www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12146-12151

Hybrid Intrusion Detection Architecture for Cloud Environment

Sumalatha Potteti[1], Namita Parati[2]
[1]Assistant Professor, Department of CSE,BRECW,Hyderabad,India,sumalatha.po@gmail.com
[2]Assistant Professor, Department of CSE,BRECW,Hyderabad,India,namianand006in@gmail.com

Abstract:
The Cloud computing system can be easily threatened by various attacks, because most of the cloud computing systems provide service to so many people who are not proven to be trustworthy. Due to their distributed nature, cloud computing environment are easy targets for intruders[1]. Intrusions have been a major problem in terms of computing resources such as grid computing, ubiquitous computing ,cloud computing, distributed computing and so on. Intrusions are hard to detect but there has been a lot of work done on detecting and removing the intrusions .The focus of intrusion detection should be mainly on detecting the intrusions at the system resources and at the network level for a predefined network. In this paper we proposed a system is to detect intrusions in the cloud computing using Behavior-based approach and knowledge-based approach. If first approach unable to detect the data, second approach again verifies the data and compare it with the signatures within the database. In the proposed system definitely we will have very low false positive alarm. This paper surveys the intrusion detection and prevention techniques and possible solutions in Host Based and Network Based Intrusion Detection System. Different Intrusion Detection techniques are also discussed namely anomaly based techniques and signature based techniques. It also surveys different approaches of Intrusion Prevention System.

Keywords: Cloud Computing, Intrusion Detection System, Intrusion Prevention System, Hybrid Architecture.

1. INTRODUCTION:

Cloud computing is a large-scale distributed computing paradigm [2]. 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. In the past three decades, the world of computation has changed from centralized (client-server not web based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing) [4]. Cloud computing is emerging day by day. People are using its services very frequently and they don't have any other alternative for its services. But users are unaware about the security and privacy concerns in a cloud environment. Since cloud computing is distributed in nature, supports multi-user and multi-domain platform, it is more prone to security threats. An IDS inspects all inbound and outbound network activities and identifies suspicious patterns that may indicate a network or system attacks from someone attempting to break into or compromise a system[7].The cloud computing uses the internet as the communication media. The Cloud computing system can be easily threatened by various attacks, because most of the cloud computing systems provide service to so many people who are not proven to be trustworthy. Due to their distributed nature, cloud computing environment are easy targets for intruders looking for possible vulnerabilities to exploit. Cloud computing have two approaches i.e. Knowledge-based IDS and Behavior-based IDS to detect intrusions in cloud computing.

2. 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. In addition, the IDS can also be defined as a defense system, which detect hostile activities in a network. The key is to detect and possibly prevent those activities that may compromise with the system security. The key feature of IDS is its ability to provide the view of unusual activity and to generate the alerts in order to notify the administrators and/or block the suspended connection. IDS tools are capable of distinguishing between the insider attacks that are originating, inside the organization and external ones (attacks and the threats by hackers). If an intrusion has been detected, IDS issues alert for notifying about this event. These alerts are based on true positives or true alarms when actual intrusion takes place and false alarms in case of wrong detection of the system. After that, administrator or IDS itself takes steps according to organizational policies. At IDS, if detection rate is high and low false positive rate then the efficiency of IDS is good and vice versa. Some of the security issues related to cloud are Authentication and Identity management , Access

control and accounting, Trust Management and Policy Integration, Secure service management, Privacy and data protection, Organizational and security management[14]. All these security issues can be addressed by implementing well proven technique called Intrusion Detection System (IDS).

2.1 IDS can be broadly classified into three main types:

a. Network Intrusion Detection System (NIDS)
b. Host-based Intrusion Detection System (HIDS)
c. Stack-based Intrusion Detection System (SIDS)

a) Network Intrusion Detection System (NIDS)

NIDS attempts to discover unauthorized access to a computer network by capturing the network traffic packets such as TCP, UDP and IPX/SPX and analyzes the content against a set of rules. Examples are: Eavesdropping, data modification, identity or IP Address Spoofing, Denial-of-Service (DoS) attacks, Man-in-the-Middle Attack etc. NIDS consist of a set of single-purpose sensors that are placed at various points in the network. These sensors monitor and analyze network traffic and send report of attack to the centralized console. The deployment of NIDS has a minute effect on the performance of the network.

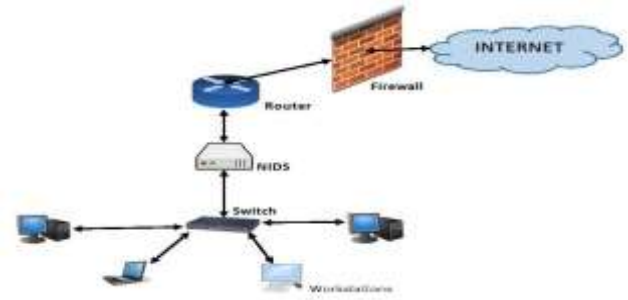

Figure 1: Architecture of NIDS

b) Host-based Intrusion Detection System (HIDS)

HIDS involves software or agent components, which monitors the dynamic behavior and state of the computer system. HIDS software runs on the server, router, switch or network machines. The agent version has to report to a console or it can run on together on the same host as shown in Figure. Examples are: Buffer overflow, rootkit, format string etc. The software creates log files of the system in the form of sources of data. The host based IDS looks at communication traffic and checks the integrity of system files to keep an eye on suspicious processes. Host based IDS doesn't provide good real time response.

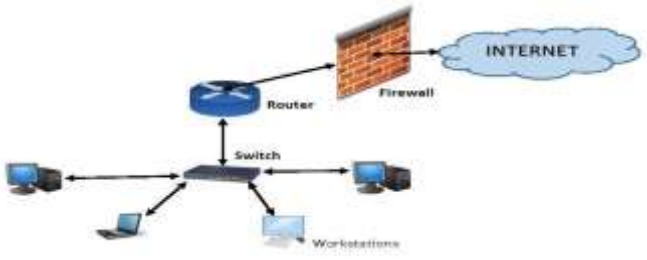

Figure 2: Architecture of HIDS

c) Stack-based Intrusion Detection System (SIDS)

This is the newest IDS[15] technology that varies from host to host, so it's an evolution of HIDS. Stack-Based IDS works integrating closely with the TCP/IP stack allowing packets to be monitored as they traverse their way up the OSI Layer and work in non-promiscuous mode.

2.2 Detection Techniques in IDS:

a) Misuse/Signature based detection:

This method uses specifically known patterns of unauthorized behavior, called signatures, to predict and detect subsequent similar attempts [3]. This method is extremely accurate for known attacks. It produces a low false alarm. With the help of this technique, we can cover a broader range of unknown attacks. Another advantage is that signatures are easy to create and understand only if the network behavior is known that is required to identify. The disadvantage of this method is that it can only detect intrusion that matches a predefined pattern, a set of signature must be continuously updated to detect a new attack and it can't detect novel attacks. Signature based detection does not work well when the user uses advanced technologies like nop generators, payload encoders and encrypted data channels [8]. The efficiency of signature based systems decreases as the number of new attacks increases because it has to create a new signature for every new attack.

b) Anomaly based detection:

Anomaly detectors are designed to identify abnormal patterns of behavior on a host or network. It functions on the assumption that attacks are different from normal activity and can be detected by systems that recognize these variations. Anomaly detectors create a list of profile data as a normal data representing normal behavior. It automatically detects any deviation of it and generate alarm. It has the capability to detect new types of errors. There are many measures and techniques that are used in anomaly detection including; Threshold detection, statistical analysis, Rule-based measures, other measures, including neural networks, genetic algorithms, and immune system models [6]. One advantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones [5]. It has the ability to detect novel attacks. But this approach produces many false alarms and dally time consuming for research intensive to obtain update accurate and comprehensive profiles of normal behavior [7] . Therefore, it needs a large set of training data with network environment system logs.

c) Specification Based detection:

The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints. The constraints depend on the area where intrusion detection is to be performed.

d) Hybrid detection:

It combines both the methods of misuse based detection and anomaly based detection to improve the abilities of current IDS

e) Specification Based detection:

The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints. The constraints depend on the area where intrusion detection is to be performed.

f) Behavior-based IDS:

Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users. The

model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. Therefore, the intrusion detection system might be complete (i.e. all attacks should be caught), but its accuracy is a difficult issue (i.e. you get a lot of false alarms).

g) Knowledge-based IDS:

Knowledge-based intrusion detection techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. The intrusion detection system contains information about these vulnerabilities and looks for attempts to exploit these vulnerabilities. When such an attempt is detected, an alarm is triggered. In other words, any action that is not explicitly recognized as an attack is considered acceptable .

3. CLOUD COMPUTING ATTACKS:

We will focus on specific problems for various kinds of attacks in the cloud [10]:

a) Wrapping attack
b) Malware Injection attack
c) Flooding attack
d) Data stealing problem
e) Accountability checking.

Some details of above attacks are as follows:

a) Wrapping Attack Problem:

When a user makes a request from his VM through the browser, the request is first directed to the web server. In this server, a SOAP message is generated. This message contains the structural information that will be exchanged between the browser and server during the message passing. Before message passing occurs, the XML document needs to be signed and canonicalization has to be done. Also, the signature values should be appended with the document. Finally, the SOAP header should contain all the necessary information for the destination after computation is done [10]. For a wrapping attack, the adversary does its deception during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message is duplicated and sent to the server as a legitimate user. The server checks the authentication by the Signature Value (which is also duplicated) and integrity checking for the message is done. As a result, the adversary is able to intrude in the cloud and can run malicious code to interrupt the usual functioning of the cloud servers [10].

b) Malware-Injection Attack Problem:

In a malware-injection attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping. This can be accomplished via subtle data modifications to change the functionality, or causing deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. Here the attacker takes his first step by implementing his malicious service in such a way that it will run in Iaas or SaaS of the cloud servers, for example as mentioned in Section I, with deleteUser and setAdminRights. This type of attack is also known as a meta-data spoofing attack [10].When an instance of a legitimate user is ready to run in the cloud server, then the respective service accepts the instance for computation in the cloud. The only checking done is to determine if the instance matches a legitimate existing service. However, the integrity of the instance is not checked. By penetrating the instance and duplicating it as if it is a valid service, the malware activity succeeds in the cloud [10].

c) Flooding Attack Problem:

In a cloud system, all the computational servers work in a service specific manner, with internal communication between them. Whenever a server is overloaded or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service specific server to offload itself. This sharing approach makes the cloud more efficient and faster executing requests [10]. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the cloud server. When processing these requests, the server first checks the authenticity of the requested jobs. Because non-legitimate requests must be checked to determine their authenticity, checking consumes CPU utilization, memory and engages the IaaS to a great extent. While processing these requests, legitimate services can starve, and as a result the server will offload its services to another server. Again, the same thing will occur and the adversary is successful in engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system [10].

d) Data Stealing Problem:

This is the most traditional and common approach to breach a user account. The user account and password are stolen by any means. As a result, the subsequent stealing of confidential data or even the destroying of data can hamper the storage integrity and security of the cloud. The providers face the first strike of such kind of problem [10].

e) Accountability Check Problem:

The payment method in a cloud System is "No use No bill". When a customer launches an instance, the duration of the instance, the amount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. So, when an attacker has engaged the cloud with a malicious service or runs malicious code, which consumes a lot of computational power and storage from the cloud server, then the legitimate account holder is charged for this kind of computation. Though the customer is not aware of the attack and until the main cause of the CPU usage is detected, the providers will charge the customers first. As a result, a dispute arises and business reputations are hampered. All the focus for charging is based on the recorded parameters [10].

4. INTRUSION PREVENTION IN CLOUD COMPUTING:

Intrusion Prevention System (IPS) is a new approach to defense networking systems, which combine the technique firewall with that of intrusion detection properly, which is a proactive technique, prevent the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor, when an attack is identified, intrusion prevention block and log the offending data [7]. IPS monitors network and take actions based on recommended rules when an event occurs. It sits inline on the network and passive in nature. IPSs take detection a step further, some see them as next generation IDS systems [8]. Intrusion prevention is an extension of intrusion detection. An

organization can't protect its network with only firewall, an extra layer of protection must be provided. An intrusion prevention system provides an extra layer of protection by scanning all the network traffic and specific browser protection.

4.1 Approaches of IPS:

One problem faced by all detection in IPS is difficult to identify and recognize analysis of packets in real-time traffic [7]. Three approaches to detect threats are;

4.1.1. Host based approach:

It is a popular approach, it checks for suspicious activity from the host or operating system level. It provides intrusion prevention by triggering an alarm.

4.1.2. Network based approach:

It identify packet all inbound-outbound in the network. In this approach, a system is installed in the network and used to create physical security zones, the network becomes intelligent and is able to quickly and precisely recognize good traffic from bad traffic.

4.1.3. Hybrid Approach:

On network-based IPS, various detection methods, protocol anomaly, traffic anomaly, and signature detection work together to determine a forthcoming attack and block traffic coming from corresponding router.

5. IDS ARCHITECTURE:

Cloud computing is a platform for the users to access various system resources and services; here security becomes a major concern. Some of the security issues are discussed above and IDS is one of the solutions suggested. The review of this paper is based on the architectures of IDS which includes multi-level, hybrid, distributed etc.

5.1 Distributed IDS:

In Cloud computing, massive amount of data is generated due to high network access rate, therefore IDS must be robust against noise data & false positives. Cloud infrastructure has enormous network traffic the traditional IDSs are not efficient enough to handle such a large data flow. Most known IDSs are single threaded and due to rich data flow, there is a need of multi-threaded IDS in Cloud computing environment, hence the distributed IDS[6] was proposed it is shown in Fig 4. Distributed IDS is an efficient and effective Cloud IDS which uses multi-threading technique for monitoring the network traffic and the malicious packets. The system then sends intrusion alarms to a third party monitoring service, which can provide instant reporting to cloud user organization management system with an advisory report for cloud service provider.

Distributed IDS is based on three modules:

Capture and queuing module receives the data packets. The captured data packets are then sent to shared queue for analysis. Analysis and process module receives the data packets from the shared queue and analyzes them against predefined rule set. With the help of an efficient matching and analysis technique the process module detects the bad packets and then the alerts are generated. Reporting module reads the alerts and produces the alert reports for the cloud user and an advisory report for the cloud service provider.

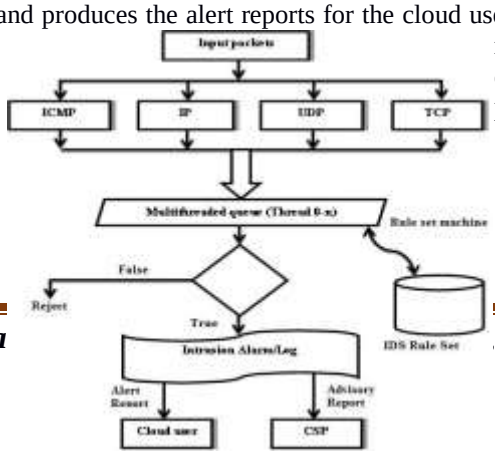

Figure 4: Flowchart for Proposed Model

5.2 Multi-Level IDS in Cloud:

Reducing the number of resources required for IDS implementation is main concern so a new system based on multilevel concept is proposed which deals with effective use of system of resources. The proposed system binds user in different security groups based on degree of anomaly called anomaly level. Refer Fig 5. It consists of AAA module which is responsible for authentication, authorization and accounting. When user tries to access the cloud the AAA checks the authentication of the user and based on it, it gets the recently updated anomaly level. Security is divided into three levels viz. High, medium and low. High Level applies patterns of all known attacks and a portion of anomaly detection when it needs for providing strong security service. Medium Level applies patterns of known attacks to rules providing strong security service. Low Level has flexible resource management and applies patterns of chosen malicious attacks that can occur at high frequency which affect more fatally.

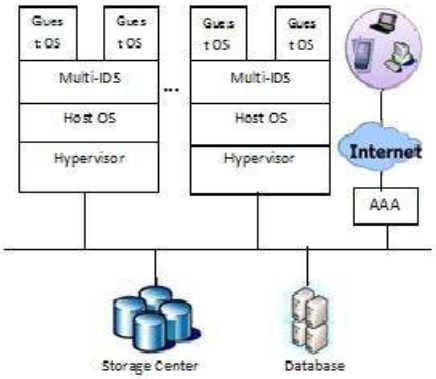

Figure 5: Multilevel Proposed Model

5.3 Improved Hybrid IDS for Cloud

There are many IDS proposed based on signature detection and anomaly detection techniques. Signature based will detect only known patterns of signatures and other will go undetected, where as anomaly detects behavior based malicious activity that leads to high false positive alarms. Many Hybrid based systems are also proposed which are combination of signature and anomaly, network IDS and Anomaly detection and third proposed hybrid system based on biological immunology and mobile agent. Advancement in technology has lead to many new attacks which results in failure of hybrid IDS so we are extending it to improved Hybrid IDS. The Improved hybrid IDS is combination of

anomaly based detection and honey pot technology with KF Sensor and Proposed system of Honey pot technology with KFSebsor Flowmatrix as shown in figure 6.

Proposed system of Honey pot technology and Anomaly based IDS:

Honey pot attracts more and more attackers, the detection obtained can be used to create new signatures and update the database. Finally anomaly can be used to detect unknown attack in the whole network. KF Sensor is a host based IDS which works on the honey pot based technology, it adds the definitions of that attacker to the database for the next time and restrict the entry of that attacker or intruder to the main network of the organization. Flow Matrix is based on Anomaly based detection methodology. It compares the samples from the normal traffic with the regular samples obtained from the network and the moment it finds the difference between the normal and the regular sample it gives an alert.

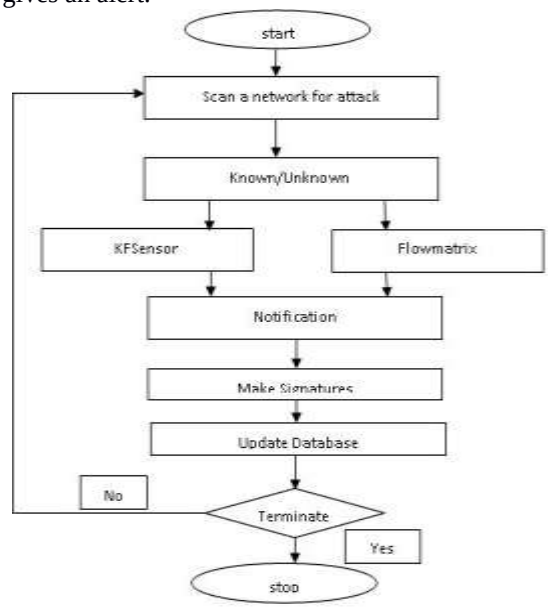

Figure 6: Flowchart for Hybrid IDS

6. CONCLUSION:

Cloud Computing has given rise to a new services paradigm to the information technology. Cloud computing is distributed in nature, hence chances of intrusion is more. Analysing various techniques of intrusion detection and prevention systems has revealed that either using anomaly or signature based techniques stand alone will not provides desired security features. Hence, a hybrid mechanism can be implemented to enhance the detection rate. In the proposed system we will use normal behavior of the system and signatures of various attacks to detect intrusions which is a hybrid IDS. In this paper, we have studied a multi-threaded cloud IDS which can be administered by a third party monitoring service which provides a advisory report to the cloud service provider and an alert report to the cloud user for a better optimized efficiency and transparency for the cloud user. Hybrid IDS combines anomaly detection and honey pot to reduce false alarms and improve performance.

7. ACKNOWLEDGMENT

It is not only customary but necessary for a researcher to mention his/her indebtedness to those who had helped in carrying out and enhance the research work.

I pay my deep regards to God, my Parents and my loving Friends for their support and wishes which made this tedious work easy and successful.

Finally, I would like to extend my thanks to all those who have contributed, directly or indirectly to make this project successful.

8. REFERENCES:

[1] Kleber Vieira, Alexander Schulter,CarlosBecker Westphall, and Carla Merkle Westphall “Intrusion Detection for Grid and Cloud Computing” (IT Professionals, Vol. 12, no. 4, 2010 pp 38-43)

[2] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. Elhariri, Ahmed M. Yousof and Sahar A. Shehata. 2012. A Hierarchical Intrusion Detection System For Cloud: Design and Evaluation. International Journal on Cloud Computing Services and Architecture (IJCSA).

[3] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, Joaquim Celestino Junior. 2013. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications.

[4] S.V. Narwane, S.L. Vaikol. 2012. Intrusion Detection System in Cloud Computing Envirnment .InInternational Conference on Advances in Communication and Computing Technologies (ICACACT).

[5] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande. 2012. Intrusion Detection System for Cloud Computing. International Journal of Scientific & Technology Research Volume 1.

[6] Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah and Al-Sakib khan Pathan. 2012.IPS: An Integrated Intrusion Handling Model for Cloud Computing Environment, International Journal of Computing and Information Technology (IJCIT).

[7] Deris Stiawan, Abdul Hanan Abdullah, Mohd. Yazid Idris. 2011. Characterizing Network Intrusion Prevention System International Journal of Computer Applicationas.

[8] V. Jyothsna, V.V. Rama Prasad, K. Munivara Prasad, 2011, A Review of Anomaly Based Intrusion Detection System, International Journal of Computer Applications.

[9] R. Base and P. Mell.2001. NIST Special Publication on Intrusion Detection Systems. National Institute of Standard and Technology. Dinesh Sequeira. 2002. Intrusion Prevention Systems- Security Silver Bullet?. SANS Institute.

[10] Kazi Zunnurhain, Susan Vrbsky “Security Attacks and Solutions in Cloud”

[11] M. Kuzhalisai and G. Gayathri, "Enhanced Security in Cloud with Multi-Level Intrusion Detection System", IJCCT, Vol. 3, Issue 3, 2012.

[12] Ajeet Kumar Gautam, Dr. Vidushi Sharma, Shiv Prakash and Manak Gupta, "Improved Hybrid Intrusion Detection System (HIDS): Mitigating False Alarm in Cloud Computing", JCT, 2012.

[13] Irfan Gul and M. Hussain, "Distributed Cloud Intrusion Detection Model", IJAST, Vol. 34, September, 2011.

[14] Pradeep Kumar Tiwari and Dr. Bharat Mishra ," Cloud Computing Security Issues, Challenges and Solution "

,IJETAE, Volume 2, Issue 8, August 2012.

[15] Chirag Modi, DhirenPatel, BhaveshBorisaniya, HirenPatel , Avi Patel , MuttukrishnanRajarajan, "A survey of

intrusion detection techniques in Cloud ", JNCA, 2013.