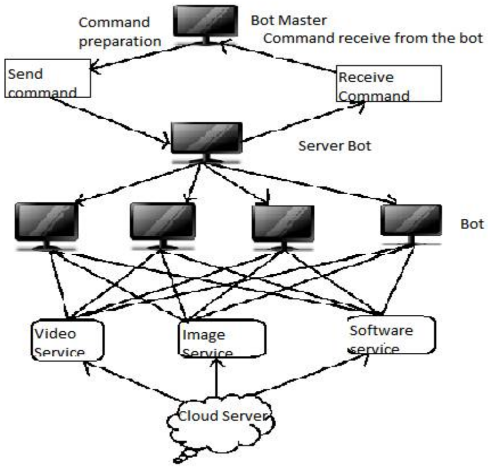
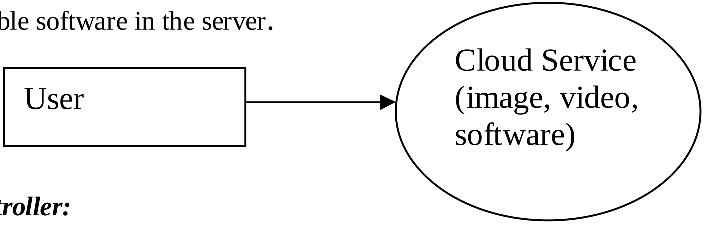


Fig 1. System Architecture

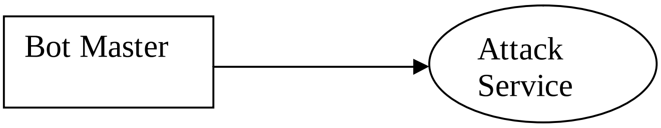
Cloud Donor:

The cloud server provides the services like video, image and software. The cloud service provider enables to user can upload and download above services. The video service is used to provide the video which is visible to all that we can also download and play the video. The image service used to view the image. The software service is used to download the available software in the server.



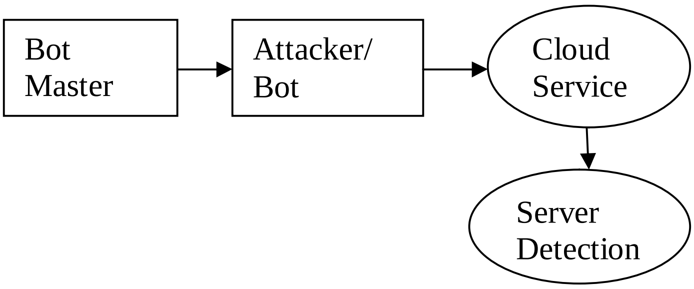
Botnet and BotController:

A Bot is kinds of malware that allow an invader to take manage over an affected computer. Bots are usually part of a network of infected machines, known as a Botnet. Botnets are controlled by Botmaster. Whenever clients call Botmasters at that time bots are created. Those clients are called attacker. In an existing approach, the DDoS detection mechanism is used to identify number of request given by the user in an particular IP address. The attacker is used to attack the server by using the genuine user IP address and attacker gives the large number of request to that server with a same IP address. The DDoS detect that attack by monitoring the largest number of request is given by the same IP address in a certain time is considered to be a DDoS attack and that particular IP is blocked by the server.



Slowly Increasing Polymorphic DDOS Attack Strategy:

SIPDAS (Slowly Increasing polymorphic DDoS Attack Strategy) can be applied to several kind of attacks that leverage recognized function vulnerabilities, in arrange to disgrace the check provided by the target application server running in the cloud. The term polymorphic is stimulated to polymorphic attack which change message sequence at every successive infection in categorize to avoid signature recognition mechanisms. Using SIPDAS, Botmasters perform attack into cloud through bots. Bots create URL, to call cloud for slow their process. If this process continues, cloud performance is slow and it does not response any other client's request. We detect the SIPDAS in cloud server side. In a stealthy DDoS Detection mechanism, the server maintains the records of the request given by the user. If the Server loads increases it checks the each individual request of an user, if the request given by the user exceeds the server limit, that particular user IP address is blocked, and the service is denied to that user.



Attack Detection:

In this module, in an existing approach, the DDoS detection mechanism is used to identify number of request given by the user in an particular IP address. The attacker is used to attack the server by using the genuine user IP address and attacker gives the large number of request to that server with a same IP address. The DDoS detect that attack by monitoring the largest number of request is given by the same IP address in a certain time is considered to be a DDoS attack and that exacting IP is infertile by the server. In a crafty DDoS Detection mechanism, the server maintains the records of the request given by the user. If the Server loads increases it checks the each individual request of an user, if the request given by the user exceeds the server limit, that particular user IP address is blocked, and the service is denied to that user. Heap Space Monitoring algorithm is used to identify number of request given by the user in an particular IP address.

ALGORITHM:

```
 if!(attackSuccessful)then
 CR=(CR + attackIncrement);
Else
 while!(attack_detected) and attackSuccessful
 tI=computeInterarrivalTime(CR,nT);
Service  degradation achieved.
if attack_detected then
 print  'Attack_detected';
 Notify to the master that the attack has been detected.
 CR=CR-attackIncrement;
```

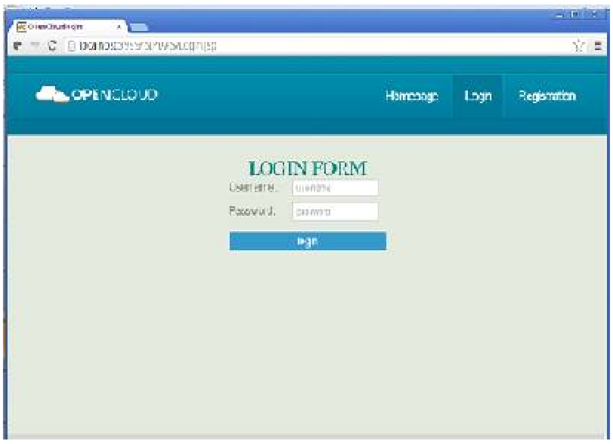
- The server maintains the records of the request given by the user.
- The attacker is used to attack the server by using the genuine user IP address and attacker gives the large number of request to that server with a same IP address.

IV. EXPERIMENTAL RESULTS

Distributed DoS (DDoS), aim at reducing the service availability and performance by exhausting the resources of the service's Host system. Even though a Denial of Service attack can be tremendously harmful to your business/website. It accounts for the maximal presentation degradation (damage) that sophisticated attackers can cause on the system using a specific amount of resource, normalized by the performance degradation credited to regular user.

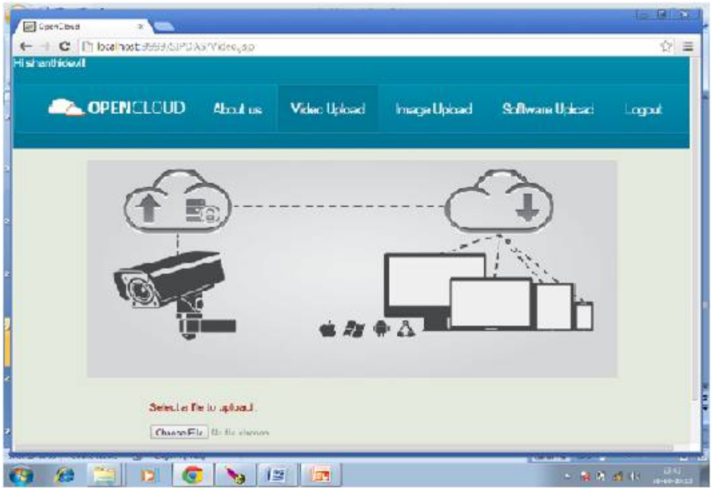
(a)Login form:

User login the login form then only service are available to the user to process the system.It provide application and storage services on remote servers.It works on the concepts of virtualization of resources. High volume of data in cloud environment could be handled by a single node IDS through a multi-threaded approach.



(b) Upload files:

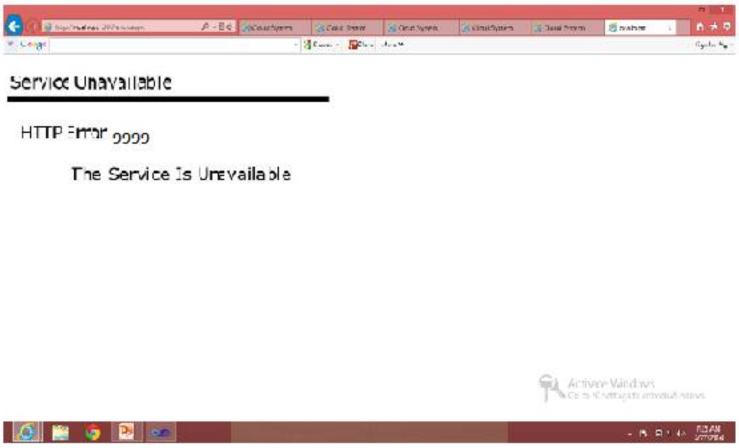
The cloud server provides the services like video, image and software. The cloud service provider enables to user can upload and download the services. The video service stores all of the user video. The site allows users to upload and view videos.



(c) Attack occur:

Using SIPDAS attack Strategy , Bot call the URL to take control over an affected computer. Bot are usually part of network of infected machine called Botnet. If you've system your website to hold 10,000 immediate visitors, the hacker can fetch your website down by simulate 100,000 concurrent visitors.

- Website-error message.
- Down the server



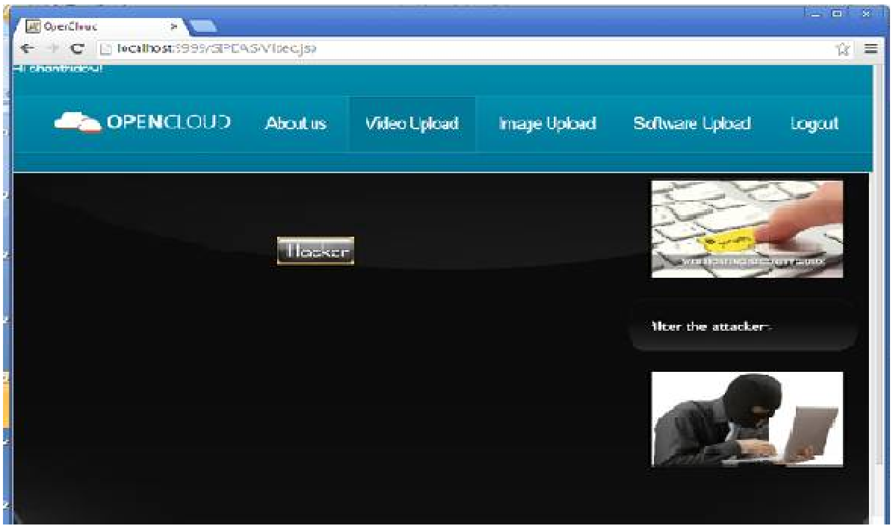
Service Unavailable

HTTP Error 9999

The Service Is Unavailable

(d) Detecting the Attacker:

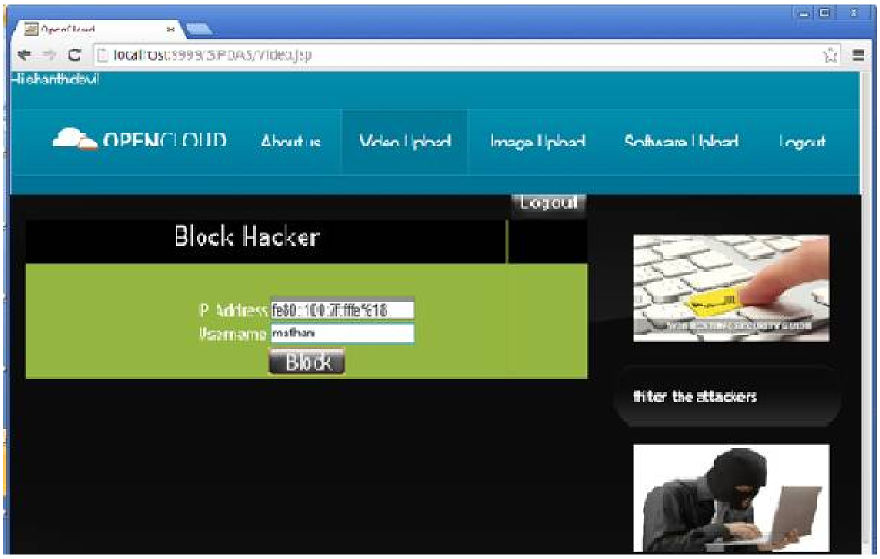
Cloud IDS handles large flow of data packet analyse them and generate reports efficiently by integrating knowledge and behaviour analysis to detect intrusion. The IDS (Intrusion Detection System) Monitors the whole website management and generate the reports simultaneously by which the hacker can be detected.



Alter the attacker-

(e) Blocked the Malicious Process:

Attackers can initiate DDoS using botnets, also known as a zombie army, which are sets of computers that can be used to simultaneously flood a target server with network traffic. The reports are analysed and the hacker is detected using IP address. Finally all these details are maintained in MYSQL Server.



P Address fe80::100:7f:fffe%18
Username mathan

V. CONCLUSION AND FUTURE WORK

There are lots of kinds of hackers on the Internet, with a wide range of hacker skills. You may have read of sophisticated illegal earrings phishing scams, etc. which are irritated by profit. DDOS are the major threats in the Internet and Web application .It exhibit a slowly-increasing polymorphic DDOS attack strategy detected using Heap Space Monitoring. Even though a Denial of Service attack can be tremendously harmful to your business/website . Easily be setup by an inexperienced hacker with limited technical ability It aims at exploiting the cloud flexibility, forcing the services to scale up and consume more resources than needed and also satisfied the customer expectation.

REFERENCES

[1] Massimo Ficco and Massimiliano Rak "Stealthy Denial of Service Strategy in Cloud Computing,"2015.

[2] Sarra Alqahtani, Rose Gamble "DDoS Attacks in Service Clouds",2015 48th Hawaii International Conference on System Sciences.

[3] Suaad Alarifi,Stephen D.Wolthusen,"Mitigation Of Cloud Internet Denial Of Service Attacks",2014 IEEE 8thInternational Symposium .

[4] shin –ying Huang Yennun Huaang, "Event Pattern Discovery On IDS Traces Of Cloud Service",2014 IEEE Fourth International Conference.

[5] Chun-Jen Chung, Student Member,Pankaj Khatkar, Student Member, Tianyi Xing,Jeongkeun Lee, Member and Dijiang Huang Senior Member, "NICE: Network Intrusion Detection and Counte rmeasure Selection in Virtual Network Systems".2013

[6] Yiduo MEI, ling LIU, senior MEMBER,xing PU, "Performance Analysis Of Network I/O Workloads in Virtualized Data Centers",2013

[7] Haishan Wu ,Asser N.Tantawi,Tao Yu ,"A Self Optimizing Workload Management Solution For Cloud Applications",2013 IEEE 20th International Conference.

[8] M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson,"Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. CloudComput. Serv. Sci., 2012.

[9] Ms.Parag,K.Shelka,Ms.SnehaSontaka, Dr.A.D.Gawanka,"Intrusion Detection System For Cloud Computing",2012 International Journal .

[10] VeronikaDurcekova,Ladislav Schwart,"Sophisticated Denial Of Service Attack Aimed At Application Layer",2012.