MANAGING INTRUSION DETECTION AND DIAGNOSIS AS A SERVICE IN CLOUD COMPUTING

Prakash Kumar Pathak
Computer Science, Research Scholar, Singhania University, (India)

ABSTRACT

The Cloud computing is an internet based distributed network technology which refer to application and services that run on a distributed network. The cloud Computing service provide flexibility scalability and Economics of Scale .Security is main concern for this feature .As more data moves from centrally located on cloud server .The personal and private data storage on cloud server. Confidential data or information which is stored on the cloud server is on the risk. If we do not appropriate measure the hacker can hake the data .Because cloud computing provides services as flexibility, scalability and cloud computing also provide virtual resource to the cloud user.

The cloud computing has a three types of service.

1) *SaaS (Software As A Service.)*
2) *PaaS (Plateform As A Service)*
3) *IaaS (Infrastructure As A Service)*

Each service level security concerns that need to address. The Cloud computing are important Vulnerable targets for intruder attacks. The reason behind that distributed network environment. For the distributed environment, Intrusion Detection System we are using to enhance the security system. Because the privacy of data even from the administrator of data at Service Provider we cannot be hidden or cannot be secure. Along with the gains achieved in cloud computing there are inherent risks.

Keywords: - Distributed Network Privacy Of Data, Data Administrator, Service Provider, Security Service.

I. INTRODUCTION

In the last decade, most people were concerned about obtaining computers in their offices, schools and homes. The main reason behind that was to get close to the world and communicate and exchange data via these devices. In contrast, today people are concerned about the Internet and its speed for effective and efficient communication. In addition, often they need extra services to the existing legacy service provided by the Internet. These services are known as some kinds of computing tasks that are delivered by the Internet Service Providers (ISP). While getting required service is the users' demand, with the advanced development of the Internet tools around the world, attackers also aim to identify various loopholes in the operating system and networks. When we talk about Clouds, The main target of the attackers is to make illegitimate and unlawful attack to the available resources in the Cloud computing settings. In order to overcome these obstacles, some actions need be taken in

the host based (HB) and Network based (NB) level. Even though the use of intrusion detection system (IDS) is not guaranteed and cannot be considered as complete defense, we believe it can play a significant role in the Cloud security architecture [1]. Some organizations are using the intrusion detection system (IDS) for both Host Based and Network Based in the Cloud computing [2]. Intrusion detection systems (IDS) which are hardware and/or software mechanisms that detect and log inappropriate, incorrect, or anomalous activities and report these for further investigations [3]. Intrusion Prevention Systems (IPS), which contain IDS functionality but more sophisticated systems that are capable of taking immediate action in order to prevent or reduce the malicious behavior [4]. Thus, this work utilizes both systems: (IDS) and (IPS) and refers to it as Intrusion Detection and Prevention System (IDPS). Furthermore, many works have been done in using one of the (IDS) techniques; either Anomaly Detection (AD) or Signature based Detection or hybrid of both. The ADS (Anomaly Detection System) can be used to detect unknown attacks in the networks which come from rogue nodes. In fact, such system is designed for the offline analysis due to their expensive. Processing and memory storage. On the other hand, the SD is used in this system to detect and identify manually the attack signature which is known as attacks in the real time traffic [5]. Therefore, both methods are essential in detecting the intrusions. So, we propose an integrated scheme which makes use of both methods to detect the attacks as soon as possible and prevent the attackers from generating the malicious activities inside the Cloud.

1.1 About Cloud Computing

Cloud computing refers to the provision of computational resources on demand via a computer network. 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 [6]. The essential characteristics of Cloud Computing include [7]: 1.On-demand self-service that enables users to consume computing capabilities (e.g., applications, server time, and network storage) as and when required. 2. Resource pooling that allows combining computing resources (e.g., hardware, software, processing, Network bandwidth) to serve multiple consumers - such resources being dynamically assigned. 3. Rapid elasticity and scalability that allow functionalities and resources to be rapidly and automatically provisioned and scaled. 4. 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.

1.2 Cloud Computing Architecture

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 [8] depending on the type of resources provided by the Cloud, distinct layers can be defined (see Figure 2). 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**) [8] [9]. In addition, it is possible to observe the significant interaction between the services model in the Cloud computing which are Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS) as shown in Figure 3. Each one of these models provides unique service to the users in the Cloud computing environment.

1.3 About Intrusion Detection System

Intrusion detection systems (IDS) are an essential component of defensive measures protecting computer systems and network against harm abuse [1]. It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper response [10]. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network [2]. There are mainly two categories of IDSs

1.4 Intrusion Detection System In Cloud Computing

As mentioned before, Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the Systems from the Internet or by Authorized users of the systems who attempt to gain additional privileges for which they are not authorized or by authorized users who misuse the privileges given to them. Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process [11]. The Intrusion Detection Service (IDS) service increases a Cloud's security level by providing two methods of intrusion detection. First method is behavior-based method which dictates how to compare recent user actions to the usual behavior. The second approach is knowledge-based method that detects known trails left by attacks or certain sequences of actions from a user who might represent an attack. The audited data is sent to the IDS service core, which analyzes the behavior using artificial intelligence to detect deviations. This has two subsystems namely analyzer system and alert system.

In order to detect the intruders the following techniques should be implemented in either HIDS or NIDS [12] [2].

II. ANOMALY DETECTION (AD)

Basically, Anomaly Detection was introduced in the late of 1980's with Intrusion detection expert system (IDES) [12]. Anomaly detectors identify abnormal unusual behavior (anomalies) on a host or network. They function on the assumption that attacks are different from "normal" (legitimate) activity and can therefore be detected by systems that identify these differences. Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation. The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm. There are many measures and techniques that are used in anomaly detection including; Threshold detection, Statistical measures, Rule-based measures, other measures, including neural networks, genetic algorithms, and immune system models

III. SIGNATURE DETECTION (SD)

Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection". The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks Misuse detection techniques, in general, are not effective against the latest attacks that have no matched rules or pattern yet. In this work, we will focus on applying IDS on IaaS which is the most flexible model for ID deployment. So, we need to identify the locations that should be considered when thinking about ID in the IaaS Cloud. There are four primary "spots" [13]:

• In the virtual machine (VM) itself: Deploying ID in the VM allows monitoring the activity of the system, and detecting and alerting on issues that may arise. • In the hypervisor or host system: Deploying ID in the hypervisor allows to not only monitor the hypervisor but anything traveling between the VMs on that hypervisor. It is a more centralized location for ID, but there may be issues in keeping up with performance or dropping some information if the amount of data is too large. • In the virtual network: Deploying ID to monitor the virtual network (i.e., the network Established within the host itself) allows monitoring the network traffic between the VMs on the host, as well as the traffic between the VMs and the host. This "network" traffic never hits the traditional network.

• In the traditional network: Deploying ID here allows monitoring, detecting, and alerting on traffic that passes over the traditional network infrastructure.

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 Accessed on: 23/02/2012

[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, no. 1, pp. 1-15, 2007.

[6] 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.

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

[8] M. Jensen, N. Gruschka, L. L. Iacono, and G. Horst, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing, pp. 109-116, 2009.

[9] R. Wu, G.-joon Ahnl, and H. Hul, "Information Flow Control in Cloud Computing", IEEE Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), pp. 1-7, 2010.

[10] U. Thakar, "HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot", The second International Conference on Innovations in Information Technology, Dubai, UAE September 26-28, 2005.

[11] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems", National Institute of StandTechnology.

[12] E-Cooke Examination of a DIDS available at:Http://csc.columbusstate.edu/Bosworth/CIAE/student Papers/cooke.edgar.pdf