IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

Intrusion Detection System in Cloud Computing

J. Vimal Rosy[1*] and Dr. S. Britto Ramesh Kumar[2]

[1]Research Scholar, St. Joseph's College(Autonomous), Affiliated to Bharathidasan University, Trichy, India

[2]Assistant Professor, St. Joseph's College(Autonomous), Affiliated to Bharathidasan University, Trichy, India

Abstract: Despite of many challenges, security stands first as a major challenge faced by cloud computing because of its open and distributed architecture. Therefore intruders get access due to its vulnerability and in turn they affect confidentiality, availability and integrity of cloud resources and offered services terribly. As the researchers and technologists long for an improvement in cloud computing security poses a major challenge due to its open and distributed architecture. So it easily falls a prey to intrusion affecting confidence, availability and integrity of cloud resources as well as offered services. Recently, IDS has become the most necessary compounds that are used in computer system security and compliance practices that save cloud environment from several kinds of threats and attacks. This research paper is presented in tune with the cloud architecture, projecting an overview of different intrusions in the cloud in defense of the challenges and essential characteristics of cloud based IDS (CIDS) and detection technique used by CIDS and their types too.

Keywords : Cloud Computing, Intrusion Detection System, Cloud Security, Signature; Anomaly ,IDS.

I. INTRODUCTION

The most desired development in the world is Cloud Computing. Then what is Cloud Computing? National Institute of Standards and Technology (NIST 2011) has beautifully defined Cloud Computing as Cloud Computing[21] is rapidly growing computational model delivering convenient, on demand networks access to shared pool of configurable computing resources such as networks, servers, storage, application, etc. as service on the internet for satisfying computing demand of users. It contains three basic abstraction layers namely system layer (It is a virtual machine abstraction of a server) next the platform layer (It is a virtualized operating system of a server) and thirdly application layer which includes web application.
The characteristics of Cloud Computing are enumerated below:

Virtual:
In physical location and underlying infrastructure, details are transparent and open to users.

Scalable:
It is the ability to break the complex workloads into pieces to be available across on incrementally expandable infrastructure.

Efficient:
Services are oriented architecture for dynamic provisioning of stored computer resources.

Flexible:
As the very word means, it is able to serve a variety of workload types may be consumer or commercial.
Apart from that, Cloud Computing has also three service models, they are (Paas) Platform as a service, (Saas) Software as a service models and Infrastructure as a service model (IaaS) delivers services to providers by maintaining large infrastructures like hosting server managing networks and other applicable resources for clients. Paas extends development and deployment tools, languages and APIs used to build, deploy and run apps in the cloud. SaaS help giving complete online applications through systems which can be directly worked out by their users and so they are worriless of installing and running software services on their own machines easily.

Threat Model for Cloud
Many researches are of the opinion that security is the stumbling block in the cloud because it cannot control over the cloud software platform and/ or infrastructure. The Cloud Security Alliance (CSA) and IEEE opine that enterprises across sector like to adopt Cloud Computing but both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers, security is a must and an important factor. Among many major issues in security, in the cloud, Detecting and preventing network intrusions becomes prominent [20]. As the network is considered as the backbone of

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

cloud, its vulnerabilities in network directly affect the security in cloud. Major two types of threats are insider and outsider attacks, attacker within a cloud network and attacker outside the cloud network respectively.

Insider Attackers

Being a serious threat issue, the authorized users may try to gain or misuse unauthorized privileges by committing fraudulently by way of revealing information to other unwanted users or modifying the same want only [22]. To site an example, an internal Dos attack is quoted against the Amazon Elastic Compute Cloud.

Outsider Attackers

The very word denotes the attack from outside. The attackers perform different attacks [23]. They are listed below. IP Spoofing, Address Resolution Protocol (ARP Spoofing) DNS Poisoning, man-in the middle, Denial of Service (Dos), Distributed Denial of Service (DDOS) attacks, phishing attack, user to root attack, port scanning, attack on virtual machine (VM) or hypervisor such as BLUEPILL and DKSM. Through these attacks, the so-called hackers gain entrance over the host and make back door channel attacks etc. Consequently integrity, confidentiality and availability are totally affected the cloud resources and offered services. To safeguard against the attacks major cloud providers like Amazon Ec2 Windows Azure, Rack space, Eucalyptus, open Nebula etc have found a way to use firewall.

It is the firewall [18] that gives protection even at the front access points of system and it depends on attacks. Through firewall identifies the packets only at the front boundary of a network, it cannot detect insider attacks absolutely. Moreover, DOS or DDOS attacks are so complex that it cannot be detected by traditional firewall. To make it clear, if there is an attack on Port 80 firewall is unable to differentiate normal and legitimate traffic from DOS attack traffic flow. So, one cannot expect only traditional firewall blocks all the intrusion. Therefore, it is not at all an efficient solution.

There is a way of overcoming such problems, an IDS offers a helping hand. The idea of IDS was proposed by Anderson in the year 1980. Since then, IDS has been playing a dominant role in the security of cloud. It is because IDS not only acts as an additional preventive layer of security, but also it detects known attacks as well as unknown ones. In fact, we learn from the guidance of NIST, Intrusion detection [18], as it is defined, the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents which are violation of computer security policies, acceptable use policies or standard security practices.

The remaining section of the study deals with the following sections:

II. Cloud Architecture

III. Possible Intrusions in the Cloud

IV. Challenges and Essential Features of Cloud IDS

V. Technology used by IDS

VI. Different types of IDS in the cloud

VII. Existing Cloud IDS

VIII. Conclusion

II. CLOUD ARCHITECTURE

The architecture of cloud is formulated with multiple cloud components communicating with each other over the Application Programming Interface (API)s usually web services. In fig1 Cloud Computing architecture [19] is described and it consists of mainly two ends. The frontend for cloud users and cloud manager and the backend for host machine, virtual network and virtual machine. The frontend is the part visualized by the client, the customer. It is also the usage of client's network or computer and the application used to get access the cloud through a user interface like a web browser.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

Fig1. Architecture of Cloud Computing

On the contrary, the cloud itself becomes the backend of the cloud computing architecture. It consists of various computers, servers and data storage devices. The cloud users use the frontend demand the instances offered services through internet. Thus, the cloud controller manages cloud applications through their entire life cycle right from provisioning to monitoring including metering and billing. Computer hardware and software handle the user's query and control the system software on its node, all form the host machines. Host operating system and hypervisor respond to queries and control request from the front end. Virtual network (internet network) is designed for VM instance interconnectivity.

III. CHALLENGES AND ESSENTIAL CHARACTERISTICS OF CLOUD IDS

The challenges in cloud IDS are listed below:

➢ **Virtual Environment is Attacked**

In a virtualized environment VMs start communicating over network backplane rather than a network. Consequently, the standard network security controls are built to this traffic and so it cannot safeguard security control for supervising and in-line blocking. In that situation a malicious user with a VM instance can do many attacks like Hyper Jacking, VM hopping, VM migration and easily control other's VM or host machine. Unless cloud NIDS have the ability to monitor and detect intrusions from network traffic between VM and the host.

➢ **High Network Traffic:**

Of late, cloud is an emerging computing model that provides various advantages fulfilling economic and business wants. So, the cloud users are approaching at very high rate.

Unexpectedly, a heavy network traffic is jammed due to a great number of cloud users. It is the IDS to handle such traffic quickly. If not, a high probability of packet dropping will be created.

➢ **NIDS Development:**

Now, monitoring and regulating both external and internal traffic has risen as a major challenge in Cloud. It has to secure and protest front end and back end of cloud because of the distributed and visualized nature of cloud. Therefore, IDS should be deployed in such a way that they can detect internal attacks, external attacks and distributed attacks like DDOS attacks in the widespread cloud network.

IDS and its most needed characteristics for the cloud. The following characteristics are needed for integrating IDS in the cloud:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

1. Detection of Attacks on Each Layer

IDS should have the capacity to detect intrusions at each component of cloud architecture (ie) at the frontend or backend. Another capacity is to detect known as well as unknown attacks thoroughly.

2. Low- Computational Cost and Faster Detection Rate

Since a large number of users try to occupy in cloud resulting a high quantity of requests create a high traffic rate in cloud, IDS should have detection fast of course, at lower cost.

3. Low False Positives and Low False Negatives

A situation where an IDS triggers a false alarm when there is no attack and it is a wrong alarm it is called low positive. Whereas, false negative is defined as an inability of IDS to detect the true intrusion during which case, malicious activity is neither detected nor alerted. So, it is needed to keep very low false negative and false positive in the cloud to admit legitimate network packets and thus protecting network against unwanted traffic. We have, fortunately, some actions to reduce the chance of false negative conditions instead of increasing the number of false positive.

IV. INTRUSIONS IN CLOUD

Cloud Computing is the peak in the dynamic IT world where researches and technologists spend their time, money and energy to shape, mould and change according to the dire requirements of Cloud Computing. Most of the organization are moving their IT systems and upholding their huge quantity and sensitive data into the Cloud Computing paradigm. No doubt, its encouraging features of easy to usage, reliability, availability, cost efficiency attract everyone in economic and business arena.

Besides, its advantages, Cloud computing blinks with security risks confidentiality, integrity and availability are questioned when uninterrupted service of cloud technology mostly attract intrudes to gain access and misuse services and resources which are provided by cloud service provider. Let me pinpoint the typical attacks namely denial of service (DOS) attack, user to root attack below.

Denial of Service (DOS) Attack:

The other name for Denial-of-Service Attack is flooding attack [23]. Here the attacker tries to flood virtual machine by sending huge amount of packets continuously from innocent hosts in the network. Also, a hacker consumes the bandwidth of the network through worms for example. They in turn replicate themselves and spread within short duration to a large number of computers, leading to network congestion. Packets can vary, UDP, TCP, ICMP or mix of them. After all, the aim of this attack is simply the denial of access for legitimate users and above all hack the resources in the cloud.

The move IT field has taken steps to diminish the attacks, the move it spreads and spoils the industry. Anyhow, Cloud Computing is not quiet and proceeds with new vigor and introduces new dimensions of defense. Let us see how attacks differ in a way. When a single server is attacked providing a certain service, the attacker causes a loss of availability of the service. This is called Direct DOS Attack [22]. When the server's network resources are completed and exhausted by processing the flood request, the other service instances on the same network machine are unable to perform their intended tasks. Such type is called Indirect DOS Attack. This kind of attack is very difficult to detect and filter. Because some packets that cause the attack are very much the same to legitimate traffic. So, IT industry is facing the biggest threat the DOS Attack. Its intensity, size and frequency of the attacks are increasing day by day as the observation criteria states.

User to Root Attack

Massachusetts Institute of Technology (MIT Lincolin Laboratory) reveals that exploits are a class of exploit where the attack starts with access to a normal user account on the system. Probably by sniffing passwords, a dictionary attack or social engineering, the attacker is able to exploit some vulnerability to reach root access to the system. They are of different types like buffer overflow attacks, Perl, xterm etc.

In buffer overflow attack [23], it overflows and generates root shells from a process running as root. It appears when application program code overfills static buffer. The mechanisms which are used to secure the authentication process are a frequent target. But till now, there are no universal standard security mechanism which can be used to prevent security risks like weak password, recovery overflows, phishing attacks, Key loggers etc. But Concerning Cloud, attacker acquires access to valid user's instances that enables him/ her for gaining root level access to VM or Host.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

V. DETECTION TECHNIQUES USED BY IDS

Figure 2 vividly shows that two main intrusion detection techniques are used by IDS. They are anomaly detection (It is based on behavior of users) and signature detection (It is based on signature of known attack). To achieve a better result and improve its performance, it is suggested to use a combination of two techniques that may be called Hybrid Detection.

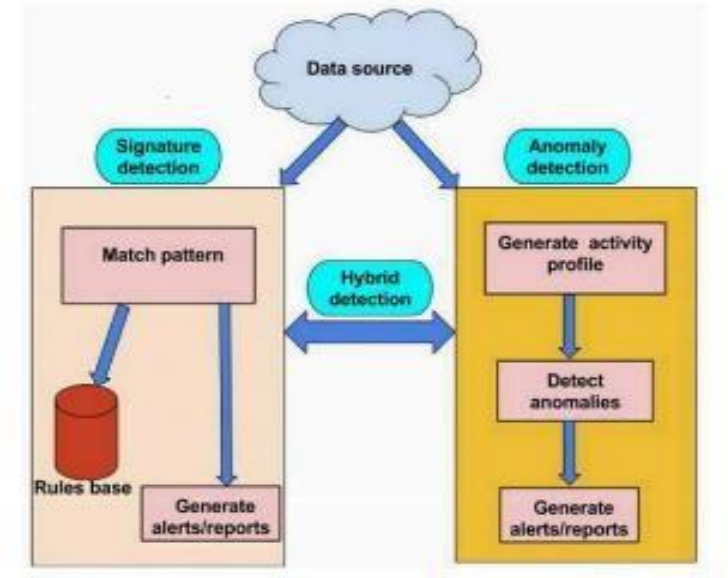

Fig2. Intrusion Detection Technique

Signature Based Detection:

The performance of signature-based detection [17] works out like this. When the information collected from a network or system, it starts comparing with a database of signatures. A signature is a predefined set of patterns or rules that coincides with a known attack; we recognize this tech as misuse detection. In a way, these signatures are composed by several elements which allows identifying the traffic. For example, in snort the parts of a signature are the header that is address source, address destination, ports and its options (example payload, metadata). To decide whether the network traffic corresponds to a known signature or not IDS makes use of pattern recognition techniques. Snort, network flight recorder, network security monitor and network intrusion detection are the approaches used by some IDS.

They easily detect known attacks with negative false alarms. So, signature-based method helps network manages with average security expertise to find out intrusions minutely. There is another advantage to add new signature without modifying the old one in the database. So, it is rather a flexible approach. Anyhow, the disadvantage is its inability to detect unknown attacks, that is to say any new attack pattern or a change in the previous attack pattern with attack signature will not be detected at all.

Anomaly Based Detection

Unlike other detections, anomaly-based IDS [17] is capable of finding out any suspicious activity on the system. It will be all right in on normal behavior rather than attack behavior. When any significant deviations or expectations from the normal behavior it takes for granted that the attacker behavior differs to that of a normal user. So, the model is being called anomaly.

The new approach [10] first compares current user activity with pre-loaded profiles of users or network in order to detect abnormal or unusual behavior causing intrusions when profiles are developed by using different features such failed login attempts, number of times a file is a particular time duration, computer usage etc. anomaly-based detection is producing the desired result against unknown attacks.

Hybrid Detection

A combination of signature based and anomaly-based techniques [17] will surely improve the efficacy of IDS and it is called Hybrid Detection. The aim of implementation of hybrid detection is based on signature and an anomaly detection technique is only to detect known and unknown attacks together.

Types of Cloud Based IDS

Fig 3 depicts the four divisions of cloud-based IDS [18] and each type is elaborately described below.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

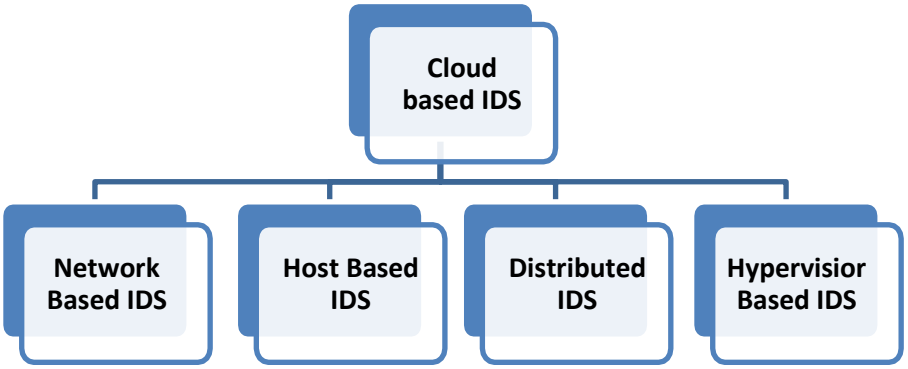

Fig 3. Types of Cloud based IDS

1. Network Based IDS (NIDS)

It is so designed that it is able to detect the captured traffic of entire network and try to analyze it for any signs of malicious activities or events such as DOS Attack, port scanning, user to root attacks etc. Not only has that it detected unauthorized use, misuse and abuse of computer network by both insider and external intruders. Usually through inspection of the IP and transport layer headers of each pocket, it performs intrusion detection. The use of anomaly and or signature-based detection makes IDS identifying the intruders instantly [18].
Both signature detection approach and the anomaly detection method the former for looking for the correlation of captured packet with signature of known attacks and the latter for comparisons of the user's current behavior with previous behavior, jointly helps IDS for detection. Moreover, if traffic is encrypted, it cannot perform analysis and detect intrusions inside a virtual network contained by hypervisor.

2. Host Based IDS (HIDS)

First of all HIDS [18] detects any unauthorized and intrusions events by monitoring and analyzing the collected information from a specific host machine. The information like file system issued, network events, system calls etc are detected intrusion for the machine. It also deeply observes modification in host kernel, host file system and behavior of the program or change of system or program it reports to network manager that system is under attack. HIDS can be more effective and improved by specifying the features that provide it more effective for detection. However, it should require more storage for information for analyzation. As for cloud computing network concerns there is possibility of deploying HIDS on hypervisor VM or host to analyze the system, user login information or access control policies and detects intrusion atmosphere. In that situation, cloud user is responsible for monitoring and management of HIDS deployed on a V and at the same time cloud provider is responsible for the deployment of HIDS on hypervisor. Above all it is the responsibility of the providers to make sure that they are providing adequate IDS in their side. Thus, HIDS is able to analyze encrypted traffic. So HIDS becomes a protector of the integrity of software.

3. Distributed IDS(DIDS)

In a distributed IDS(DIDS) [18] numerous IDS (such as NIDS, HIDS) are deployed over a large network in order to monitor and analyze the traffic for intrusive detection behavior. The partaking IDS can communicate with each other or with a centralized server. Each individual IDS has its own functional components. They are detection components and correlation manager. The first one examines systems behavior and transmits the collected information in a standard format to the correlation manager. The other one, correlation manager combines data from multiple IDS and generates high level alerts to keep off a correspondence to an attack analyze phase makes use of signature based and anomaly-based techniques. Therefore, IDS can fulfill detection of known as well as unknown attacks. Again, in case of cloud, DIDS can be placed at any of two positions at processing server or at host machine.

4. Hypervisor Based Intrusion Detection System

By way of improving the system, Hypervisor Based Intrusion Detection System
[18] is introduced. It provides a platform to run VMS. Hypervisor Based IDS is deployed on the hypervisor layer. There available information for detection of anomalous activities and events are allowed for monitoring and analyzing them. Here, the type of information based on communication between VMS and communication within the hypervisor based virtual network is monitored and analyzed.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114106

VI. ANALYSIS OF EXISTING CLOUD-BASED INTRUSION DETECTION SYSTEM (CIDS)

We pass on to this section where different (CIDS) [17] are presented and the same are classified into three categories based on the intrusion detection techniques used by each system. The categories are signature based, anomaly based and hybrid. Let us check each system and analyze them to evaluate whether they meet out the security requirements of clouds or not and useful in cloud computing.

Signature Based Detection

Signature Based IDS, it analyses the content of each packet at layer and compares it with a set of pre-defined signatures. The advantages are listed below.

1. It works similar to Antivirus.
2. With low false positive rates.
3. It is highly effective towards well-known attacks.

At the same time, it fails to identify zero-day attacks and advanced malware attacks. So, it can be passed by changing the signature of attacks. By using multi server in private cloud to detect malicious activities and events and to protect cloud resources and services against intrusions from both inside and outside of the system [17]. Each sensor installed in the private cloud is based on snort IDS and it works accordance with geared short IDS rules installed on their own selves to catch intrusion. Once intrusions behavior is detected by each IDS sensor, it will generate alert and store it into an alert and store it into an alert event database [17].

Anomaly based Detection

Anomaly based IDS detects the abnormal behavior in the computer systems and computer Networks. Thus, the deviation from the normal behavior is considered a attacks. In an anomaly detection, it monitors network traffic. Then it compares it with an established baseline for normal use. Apart from it, also classifies it whether it is normal or anomalous. It is clear that it is based on rules rather than patterns or signatures. It can be easily accomplished by using at strict mathematical mode. Additionally, it is prone to high false positive rate. So, it is more effective and accomplishing. A. Patel et al. in [8], Lee et al. in [9] and Dastjerdi et al. in [10] have used anomaly-based intrusion detection system to identify intrusions in cloud.

Hybrid based Detection

HIDS is introduced to identify known and unknown attacks as well [17]. This method is the combination of IDS for identifying known attacks and ADS is for unknown attack identification. Whenever it occurs with high false alarm. It creates signature based on anomaly detected and stored in signature dbase.

CONCLUSION:

To safe guard confidentiality, integrity and availability of cloud resources and services, it has been our task of trying several intrusions which have been described earlier fire wall only may not be capable of defending the cloud sufficiently, of course against these threats. Really, it has no ability to detect insider attacks not only over physical n/w but also over virtual n/w within hypervisors. Meanwhile, few DOS attacks are so complex that it cannot detect by using traditional firewall. So, a second line of defense after the firewall is needed to address this issue incorporating the IDS in cloud environment. It will surely enhance the security. The IDS is an important component to detect cyber-attacks. In continuation of further research, we have laid emphasis the challenges and essential characteristics of cloud-based IDS. To achieve this, a detailed description of various techniques and types is also provided. In fine, we conclude that the hybrid ids approach is sure for certain is the best detection technique used by the IDS. But the most cloud-based IDS do not consider at tall the performance, challenges of the Cloud Computing. In order to have an efficient and effective CIDS, we have to use the hybrid approach to detect intrusions. It will in a way, satisfy security issues and performance challenges of Cloud Computing as well.

REFERENCES:

[1] F. Grobert, C. Willems, and T. Holz, “Automated identification of cryptographic primitives in binary programs.,”in RAID, Springer, vol. 6961, 2011, pp. 41–60.
[2] P. Ghosh, A. K. Mandal, and R. Kumar, “An efficient cloud network intrusion detection system,” in Information Systems Design and Intelligent Applications, Springer, 2015, pp. 91–99.
[3] S. Yu, X. Gui, J. Lin, F. Tian, J. Zhao, and M.Dai, “A security-awareness virtual machine management scheme

DOI: 10.17148/IJARCCE.2022.114106

based on chinese wall policy in cloud computing," The Scientific World Journal, vol. 2014.

[4] Brandon Lokesak (December 4, 2008). "A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems" (PPT). www.iup.edu.

[5] Z. Al-Mousa and Q. Nasir, "Cl-cidps: A cloud computing based cooperative intrusion detection and prevention system framework," in Future Network Systems and Security, Springer, 2015, pp. 181–194.

[6] C. Mazzariello, R. Bifulco and R. Canonico, "Integrating a Network IDS into an Open-Source Cloud Computing Environment", 2010 Sixth International Conference on Information Assurance and Security, pp. 265-270.

[7] A. Bakshi, Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in Virtual Machine", 2010 Second International Conference on Communication Software and Networks, pp. 260-264.

[8] A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior and C. Wills, "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System", Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), pp. 223-234.

[9] J. H. Lee, M. W. Park, J. H. Eom, T. M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", ICACT, 2011, pp. 552-555.

[10] W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, 2004.

[11] K. Vieira, A. Schulter, Carlos B. Westphall, and C. M. Westphall, "Intrusion Detection for Grid and Cloud Computing", IEEE Computer Society, (July/August 2010), pp. 38-43.

[12] S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, A. Misra , "Intrusion Detection System in Cloud Computing Environment", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011), pp. 235- 239.

[13] S. Bharadwaja, W. Sun, M. Niamat, F. Shen, "Collabra: A Xen Hypervisor based Collaborative Intrusion Detection System", Eighth International Conference on Information Technology: New Generations, 2011, pp. 695-700.

[14] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, et al., "NIST cloud computing reference architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500- 292)," 2012.

[15] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert systems with Applications, vol. 29, pp. 713- 722, 2005.

[16] Dr. S.Vijayarani and Ms. Maria Sylviaa.S; (2015). "Intrusion Detection System: A Study." International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1.

[17] H. J. Liao, C. H. R. Lin, Y. C. Lin, K. U. Tung, "Intrusion Detection System: A Comprehensive Review", Journal of Network and Computer Applications 36 (2013), pp. 16-24.

[18] M. Parag, K. Shelke, M.Sontakke and Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.

[19] "Luit Infotech: What is Cloud Computing", Download, pp 1-3. http://www..luitinfotech.com/kc/what-is-cloud-computing.pdf 2013.

[20] Martin L , Trust and security to shape government cloud adaptation http://www.lockheedmartin.com/cloud computing –White paper pdf.

[21] National Institute of Standards and Technology (NIST). (2001). Intrusion detection Systems (Publication No. 800-31). Gaithersburg. MD: National Institute of Standards and Technology (NIST).

[22] A. J. Duncan, S. Creese, and M. Goldsmith, "Insider Attacks in Cloud Computing," Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,Liverpool, 2012, pp. 857–862.

[23] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M.Rajarajan, "A survey of intrusion detection techniques in Cloud,"Journal of Network and Computer Applications, vol. 36, no. 1, pp.42–57, January 2013.

