International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 7 July 2018

A Survey on Intrusion Detection System (IDS)

Priyanka Alekar
Department of Computer Science & Engineering SKSITS, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Indore, Madhya Pradesh, 452010, India
priyanka.alekar111@gmail.com

Abstract: *Rapid growth of resources and escalating cost of infrastructure is leading organizations to adopt cloud computing. Cloud computing provides high performance, efficient utilization, and on-demand availability of resources. In modern days, with the increasing popularity of cloud computing, security in cloud has become a significant issue. As 'prevention is better than cure', detecting and blocking an intrusion is better than responding to an intrusion after a system has been compromised. With the increasing amount of network throughput and security threat, the study of intrusion detection systems (IDSs) has received a lot of attention throughout the computer science field. Though there is a number of existing literatures to IDS issues, in this paper, we attempt to give a more elaborate survey of prior comprehensive analysis.*

Keywords: *Intrusion Detection System, Cloud Computing, Security, Different IDS, Attack Prevention.*

1. INTRODUCTION

Cloud computing is a large-scale distributed computing paradigm [1]. It is a collection of sources in order to enable resource sharing in terms of scalability, managed computing services that are delivered on demand over the network. Its users need not to buy infrastructure, software, resources, as a result saving a large amount of expenditure. Cloud basically provides services through a third party. The third party provides services and resources on rent and users pay per use. This will save a lot of money and provides a greater flexibility to move from one service to another service [2].

Cloud Computing provides services in three ways: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud Computing provides its services over the internet. There are number of users, who use the cloud services over the untrusted network. This model of cloud makes the cloud vulnerable. The applications over the cloud are increasing rapidly and along with these applications vulnerabilities and numbers of attacks are also increasing [3]. Cloud computing paradigm has a service-oriented architecture which has led to a drastic alteration on how services are provided and managed. Intrusion detection techniques are used in any computing environment as a layer of defense. The basic aim is to detect any malicious activity well before any significant harm is possible. The general idea is to detect and identify attacks by either analyzing system artifacts (such as log files, process lists, etc.), or by keeping track of network traffic.

The distributed nature of cloud environment makes it most vulnerable and attractive environment for the intruders to perform attacks. Intrusion detection systems can be used to enhance the security of such systems by systematically examining the logs, network traffic as well as configurations.

Rest of the paper is organized as follows. Section 2 discusses background scenario of the IDS and their relevancy in cloud computing. Section 3 describes the different literature survey by researchers who have presented prior work of IDS. Finally, Section 6 concludes with references at the end.

2. BACKGROUND

The background of a study is an important part of our research paper. It provides the context and purpose of the study. Hence there is need for background study that contributes to prepare proposed system.

2.1 Intrusion Detection System (IDS)

An intrusion is an activity or regularly set of activities which compromise the information assurance. Intrusion detection system (IDS) is hardware or software application

basically uses to monitor the network activities and report the malicious activities to the network administrator. Intrusions detection systems have a variety of techniques present aims to detect suspicious traffic in different ways. Intrusion detection prevention systems (IDPS) attempts to detect and respond to intrusions against information and information systems. Most of the IDSs are built with a set of components that together define an IDS model [4] [5].

From figure 1, data collections have responsibility to provides information to the system to take decision whether a specific activity is intrusive or not. It collects User logs, System logs, system calls etc. for the other IDS components for the further decision making. This module is very important because without it other modules are un-functional. It audit data reduction i.e. instead of passing the whole raw data to Analysis module to decide whether a activity is malicious or not, it eliminate audit information believed to be unimportant for intrusion analysis. It helps in reducing the total complexity of the analysis module.

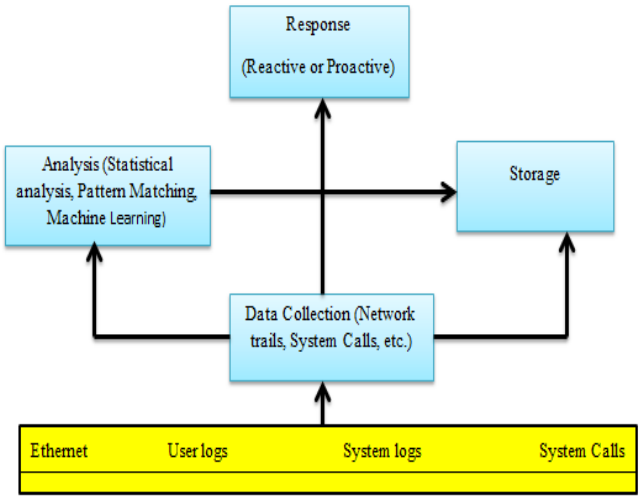

Figure 1: Generic Intrusion Detection System Model

Behaves as an extra layer of protection and provides other security mechanisms. Following are the importance of the intrusion detection system:

- ✓ Detects intrusions and other suspicious events.
- ✓ Detects an attack in its initial stages when the attacker just starts to scan a port to determine vulnerable ports.
- ✓ Prepares reports about the detected activities for system administrator.
- ✓ An easy technique for analysing the security measures.

2.1 Approaches of Intrusion Detection System

Intrusion detection system (IDS) is an essential component of defensive measure to protect network and computer system against various attacks. The main aim of IDS is to detect the attacks and generate the proper response. It is defined as techniques which are used to detect and respond to the intrusion activities from malicious host or network. There are some approaches of intrusion detection system are: Misuse Detection and Anomaly Detection.

Misuse Detection: Misuse detection is also called signature-based or rule based detection. In this detection approach, user's activities are compared with the attackers' known behaviours, to penetrate a system or network. In misuse detection, gathered information is analysed and compared with large databases for attack signatures.

Advantage:

Misuse or signature-based detection is useful, because its detection rate is high and false alarm rate is low for known attacks [6].

Drawbacks Instead of numerous benefits, misuse detection systems also have some limitations.

- ✓ The first drawback is the problem of maintaining state information for signatures in which the intrusive activity encompasses multiple discrete events.
- ✓ The second drawback is that your misuse detection system must have a signature defined for all of the possible attacks that an attacker may launch against your network.

Anomaly Detection: An Anomaly-Based Intrusion Detection System is a system for detecting computer intrusions and classifying it as either normal or anomalous. The classification is done by heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that different from normal system operation. It is unlike from signature based systems which can only detect attacks for which a signature has previously been created. In order to determine what attack traffic is, the system must be learned to recognize normal system activity .one can use another method to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection. Anomaly-based Intrusion Detection does have some disadvantage, namely a high false positive rate and the ability to be fooled by a correctly [7].

Advantage:

- ✓ Anomaly detection can detect unknown attacks easily, but its misjudgement rate is high. It can also detect previous unknown threats [7].

Drawbacks

- ✓ Like every IDS, anomaly detection systems also suffer from several drawbacks
- ✓ The first drawback is that the system should be trained to create the appropriate user profiles.
- ✓ Another drawback of anomaly detection is complexity of the system and the difficulty of associating an alarm with the specific event that triggered the alarm.

2.3 Classification of Intrusion Detection System

Cloud-based IDS can be divided into three types. These types are shown in Figure 2. We will describe each of them in the following subsections.

(i) Network-based IDS
(ii) Host-based IDS
(iii) Distributed IDS

(i) Network-based IDS (NIDS)

Network-based IDS are standalone hardware appliances which include network intrusion detection capabilities. They are mostly deployed on strategic point in network infrastructure such as at a boundary between networks, virtual private network servers, remote access servers, and wireless networks. NIDS monitors network traffic going through particular network segments or devices. It can capture and analyse data to detect known attacks or illegal activities or analyse network and application protocol activity to identify anomalous and suspicious activity by traffic scanning .NIDS can also be referred as "packet sniffers", because it captures and collect the data in the form of internet packets passing through communication mediums [8]

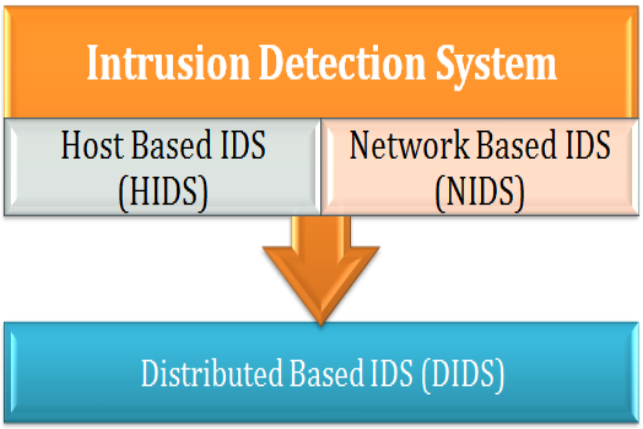

Figure 2: Classification of cloud based IDS

(ii) Host-based IDS (HIDS)

In Host-Based IDS, the characteristics of a single host are monitored and the events of that host are observed for any malicious activity. They can monitor network traffic, logs, processes; operations performed by applications, file access and modification, and any configuration change in system The deployment of HIDS is usually done on critical hosts [9]. Critical host includes servers or systems that are publicly accessible and have some sensitive information they are placed on one server or workstation, where data is collected from different resources and machine analyse the data locally [10]

(iii) Distributed IDS (DIDS)

Distributed IDS (DIDS) consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data. By having these co-operative agents distributed across a network, incident analysts, network operations and security personnel are able to get a broader view of what is occurring on their network as a whole.

3. LITERATURE SURVEY

To provide better security is the most important aspect of cloud computing. As we know for what purpose cloud used. Generally, cloud user uses cloud to store their data and important files and all. In this concern for IDS improvement previously work done in this domain of study.

Cloud Computing is a new type of service which provides large scale computing resource to each customer. Cloud

Computing systems can be easily threatened by various cyber attacks, because most of Cloud Computing systems provide services to so many people who are not proven to be trustworthy. Therefore, a Cloud Computing system needs to contain some Intrusion Detection Systems (IDSs) for protecting each Virtual Machine (VM) against threats. In this case, there exists a trade- off between the security level of the IDS and the system performance. If the IDS provide stronger security service using more rules or patterns, then it needs much more computing resources in proportion to the strength of security. So the amount of resources allocating for customers decreases. Another problem in Cloud Computing is that, huge amount of logs makes system administrators hard to analyze them. **Jun-Ho Lee et al. [11]** propose a method that enables Cloud Computing system to achieve both effectiveness of using the system resource and strength of the security service without trade-off between them.

Turki Alharkan et al. [12] described prototype of IDSaaS. In a public cloud computing environment, consumers cannot always just depend on the cloud provider's security infrastructure. They may need to monitor and protect their virtual existence by implementing their own intrusion detection capabilities along with other security technologies within the cloud fabric. Intrusion Detection as a Service (IDSaaS) targets security of the infrastructure level for a public cloud (IaaS) by providing intrusion detection technology that is highly elastic, portable and fully controlled by the cloud consumer.

Intrusion prospects in cloud paradigm are many and with high gains, may it be a bad user or a competitor of cloud client. Distributed model makes it vulnerable and prone to sophisticated distributed intrusion attacks like Distributed Denial of Service (DDOS) and Cross Site Scripting (XSS). Confronting new implementation situations, traditional IDSs are not well suited for cloud environment. To handle large scale network access traffic and administrative control of data and application in cloud, a new multi-threaded distributed cloud IDS model has been proposed. **Irfan Gul et al. [13]** proposed cloud IDS which handles large flow of data packets, analyze them and generate reports efficiently. Transparent reports are instantly send for information of cloud user and expert advice for cloud service provider's network misconfigurations through a third party IDS monitoring and advisory service.

Security has been one of the top concerns in clouds. It is challenging to construct a secure networking environment in clouds because the cloud is usually a hybrid networking system containing both physical and virtually overlaid networks. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have been widely deployed to manipulate cloud security, with the latter providing additional prevention capabilities. **Tianyi Xing et al. [14]** investigates into an OpenFlow and Snort based IPS called "SnortFlow", in which it enables the cloud system to detect intrusions and deploy countermeasures by reconfiguring the cloud networking system on-the-fly. The evaluation results demonstrate the feasibility.

With the thriving technology and the great increase in the usage of computer networks, the risk of having these network to be under attacks have been increased. Number of techniques have been created and designed to help in detecting and/or preventing such attacks. One common technique is the use of Network Intrusion Detection / Prevention Systems NIDS. Today, number of open sources and commercial Intrusion Detection Systems are available to match enterprises requirements but the performance of these Intrusion Detection Systems is still the main concern. **Adeeb Alhomoud et al. [15]** have tested and analyzed the performance of the well know IDS system Snort and the new coming IDS system Suricata. Both Snort and Suricata were implemented on three different platforms (ESXi virtual server, Linux 2.6 and FreeBSD) to simulate a real environment. Finally, in our results and analysis a comparison of the performance of the two IDS systems is provided along with some recommendations as to what and when will be the ideal environment for Snort and Suricata.

4. CONCLUSION

In cloud computing environment there are many benefits and more customer usage demand. It gives cost benefits by providing ready infrastructure and effective resource management. However, security is the main issue which needs to be resolved on priority basis. Therefore it is a "network of networks" over the internet, therefore chances of intrusion is more with the intellect of intruder's attacks. Different IDS techniques are used to oppose malicious attacks in traditional networks. This paper basically, introduced vast variety of intrusion detection system and their counter measure for the prevention of online/offline network. Hence, finally this study is delivered existing work of the different IDS system.

REFERENCES

[1] Kholidy, Hisham A., Fabrizio Baiardi, Salim Hariri and Esraa M. Elhariri, "A Hierarchical Intrusion Detection System for Clouds: Design and evaluation", International Journal on Cloud Computing: Services and Architecture (IJCCSA) 2, no. 6 (2012).

[2] Chonka, Ashley, Yang Xiang, Wanlei Zhou, and Alessio Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks", Journal of Network and Computer Applications 34, no. 4 (2011): pp. 1097-1107.
[3] Iti Raghav and Shashi Chhikara, "Intrusion Detection and Prevention in Cloud Environment: A Systematic Review", International Journal of Computer Applications (IJCA), Volume 68– No.24, April 2013.
[4] Nita Prakash Saware, Manish Umale and Nidhi Maheswarkar, "Detecting Intrusions in Multitier Web Applications", International Journal of Engineering Research and Applications (IJERA), Vol. 3 , PP.2007-2014, Jul-Aug 2013.
[5] Priyanka Sharma and Rakesh Singh Kunwar, "Cyber Attacks on Intrusion Detection System", International Journal of Information Sciences and Techniques (IJIST), Volume 6, No.1, March 2016.
[6] A. Abraham, R. Jain and J. Thomas, "D-SCIDS: Distributed soft computing intrusion detection system," Journal of Network and Computer Applications, vol. 30, pp. 81-98, 2007.
[7] Carter, Earl, and Rick Foreword By-Stiffler, Cisco secures intrusion detection systems, Cisco Press, 2001.
[8] Uttam Kumar and Bhavesh N. Gohil, "A Survey on Intrusion Detection Systems for Cloud Computing Environment", International Journal of Computer Applications (IJCA), Volume 109 – No. 1, January 2015
[9] Indraneel Mukhopadhyay, Mohuya Chakraborty, Satyajit Chakrabarti, A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems", Journal of Information Security, 2011, PP. 28-38.
[10] Hussain Ahmad Madni Uppal, Memoona Javed and M.J. Arshad, "An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications", International Journal of Computer Science and Telecommunications, Volume 5, February 2014.
[11] Jun-Ho Lee, Min-Woo Park and Jung-Ho Eom, "Multi-level Intrusion Detection System and log management in Cloud Computing", 2011 13th International Conference on Advanced Communication Technology (ICACT), 13-16 Feb. 2011, Seoul, South Korea, IEEE.
[12] Alharkan, Turki, and Patrick Martin, "IDSaaS: Intrusion detection system as a service in public clouds", In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID 2012), pp. 686-687
[13] Irfan Gul and M. Hussain, "Distributed Cloud Intrusion Detection Model", International Journal of Advanced Science and Technology, Volume 34, September, 2011
[14] Tianyi Xing, Dijiang Huang, Le Xu and Chun-Jen Chung, "SnortFlow: A OpenFlow-based Intrusion Prevention System in Cloud Environment", 2013 Second GENI Research and Educational Experiment Workshop, 2013 IEEE
[15] Alhomoud, Adeeb, Rashid Munir and Abdullah Al-Dhelaan, "Performance evaluation study of intrusion detection systems." Procedia Computer Science 5 (2011): pp. 173-180.