An Approach For Intrusion Detection System In Cloud Computing

M.Madhavi

Computer Science and Engineering
ANURAG Engineering College,Kodad.
Andhra Pradesh

***Abstract:*Today, many organizations are moving their computing services towards the Cloud. This makes their computer processing available much more conveniently to users. However, it also brings new security threats and challenges about safety and reliability. In fact, Cloud Computing is an attractive and cost-saving service for buyers as it provides accessibility and reliability options for users and scalable sales for providers. In spite of being attractive, Cloud feature poses various new security threats and challenges when it comes to deploying Intrusion Detection System (IDS) in Cloud environments. Most Intrusion Detection Systems (IDSs) are designed to handle specific types of attacks. It is evident that no single technique can guarantee protection against future attacks. Hence,there is a need for an integrated scheme which can provide robust protection against a complete spectrum of threats.**

***Keywords*— Put your keywords here, keywords are separated by comma.**

I. INTRODUCTION

Cloud computing refers to the provision of computational resources on demand via a computer network (Figure 1). Users or clients can submit a task, such as word processing, to the service provider, such as Google, without actually possessing the required software or hardware. The consumer's computer may contain very little software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal connected to the Internet. Since the Cloud is the underlying delivery mechanism, Cloud based applications and services may support any type of software application or service in use today . The essential characteristics of Cloud Computing include

On-demand self-service that enables users to consume computing capabilities (e.g.,applications, server time, network storage) as and when required.

Resource pooling that allows combining computing resources (e.g., hardware, software, processing, network bandwidth) to serve multiple consumers - such resources being dynamically assigned.

Rapid elasticity and scalability that allow functionalities and resources to be rapidly and automatically provisioned and scaled.

Measured provision to optimize resource allocation and to provide a metering capability to determine usage for billing purposes Extension to existing hardware and application resources, thus, reducing the cost of additional resource provisioning. The cloud is not simply the latest fashionable term for the Internet. Though the Internet is a necessary foundation for the cloud, the cloud is something more than the Internet.

The cloud is where you go to use technology when you need it, for as long as you need it, and not a minute more. There is no need not install anything on the desktop and only pay for the technology when it is actually used.

The term ‘cloud’ first appeared in the early 1990s, referring mainly to large ATM networks. Cloud computing began in earnest at the beginning of this century, just a few years ago with the advent of Amazon’s web-based services. Recently, Yahoo and Google announced plans to provide cloud computing services to some of USA’s largest universities: Carnegie Mellon, University of Washington, Stanford, and MIT. IBM quickly announced plans to offer cloud computing technologies, followed almost at once by Microsoft. More recent entries into the fray include well known companies: Sun, Intel, Oracle, SAS, and Adobe. All of these companies invested mightily in cloud computing infrastructure to provide vendor-based cloud services to the masses Table 1 demonstrates a comparison between the traditional computing services and the web-basedcloudservices.

Table 1: The Old IT Infrastructure versus the Cloud

Traditional	Cloud
File Server	Google Docs
MS Outlook, Apple Mail	Gmail, Yahoo, MSN
SAP CRM/Oracle CRM/Siebel	SalesForce.com
Quicken/Oracle Financials	Intacct/NetSuite
Microsoft Offce/Lotus Notes	Google Apps
Stellent	Valtira
Off-Site Backups	Amazon S3
Server, Racks, and Firewalls	Amazon EC2, GoGrid, Mosso

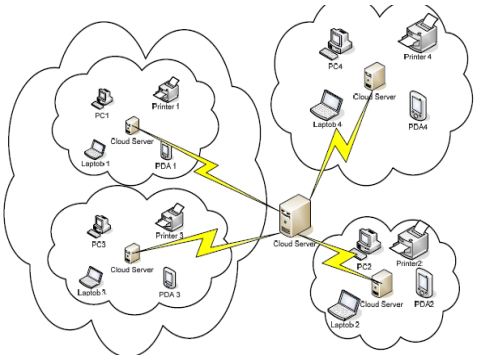

Fig.1 Cloud computing

Cloud computing comprises of two different services components for the users namely as software and hardware over the Internet .However , there are various Cloud service delivery models that are developed, which can be divided into three layers depending on the type of resources provided by the Cloud, distinct layers can be defined . The bottom-most layer provides basic infrastructure components such as CPUs, memory, and storage, and is henceforth often denoted as Infrastructure as a Service (**IaaS**). Amazon's Elastic Compute Cloud (EC2) is a prominent example for an IaaS offer. On top of IaaS, more platform-oriented services allow the usage of hosting environments tailored to a specific need. Google App Engine is an example for a Web platform as a service (**PaaS**) which enables to deploy and dynamically scale Python and Java based Web applications. Finally, the top-most layer provides the users with ready to use applications also known as Software as a Service (**SaaS**).

II SERVICE MODELS IN CLOUD COMPUTING

Software as a Service (SaaS)

SaaS is a model for which the applications are hosted as services to customers who access it via the Internet. When the software is hosted off-site, the customer doesn't have to maintain it or support it. On the other hand, it is out of the customer's hands when the hosting service decides to change it.

Platform as a Service (PaaS)

PaaS on the other hand, delivers the cloud services differently. As the name suggests, PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install any kind of software.The services provided in PaaS model include application design, development, testing,deployment, hosting, team collaboration, web service integration, database integration, and versioning .

However, PaaS lacks the interoperability and portability among different providers. In other words, if an application is created with one cloud provider and then the customer decides to move to another provider, then she may not be able to do so or it may require high prices for the application to run in the new provider's cloud. Google App Engine is an example of PaaS clouds where users can create their own applications with either python or Java and deploy it on Google's cloud.

Infrastructure as a Service (IaaS)

Sometimes referred to as HaaS or Hardware as a Service , it is considered the next form of services available in cloud computing. Where SaaS and PaaS are providing applications to customers, IaaS doesn't. In the simplest form, IaaS provides the organizations with hardware resources that can be used for anything. The advantage is that instead of buying servers, software, racks, and having to pay for the datacenter space for them, the service provider rents those resources. And by renting resources we mean any resources than a person can think of, including Server Space, Network Equipment,Memory, CPU Cycles, Storage Space, etc… Additionally, the infrastructure resources can be scaled up or down based on the application resource needs.

III SECURITY SERVICES IN THE CLOUD

Security services provided in the cloud have the potential to provide cost savings and faster deployment compared with equivalent-capacity,premises-based equipment, but providers are yet to deliver on customer expectations.Currently many traditional security systems are provided as services in the cloud. These systems have been made available to end user to provide the security products for users in a service-based manner. Such model is referred to as Security-as-a-Service model . This included many product services and types like Remote Vulnerability Scanning Webroot® Email and web Security SaaS , and Panda® Managed Office Protection .In this thesis, we introduce the usage of intrusion detection systems as services in cloud computing environments.

The basic concept is that NIDS are used frequently as a main component in perimeter network security. While deploying and configuring NIDS is considered an infrastructure type security measure, IaaS service models still have limited support to offering intrusion detection as services. By limited we mean, that even when cloud subscribers wish to deploy an IDS system in their cloud's network segments,they will need to do this task entirely themselves. An example of this is the usage is Amazon Elastic Compute Cloud (EC2) where users can purchase and use Amazon Machine Image (AMI) that comes with "SNORT" IDS on it . As we shall see in the next chapter, other proposals have been introduced to enable intrusion detection for the protection of the cloud itself not the cloud's subscribers. And for many, the distinction between the cloud protection and the cloud clients' protection is unclear.

IV INTRUSION DETECTION SYSTEM

Intrusion detection systems (IDS) are an essential component of defensive measures protecting computer systems and network against harm abuse . It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper response. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network.

There are mainly two categories of IDSs, network based and host based. In addition, the IDS can be defined as a defense system, which detects hostile activities in a network. The key is to detect and possibly prevent activities that may compromise system security, or some hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans.

One key feature of intrusion detection systems is their ability to provide a view of unusual activity and to issue alerts notifying administrators and/or blocking a suspected connection. Intrusion detection is defined as the process of identifying and responding to malicious activity targeted at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks

originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers). Once an intrusion has been detected, IDS issues alerts notifying administrators of this fact.
The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) – following the organization's security policy (Figure 4). An IDS is an element of the security policy. Among various IDS tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources.

A. *Host Based Intrusion Detection System (HIDS)*

This type of IDS involves software or agent components, which is run on the server, router, switch or network appliance. However, the agent versions must report to a console or can be run together on the same host as depicted in Fig 2. Basically, HIDS provides poor real-time response and cannot effectively defend against one-time catastrophic events. In fact, HIDSs are much better in detecting and responding to long term attacks such as data thieving .

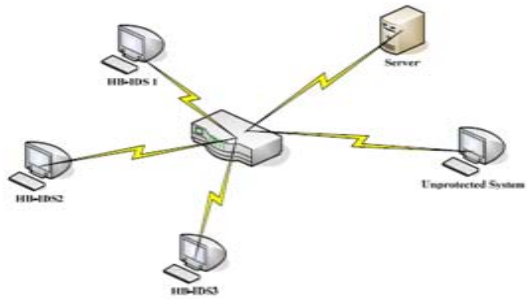

Fig 2.HIDS

B. *Network Based Intrusion Detection system(NIDS)*

This type of IDS captures network traffic packets such as TCP, UDP and IPX/SPX) and analyzes the content against a set of RULES or SIGNATURES to determine if a POSSIBLE event took place.False positives are common when an IDS system is not configured or "tuned" to the environment traffic it is trying to analyze . Fig 3 shows the network based Intrusion DetectionSystem .

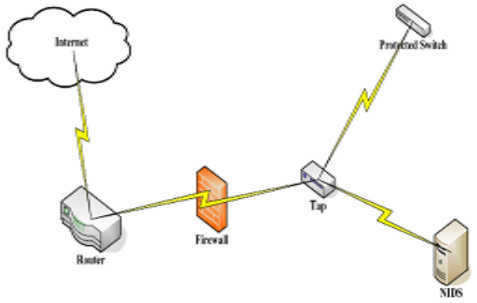

Fig 3.NIDS

NIDS	HIDS
Broad in scope	Narrow in scope
Easier setup and configure	More complex setup and configuration
Better for detecting attacks from the Outside.	Better for detecting attacks from the inside.
Less expensive to implement	More expensive to implement
Detection is based on what can be recorded on the entire network	Detection is based on what any single host can record
Examines packet headers	Does not see packet headers
OS-independent	OS-specific
Detects network attacks as payload is analyzed	Detects local attacks before they hit the network
Detects unsuccessful attack attempts	Verifies success or failure of attacks

Table 2 differences between the Host based Intrusion Detection system

(HIDS) and Network Based Intrusion Detection System. However, the host-based and network-based systems are both required in the Cloud computing environment because they offer significantly different benefits. For an IDS, we need to use detection, deterrence, response, damage assessment, attack anticipation, and prosecution.As has been discussed earlier about IDS and its advantage, Figure 8 shows the framework of the IDS activities.
However, the main task of IDS is defending a computer system by detecting an attack and possibly repealing it. Detecting hostile attacks depends on the number and type of appropriate actions (Figure 8). Intrusion prevention requires a well-selected combination of "baiting and trapping" aimed at both investigations of threats. Diverting the intruder's attention from protected resources is another task. Both the real system and a possible trap system are constantly monitored. Data generated by intrusion detection systems is carefully examined (this is the main task of each IDS) for detection of possible attacks (intrusions). In the Table 3, we summarize the functionalities of IDS .

1	Monitoring and analyzing both user and system activities.
2	Analyzing system configurations and vulnerabilities.
3	Assessing system and file integrity.
4	Ability to recognize patterns typical of attacks.
5	Analysis of abnormal activity patterns.
6	Tracking user policy violations.

Table 3.Functionalities of IDS

V .CONCLUSION

Cloud computing is a "network of networks" over the internet, therefore chances of intrusion is more with the erudition of intruder‟s attacks. Different IDS techniques are used to counter malicious attacks in traditional networks. For Cloud computing, enormous network access rate, relinquishing the control of data & applications to service provider and distributed attacks vulnerability, an efficient, reliable and information transparent IDS is required. In this report, a multi-threaded cloud IDS model is proposed which can be administered by a third party monitoring service for a better optimized efficiency and transparency for the cloud user

ACKNOWLEDGMENT

The making of the paper needed co-operation and guidance of a number of people. I therefore consider it my prime duty to thank all those who had helped me for making it successful. I am thankful to my friends and my beloved husband for his cooperation.

REFERENCES

[1] J. Mchugh, A. Christie, and J. Allen, "Defending Yourself: The Role of Intrusion Detection Systems", IEEE Software, Volume 17, Issue 5, Sep.-Oct., pp. 42-51, 2000.

[2] K. V. S. N. R. Rao, A. Pal, and M. R. Patra, "A Service Oriented Architectural Design for Building Intrusion Detection Systems", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 11-14, 2009.

[3] E-Banking - Appendix B: Glossary, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html, Accessed on: 23/02/2012

[4] Information Technology at Johns Hopkins-Glossary G-I, http://www.it.jhmi.edu/glossary/ghi.html

[5] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE transactions on dependable and secure computing, vol. 4.