An Integrated Intrusion Handling Model for Cloud Computing

RAGHAV RAWAT UPES

College of Engineering Studies, UPES, Dehradun, India
raghavrwt5@gmail.com

APARNA TRIPATHI UPES

College of Engineering Studies, UPES, Dehradun, India
aparnatripathi6288@gmail.com

ABSTRACT - Today, numerous associations are moving their computing administrations towards the Cloud. This makes their PC preparing accessible significantly more advantageously to clients. Be that as it may, it likewise brings new security dangers and difficulties about wellbeing and unwavering quality. Truth be told, Cloud Computing is an appealing and cost-sparing administration for purchasers as it gives openness and dependability choices to clients and versatile deals for suppliers. Notwithstanding being appealing, Cloud highlight postures different new security dangers and difficulties with regards to sending Intrusion Detection System (IDS) in Cloud situations. Most Intrusion Detection Systems (IDSs) are intended to handle particular sorts of assaults. It is apparent that no single procedure can promise insurance against future assaults. Subsequently, there is a requirement for a coordinated plan which can give vigorous insurance against a complete range of dangers. Then again, there is awesome requirement for innovation that empowers the system and its hosts to shield themselves with some level of insight keeping in mind the end goal to precisely distinguish and square noxious movement and exercises. For this situation, it is called Intrusion aversion framework (IPS). Along these lines, in this paper, we stress on late executions of IDS on Cloud Computing situations as far as security and protection. We propose a powerful and proficient model termed as the Integrated Intrusion Detection and Prevention System (IDPS) which consolidates both IDS and IPS in a solitary instrument. Our system likewise incorporates two strategies in particular, Anomaly Detection (AD) and Signature Detection (SD) that can work in collaboration to distinguish different quantities of assaults and stop them through the ability of IPS.

Key Words: Cloud computing, Intrusion detection system, Intrusion prevention technique,Anamoly Detection, Signature Detection

INTRODUCTION

As Green IT has been issued, many companies have started to find ways to decrease IT cost and overcome economic recession. Cloud Computing service is a new computing paradigm in which people only need to pay for use of services without cost of purchasing physical hardware. For this reason, Cloud Computing has been rapidly developed along with the trend of IT services. Cloud Computing can be defined as internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. It is efficient and cost economical for consumers to use computing resources as much as they need or use services they want from Cloud Computing provider. Especially, Cloud Computing has been recently more spotlighted than other computing services because of its capacity of providing unlimited amount of resources. Moreover, consumers can use the services wherever Internet access is possible, so Cloud Computing is excellent in the aspect of accessibility. Cloud Computing systems have a lot of resources and private information, therefore they are easily threatened by attackers. Especially, System administrators potentially can become attackers. Therefore, Cloud Computing providers must protect the systems safely against both insiders and outsiders.

Security issues in the cloud

Cloud computing has emerged as a promising IT services provisioning paradigm, but its security issues are impending its widespread adoption [1]. Security threats can be categorized as follow:

1. **Non-availability of cloud services**

Non-availability of services due to Cloud outages can cause monetary loss to cloud user organization. A deliberate and comprehensive Service Level Agreement (SLA) must be written among user and provider covering all the relevant legal and service provisioning issues and details.

2. **Network and host based attacks on remote Server**

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology. Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks are launched to deny service availability to end users.

3. **Cloud security auditing**

Cloud auditing is a difficult task to check compliance of all the security policies by the vendor. Cloud service provider has the control of sensitive user data and processes, so an automated or third party auditing mechanism for data integrity check and forensic analysis is needed. Privacy of data from third party auditor is another concern of cloud security.

4. **Lack of data interoperability standards**

It results into cloud user data lock-in state. If a cloud user wants to shift to other service provider due to certain reasons it would not be able to do so, as cloud user's data and application may not be compatible with other vendor's data storage format or platform. Security and confidentiality of data would be in the hands of cloud service provider and cloud user would be dependent on a single service provider.

5. **Cloud data confidentiality issue**

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques. However, encrypted data can be secured from a malicious user but the privacy of data even from the administrator of data at service provider's end could not be hidden. Searching and indexing on encrypted data remains a point of concern in that case.

6. **Sub-contracting cloud services**

Cloud user makes a contract or agreement for service provisioning with the cloud service provider. Subcontracting of cloud services by cloud service provider to another service provider poses security issues like non-repudiation or not owing the responsibility, if something goes wrong with precious data and application of cloud user.

Above mentioned cloud security issues are a few and dynamicity of cloud architecture are facing new challenges with rapid implementation of new service paradigm.

INTRUSION DETECTION IN CLOUD COMPUTING

Cloud computing 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. The cloud computing definition of NIST includes *five essential features*, *three service models* and *four deployment models* .The five essential features are resource pooling, broad network access, rapid elasticity and scalability, metered services (pay per use), on demand service. The *three service models* are *Infrastructure asa Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)*; the *four deployment models* are *community* cloud, *public* cloud,*hybrid cloud,and private cloud*. In a cloud computing environment, each of these models has their own significant services different from each other.

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.

In a traditional network, IDS monitor detects, and alert the administrative user by deploying IDS on key network choke points on the user site. But in Cloud network IDS has to be placed at cloud server site and entirely administrated and managed by the services provider. The intrusion data communicates through the service provider and user has to depend on him. The cloud service provider would not like to notify user about the loss and hide the information to make a good image and reputation. So an unbiased third party

Monitoring service can guarantee adequate monitoring and alerting for cloud users. The Intrusion detection message exchange format (IDMEF) is an XML standard format that has been used for message exchanged among IDS sensors. The IDMEF contains the attack name or signature, time of creation and analysis, source and target of intrusion. Alerts generated are sent to ‘Event Gatherer’ program. Event Gatherer receives and convert alert messages in IDMEF standard and stores in event database repository with the help of Sender, Receiver and Handler plug-ins. Figure 1 represents IDPS ACTIVITIES FRAMEWORK

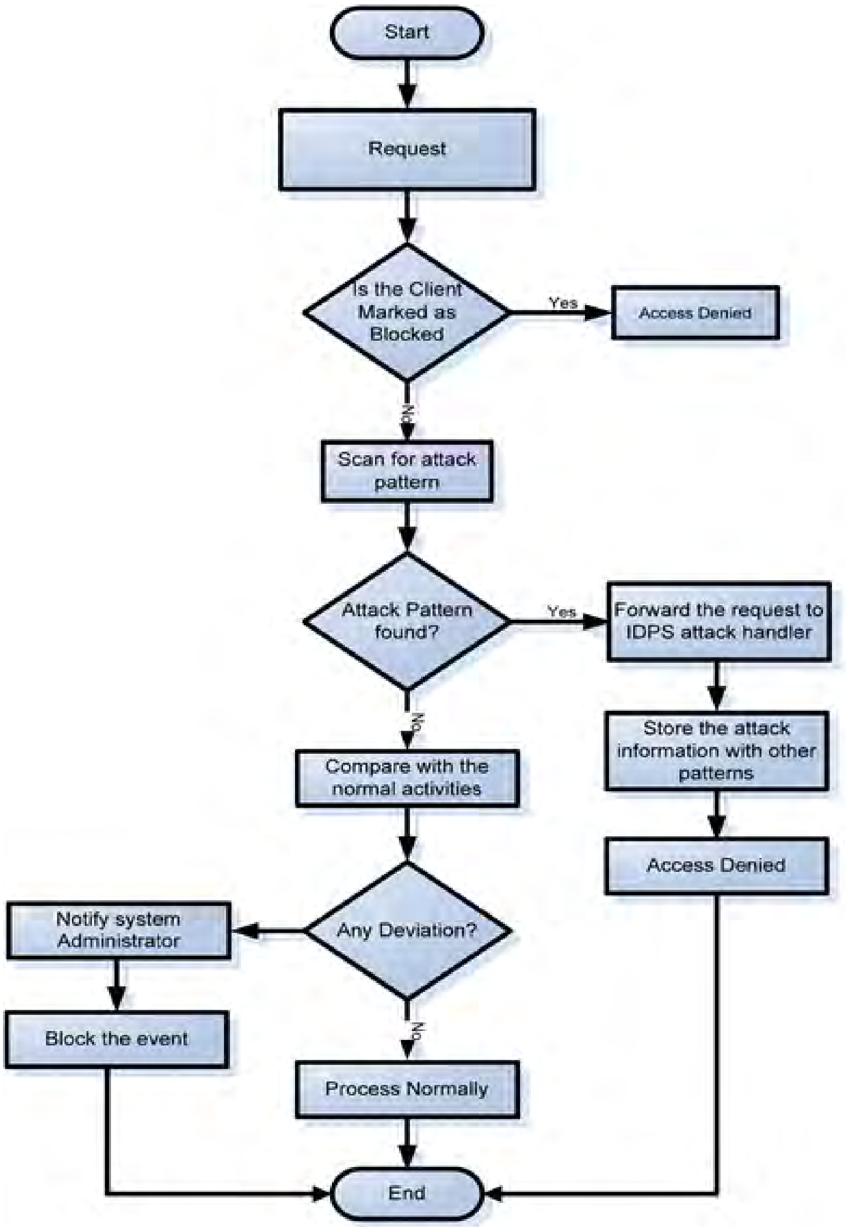
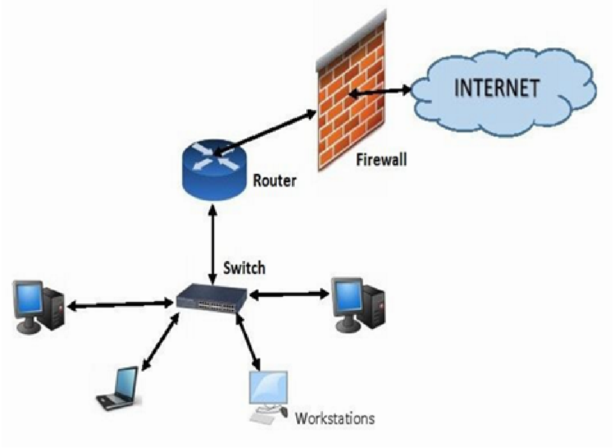

Start
Request
Is the Client Marked as Blocked
Yes
Access Denied
No
Scan for attack pattern
Attack Pattern found?
Yes
Forward the request to IDPS attack handler
Store the attack information with other patterns
Access Denied
No
Compare with the normal activities
Any Deviation?
Notify system Administrator
Block the event
No
Process Normally
End

Figure 1: IDPS Activities Framework

Host Based IDS (HIDS)

HIDS [2] 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.



Advantages of Host Based Detection System

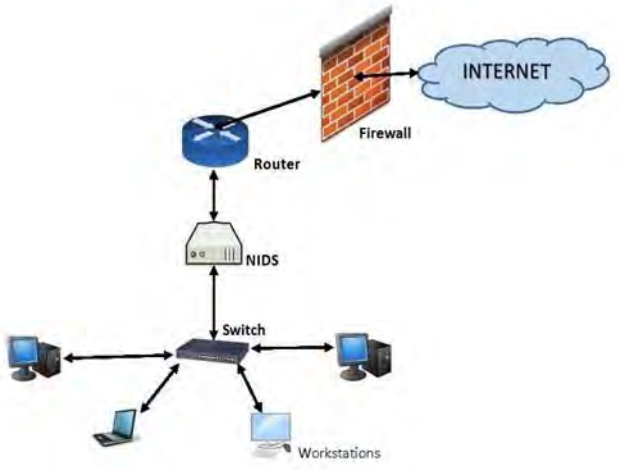
1. Verifies success or failure of an attack: Since a host based IDS uses system logs containing events that have actually occurred, they can determine whether an attack occurred or not.
2. Monitors System Activities: A host based IDS sensor monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executable etc.
3. Detects attacks that a network based IDS fail to detect: Host based systems can detect attacks that network based IDS sensors fail to detect. For example, if an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the network sensors.
4. Near real time detection and response: Although host based IDS does not offer true real-time response, it can come very close if implemented correctly.
5. Lower entry cost: Host based IDS sensors are far cheaper than the network based IDS sensors.

Disadvantages of Host Based Detection System

1. Host based IDSs are harder to manage, as information must be configured and managed for every host.
2. The information sources for host based IDSs reside on the host targeted by attacks, the IDSs may be attacked and disabled as part of the attack.
3. Host based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of- service attacks.

Network Based Detection System

NIDS[3] 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.



Advantages of Network Based Detection System

1. A few well-placed network-based IDS can monitor a large network.
2. The deploying of NIDSs has little impact upon an existing network. NIDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a
3. NIDSs can be made very secure against attack and even made invisible to many attackers.

Disadvantages of Network Based Detection System

1. NIDSs may have difficulty possessing all packets in a large or busy network and, therefore, may fail to recognize an attack launched during period of high traffic.
2. Many of advantages of NIDSs don’t apply to more modern switch-based networks.
3. NIDSs cannot analyze encrypted information. This problem is increasing as organizations and attackers use virtual private network.
4. Most NIDSs cannot tell whether or not an attack was successful; they can only find that an attack was initiated.

Intrusion Prevention System in Cloud Computing

An **Intrusion Prevention System** (**IPS**) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

There are only a few workings that talked about IPS in Cloud Computing. Generally an IPS sits inline on the network and monitors it, and when an event happens, it takes action, based on prescribed instructions. This is unlike IDS, which does not sit inline and is passive. Because IPSs take detection a step more, some see them as next generation IDS systems. Others, however, think in wider terms and consider the IPSs as yet another tool in the security infrastructure that could help preclude intrusions. IPS has been developed out of IDS but, the two are really different security products that have different functionalities and strengths as shown in Table [4].

IDS	IPS
Mounted on network segments (NIDS) and on host (HIDS)	Mounted on network segments (NIDS) and on host (HIDS)
Sits on network passively	Sits inline (not passive)
Cannot analyze encrypted traffic	Better at defending applications
Central management control	Central management control
Better at detecting hacking attacks	Ideal for blocking web defacement
Alerting product (reactive)	Blocking product (proactive)

Intrusion Detection System in Cloud Computing

As said some time recently, Intrusion detection is the procedure of watching the occasions happening in a PC framework or organize and looking at them for indications of intrusions, characterized as endeavors to trade off the privacy, uprightness, accessibility, or to sidestep the security systems of a PC or system. Intrusions are actuated by aggressors getting to the frameworks from the Internet or by authority clients of the frameworks who attempt to increase extra benefits for which they are not approved or by authority clients who abuse the benefits given to them. Interruption Detection Systems (IDSs) are programming or equipment creates that motorize this observing and investigation process. The Intrusion Detection Service (IDS) administration upsurges a Cloud's security level by giving two techniques for interruption detection [5].

- First method is behavior-based method which orders how to associate recent user actions to the usual behavior.
- The second approach is knowledge-based technique that recognizes known follows left by attacks or certain structures of activities from a client who may speak to an assault. The reviewed information is sent to the IDS administration center, which analyzes the conduct utilizing computerized reasoning to see deviations. This has two subsystems particularly analyzer framework and ready framework.

In order to detect the intruders the following techniques should be employed in either HIDS or NIDS.

Anomaly Detection (AD)

Fundamentally, Anomaly Detection was presented in the late of 1980's with Intrusion identification master framework (IDES) [6]. Inconsistency finders distinguish strange abnormal conduct (peculiarities) on a host or system. They work on the suspicion that attacks are unique in relation to "typical" (genuine) action and can consequently be identified by frameworks that distinguish these distinctions. Peculiarity finders build profiles speaking to ordinary conduct of clients, has, or organize associations. These profiles are built from chronicled information gathered over a time of typical operation. The indicators then gather occasion information and utilize an assortment of measures to decide when checked movement goes amiss from the standard. There are numerous measures and procedures that are utilized as a part of oddity discovery including; Threshold location, Statistical measures, Rule-based measures, different measures, including neural systems, hereditary calculations, and insusceptible framework models [7].

Signature Detection (SD)

Abuse locators investigate framework movement, searching for occasions or sets of occasions that match a predefined example of occasions that depict a known assault. As the examples relating to known attacks are called marks, abuse recognition is now and then called "signature-based location". The most well-known type of abuse identification utilized as a part of business items indicates every example of occasions relating to an assault as a different mark. Nonetheless, there are more refined ways to deal with doing abuse identification (called "state-based" investigation systems) that can influence a solitary mark to identify gatherings of attacks [8]. Abuse location methods, as a rule, are not compelling against the most recent attacks that have no coordinated guidelines for example yet. In this work, we will concentrate on applying IDS on IaaS which is the most adaptable model for ID organization. In this way, we have to distinguish the areas that ought to be considered when contemplating ID in the IaaS Cloud. There are four essential "spots"[9]:

• In the virtual machine (VM) itself: Deploying ID in the VM permits checking the action of the framework, and identifying and alarming on issues that may emerge.

• In the hypervisor or host framework: Deploying ID in the hypervisor permits to screen the hypervisor as well as anything going between the VMs on that hypervisor. It is a more concentrated area for ID, however there might be issues in staying aware of execution or dropping some data if the measure of information is too vast.

• In the virtual system: Deploying ID to screen the virtual system (i.e., the system built up inside the host itself) permits checking the system movement between the VMs on the host, and in addition the activity between the VMs and the host. This "system" activity never hits the customary system.

• In the traditional network: Deploying ID here allows to monitor, detect, and alert on traffic that passes over the traditional network infrastructure.

Limitations and Relevant Works

Numerous endeavors have been taken in the range of Cloud registering and interruption identification framework yet at the same time there are more assaults that have not been recognized. In the specialists worked in this field to beat the present security dangers in the Cloud processing through executing IDS in Cloud environment which is dependable of observing the use of assets for the virtual machine utilizing information procured from virtual machine screens. All the more particularly, all observing operations are done outside the virtual machines so the assailant can't change the framework on account of inhabitant's occurrence is broken. Notwithstanding, there are numerous sorts of interruptions that this strategy can't recognize, for example, getting to the record of approved clients with no consent. Furthermore, if anomalous action happens, it will be recognized as interruption regardless of the fact that it is approved action. Consequently, all these holes ought to be considered amid actualizing IDS inside Cloud environment. In the creators concentrated on number of basic issues identified with security and protection in Cloud processing environment from alternate points of view, for example, information stockpiling security, client character in Cloud registering, and secure virtualization, and so on. In addition, they introduced the greater part of the assaults and dangers against the Cloud with clarification of the latest answers for such assaults with their restrictions to be comprehended. While, in [10] the authors concentrated on one problem regarding ensuring the integrity and correctness of user’s data in the Cloud through proposing an efficient and resilient scheme against malicious data modification attack, and even server colluding attacks. On the other hand, many other researchers as in [11] are interested in distributing the IDS among the nodes of the grid within Cloud computing environment in order to monitor each node and alert the other nodes when an attack occurs. They proposed Grid and Cloud Computing Intrusion Detection System (GCCIDS) which is designed to cover the attacks that network- and host-based systems cannot detect. Their proposed method used the integration of knowledge and behavior analysis to detect specific intrusions. However, the proposed prototype cannot discover new types of attacks or create an attack database which must be considered during implementing IDS. In [12], the authors proposed an efficient model that used multithreading technique for improving IDS performance within Cloud computing environment to handle large number of data packet flows. The proposed multi-threaded NIDS is based on three modules named: capture module, analysis module and reporting module. The first one is responsible of capturing data packets and sending them to analysis part which analyzes them efficiently through matching against pre-defined set of rules and distinguishes the bad packets to generate alerts. Finally, the reporting module can read alerts and immediately prepare alert report. The authors conducted simulation experiments to show the effectiveness of their proposed method and compared it with single thread which presented high performance in terms of processing and execution time. However, the problem of detecting new types of attacks still needs many works to be done. Even though, the researchers in [13] presented a hybrid method of integration between AD method and SD method which solved many of the previous problems, still there is a problem in stopping the attack rather than just detecting it. Obviously, the previous works focused in applying only one approach or techniques of IDS in the Cloud computing such as applying only AD or SD mechanism or even using a hybrid of both while, in this work we proposed an integrated scheme of these two techniques AD and SD in addition to the combination of two systems ID and IP which will be elaborated in details in the next section. The purpose of proposing such method is to get higher security level and to solve some gaps within the previous works as mentioned earlier.

PROPOSED FRAMEWORK

The move from traditional client/server to service-based models is renovating the way technology departments think about, designing, and distributing computing technology and applications. However, the enhanced value offered by cloud computing advances have also shaped new security vulnerabilities, including security issues whose full effects are still evolving. The reasons may lie with the ripening of cloud but most importantly, higher tactical decision by execution in cloud acceptance. In fact, such attacks leads to impairment in ability to have physical access to the server holding its information. As a result potentially sensitive data is at threat from insiders attack. According to an analysis, insider attack are the third top threat in cloud computing frame. In this paper, a new way has been proposed to protect the data and resources in the cloud computing environment which is centered on the rational implementation of Intrusion Detection System (IDS) over the cloud computing infrastructure. We have basically engrossed on one layer of the cloud computing which is known as IaaS. Moreover, an integrated model to deploy Intrusion Detection and Prevention System (IDPS) that consists of AD and SD is also been proposed.

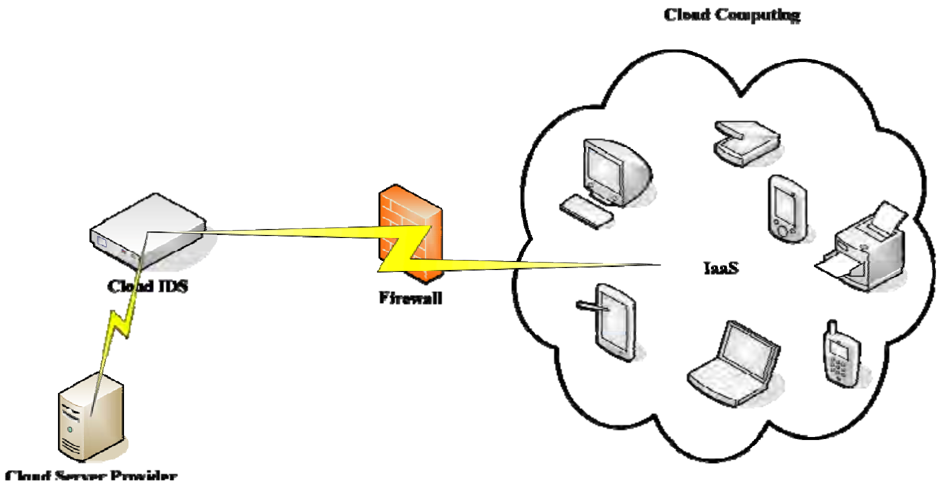


Figure 2: The Proposed Cloud IDS

These two methods will work compliantly to perform an in-depth analysis on resources located on the Cloud to perceive the intrusions and anomalies that may pose risk to the Cloud environment. These two kinds of attacks are different kinds of abnormal traffic trials in an open network atmosphere, whereas the intrusion takes place when an unofficial access of a host computer system is tried while an anomaly can be observed at the network connection level. Therefore, if any of these attacks has been perceived by the proposed integrated scheme then it will associate it with the known threats (signatures) and produce an alarm in the case of identical according to Signature Based Detection technique. On the other hand, if it is not identical to any of the existing patterns, then the planned model will perceive it as abnormal behavior according to Anomaly based Detection Method and also produce an alarm and save that result as a new threat within the other signatures. In addition, the proposed system is provided also with hindrance capabilities rather than just detection so it can further halt the attack itself as noted in the following:

- Dismiss the user session that is being used for the attack
- Block admittance to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute
- Block all admittance to the targeted host, service, application, or other resource.

The integrated model uses signature matching with usual traffic summarizing to improve attack detection. Furthermore, we propose to deploy our IDS in the virtual machine itself as well as the virtual network in order to monitor the actions of the system in addition of monitoring the packet traffic in the network to filter the malicious packets coming from untrusted sources (see Figure 2). The fact is that in the Cloud computing most of the resources will be stored and accessed on the remote servers. However, the consumers do not have to worry about the maintenance and the upgrading of the software and hardware. But, the issue is when there is a flow of the packets from one source to destination; the security in terms of data integrity will not be accurate as we have the Cloud IDS placed in specific location in the NIDS.

CONCLUSION

Cloud computing has spurred the acquaintance of another administration with the Information Technology (IT) discipline. The utilization of Cloud computing will lessen the framework support cost, adaptability for information and applications, accessibility of information administrations and pay as you utilize highlights. Since Cloud computing is understood as a system of systems over the World Wide Web, subsequently, the likelihood of having different sorts of vulnerabilities bringing about assaults is high. Remembering this, in this paper we talked about various strategies of an interruption discovery framework that has been utilized to counter vindictive assaults in Cloud figuring environment. For Cloud registering, a few system access rates are utilized and control of information and applications are required for every administration supplier. Consequently, an effective, dependable and data straightforward IDS is required.

Numerous analysts imagine that utilizing AD could give sensible level of security to the Cloud while, others surmise that utilizing SD may give better security. Truth be told, both techniques are imperative for sending IDS in the Cloud and they supplement each other. In this manner, we have proposed a strategy for consolidating both procedures as an incorporated IDS system to profit by both of these methods in identifying however much attacks as could be expected.

Our proposed framework is given anticipation abilities which make it interesting among different past arrangements as far as halting the assault as opposed to simply distinguishing or reporting cautions. For future exploration work, we recommend to do the execution of our proposed IDPS approach in a genuine Cloud computing environment to confirm our imagined result. Additionally, we plan to convey a honeypot in the proposed engineering to guarantee great execution, we wish to build the level of security in the Cloud computing environment and abatement the dangers to Cloud situations through concentrating on the issue of how information are put away in the Cloud.

REFERENCES

[1] Richard Chow, Philippe Golle, Markus Jakobsson, ‘Controlling data in the cloud: Outsourcing computation without obstructing Control’, ACM computer and communication security workshop, CCWA 09, November 13, 2009.

[2] Iti Raghav, Shashi Chhikara, Nitasha Hasteer, ‘Intrusion Detection and Prevention in Cloud Environment: A systematic Review’, International Journal of Computer Application, April 24, 2013.

[3] Iti Raghav, Shashi Chhikara, Nitasha Hasteer, ‘Intrusion Detection and Prevention in Cloud Environment: A systematic Review’, International Journal of Computer Application, April 24, 2013.

[4] J. Nikolai, “Detecting Unauthorized Usage in a Cloud using Tenant”, available at: http://www.homepages.dsu.edu/malladis/teach/717/Papers/nikolai.pdf.

[5] R. Bace and P. Mell, “NIST Special Publication on Intrusion Detection Systems”, National Institute of Standards and Technology, 2001

[6] E. Cooke, “Examination of a HIDS (SNORT + ADS)”, available at: http://csc.columbusstate.edu/bosworth/CIAE/StudentPapers/cooke.edgar.pdf.

[7] R. Bace and P. Mell, “NIST Special Publication on Intrusion Detection Systems”, National Institute of Standards and Technology, 2001

[8] R. Bace and P. Mell, “NIST Special Publication on Intrusion Detection Systems”, National Institute of Standards and Technology, 2001

[9] “Intrusion detection in a cloud computing environment” Available at: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment, accessed on February 2012.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing”, 17th International Workshop on Quality of Service, 2009 (IWQoS’09), pp. 1-9, 2009.

[11] K. Vieira, A. Schulter, C.B. Westphall, and C.M. Westphall, “Intrusion Detection for Grid and Cloud computing”, IT Professional, Volume: 12 Issue: 4, pp. 38-43, 2010.

[12] I. Gul and M. Hussain, “Distributed Cloud Intrusion Detection Model”, International Journal of Advanced Science and Technology, vol. 34, pp. 71-82, 2011.

[13] E. Cooke, “Examination of a HIDS (SNORT + ADS)”, available at: http://csc.columbusstate.edu/bosworth/CIAE/StudentPapers/cooke.edgar.pdf.