A Survey on Virtualization Based Intrusion Detection System in Cloud Environment

[1]Jaimin Khatri, [2]Mr. Girish Khilari
[1]IT Systems & Network Security,
[1]Gujarat Technological University, Ahmedabad, India

Abstract **- Nowadays all are working with cloud. 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. So providing security has become a major concern for Cloud Computing. Intrusion Detection Systems have become a needful component in terms of network security. In this paper, we will study basics of Cloud Computing, Existing techniques to detect intrusions and threat in cloud environment and Virtualization based Intrusion Detection System in cloud environment. By this study we can discover strong mechanism to detect DOS (Denial of service) and DDOS (Distributed Denial of service) attacks.**

IndexTerms **– Cloud Computing, Intrusion Detection System, Host Based IDS, Network Based IDS, Virtualization.**

I. INTRODUCTION

Cloud computing is an internet based computing where virtual shared servers provide Infrastructure, Platform, Application , Elastic resources , devices and hosting to customer as a service on "pay-for-use" basis. Cloud computing is the delivery of on-demand network access to a shared pool of configurable computing resources everything from applications to Data Centers over the Internet.[1][3] Figure.1 shows the concept.

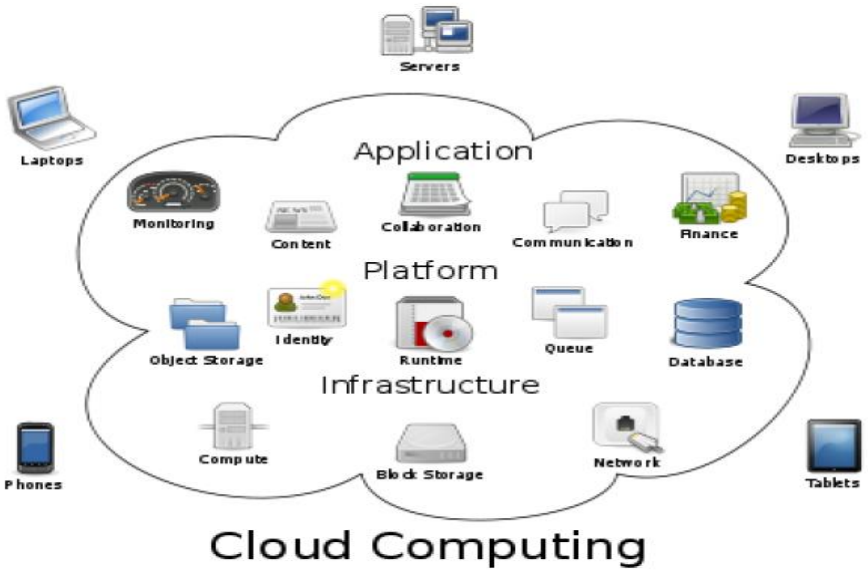

Figure 1: Cloud Computing Infrastructure [2]

Cloud computing has various services provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability. Cloud computing provides three services namely Software as a Service (Saas), Platform as a Service (Paas), Infrastructure as a Service (Iaas). [3][10]

This paper organized as follows: Section II briefly discusses about Intrusion Detection System, Host based IDS and Network based IDS. Section III discusses existing technique of Intrusion Detection System in cloud Environment. Section IV describes Virtualization Based IDS in cloud Environment. Section V draws conclusions.

II. INTRUSION DETECTION SYSTEM[5]

An intrusion detection system (IDS) is an essential component of defensive measures protecting computer systems and network against harmful misuse. It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper reply. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network. [5]

IDS can be defined as a defense mechanism, which detects antagonistic activities in a network. The key is to detect and possibly prevent activities that may compromise system security, or some hacking attempt in progress including reconnaissance/data collection phases that involve port scans. [6]

One key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection. IDS tools are capable of distinguishing between insider attacks Originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers). Once an intrusion and threat has been detected, IDS issues alerts notifying cloud administrators. The next step is undertaken by the administrators or the IDS itself.

There are two main categories of intrusion detection technique.

1. Misuse detection - Misuse Detection model refers to detection of intrusions that follow well-defined intrusion patterns. It is very useful in detecting known attack pattern.
2. Anomaly 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).

The IDS can be further classified according to data collection.

Host Based IDS

Host-based IDSs (HIDS) operate on information collected from within an individual computer system. A Host-based IDS basically monitors the incoming and outgoing packets from the computer system only and would alert the user or administrator if suspicious activity is detected.

Host Based IDSs analyze the suspicious activities like system call, processes and configuration access by observing the situation of host. It is used to protect valuable and private information on server systems. HIDSs are able to assign as NIDS if they are installed on a single host and configured to detect network activities. HIDS is composed of sensors located on servers or workstations which are made to prevent the attacks to a host. [8] [9]

Network Based IDS:

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 based on specified points and placed between the end point devices like firewalls, routers. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing the network traffic for signs of malicious activities and events. Network traffic stacks on each and every layers delivers the data coming from a layer to another layer. [8][9]

III. EXISTING TECHNIQUE OF CLOUD IDS MODEL

Distributed Cloud Intrusion Detection Model [4]

To handle a large number of data packets flow in such an environment using multi-threaded IDS approach. The multi-threaded IDS would be able to process large amount of data and could reduce the packet loss. The proposed 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 cloud user can accesses its data on servers at service provider's site over the cloud network. User requests and actions are monitored and logged through a multi-threaded NIDS. The alert logs are readily communicated to 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.

IV. VIRTUALIZATION BASED INTRUSION DETECTION SYSTEM IN CLOUD ENVIRONMENT

Virtualized Intrusion Detection System is help to handle the large scale network access traffic and protect the data and applications in cloud from malicious attack and vulnerabilities. A cloud IDS Model having the characteristics of virtualization to provide better security in cloud environment. This architecture will be capable of 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. [5]

The architecture of cloud IDS Model, there are main four components. Figure.2 shows the architecture of cloud IDS Model.

1. IDS Controller - An IDS controller will create different instances of IDS for each user and these instances are deployed between each user and Cloud Service Provider (CSP). These instances are named as Mini IDS and it will work on each specific user.
2. Multi threaded Cloud IDS - Multithreaded Cloud IDS is deployed on the bottleneck of network points such as router, gateway outside the virtual machine and monitor the network traffic.
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.

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

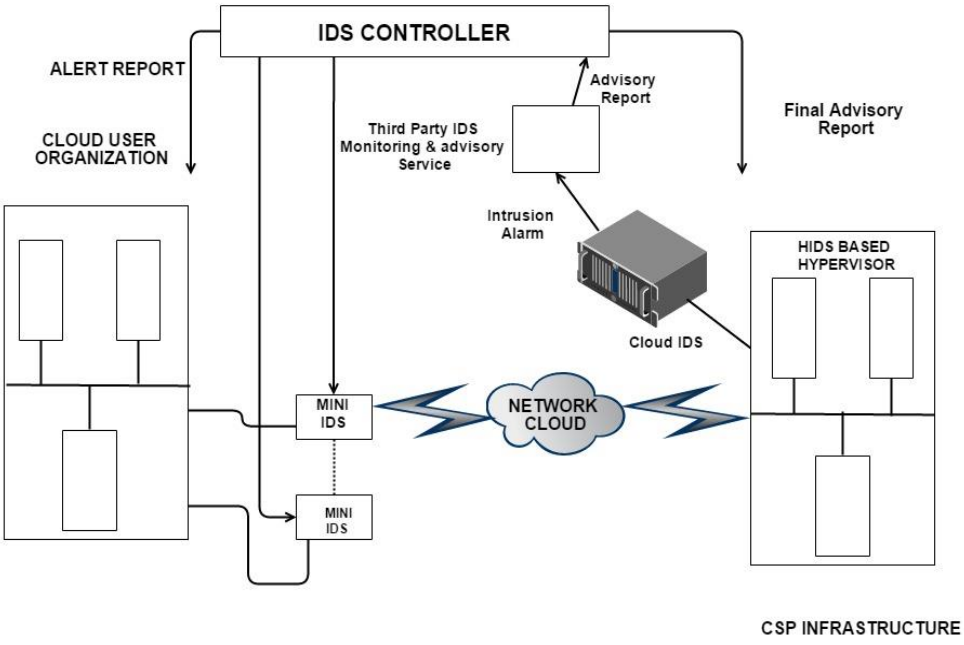

Figure 2: Architecture of Cloud IDS Model

V. Conclusion

In this paper we mainly concentrate on survey of Intrusion Detection System (IDS) in Cloud Environment The main advantage of using virtualization based IDS is the isolation of the monitored environment, providing security and preventing threats having access to user information or to disable protection in the underlying system. As the cloud environment provides more resources for various users, the IDS can increase the number of sensors to monitor the growth of the cloud. With this flexibility, the IDS become more functioning in detecting intrusion in cloud computing environments.

VI. Acknowledgment

I would like to thank to all who supported me and guided me throughout the survey. I am very thankful to them. It was impossible to complete this without them.

References

[1] Manthira Moorthy S, Virtual Host based IDS for Cloud, International Journal of Engineering and Technology (IJET),Vol 5 No 6 Dec 2013-Jan 2014

[2] Ms Deepavali p Patil, Prof.Archana C.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.

[3] Mohod A G, 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).

[4] Irfan Gul , M.Hussain Distributed Cloud Intrusion Detection Model International Journal of Advance science and technology vol.34,September,2011.

[5] Partha Ghosh, Ria Ghosh ,Ruma Dutta An alternative model of virtualization based IDS in cloud computing. International Journal of scientific & Technology Research volume 3, issue 5, May 2014.

[6] 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.

[7] 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

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

[9] http://en.wikipedia.org/wiki/Intrusion_detection_system.

[10] http://www.ibm.com/cloud-computing/in/en/