International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 6,June 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Hypervisor Based Intruder Detection in Cloud Environment

Tarun A.Saluja [1], Jay Vala [2], Bhargesh Patel[3]

[1]*Information Technology, PG Scholar, G.H.Patel College of Engineering*
[2]*Information Technology, Assistant Professor, G.H.Patel College of Engineering*
[3]*Information Technology, Assistant Professor, G.H.Patel College of Engineering*

Abstract— Cloud computing is becoming much popular due to many of its advantages like high performance, distributed computing, high security, pay per use modules etc. . . . Cloud is evolved from simple networking applications. Grid/Cluster/Utility Computing helped formation of basic infrastructure as a service concept. Distributed concurrent and parallel processing with service oriented architecture set a platform for virtualization of resources, making cloud computing possible.
The cloud computing model has the ability to scale computer resources on demand, and give users a number of advantages to progress their conventional cluster system. In addition, there is no upfront investment to update infrastructure, labour and no ongoing expenses.
Virtualization, which allows multiple Virtual Machines (VMs) to reside on a single physical machine, has become an indispensable technology for today's IT infrastructure. It is known that the overhead for virtualization affects system performance; yet it remains largely unknown whether VMs are more vulnerable to networked Denial of Service (DoS) attacks than conventional physical machines. A clear understanding here is obviously critical to such networked virtualization system as cloud computing platforms.
The problem we see is recurrence of the same mistakes that were made with the development of the internet. These mistakes were related to functionality and performance which took precedence over security.

Keywords- Cloud computing, Networking, Types of attack

I. INTRODUCTION

In this section we are going to elaborate the introduction about the cloud computing, properties, its advantages, Types of service provide by the cloud, its architecture and Types of cloud. And further in this section we also going to elaborate about the attacks, Types of attack and what are the effects of attack on cloud environment.

1.1 Cloud Computing:-

Cloud computing refers to a large group of interconnected computers. These computers can be personal computers or network server; they can be public or private. Cloud computing is internet-based computing where by shared resources, software's and information provided to computers and other devices on demand through internet.
It starts with the front-end interface seen by individual users. This is how users select a task or service. The user's request then gets passed to the system management, which finds the correct resources and then calls the system appropriate provision services. These services carve out the necessary resources in the cloud, launch the appropriate web application and either creates or opens the requested document. After the web application is launched, the system monitoring and metering function track the usage of the cloud so that resources are apportioned and attribute to the proper users.[1]

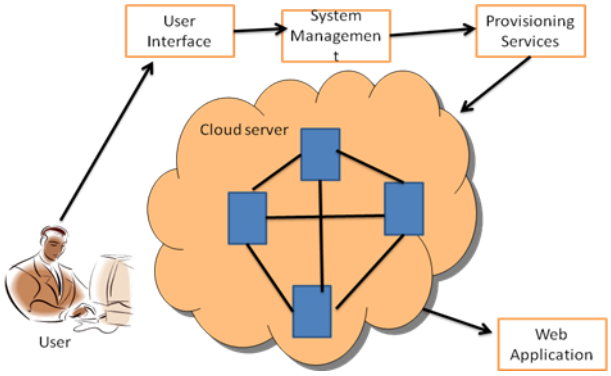

Figure 1:- Cloud computing and its architecture

1.1.1 Types of Cloud Services:

Figure 2:- Cloud service

- **IAAS(Infrastructure As A Service)**

Rather than purchasing or leasing space in an expensive datacenter, labor, real estate, and all of the utilities to maintain and deploy computer servers, cloud networks and storage, Cloud buyers rent space in a virtual data center from an IaaS provider. They have access to the virtual data center via the Internet. This type of cloud computing provides the "raw materials" for IT, and users usually only pay for the resources they consume, including (but not limited to) CPU cores, RAM, hard disk or storage space, and data transfer – example IaaS providers include ProfitBricks, Amazon EC2, or the Rackspace Cloud. All three providers allow users to "rent" virtual servers and storage while creating networks to tie them all together .[2]

- **PAAS(Platform As A Service)**

Platform as a Service (PaaS) is a delivery of a computing platform over the web. PaaS enables you to create web applications quickly, without the cost and complexity of buying and managing the underlying software/hardware. PaaS provides all the facilities required to support the complete life cycle of building and delivering web applications entirely on the web. [3]

- **SAAS (Software As A Service)**

Cloud Applications or Software as a Service (SaaS) refers to software delivered over a browser. SaaS eliminates the need to install and run applications on the customer's own computers/servers and simplifies maintenance, upgrades and support. Examples of SaaS are Face book, Sales Force, Base Camp, etc. [4]

1.1.2 Types of Cloud

- Public
- Community
- Private
- Hybrid

1.1.3 Attacks[1]:-

Attack:-

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. [5]

Types of Attacks:-

Some attacks are **passive**, meaning information is monitored; others are **active**, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

There are so many attacks but some are mention below:-[6]

A. Data Modification

After an attacker has read the data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if no confidentiality for all communications is required, a user does not want any messages to be modified in transit.

B. Eavesdropping

In general, the majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, data can be read by others as it traverses the network.[6]

C. Identity Spoofing (IP Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete data.

D. Denial-of-Service Attack

The denial-of-service attack prevents normal use of your computer or network by valid users. After gaining access to network, the attacker can do any of the following

- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.[6]

E. Sniffer Attack

A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze the network and gain information to eventually cause the network to crash or to become corrupted.

- Read communications.[6]

II. PROPOSED WORK:-

Hypervisor, as it is a heart of the system if a user is sending request for particular resource continuously, the hypervisor is going to stay busy for the allocation of a resources.
But at certain level the particular user can be denied from sending more request because if the request comes continuously than hypervisor is going to stay busy in either start the service or stop the service, so this scenario is known as DDOS attack
The uniqueness of the work is that till now the attacks have been made on particular website but in our work the scenario is what will be the consequences on system when the attack is made on the hypervisor.

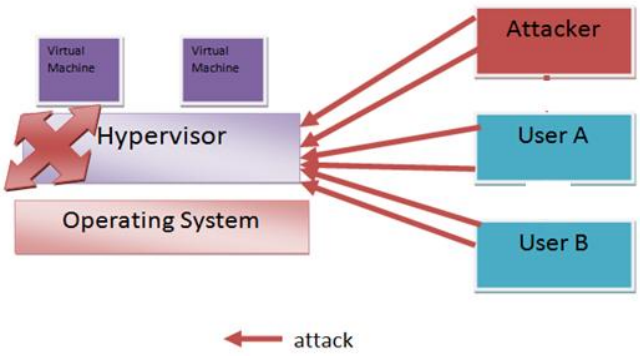

Figure 3:- Attacking Scenario on System

III. EXPERIMENTAL ANALYSIS AND RESULTS

To carry out our simulation process we used wireshark which is the network analysis tool by which we can get the detail information regarding the packets transferred from destination to source & also we can fetch the detail from which IP address the maximum number of packets are transferred.
Along with wireshark we use shorewall to block the particular IP address from where the maximum number of request or packet transferred/received.

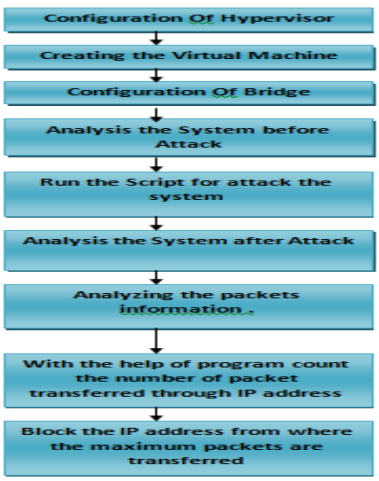

Figure 4:- Simulation Steps

For the simulation we must follow the steps which we discussed in the given figure.

Step 1:- is used to configure the Hypervisor which is the heart of Cloud.
Step 2:- Creating the virtual Machine
Step 3:- Configuration of bridge, it works as a interface between host OS and Guest OS
Step 4:- Analysis of system in normal scenario i.e how normal system works.
Step 5:- Run the Script for attack which just increase the traffic.
Step 6:- Analysis the effect of the script /attack on system.
Step 7:- Analysis the TCP packet information i.e. how many packet is transferred by particular IP.
Step 8:- Run the program/script to fetch the unique IP who is sending maximum packet among all and compare it threshold value.
Step9:- Block that particular IP.

IV. RESULTS

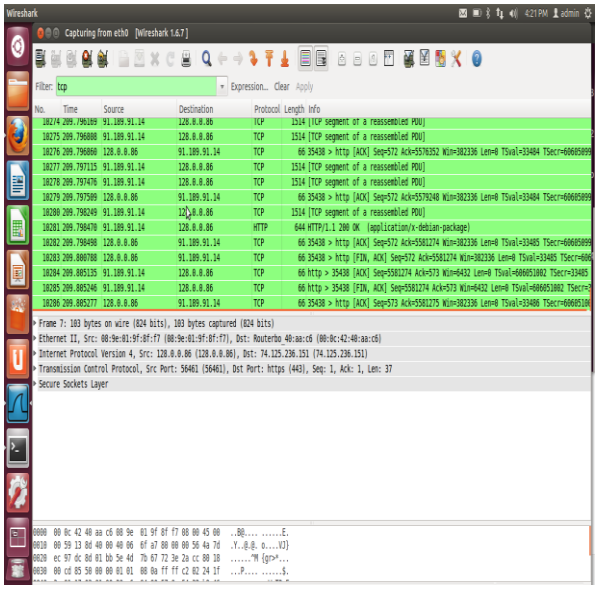

Figure 5:- Results before Attack

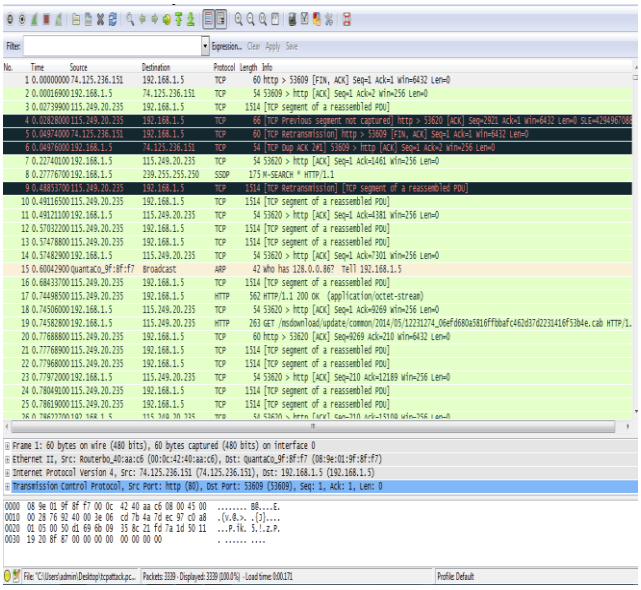

Figure 6:- Results after Attack

Figure 7:-Flowchart before Attack

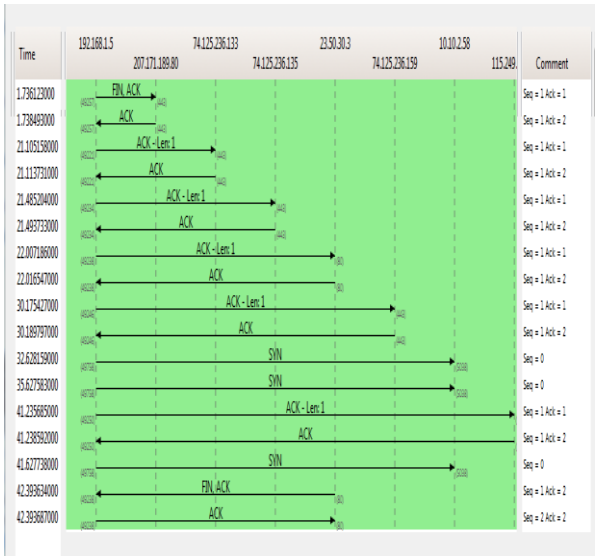

Figure 8:- Flowchart after attack

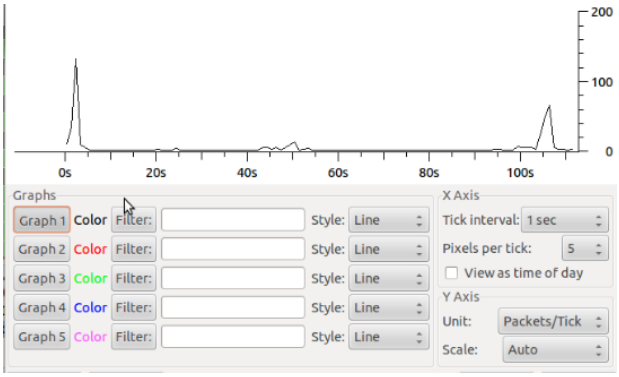

Figure 9:- Graph before attack

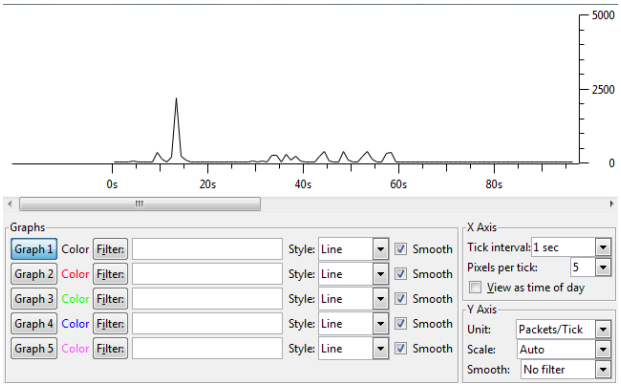

Figure 10:- Graph after Attack

V. CONCLUSION AND FUTURE WORK

As it is a world of internet now a day's technology is increasing day by day, so there are many advantages of internet but at the same time there are certain disadvantages also. Among so many disadvantage one of the disadvantage is that of attacks on your system/server i.e. suppose the user is requesting for certain service the request can be processed with the help of hypervisor and the user get the appropriate response for his/her request, but if the user is sending so many request the hypervisor get confused regarding which service need to start or which service need to be stop. So in this case the hypervisor will block the particular user from sending the request for the resources. User can be blocked with the help of block the IP address or by blocking the MAC address of the user.

From the work done till now we concluded that there is vast number of attack is possible when it comes to large network and as we are using the linux based server there is no such kind of inbuilt security system by which we can stop the attack. So if the attacker is attacking on your system or server we can able to detect the IP address of the particular user/attacker and also analyze the number

of TCP packet transferred or received by the user. After fetching the address of the attacker with the help of detecting technique which is specified earlier in report we can also able to block the attacker from sending the packets.

So with the help of our work we can analyze the number of packet transferred and also able to get the address of the attacker and later on we can block the particular attack from sending the request.

In future work , the user can try to analyze the different protocol of the network which are available and also try to a new technique to identify the attacker and later on the user can also generate his/her own rule to block the attacker.

REFERENCES

[1]. Tarun A.Saluja, Jay Vala, Aniruddha Kurtkutti, "Survey of DDOS attack in Cloud Environment" in IJRIT, International Journal of Research in Information Technology, Volume1 Issue1 Jan 2013
[2]. https://www.profitbricks.com/what-is-iaas
[3]. http://www.zoho.com/creator/paas.html
[4]. http://www.wolfframeworks.com/cloudcomputing.asp
[5]. http://en.wikipedia.org/wiki/Attack_(computing)
[6]. http://technet.microsoft.com/en-us/library/cc959354.aspx#mainSection

