*IOSR Journal of Computer Science (IOSR-JCE)*
*e-ISSN: 2278-0661, p-ISSN: 2278-8727*
*PP 81-85*
*www.iosrjournals.org*

# Comparative Study and Analysis of Cloud Intrusion Detection System

Pramod Bide[1], Rajashree Shedge[2]
[1,2]Department of Computer Engg, Ramrao Adik Institute of technology/Mumbai University, India

**ABSTRACT :** *Cloud computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. Denial of- Service (DoS) attack or Distributed Denial-of-Service (DDoS) are major security issues in cloud environment. The best solution to protect the cloud from these attacks is use of IDS. IDS have become popular cloud security technology to detect cyber attacks in wide variety of networks. In this paper we will discuss comparative study of various existing integrated intrusion detection systems available to secure cloud. The cloud networks have their own characteristics which are the reason for threats to the security in cloud, cloud intrusion detection system is better solution to achieve a higher level of security maintaining its uniqueness. The cloud intrusion detection system is the most widely used technique where the system consists of IDS connected over the network in combination with Apriori, Bayesian, and Classification algorithms. The paper discusses architectures of cloud Intrusion Detection System and techniques to detect them*
***Keywords*** *– Cloud Computing, Data Mining, DDoS, IDS.*

## I. INTRODUCTION

Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources. SaaS delivers software as a service over the internet to the users thereby eliminating the need to install the application. Platform as a Service (PaaS) provides access to operating systems, database and component services. Infrastructure as a service (IaaS) refers to computing resources as a service. IaaS doesn't allow the user to control the infrastructure but gives the control of operating systems, storage devices. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Host System. The Cloud Intrusion detection System (CIDS)[1][2][3][4]. has a scalable and elastic architecture with a peer to peer solution and no central coordinator. Hence, there is no single point of failure. CIDS architecture distributes the processing load at several cloud locations and isolates the user tasks from the cloud by executing them in a monitored virtual machine [6].

The paper focuses on the various cloud IDS architectures used for detection of different attacks and vulnerabilities introduced in cloud networks [9]. A detail study of attacks and challenges faced in cloud networks is performed and many proposed architectures are compared. The main aim is to understand the detection techniques applied by different people in order to make system more efficient and improved than others.

Rest of this paper is organized as follows Section 2 gives the brief knowledge of architecture of Cloud Intrusion detection System. Section 3 gives the detailed comparison and analysis of different CIDS methods discussed in Section 2 by considering different parameters. Section 4 gives analysis. Section 5 concludes work and CIDS techniques used so far with the references at the end.

## II. IDS ARCHITECTURES IN CLOUD

Many IDS have been designed and suggested for Cloud networks,. The Cloud networks are more to different types of attacks due to their dynamic and absence of intermediate device between the nodes. Some of them will be discussed in the paragraphs to follow. The review of this paper is based on the

architectures of IDS which includes Genetic based, Apriori based, Bayesian based, Sensor based, and Hybrid etc.

### 2.1. Genetic algorithm based IDS

Anand Kannan and Gerald Q. Maguire, Ayush Sharma and Peter Schoo [12] proposed a new intrusion detection system in which we have developed a new genetic algorithm based feature selection algorithm. Moreover, an effective classification algorithm called Fuzzy Support Vector Machines has been used in this work for effective classification of network trace data. From the approaches used in this work, it was possible to find the intruders effectively. Proposed Feature Selection Technique Using GA Genetic based feature selection algorithm has been used in this work in order to select suitable subset of features so that they are potentially useful in classification. Another advantage of GA based feature selection in this work is that it finds and eliminates the redundant features if any because these redundant features may misguide in clustering or classification. The reduction in number of features reduces the training time and ambiguousness, thus a weighted sum genetic feature selection algorithm has been proposed which has increased global search capability and is better in attribute interaction when compared to other algorithms such as the greedy method.Fig.1 shows the architecture of Genetic Cloud IDS.

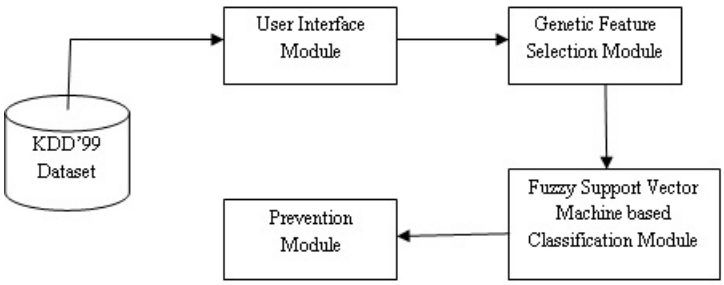


Figure 1.Genetic Algorithm based IDS

### 2.2. Apriori based Cloud IDS

Chirag N. Modi, Dhiren R. Patela, Avi Patel, Muttukrishnan Rajarajan [2] proposed a we combine Snort and signature apriori algorithm in our NIDS module. The network may be external network or internal network. We use Snort for detecting network intrusions, whereas the signature apriori algorithm is used to generate new possible signatures from partially known signatures. The Snort and signature apriori algorithm are chosen due to their following characteristics: Snort- It uses a signature based detection technique. Snort is configurable, free, widely used, can run on multiple platforms and is constantly updated. It captures network data packets and checks their content with the predefined patterns for any correlation. The detection engine of Snort allows registering, alerting and responding to any known attack Signature Apriori- It takes to capture packets and partially known signatures as input. As an output, it generates new attack signatures. These new signatures are used in Snort for detecting the derivatives of known attacks. In the proposed design, signature apriori is combined with Snort for accurate and efficient detection. The proposed method has less training time compared to other classification techniques. Workflow of NIDS module is shown in Fig. 2 and Fig. 3 Network packets are captured from network using Snort. Snort will monitor those network packets and allow/deny them based on the configured rules. Also, captured packets, partially known attack signatures and support threshold are given as input to the signature apriori algorithm. Security administrator updates known signature database. Using given input, signature apriori generates new possible signatures and updates them as rules in Snort

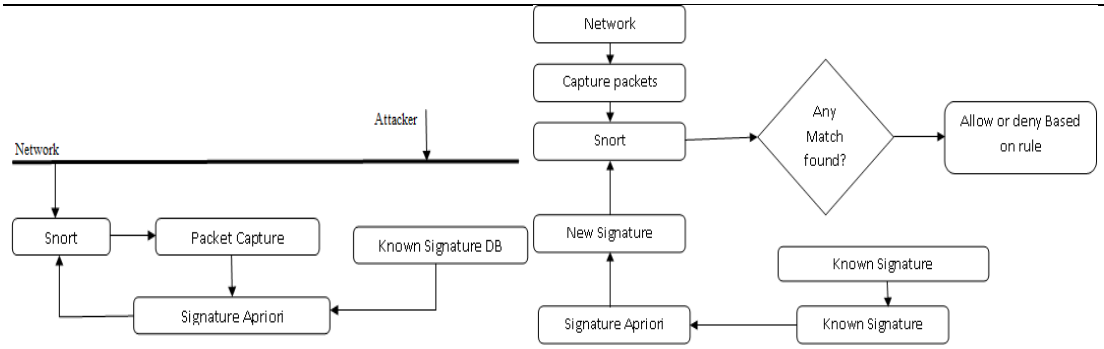


Figure 2. Apriori Based Cloud IDS




Figure 3. Flowchart of Apriori Based Cloud IDS

2.3. Sensor based Cloud IDS

Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi [4] proposed key components the framework and their interactions. Events Collectors: Is software monitoring sensors that collect security events such as log entries from the VM operating system, audit data, and user signatures. In testbed, there are HIDS sensors and NIDS sensors that extend Snort to monitor, respectively, the host operating system and the network traffic flowing through the virtual switch. Events Correlator: integrates and correlates host and network events collected from Events Collector hosted at different VMs. The correlation groups events according to the source IP address of the user and the session start time and end time. This allows correlating the behaviors of the same user in several VMs to detect a suspected behavior spanning multiple VMs.

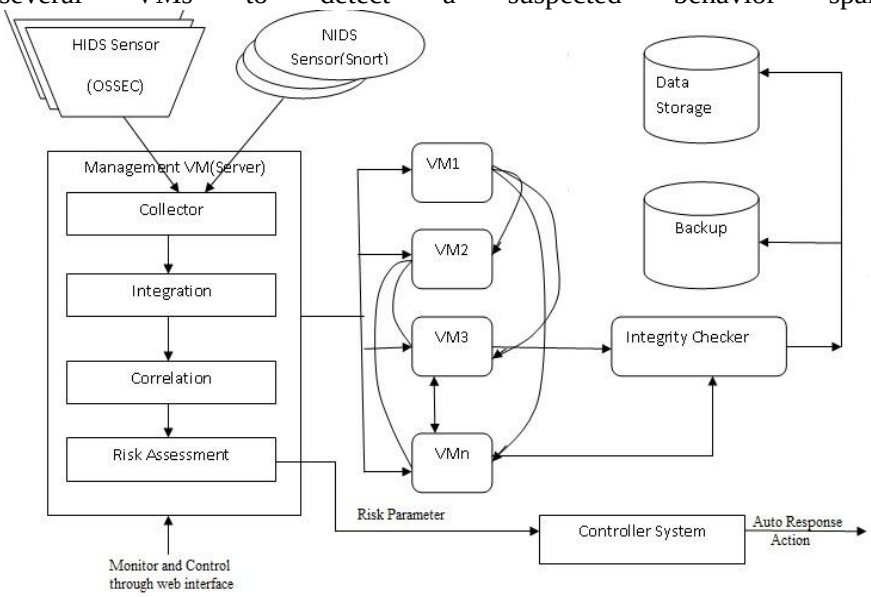


Fig. 4 Sensor Based Cloud IDS

2.4. Bayesian based Cloud IDS

Chirag N. Modil, Dhiren R. Patell, Avi Patel, RajarajanMuttukrishnan[3] proposed NID S module consists of three main components Packet Pre-processing, Analyzer and Storage. Fig.5 Architecture of proposed NIDS module. Pre-processing module processes captured packets in specific format by removing redundant information that has very low correlation with detection. Analyzer applies detection techniques (signature based and anomaly based) on captured packet. It consists of Snort, Bayesian classifier and Alert Log. Alert Log system logs intrusion event and sends alert message to NIDS module at other processing side. Other NIDS modules store such alert in their storage. Storage module stores network events. Knowledge base stores rules (related to known attacks) that are used by Snort, whereas the behavior base stores network events (normal events and intrusions) that are

used by Bayesian classifier. NIDS module uses two types of detection techniques to achieve high level security in Cloud, Signature based Detection, Anomaly Detection.

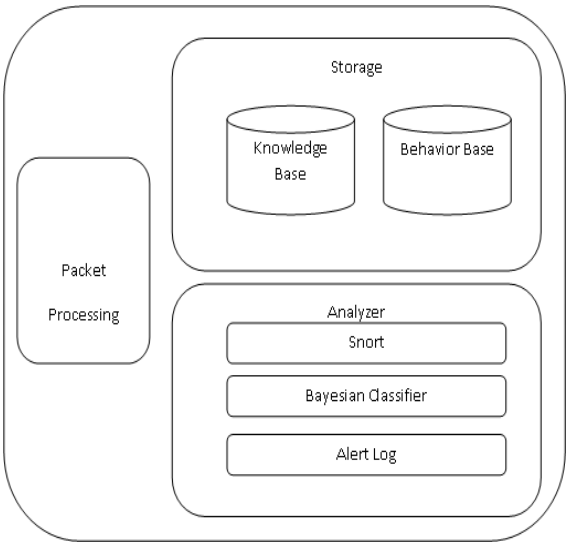


Figure 5.Bayesian based IDS

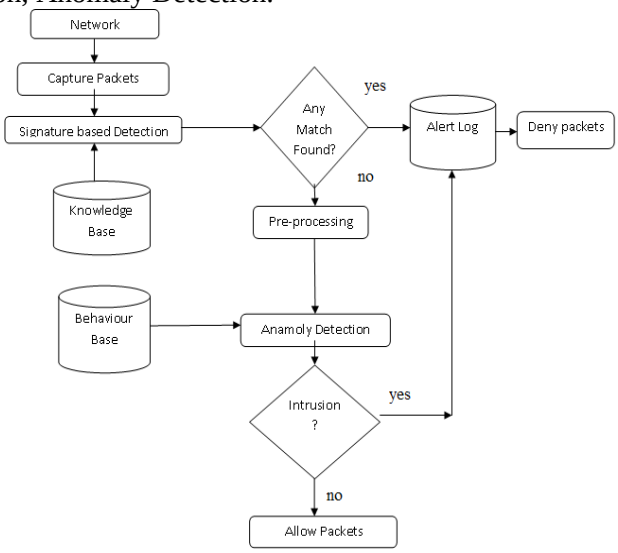


Figure 6. Flowchart of Bayesian based IDS

NIDS module uses both techniques that are complimented of each other. Workflow of NIDS modules is shown in Fig. 6. Network packets are captured from network (external or internal). Then signature based detection technique is applied on captured packets to detect intrusions using Snort. It logs intrusion packets in alert database. Non-intrusion packets are preprocessed for anomaly detection. Bayesian classifier is applied to predict class label (normal or intrusion) of non-intrusion packets by observing base. Intrusions (predicted by Bayesian classifier) are logged into alert log database, whereas the normal packets are considered as legitimate packet and allowed into the system NIDS on other servers updates their knowledge base with the alerts found in alert database. So, other servers can detect such unknown. In our NIDS framework, signature based detection technique is applied prior to anomaly detection. So, anomaly detection has to detect only unknown attacks. This improves detection time. Sending alert of intrusion to NIDS at other servers improves detection rate in whole Cloud environment

## III. Comparison

Comparison of Existing Cloud Intrusion Detection System.

| Proposed Models / Parameters | Genetic Algorithm based | Apriori Based | Bayesian Classifier Based | Hierarchical autonomous-IDS |
|---|---|---|---|---|
| Type of IDS used. | HIDS and NIDS | NIDS | NIDS | NIDS |
| Addressed Attacks | DoS, DDoS | Attacks on Ports, DoS | Insider attack (DoS), (DDoS) | DDos, Hosted Based, Network based. |
| False error Rate | Low | Low | Medium | Low |
| Positioning in Cloud | At Host And at Network | | At Network | At Host, Virtual Machine and at Network. |

| | | | | |
|---|---|---|---|---|
| Detection Rate | High | High | Low | High |
| Computational Cost | High | Low | Low | Medium |

We have considered five different Intrusion detection systems in Cloud networks. All Cloud Intrusion Detection System uses Signature and Anomaly Detection techniques and focuses on Cloud Infrastructure. Cloud networks are more prone to attacks. We have considered various Cloud intrusion detection Systems for comparison. Clouds are more prone to intrusions due to its many characteristics that it exhibits. A Genetic IDS uses signatures and anomaly detection techniques to provide security in cloud Alert System. It's a Apriori based IDS that addresses attacks like packet dropping, attacks on ports etc. A Bayesian classifier IDS based on Snort and Bayesian algorithm for intrusion detection.It's a Hierarchical and Autonomous based IDS that provides high degree of protection as well as self resilience has a small disadvantage of being less robust. Almost all above discussed CIDS uses Signature and anomaly based detection techniques and uses NIDS for attack detection.

## IV. CONCLUSION

There are many proposed system for detecting intrusions in Cloud networks, we have studied four CIDS. Genetic based CIDS reduces malicious packet searching time, accuracy and detection rate is high.Apriori based CIDS ensures low false positives and computational cost. Bayesian based CIDS is compatible with all services, detection rate and accuracy is high. Sensor based CIDS provides self resilience in case of failure, also the detection rate, accuracy is high. So, we conclude that Genetic and Sensor based CIDS are the best architectures for securing infrastructure of a cloud. The area we have concentrated in Cloud networks is IAAS and DDoS for studying Cloud IDS architectures in various forms.

.

## References

[1] Anand Kannan and Gerald Q. Maguire, Ayush Sharma and Peter Schoo,"Genetic Algorithm based Feature Selection Algorithm for Effective Intrusion Detection in Cloud Networks" , IEEE, 2012.
[2] Chirag Modi, Dhiran Patel, Avi Patel, Muttukrishanan Rajarajan, "Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing", ICCCS,2012..
[3] Chirag Modi, Dhiran Patel, Avi Patel, Muttukrishanan Rajarajan, "Bayesian Classifier and Snort based Network Intrusion Detection System in Cloud Computing", IEEE,2012.
[4] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi ," HA-CIDS: A Hierarchical and Autonomous IDS for Cloud Systems."IEEE, 2012.
[5] Chirag Modi, Dhiran Patel, "A Novel hybrid- Network Intrusion Detection System in Cloud Computing", IEEE,2013..
[6] Panagiotis Kalagiakos and Margarita Bora, "Cloud Security Tactics: Virtualization and the VMM", IEEE, 2012.
[7] Praveen Kumar, Bhaskar Naik,"A survey on Cloud Intrusion detection System".IJSWS, 2013.
[8] Chirag Modi, Dhiran Patel, Bhavesh Borisaniya, Hiren Patel."A Survey of Intrusion Detection Techniques in Cloud", JNCA, 2013.
[9] Pradeep Kumar Tiwari and Dr. Bharat Mishra ," Cloud Computing Security Issues, Challenges and Solution " ,IJETAE, Volume 2, Issue 8, August 2012.
[10] Chirag Modi, DhirenPatel, BhaveshBorisaniya, HirenPatel , Avi Patel , MuttukrishnanRajarajan, "A survey of intrusion detection techniques in Cloud ", JNCA, 2013.
[11] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyati, Joaquim Celestino Junior, "An Intrusion Detection and prevention system in Cloud Computing", JNCA, 2012.
[12] Chi- Chun Lo,Chun-Chieh Huang, Joy Ku, "A Cooperative intrusion Detection System framework for Cloud Computing Networks", IEEE,2010
[13] Mervat Adib bamiah, Sarfraz Nawaz Brohi, "Seven deadly Attacks and vulnerabilities in Cloud Computing", IJAEST, Vol No. 9, 2011
[14] Huaglory Tianfield, "Security Issues In Cloud Computing", IEEE, 2012.
[15] K.Divya, S.Jeyaatha, "Key Technologies in Cloud Computing", IEEE, 2012.
[16] Snort-Homepage. [Online]. Available: https://www.snort.org/
[17] KDDcup1999.[Online].Available:https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html