Intrusion Detection and Prevention System in enhancing Security of Cloud Environment

Koushal Kumar
Assistant Professor, Department of Computer applications
Sikh National College, Qadian (GSP)

Abstract: **These days, many service providers host their services on cloud platform to provide easy and simple accessibility of computing resources to cloud consumers. The major benefits cloud computing provides is network based access to computing and data storage services on a pay per usage model. While Cloud services provide adaptability, scalability and economical assurance, there have been commensurate concerns about security. Because of the distributed nature and open structure of the cloud computing its resources, data and applications are easy and attractive target for potential cyber attacks by intruders. In this manner integrity, secrecy and availability of all these resources need to be defended against various conceivable threats. So Intrusion Detection and prevention systems (IDPS) are deployed in the cloud environment to detect malicious behavior over the network and in the host machines. IDPS is a software or hardware system that has all the capabilities of intrusion detection and can react effectively in case of possible intrusions. In this paper author examining the impact of applying IDPS in cloud environment and trying to find out how IDPS helps in maintaining the security of cloud resources with a brief explanation about the types of IDPS used in cloud environment.**

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

I. INTRODUCTION

Cloud Computing has recently came into light as a progressive paradigm for managing and delivering services over the internet. The vision of this new computing paradigm is unbounded, with interesting potential to enhance our everyday life and has a great importance in technical, social, and monetary aspects. Cloud computing is viewed as promising computing paradigm which gives virtually boundless storage capabilities abilities, high accessibility, tremendous fault tolerance, scalability and extensive processing power. The term cloud has been utilized to allude to platforms for distributed computing where shared resources such as software, platform, infrastructure, storage and information are provided to consumers over the internet on request premise. Experts from various domains of computer technology are expecting an immense growth of cloud computing with time and foresee that in the few coming years cloud innovation will reshape the traditional computing. Cloud computing is the consequence of the development and adoption of existing technologies and paradigms. The foundation of cloud computing is based upon grid computing, utility computing, distributed computing and cluster computing [1]. Numerous IT giants companies, such as Amazon, Oracle, Google, facebook, and Microsoft and so on, accelerate their paces in developing cloud computing systems and facilitating its services to a larger group of users. The objective of cloud computing is to enable clients to take profit from all of these technologies, without the requirement for profound learning about each one of them. Users just need to have access of internet via different devices and cloud services are just one click away and can be accessed from anywhere. The users who wish to utilize cloud computing based services provided by cloud computing providers over the web can use a variety of devices like PC, laptop, Smartphone's and PDA. Figure 1 show the general high level architecture of cloud computing which clearly illustrates the

three layers model and functioning of layers is explained in section II of this paper. Cloud data storage is a major component in the cloud computing paradigm because without cloud storage we cannot expect cloud services. Following are some of examples which provide cloud storage publically without any charges.

- Skydrive associated with Microsoft allow the customers to store manage and share nominated files on the Microsoft public cloud storage.
- IBM cloud offers different storage options, including archive, backup and data storage features 24*7 for customers.
- Email services, such as Gmail, Hotmail and Yahoo provides free storage services to users for storing user emails and attachments in their respective storage clouds.
- Facebook and you Tube offers their users to store and share photos and video over the web.

Cloud computing enables organizations to avoid upfront infrastructure costs (e.g., purchasing servers) as it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure [2] [3]. Cloud providers commonly utilize a "pay as you go" model and provide better utilization of resources and hence reduced service access cost to individuals. Figure 1 shown below illustrates the architecture of cloud model.

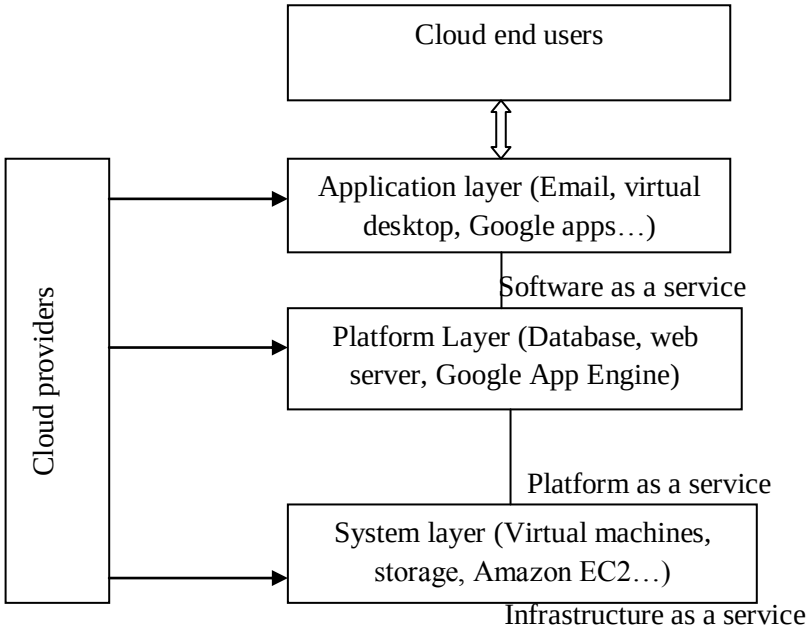

Figure 1: Architecture of cloud storage

Clouds storage model can be Partioned into three main categories a) Public cloud b) Private cloud c) Hybrid cloud. In Public cloud model resources or services are progressively allowed over the web by third party cloud provider to the clients as per their requirements. All the administrable tasks related with cloud storage such as upgrading, modification, replacement and deletion are carried out by cloud providers. One of the important benefits cloud provides to its customers is pay per use model where the customers pay for services or computing resources they have used. They can scale up or scale down the usage according to their needs also known as elasticity which is another feature of cloud computing. For example by implementing cloud storage feature, an organization pays only for the amount of storage that

is actually used rather than paying for spare capacity that remains idle until needed. In public cloud applications and resources from various customers are likely to be combined together on the centralized cloud server storage. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds. Security and multitenancy are critical factor behind the slow adoption of cloud computing, thus its responsibility of cloud providers to provides secure encryption for sensitive data along with username and password level security. While on the private cloud resources, services and infrastructure are maintained on a private network (intranet). The management of data and resources can be done either by the client or can be outsourced to a service providers depends upon requirements of the organization. Private clouds offer the greatest level of security and control because data is secure behind enterprise firewall and another security components [4]. On the other hand a hybrid cloud includes a variety of public and private options with multiple providers. Hybrid cloud paradigm merges multiple public and private cloud models together for resource management purposes for example, critical data of enterprises can be stored in a dedicated local private cloud for security reason and less important data can be maintained in public cloud storage. However it adds a significant level of complexity in resource distribution over public and private clouds. Figure 2 illustrating the types of cloud.

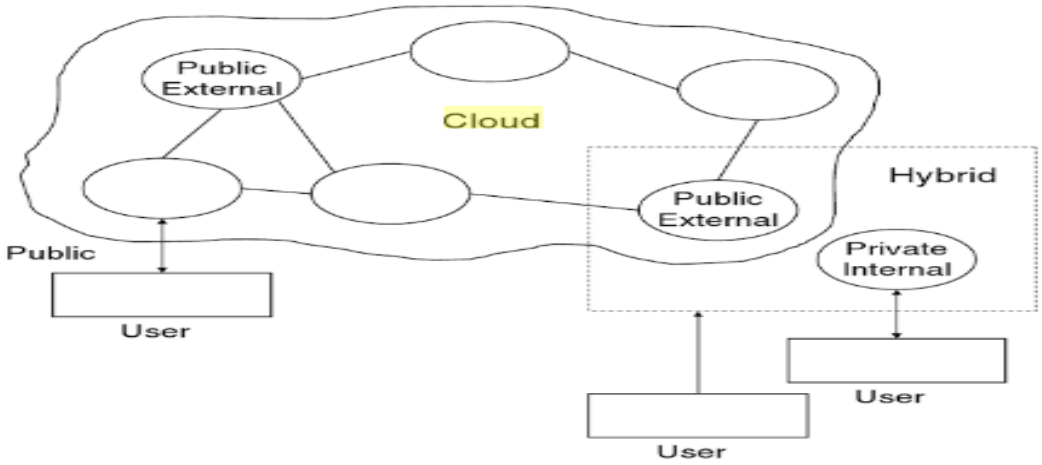

Figure 2: Types of Cloud Computing

Along with various advantages of Cloud computing it likewise brings new security assaults and challenges about safety and reliability of customer's resources stored over the web. The fully distributed and open structure of cloud computing services turns into a significant more alluring target for potential intruders. There are various security threats in cloud model, and these relies on the service provision and deployed cloud models. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own cloud and migrating to Cloud services. According to experts who are working the cloud computing field cloud environments face many of the same threats as conventional corporate networks due to immense data storage on cloud server. Similar to "firewall" another buzzword has recently become very popular i.e., Intrusion Detection and Prevention System (IDPS) which are one of the practical solution to resist all kinds of cyber attacks [5]. Experts believe that security risks associated with cloud environment hinders its widespread adoption. Efficient intrusion detection and prevention systems (IDPS) should be incorporated in Cloud infrastructure to mitigate all kinds of possible attacks in network.

II: CLOUD SERVICE MODELS

The ability to perform Intrusion detection in the cloud is heavily dependent on the type of model you are using for your cloud environment. Choosing the right service model is a dominant success factor for delivering cloud services. Each cloud model serves a level of abstraction which reduces the effort needed by the service consumer to use the system services. Clouds computing service models can be classified into the three types SaaS, PaaS and IaaS.

SaaS (Software as a Service) provides ready online software solutions with software as a service (SaaS) permits organizations to get into business functionality a very low cost normally less than paying for licensed applications in view of the fact that SaaS charges are built on a monthly fee. Software-as-a-Service eliminates the all possibilities for organizations to handle the installation, set-up, daily preservation and maintenance: examples include online mail, project-management systems, and social media platforms.

PaaS (Platform as a service) model, serves both hardware and software infrastructure to cloud service consumers. The platform cloud provides a high-level integrated environment to develop, test, and deploy custom applications. In PaaS cloud suppliers brings a computing platform, naturally comprising Operating System, Programming Language execution environment, database and web servers. User applications can be develop on this virtualized cloud platform without worrying about the handling of underlying cloud infrastructure.

Infrastructure-as-a-Service (IaaS): In a traditional approach on-premise data center, the IT team is responsible for building and managing everything. For example the team is purchasing commercial or business software products, they have to manage and install it on one to many servers by ensuring the adequate level of security requirements. But in cloud infrastructure such as hardware, servers, routers, storage, and other networking modules all are granted by the IaaS supplier. The end user takes on these offered services based on their requirements and pay for what they have used. The end user does not need to supervise or monitor the core cloud infrastructure, rather cloud service consumers can focus more on their business problems [6].

III. INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

Intrusion can be characterized as a deliberate and unauthorized attempt of damaging the privacy, integrity, or availability of system resources. Attacks on the network mostly occur in distinctive groups called incidents. Although many incidents are malicious and vulnerable in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization. The greater the information sent or received into the cloud or from the cloud, the greater the security risk. An Intrusion detection System (IDS) is defined as an effective security technology, which can detect, prevent and possibly react to computer related malicious activities. Modern IDS have the ability to analyze, identify and respond in real time to malicious threats. These systems are thus called IDPS as they seek to monitor the behavior of users, networks or computer systems in order to detect and prevent intrusions. The primary goal of Intrusion Detection and Prevention System (IDPS) is to provide a view of unusual activity happening in your network and to generate alerts notifying administrators or blocking a suspected connection. An IDPS records and monitors all inbound and

outbound network traffic and identify suspicious activities which tries to break network security policies and takes corresponding actions [7]. Modern IDPSs can remove or replace malicious part of the vulnerable data packet to make it benign. An IDPS are composed of from four different fundamental components such as sensors (event detector), analyzers, databases and central response engine. Sensors detect security events, console monitors events and Central Engine records events logged by the sensors in a database and use a system of rules to generate alerts from security events received. ***Figure 3*** illustrates the typical basic model of IDPS.

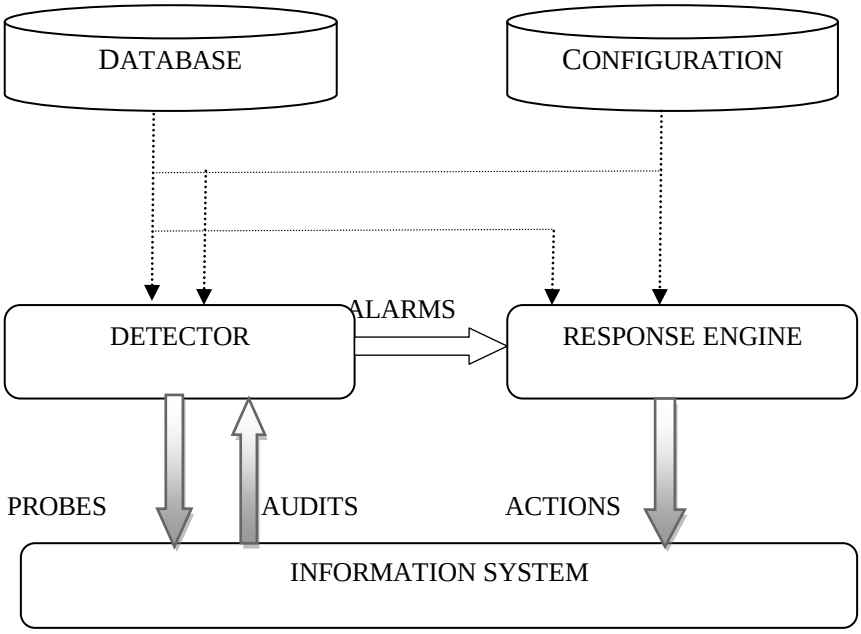

Figure 3: A simple IDPS in Cloud Computing

IV. ATTACKS TYPES IN CLOUD ENVIRONMENT

While moving from conventional service providing approach to cloud computing based approach new security and protections challenges has risen in the recent time. The majority of the attacks or intrusions are mainly centered on the availability of services, manipulation, confidentiality and integrity of the data. In cloud computing security threats are from outsiders as well as from insider's users. Thus security of the cloud resources can be considered in two aspects: Physical security and cyber security. Physical security is the protection of hardware, software, networks and data from physical actions and events that could cause serious loss or damage to cloud environment. This includes twenty four and seven days monitoring for conditions like heat, humidity, fire, flood, natural disasters etc. cyber security deals with the techniques of protecting computers, networks resources, users data from unauthorized access or attacks that are aimed for exploitation. Broadly we can classify security related attacks in two categories I.e. **Passive Attacks and Active Attack**

The major difference between both kinds of attack is the way how intruder makes use of information. The term passive indicates that the attacker does not attempt to perform any modification to the data. In passive attack mode intruder only monitor the transmission of information that is send by source to destination but does not affect the system resources. In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non disruptive but are information seeking, which may be critical in the operation. A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. Passive attackers mainly perform the following activities

• Network traffic analysis

• Decrypting weakly encrypted message

• Collecting authentication information (passwords)

Passive attacks are very hard to detect so general approach to deal with passive attacks is to apply prevention actions. On the other hands ***Active attacks*** are based on modification of the original secret message or creating a false message so that receiver could not understand the original message. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network. The action of an active attacker includes injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non-repudiation paradigm. These kinds of attacks can be detected with some extra effort. In active attacks intruder try to access system resources and harm the system and its operations. Masquerade, Replay, Alteration of message, Denial of service attack (DOS) etc are the category of active attacks. The most popular active attacks in the cloud computing environment are discussed briefly here:

Denial of Services (DOS): Network layer of the TCP/IP model is the main point of DOS attack, this attack is accompanied with IP spoofing and flooding. These types of attack prevent legitimate users from accessing some services or resource, which they are eligible for by flooding unnecessary packets over the network. If DoS is initiated from more than one source machine which are controlled by a master node then it is referred as Distributed Denial of Service attack (DDoS) attack. While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flooding attacks can be more difficult to recover from.

Spoofing this is when a suspicious third party user impersonates another device or user on a network in order to attempt attacks against network hosts. This type of attack is usually considered as an access attack and there are various types of spoofing attack like ARP spoofing, DNS server spoofing etc.

Backdoor path attacks Hackers continuously access the infected machines by exploiting passive attack to compromise the confidentiality of user information. Hacker can use backdoor path to get control of infected resource launches DDoS attack [8]. This attack targets the privacy and availability of cloud users.

Virtual Machine Attacks: Virtual machines are one of the most attack prone part of the virtualized environment. In cloud environment attackers effectively control the virtual machines since they are easily accessible by tenant's users. The most common attacks on virtual layer are Sub Vir, BLUEPILL, and DKSM which allow hackers to manage host through hypervisor. Attackers easily target the virtual

machines to access them by exploiting the zero-day vulnerabilities in virtual machines [9] this may damage the several websites based on virtual server.

Service Hijacking: Service hijacking may redirect the client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. Phishing attack, fraud, exploitation of software vulnerabilities, reused credentials, and passwords may pose service or account hijacking. This threat can affect IaaS, PaaS, and SaaS.

Hacked interfaces and API: For all intents and purposes each cloud administration and application now offers APIs. Various IT developer groups utilizes interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management, orchestration, and monitoring. The security and accessibility of cloud services from authentication, authorization, encryption and activity monitoring is fully dependent on the security of the API provided. Risk increases with third parties that rely on APIs and build on these interfaces. APIs and interfaces poorly written in code tend to be the most exposed part of a system because they're usually accessible from the web.

Denial of Service (DoS) attack: Expert believes that Denial of Service (DoS) attack is one of the major threats and among the hardest security problems in cloud environment. According to the WWW Security a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. The hacker uses bots (zombies) for flooding a system with a large number of packets to render the available resources unreachable. The main aim of a DoS attack is the disruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the networks bandwidth or its connectivity.

User to Root (U2R) attack: These kinds of attacks are exploitations in which the intruder accesses the system with a normal user account and attempts to misuse the vulnerabilities in the system in order to gain extra privileges. The U2R attacks leads to several vulnerability such as sniffing password, a dictionary attack and social engineering attacks, with this attack, integrity of the cloud is being violated.

Root to Local (R2L) attack: In this type of attack the intruder who has no access privileges to use a remote machine deliberately sends malicious packets to that machine over the network and try to exploits some vulnerabilities in that machine. Examples are FTP write, guess password, and IMAP attacks.

Insider Attack: Insider is defined as a former or current employee/associate of the cloud service provider which has privileged access and authority to perform modifications in the cloud environment. Insider attacks are organized as they have information about the user and provider. Malicious insider attack is considered one of the highest possible risk attacks on a cloud computing service environment.

Port scanning: Port scanning is used by the attacker to obtain information about open, closed, filtered, and unfiltered ports. The attacker then uses this information to launch attacks on open ports. Different techniques are used in order to perform port scanning. This attack targets the confidentiality and integrity of the cloud.

Backdoor Channel Attack: It is a passive attack, which allows hackers to gain remote access to the compromised system. The system is compromised by shellcode, Trojan, and other similar exploitations. After the node is compromised the intruder has full access to the system and data available.

IP Spoofing Attack: In computer networking, IP spoofing is the creation of Internet Protocol (IP) packets with a forged IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. Figure 4 shown below categorizes the security attacks in active and passive category

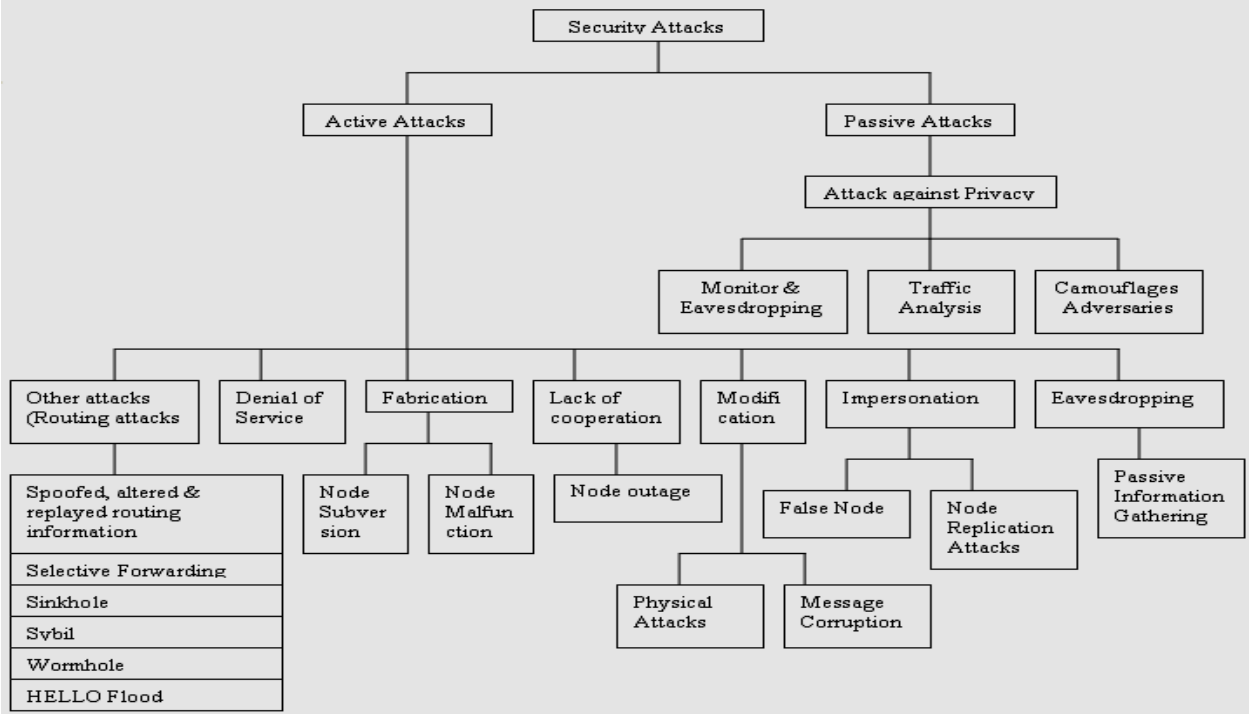

Figure 4: Category of Active and Passive attacks

V. INTRUSION DETECTION METHODS

There are two primary approaches for analyzing events to detect attacks: Misuse Detection Approach and Anomaly Detection Approach.

Misuse-based Detection or Signature based*:** Misuse based intrusion detection uses information of already occurred attack patterns to identify attacks. Abnormal behaviour is detected by matching pre-defined patterns of known attacks recorded in databases. So from its working principle it is clear that misuse detection is fully effective in identifying known attacks at the same time fewer false positive alarms, but it is useless when encountered with unknown patterns of attacks for which the signatures are not yet updated in the pattern matching database [10]. ***Figure 5 shows the typical misuse detection model which consist of four main components: namely, Data collection module, user profile, misuse detection and response engine. Data are collected from one or many data sources including audit trails, network traffic, system call trace, etc. the collected raw data is first preprocessed and converted into a form which is easy to analyses. The user profile is used to characterize normal and abnormal behaviors [11]. The profiles are matched with actual system activities and reported as intrusions in case of deviations.

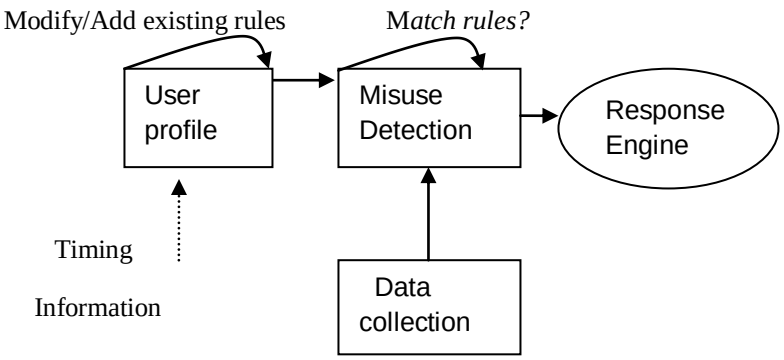

Figure 5: A typical misuse detection model

***Anomaly based*:** Anomaly based approach works on the limitation of misuse based detection approach. As we know new attacks signature cannot be detected before it is analyzed so anomaly detection in network is a dynamic field. Anomaly based detection method works on the principle of finding exceptional behavioral patterns among data instances or network traffic that do not conform to the expected normal behavior [12]. Any instance or behavior deviating from this normal behavior is termed malicious and is categorized as abnormal and alarm is generated to notify the administrator. Anomaly based detection is widely used in Credit card verification to detect frauds. The main challenges of anomaly based detection system are defining what a normal behavior is, deciding the threshold to trigger the alarm and preventing false alarms. A typical anomaly based model is shown in **Figure 6.** It consists of four components, namely data collection, normal system profile, anomaly detection and response. Normal user activities or traffic data are obtained and saved by the data collection component.

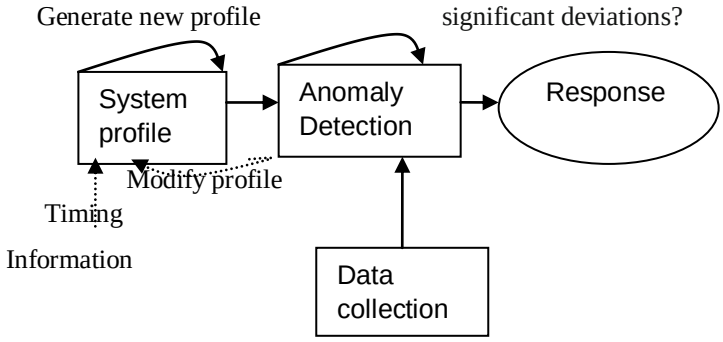

Figure 6: A typical anomaly detection model

VI. LITERATURE REVIEW OF EXISTING WORK DONE

Patel et al. [13] presented an idea of autonomic agent-based intrusion detection scheme utilizing the standards and principles of automatic computing. Anomaly based IDS are used to monitor the system activities and network traffic passing through autonomous sensors for detection of suspicious incidents. H. Debar et al. [14] accompanies the outcomes that the intrusion-detection systems (IDSs) can offer additional security measures for cloud like environments by monitoring configurations settings, logs

report, network traffic, and user actions to identify typical attack behavior. Lee et al. [15] propose another strategy that recognizes malicious behavior of an intrusion by anomaly level of resource utilization by the user. The anomaly level based detection monitor the recent usage history of the suspicious user and stored the relevant information in the log file. The log files are available for the administrator for auditing and finding out the malicious users among normal users. Foster et al. has given the model which is suited for heterogeneous environment like grid and cloud environment. This kind of communication model requires compatibility between heterogeneous hosts, various communication mechanisms, and permission control over system maintenance and updates—typical features in grid and cloud environments [16]. Amir Vahid Dastjerdi et al. proposes IDS based on Mobile agents technology to provide intrusion detection for cloud applications regardless of their locations and that handles attacks for cloud applications from the SaaS point of view [17]. Vieira et al. propose IDS for grid and cloud computing platform. It is collaboration of behavior based anomaly detection method and knowledge based anomaly detection technique to detect intrusions. It works in a cooperative manner where each node can detect intrusion and generate alerts for other nodes as well [18]. Grzech recommends implementing IDS with a three layered hierarchy with the bottom layer monitoring local inbound, outbound data for analysis by administrators by the middle layer nodes of network, and correlation at the upper level using various correlation methods [19]. Vincent Shi-Ming Huang Hsinchu at al. proposed a new distributed denial of service (DDos) mitigation model which consists of Source Checking and Counting module, Multi-Stage Attack Detection module, and Question Generation module [20]. Tupakula et al. [21] propose a VMM-based technique which discussed VM domains (i.e. VMs hosted on same hypervisor in one domain). It is stated that, in a cloud, different hypervisors host VMs of different consumers and different VMs of the same consumer can be hosted by several hypervisors within the cloud. Vieira et al. [22] comes with an intrusion detection system model which is suitable for both grid and cloud computing (GCCIDS). It is a combination of behavior based and knowledge based techniques at middleware layer to detect intrusions. It works in a cooperative manner where each node can detect intrusion and generate alerts for other nodes as well. Bakshi et al. [23] propose a typical NIDS for virtualized environments for the detection of DDoS attacks. A NIDS is installed on a virtual switch (through which traffic of all VMs collectively passes). This is analogous to a NIDS being placed at the boundary server in a traditional computing environment. Garfinkel et al. [24] comes with a prototype model which is based on VMI for intrusion detection. This technique is based on the assumption that the VMM is simple and implemented correctly. This feature marks VMM safe and difficult for the attacker to compromise.

VII: TYPES OF IDS USED IN CLOUD

Intrusion detection in a cloud environment can be much more arduous depending on the available resources in the cloud and the level of management or control of the devices, services or configuration required. Any intrusion detection device must be capable of handling the volume of traffic that is expected to pass through it in order to be effective. There are mainly four types of IDS used in Cloud: Host based intrusion detection system (HIDS), Network based intrusion detection system (NIDS), Hypervisor based intrusion detection system and Distributed intrusion detection system (DIDS). HIDS and NIDS is a category of conventional IDS which is less effective in detecting intrusions in nowadays cloud scenario. Thus NIDS and HIDS are not much suitable for cloud virtualized environment.

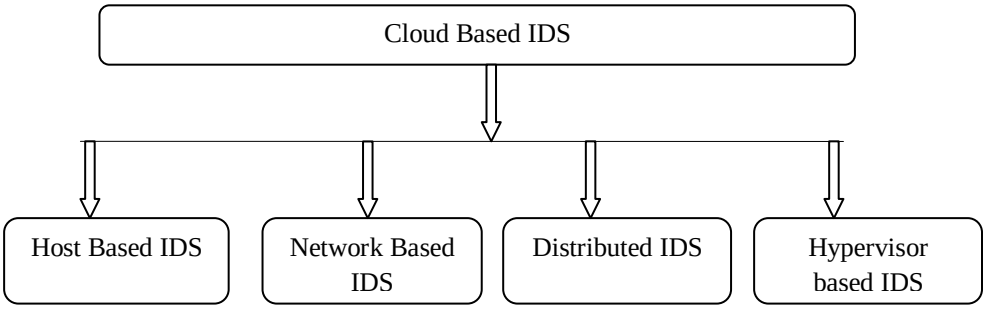

Figure 6: Types of Cloud based IDS

HIDS: Host-based intrusion detection systems installed on a single device either on server side or on workstation, to monitor multiple data on one specific machine, such as system log files, audit trails of operating system data structures, file system used, network events and system calls etc. The goal is to identify attacks and attempts of unauthorized access to the machine itself. HIDS observes modification in host kernel, host file system and behaviour of the program. Upon detection of deviation from expected behaviour, it reports the existence of attack. ***Fig 7*** shows the Host-based Intrusion Detection. With respect to Cloud computing, HIDS be placed on a host machine, to detect intrusive behavior through monitoring and analyzing log file, security access control policies, and user login information. A HIDS for its functioning look for repeated attempts to login by an intruder or it will examine the attempted access to the files that should normally be accessed by the user. Typically, the HIDS is integrated with operating system and has high visibility over all the actions that take place on the system. If we compare HIDS with Network based intrusion system (NIDS) we can say that NIDS has significantly less visibility than HIDS and has to base its decisions almost entirely on an examination of network traffic.

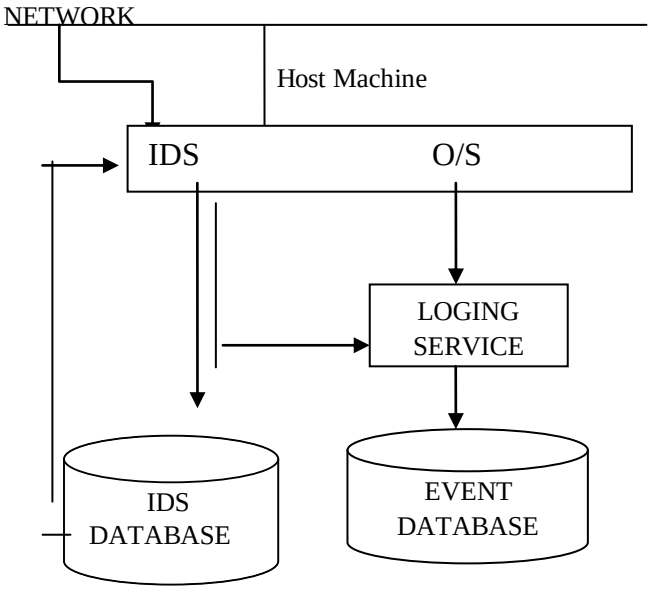

Figure 7: A Host Based IDS

NIDS: A network-based intrusion detection system (NIDS) captures the traffic of entire network for analysis of malicious packets going in or out of the network. NIDS protect the whole network from network-based attacks such as Denial-of-Service Attack (DoS), port scans, IP Address Spoofing, Man-in-

the-Middle Attack etc. A NIDS reads all inbound packets and looks for their correlation with suspicious patterns or users current behaviour with their already known profile in real time. The network traffic can be examined either at the host or at points more remote from the host such as at firewall or routers. When threats are discovered, based on its severity, the system can take action such as notifying administrators, barring the source IP address from accessing the network or reroute the traffic to a quarantine location. NIDS has stronger detection mechanism to detect network intruders by comparing current behaviour with already observed behaviour in real time. NIDS mostly monitors IP and transport layer headers of individual packet and detects intrusion activity. NIDS has very limited visibility inside the host machines. In Cloud environment, installing NIDS is the responsibility of Cloud provider. ***Figure 8*** shows a NIDS deployed in a network.

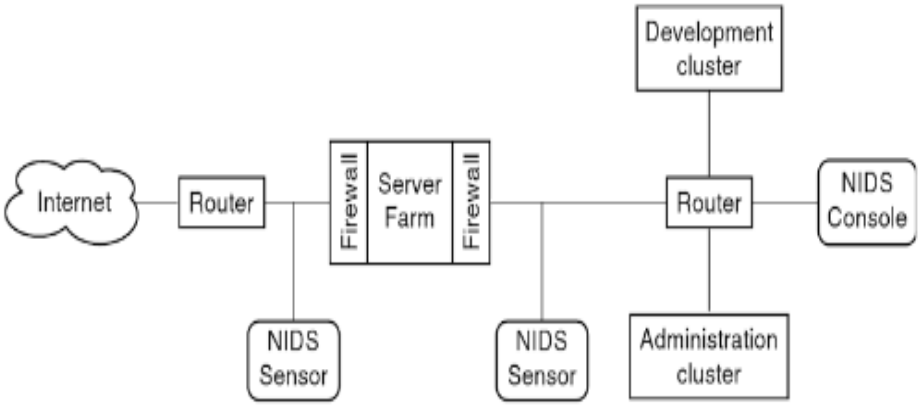

Figure 8: NIDS Model

Hypervisor based IDS: Hypervisor based IDS helps in monitoring and analyzing the data communications among different virtual machines. Hypervisor based IDSs is placed at the hypervisor layer and availability of information is one of the benefits of hypervisor based IDS. It helps in analyze the available information for detection of anomalous actions of users. The information is based on communication at multiple levels like communication between VMs, VM and hypervisor, and communication within the hypervisor based virtual network.

Distributed IDS (DIDS): One type of self-monitoring system is the distributed intrusion detection systems, a security system, designed to detect suspicious activity with a system. DIDS is used in larger networks. A Distributed IDS (DIDS) consists of several IDS (E.g. HIDS, NIDS etc.) over a large network, all of which communicate with each other, or with a central server that enables network monitoring. Each of these individual IDSs has its two components: detection component and correlation manager. Detection component examine the system's behavior and transmits the collected data in a standard format to the correlation manager. Correlation manager combines data from multiple IDS and generate high level alerts that keep up a correspondence to an attack. Table 1 show and compare various types of IDPS according to their deployment position in cloud.

Table 1: IDPS Comparisons

IDPS types	Positing in cloud	Deployment and monitoring authority
Host based Intrusion detection system (HIDSs)	In every virtual machine, hypervisor/host system	On VMs; cloud users on Hypervisor: cloud provider
Network based intrusion detection system (NIDS)	In external network or in virtual network	Cloud provider
Distributed intrusion detection system	In external network, on Host, on Hypervisor or on VM	On VMs: cloud users otherwise: Cloud provider

VIII: CONCLUSIONS

Cloud Computing is an emerging methodology that is quickly changing how computing is done. Since cloud computing is a "Network of Networks" over the internet, therefore chances of intrusion is more with the erudition of intruder`s attacks. The confidentiality, integrity, and availability of a computer system are guaranteed utilizing IDS. Because of the exponential growth of cloud users, IDSs for cloud computing are in great demand. In this paper, authors have discussed existing solutions for intrusion detection in the cloud, types of Cloud based IDS including: network-based, host-based, distribution based, and virtual machine introspection based systems.

References

1 P. Mell, T. Grance, "The NIST Definition of Cloud Computing", Special Publication 800-145, Sep. 2011.

2 I. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey," Computers, vol. 3, no. 1, pp. 1–35, Feb. 2014.

3 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, 2013.

4 P. Jain, D. Rane, and S. Patidar, "A Survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment", IEEE 2011 World Congress on Information and Communication Technologies, pp. 456-461, 2011.

5 Paul Innella "The Evolution of Intrusion Detection Systems"-Tetrad Digital Integrity, LLC. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.

6 Subashini, V Kavitha "A survey on security issues in service delivery models of cloud computing" Journal of Network and Computer Applications, 34 (2011), pp. 1–11

5 K Scarfone, P Mell "Guide to Intrusion Detection and Prevention Systems"(IDPS) Special Publication, 800, NIST (2007) p. 94

6 Siva S. Sivatha Sindhu , S. Geetha , A. Kannan "Decision tree based light weight intrusion detection using a wrapper approach" Expert Systems with Applications 2012

7 M-Y Su, G-J Yu, C-Y Lin "A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach" Computers & Security, 28 (2009), pp. 301–309.

8 Andreas Haeberlen, "An Efficient Intrusion Detection Model Based on Fast Inductive Learning", Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007.

9 M. Bahrololum and M. Khaleghi, "Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008.

10 W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to cloud computing," Cloud Computing, pp. 1-41, 2011.

11 Z. Mahmood, "Cloud Computing: Characteristics and Deployment Approaches", 11th IEEE International Conference on Computer and Information Technology, pp. 121-126, 2011.

12 J. Weng and G. Qin, "Network Intrusion Prevention Systems", JTB_Journal of Technology and Business, pp. 37-49, October 2007.

13 A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior, C. Wills, and P. Federal, "Autonomic agent-based self managed intrusion detection and prevention system," In Proceedings of the South African Information Security Multi-Conference pp. 223-234, 2011.

14 H. Debar, M. Dacier, and A. Wespi, "Towards a Taxonomy of Intrusion Detection Systems," in Int'l J. Computer and Telecommunications Networking, vol. 31, no. 9, pp. 805–822, 2009.

15 J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung, "Multi-level intrusion detection system and log management in cloud computing," Advanced Communication Technology (ICACT), 2011 13th International Conference pp. 552-555, 2011.

16 I. Foster et al., "A Security Architecture for Computational Grids," Proc. 5th ACM Conf. Computer and Communications Security, in ACM Press, pp. 83–92, 2006.

17 Amir Vahid Dastjerdi, Kamalrulnizam Abu Bakar, Sayed Gholam Hassan Tabatabaei, "Distributed Intrusion Detection in Clouds Using Mobile Agents", Third International

Conference on Advanced Engineering Computing and Application in Sciences, October 11-16, 2009 - Sliema, Malta

18 K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," IT Professional Magazine, vol. 12, no. 4, pp. 38, 2010.

19 Grzech, A. P. Optimal monitoring system for a distributed intrusion detection system.(report). Artificial Life and Robotics 14, 3 (2009), 453.

20 Vincent Shi-Ming Huang Hsinchu, Taiwan and Ming Chiang "A DDoS Mitigation System with Multi-Stage Detection and Text-Based Turing Testing in Cloud Computing" Advanced Information Networking and Applications Workshops (WAINA), IEEE 2013.

21 U. Tupakula, V. Varadha rajan, and D. Dutta, "Intrusion Detection Techniques for Virtual Domains," 2012 19th International Conference on High Performance Computing, pp. 1 - 9, 2012.

22 K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," IT Professional Magazine, vol. 12, no. 4, pp. 38, 2010.

23 A. Bakshi, and Y. B. Dujodwala, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, pp. 260-264, 2010.

24 T. Garfinkel, and M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection," In NDSS vol. 3, pp. 191-206, 2003.