Virtualization Intrusion Detection System in Cloud Environment

Ku.Rupali D. Wankhade.
Department of Computer Science and Technology

Abstract - Nowadays all are working with cloud Environment(cloud computing). The massive jumps in technology led to the expansion of Cloud computing as the most accepted medium for communication but it has also increased the scope of attacks. To providing a security in a Distributed system require user authentication password or digital certificates in data transmission. To handle laege amount network accessin traffic and administrative control of data and application in cloud, So security has become a major issue for Cloud Environment. Intrusion Detection Systems have become a needful component in terms of network security. Cloud Computing environment is threatened by different types of cyber-attacks. The proposed architecture provides implementation of Suricata intrusion detection system to secure virtualized server in cloud platform and validated intrusion detection system in detecting DDOS attack against the virtualized environment and protect cloud efficiently from vulnerability. In this paper, we will study basics of Cloud Computing, Type of IDS for securing virtualized server, Existing techniques to detect intrusions and threat in cloud environment and Virtualization based Intrusion Detection System in cloud environment.

Index Terms- Cloud Computing, Intrusion Detection System(IDS),Virtualization,Network setup,Suricata.

1. Introduction

Cloud computing is an internet based computing system where virtual shared servers provide Infrastructure, Platform, Application , Elastic resources , devices and hosting to customer as a service on "pay-as for-use" basis. Cloud computing is the delivery to demand network access to a shared pool of configurable computing resources everything from applications to Data Centers to the help of the Internet. The Cloud Computing infrastructure stores the software, application and data. Cloud applications are accessible from any device, including a laptop, cell phone and smart phone, when this application is connecting to the internet, which are showing in fig 1.

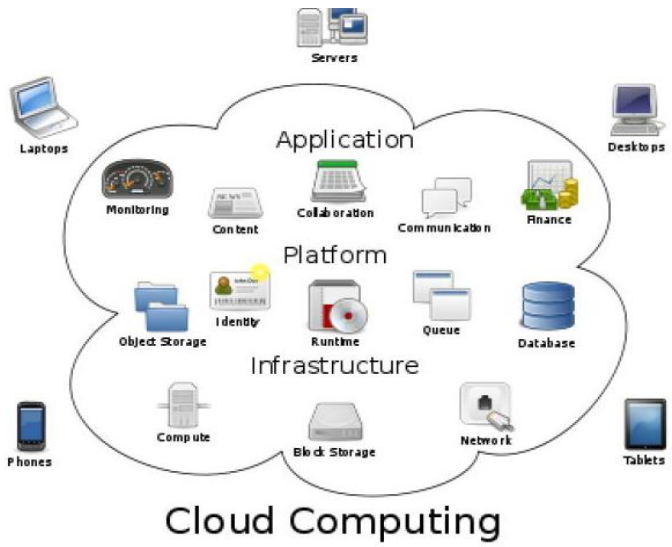

Figure 1: Cloud Computing Infrastructure

Virtualization is an essential technique in cloud computing Environment, to providing different type of resource infrastructure for cloud clients; it delivers the resources by deploy virtual machines over the virtual machine monitor, also known as the hypervisor. Virtualization is the mainconcept in the cloud because the complexity avoid through virtualing the hardware and software.

There are various threats that can affect the virtualization in the cloud environment like DDoSattack,becauseimpotant data in cloud is protracting to any instructing. The instruction detection technique used to detect threats and attacks in cloud or virtualized server. Intrusion detection is a strong mechanism plays important role in securing networks. However, virtualized server in cloud environment carries a huge amount of traffic, therefore implementing Intrusion Detection System (IDS) in a cloud environment requires scalable and virtualized infrastructure. This paper is organized as follow:

1.1 discusses intrusion detection techniques and methods for cloud environment .

1.2 Types of IDS for securing virtualized server.

1.3 Anexisting system. 4 describe and design virtualized based IDS in the cloud environment,Finally conclusion.

2. Intrusion Detection System

Intrusion detection systems (IDS) are an essential component of protecting computer systems and network. To detect computer attacks and provide the proper response this is the main aim of IDS. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network. There are mainly two categories of IDSs, network based and host based. IDS is key to detect and possibly prevent activities that may compromise system security, or some hacking attempt in progress including data collection phases that involve for example, port scans. Once an intrusion has been detected IDS issues alerts notifying administrators. The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) – following the organization's security policy (Figure 2). An IDS is an element of the security policy

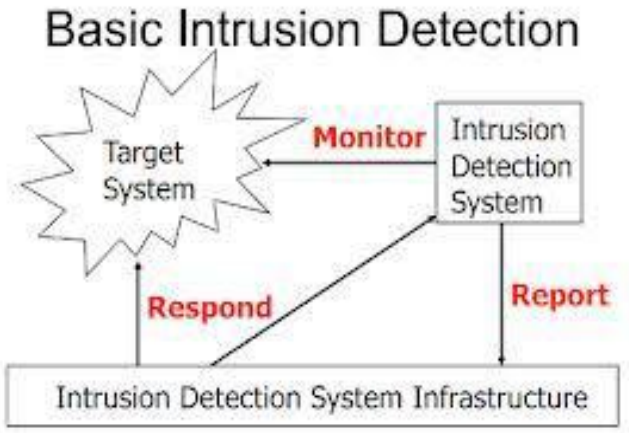

Fig 2.Intrusion Detection System Infrastructure

2.2.1 Signature Based Detection

Signature-based detection is also known as Pattern-based detection, which detects attacks based on the signature. In general, the signature-based detection method is not used to detect latest attacks because no matched rules or patterns have been configured. This type of detection method can be used in the host based or network based IDS. Therefore, in the cloud environment, signature-based detection can be used in virtual machines, hypervisors or virtual networks to monitor the activities and detect attacks.

2.2.2 Anomaly Based Detection

Anomaly detection refers to detection performed by detecting changes in the patterns or behavior of the system. It can be used to detect predefined known and unknown attack. Anomaly Detection identifies abnormal behavior (anomalies). At the start, anomaly-based detection constructs a clear view of the normal behavior of users, hosts or network segments, then it sends alert if new events occur that contradict the normal behavior. In the cloud environment, anomaly-based detection uses different models to determine unusual behavior such as old detection, statistical model, rule-based model, and other

models, including neural networks, genetic algorithm, and immune system model.

3. Types of IDS for Securing the virtualized Server

3.1 Host-based IDS (HIDS)

This type of IDS involves software components, which is run on the server, router, switch or network appliance. However, the agent versions must report to a console or can be run together on the same host as depicted in Fig 3. Basically, HIDS provides poor real-time response and cannot effectively defend against one-time catastrophic events. HIDSs are much better in detecting and responding to long term attacks of data. AHost-based IDS basically monitors the incoming and outgoing packets from the computer system only and to alert the user or administrator suspicious activity is detected. The suspicious activities like system call, processes and configuration access observing by host. It is used to protect valuable and private information on server systems. HIDSs are able to assign as NIDS(Network base IDS) if they are installed on a single host and configured to detect network activities.

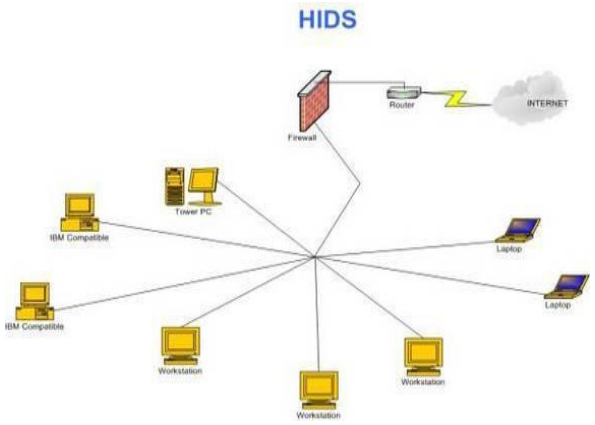

Fig 3 Host Based Intrusion Detection System

3.2 Network-based IDS (NIDS)

Network-based IDSs (NIDS) can observe, monitor and analyses the specified and pre-identified network traffic. This type of IDS captures network traffic packets such as (TCP, UDP and IPX/SPX) and analyzes the content against a set of RULES or SIGNATURES to determine if a POSSIBLE Occurrence took place. It can detect different conditions on specified points and placed between the end point devices like firewalls, routers. A NIDS is intrusion detection systems that discover unauthorized network by analyzing the network traffic for signs of malicious activities and events. Network traffic delivers the data coming from a layer to another layer. NIDS can be implemented on the cloud server which interacts with the external network (user network) to detect attacks against virtual machines and hypervisor. NIDS detects attacks by inspecting the IP and transport layer headers of each packet. One of the limitations of NIDS is that it may not be useful if an attack occurs within a virtual network which runs inside the hypervisor.

3.3 Hypervisor IDS

This is designed and used for hypervisors only; it also monitors communication between virtual machines, communication between virtual machines and the hypervisors, or communication within the hypervisor. The advantage of hypervisor IDS is that it provides information availability.

4. Existing of Cloud IDS Model

4.1 Distributed Cloud Intrusion Detection System

A large number of data packets flow in cloud environment using multi-threaded IDS approach. The IDS would pass the monitored alerts to a third party monitoring service, who would

directly inform the cloud user about their system is under attack. The third party monitoring service would also provide expert advice to cloud service provider for misconfigurations and intrusion loop holes in the system. The user can accesses its data on servers at service provider's side over the cloud networks. Among various IDS tasks, intruder identification is one of the fundamental ones. cloud user with an expert advice for cloud service provider.

Problems identified in Existing System

1. Difficult to detect network intrusion in virtual network and detect intrusion from encrypted traffic.
2. IDS sensors are deployed at many places that reduce the performance of overall system.
3. It cannot detect insider attack as well as known attack since only snort is used.

5 Proposed Architecture

5.1 Position in the cloud to deploy IDS

A IDS having the characteristics of virtualization to provide better security in cloud. This model provides the advantage of virtualization of IDS model. The IDS can be deployed in the cloud at the front end, at the backend or in the virtual machine.

5.1 Implementing IDS at the front end of cloud will detect attacks on the end users network where deployment of IDS is not useful in detecting internal attacks.

5.2 Implementing IDS at the backend of the cloud environment (at server point) will detect all internal attacks on cloud and all external attacks which come from the end user network.

5.3 Implementing IDS on virtual machine within the cloud environment will detect attacks on those machines only. Figure 5.1 shows the architecture of proposed cloud IDS Model.

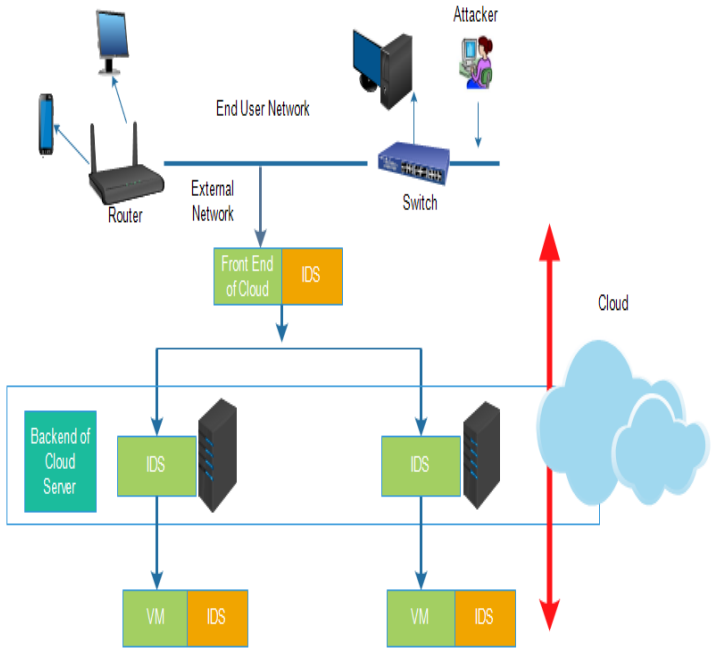

Figure 5-1: Position in the cloud at which IDScan be deployed

5.2 Suricata IDS

Suricata IDS is an open source next generation Intrusion Detection and prevention Engine, that can be used to monitor events in virtualized server in cloud and detect attacks. Suricata has differert modes which can be used but the main function of suricara for IDS in networks is capturing all incoming packet,analyzing this packets and finally give the alert if a packet is matching the configured rule. Figure 5.2 shows the flowchart of suricata.

Suricata has three modes, logging mode, sniffer mode, and NIDS mode. In the Logging mode, every packet will be logged into log folder and using this mode is not useful. The sniffer mode prints TCP/IP packet header to the screen. The NIDS mode will create rules based on the administrator policies. This three mode sent alerts to log server to be seen by the

administrator. If Suricata gives alert of an attack occurs in network then administrator should shut down the connection with the network. Therefore, Suricata can be used as security method to detect any attacks against virtualized environment.

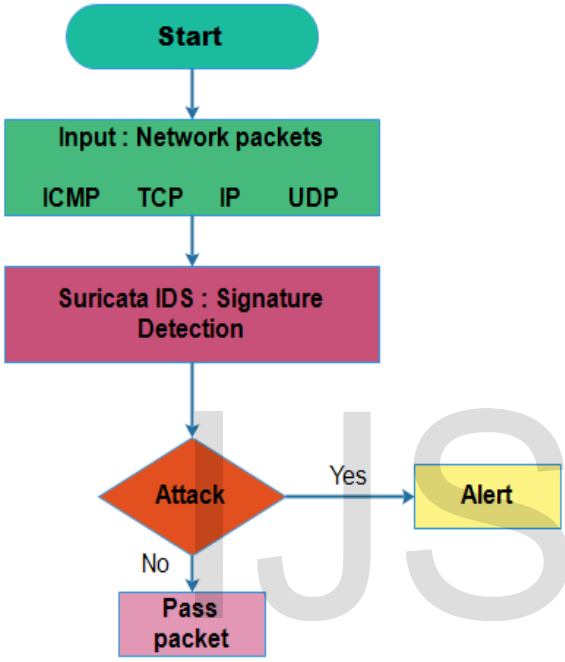

Figure 5-2: Flowchart of proposed Cloud IDS Model

6. VirtualizationOfIntrusion Detection System

Virtualized Intrusion Detection System is handle the network access traffic and protect the data and applications in cloud from malicious attack and vulnerabilities. IDS Model havingcharacteristics of virtualization to provide better security in cloud environment. Thisarchitecture detecting insider and outsider attacks and host and port scanning performed by every host in a network. The cloud IDS Model uses a Virtualized IDS system and both NIDS and HIDS efficiently to block malicious traffic. It generates a report with the help of both IDS Controller and Third Party monitoring and advisory service to Cloud Service Provider and also generates an alert report for Cloud users.

The architecture of cloud IDS Model, there are main four components.

6.1 IDS Controller - An IDS controller will create different instances of IDS for each user and these instances are deployed between user and Cloud Service Provider (CSP). These instances are named as Mini IDS and it will work on each specific user.

6.2 Multi threadCloud IDS– Multi thread Cloud IDS is deployed on the bottleneck of network points such as router, gateway outside the virtual machine and monitor the network traffic.

6.3 Third party monitoring & advisory Service - The third party monitoring service is for monitoring the alerts sent by cloud IDS and generating advisory reports to IDS controller. The IDS Controller reduces the workload of single IDS for cloud environment. It also generates a final advisory report to CSP and a alert report to cloud users

6.4 HIDS Based Hypervisor - It works on the server and analyses the encrypted and fragmented data by signature and behavior analysis on them.

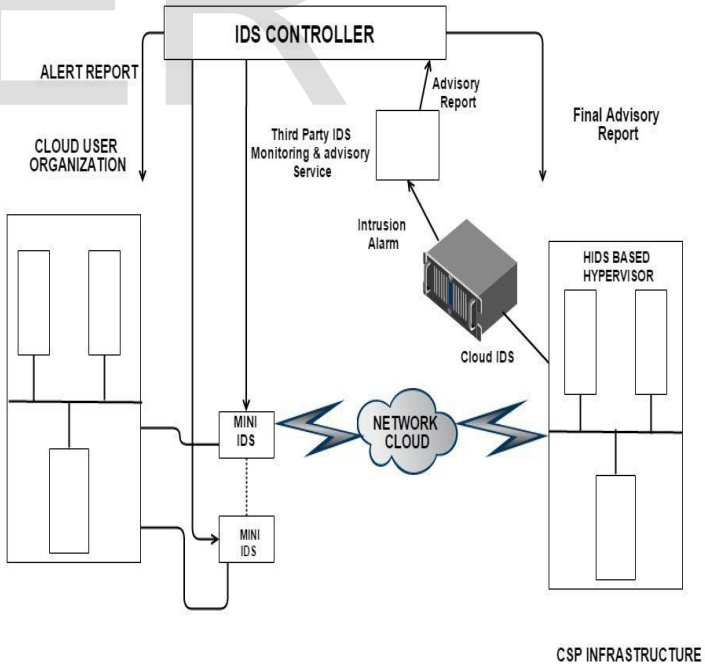

Figure 6: Architecture of Cloud IDS Model

7. Proof of Concept

An experiment is conducted by building the own virtualized server in cloud environment, then implementing the Suricata intrusion detection system against the virtualized platform.

7.1 setup of virtualized server

7.1.1 Physical Machine specification.

The important factor is used in physical machine that are the processor type, RAM size and Hard disk Size. The Processor type checks whether the Physical Machine supports virtualization or not. RAM and hard disk should be large enough to run different platform on one physical machine. Processor type of the host machine is core –i5 2340 which supports virtualization technology. The processor speed is 2.40 GHz, which is the minimum speed required in virtualization. The RAM Size is 4 GB & Hard disk size is 500 GB. The size of RAM & Hard disk is enough to avoid physical Machine crashing & increase the performance of virtual machine on the physical machine.

7.1.2 Physical Machine OS

To install Kernel-based virtual machine and build the virtualized server, the operating system of the physical machine is Ubuntu 14.04 LTS

7.1.3 Hypervisor

Hypervisor is a program that allows multiple operating systems to share a single piece of hardware. In our experiment Kernel-based virtual Machine (KVM) was installed on Ubuntu OS. To manage the virtual machines, a tool known as virtual manager was installed. Then three virtual machines were created on top of the Kernel-based virtual Machine,FTP server, web server, and desktop server. On the FTP server which is on Ubuntu virtual machine, cloud user can take backup file. On the Web Server which is on windows server 2008 virtual machine, cloud user can access different websites that are created. On the Desktop server which is on windows 7 ultimate virtual machine, cloud user can remotely access desktop placed on the virtualized platform in the cloud using remote desktop Protocol (RDP) which uses software known as Remote Desktop Connection.

8. Network Setup

Connection between the virtualized servers and external user set up as shown in Figure 8. External users use public IP addresses to access the virtualized servers and the private IP addresses are known by the cloud provider only. Nat feature was configured to map public IP addresses to private IP addresses. Then Suricata is used on separate Linux machine to detect any attack against the virtualized servers. Suricata topology is considered a network IDS in the backend of the cloud environment, so threats can be detected in virtualized servers.

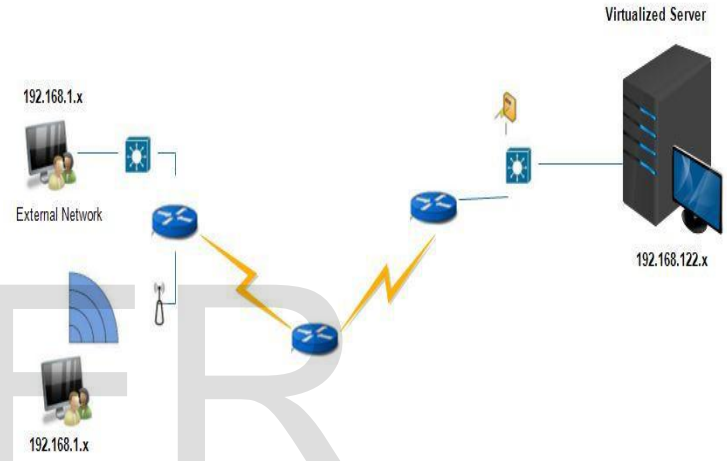

Figure 8 Network Setup

9. Conclusion

Intrusion Detection System (IDS) is the main advantage of cloud computing to using virtualization based IDS, providing security and preventing threats to access user information or to disable protection in the underlying system. The cloud provides more resources for various users, the IDS can increase the number of sensors to monitor the growth of the cloud. In this paper, evaluate the Suricata IDS against the virtualized server is proposed to secure the virtualized server from attacker and various thread.This architecture will be capable of detecting attacks and port scanning performed by external hosts.

10. Acknowledgement

I would like to thank to all member who supported me and guided me throughout their knowledge. I am really very thankful to them. It was impossible to complete without them.

11. References

Papers**:**

[1]Jaimin K. Khatri, Mr.GirishKhailari. International Journal of Science, Engineering and Technology Research Advancement in Virtualization Based Intrusion Detection System in cloud Environment, (IJSETR), Volume 4, Issue 5, May 2015

[2] ManthiraMoorthy S, Virtual Host based IDS for Cloud, International Journal of EngineeriTechnology (IJET),Vol 5 No 6 Dec 2013-Jan 2014

[3] MsDeepavali p Patil, Prof.ArchanaC.Lomte Implementation of Intrusion Detection System for Cloud Computing International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[4]Alaspurkar S J. Analysis of IDS for Cloud Computing, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Vol.2, Issue 3, pp.344-349(2013).

[5] IrfanGul ,M.Hussain Distributed Cloud Intrusion Detection Model International Journal of Advance science and technology vol.34,September,2014.

[6] ParthaGhosh, RiaGhosh ,RumaDutta An alternative model of virtualization based IDS in cloud computing. International Journal of scientific & Technology Research volume 3, issue 5, May 2014.

[7] Dhage, *et al.*, "Intrusion detection system in cloud computing environment," presented at the Proceedings of the International Conference Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India, 2011.

[8] M.Madhvi, (IJCSIT),An approach for Intrusion Detection system in cloud computing, International Journal of Computer Science and Information Technologies, Vol. 3 (5), 2012, 5219 – 5222

[9] V. Marinova-Boncheva, "A short survey of intrusion detection systems," Problems of Engineering Cybernetics and Robotics, vol. 58, pp. 23–30, 2007.

Websites:

[10] C. B. Lee, C. Roedel, and E. Silenok, "Detection and characterizationofport scan attacks," 2003. [Online]. Available: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.161.7079

[11]SuricataIDS/IPS"[Online].Available: http://www.openinfosecfoundation.org/