A Study of Various Attacks and Intrusion Detection System in Cloud

Piyush Pareta[1], Manish Rai[2]

[1]RGVP University, RKDF College of Engineering, Bhopal, India

[2]RKDF College of Engineering, RGVP University, Bhoapl, India

Abstract: ***Cloud computing is the computing that uses resources either software or hardware over the Internet. It is the computing over the network. Today, almost every IT services are provided using this innovative technology. Cloud computing is the model that provides convenient on demand access of various services by using shared pool of configurable computing resources. Using of such shared pool of computing resources, this computing is targeted by various Cloud intruders, attackers and therefore exists number of new risks and threats due to its operational dependency over the network i.e. distributed environment which has number of vulnerabilities. In order to solve this security problem, there are number of security solution, models and schemes. This paper explains about security issues in cloud and focuses on various kinds of attacks such as Insider Attack, Man-in-the Middle Attack, DoS Attacks. Lastly it explains the need of effective Intrusion Detection and Prevention System in order to overcome such attacks.***

Keywords: CSP (Cloud Service Provider), Threats, Attacks, Security, DoS (Denial of Service), SSL (Secure Socket Layer), DS (Digital Signature)

1. Introduction

Cloud computing is the latest trend and innovation of computing. It gets its name as "cloud" due to its computing over the Internet. This computing mainly relies on various pools of shared resources and is configured and deployed by using concept of Virtualization [17]. The shared pool of resources is used as client server architecture depending on storage and network. It works on pay as-you-use mode between cloud service provider and cloud users. This computing overall reduces operating cost. In September 2011, the definition and specifications of cloud computing were standardized by the U.S. National Institute of Standards and Technology (NIST) [16]. NIST states that "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Based on deployment model, cloud computing is categorized as Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud. The services provided in cloud computing is mainly categorized into three ways. Firstly, Software-as-a-Service (SaaS) that is providing the customer with capability to use application, software running in remote on demand [18]. Example: Salesforce.com, Microsoft Azure, Zoho, etc. Secondly, Platform-as-a-Service(PaaS) where consumer is provided with capability to enjoy any platform when needed [18]. Examples of such cloud service providers are Microsoft Azure service platform, force.com, Google App Engine, etc and Lastly, Infrastructure-as-a-Service (IaaS) that provides the consumer with the capability to provision processing, storage, networks when required. Examples: Amazon EC2, S3, Sun's cloud service, Go Grid, 3 Tera, etc [18]. The above description explains about the cloud computing that it contains two important end the service provider termed as Cloud Service Provider (CSP) and Cloud User. Cloud computing has number of advantages like cost reduction of computation, resource sharing that may be software or hardware, time saving, etc. But still this type of computing mainly rely on network for its working and it is well known that there are number of vulnerabilities like hardware, software or protocol vulnerability in the network. This results in many security and privacy problem as the cloud data are present and accessed using various intermediate servers working in distributive environment. Security issues such as Confidentiality, Integrity, Authentication, Availability and Trust [6][8] are the major concern in this type of computing. The next section of the paper describes about some popular attacks and IDS.

2. Attack in Cloud

Security of data in cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. To ensure adequate security in cloud computing, various security issues, such as authentication, data confidentiality and integrity, and non-repudiation, all need to be taken into account.

a) Insider Attack

The insider attack is the attack that occurs due to the authentication problem and privileged authority. It is a kind of intruder that acts like genuine or authorized object [13]. In this kind of attack, an attacker can be passive entity that is present inside the system and steals confidential credentials and make use of it in order to perform modification and harms the services and computation. These kinds of attacks are very difficult to detect as the attacker acts like a authenticate entity. The solution for such is Intrusion Detection System.

b) Denial-of-service Attack

This type of attack is very difficult to detect. In this type of attack, the attackers (hackers) perform some procedure to hinder the availability issue of security in cloud. It is done in such a way that the attacker sends excessive message or packets asking for authenticated request again and again, causing flooding [21]. These packets can be any TCP or UDP or in most cases ICMP or may be the combination of different protocol. These kind of attacks send large packets sometime also known as Zombies and hence result in DoS (Denial of Service) or sometime DDoS(Distributed Denial of Service) in cloud computing. In order to overcome this attack there should be certain mechanism of regular monitoring and is done by some algorithm implemented in Intrusion Detection System.

c) Port Scanning

This type of attack firstly identifies ports that are opened. It then retrieves certain information about services that are running on system and hinders those services. Some common port scanning attacks are window scanning, TCP, UDP scanning.

d) Attacks on Virtualization

After compromising hypervisor, control of the virtual machines in the virtual environment will be captured [1]. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates. Multiple virtual machines use the same resource pool, especially hardware and with this kind of access side channel data has a chance to be captured, which flow one virtual machine to other [12]

e) Side channel Attacks

A passive attack type in which intruders compromise a node in the cloud and use this compromised node as a zombie resource to execute a DDoS attack [1]. Trojans and similar structures on the system are help to compromise the system. After compromising system become a zombie and also data can be reachable on the system.

3. Intrusion Detection System

An intrusion detection system (IDS) is defined as the system that consists of any hardware or software application that is used for detecting unwanted behavior that may occur in any network or any computer [2]. It monitors network as well as any system activities that may arise from any malicious activities or policy violations. Besides this intrusion detection system also generates various alarm in order to generated reports to a management station. It is mainly meant for detecting various Passive Attacks in any network. Intrusion detection system are implemented in variety of ways such as Host-Based IDS, Network based IDS, Hybrid IDS, etc.

a) Intrusion Detection Techniques

IDS are classified into two broad categories. These classifications are according to various approaches that are used to detect the abnormal behaviour. The detailed explanation of these is techniques are illustrated below:

Anomaly based intrusion detection system: Anomaly-based intrusion detection (ABID) systems flag as anomalous observed activities that that behave differently than the defined normal behaviour of the system. This system basically works by detecting the processes deviating from the expected behaviour or the nodes behaving abnormally. The other name used for ABID systems is behaviour-based intrusion detection. The process of modelling the normal behaviour of network nodes is known as training. The model additionally goes about as a profile of client or system conduct. A profile comprises of data about the arrangement of parameters which are particularly equipped to the target being checked. Testing for interruption includes analysis of the typical conduct model inferred throughout the preparation stage with the current model of the system or clients.

Knowledge based intrusion detection system: Knowledge based intrusion detection systems keep up an information base that holds marks or examples of well-known attacks and searches for these examples trying to discover them. KBID relies on knowledge about attacks so anything not explicitly recognized as an attack based on existing knowledge is declared as nonintrusive or acceptable. However, the case of an event or a series of events that has degraded the network performance can be identified as an unknown attack because it does not match the existing rules of attacks, and the system can update the knowledge base by adding a certain new rules or policies. Some KBID systems use expert systems for intrusion detection. An expert system maintains the knowledge of known attacks in a knowledge base in the form of a set of rules. Captured audit data from a monitoring network are translated into facts and then an inference engine uses these facts and rules present in the knowledge base to detect a malicious activity in the network.

4. Related Work

The paper [1] defines various different attack types, which affect the availability, confidentiality and integrity of resources and services in cloud computing environment. Additionally, the paper also introduces related intrusion detection models to identify and prevent these types of attacks. It mainly gives the survey of various IDS model used together with different attacks they focus on for its working.

The paper [2] gives about an intrusion detection system th at is used to detect the attacks efficiently by using anomaly based approach in IDS. It explains about importance to detect attacks at a beginning stage in order to reduce their impacts. This research work proposed a new approach called outlier detection where, the anomaly dataset is measured by the Neighborhood Outlier Factor (NOF). Here, trained model consists of big datasets with distributed storage environment for improving the performance of Intrusion Detection system.

The paper[3], proposed encryption algorithm Hybrid DESCAST has been designed to provide the security of huge, volume of data sent through the media and the same will remain encrypted in the cloud sever. This cipher text will be decrypted only when the same is required to be used by the authenticated user. Problems of individual DES and CAST

Block Cipher Algorithm have been tackled by our proposed encryption algorithm. Complexity and Computation time for encryption and decryption for our proposed algorithm is higher than the individual DES and CAST algorithm. This paper is focused to provide security of data in cloud server, as well as for the data while transferring from client to cloud server and vice versa.

Praveen Kumar Rajendran, B. Muthukumar et al , in paper [4] explains about give an overall idea about Cloud computing, Intrusion, types of Intrusion Detection Systems and earlier works done on Intrusion Detection System. The key proposal of this paper is to give an overall idea for building a Hybrid Intrusion Detection System that would detect any type of intrusion into the cloud. This paper is the source of inspiration of my research work. It explains about hybrid concept and implemented using.Net framework as front end and SQL Server as back end to store the information. The Hybrid Intrusion Detection system has been deployed in Microsoft Azure Cloud environment. The Dynamic characteristic of Hybrid Intrusion Detection System is achieved by building a simple and informative User Interface.

In paper [5], author proposed distributed IDS that handle large flow of data packets, analyze them and generate reports efficiently. Transparent reports are instantly send for information of cloud user and expert advice for cloud service provider's network mis-configurations through a third party IDS monitoring and advisory service.

The paper [19] Hassen Mohammed Alsafi et al, proposes an effective and efficient model termed as the Integrated Intrusion Detection and Prevention System (IDPS) which combines both IDS and IPS in a single mechanism. Our mechanism also integrates two techniques namely, Anomaly Detection (AD) and Signature Detection (SD) that can work in cooperation to detect various numbers of attacks and stop them through the capability of IPS.

The paper [20] El-Sayed M. El-Alfy et al [5], presented a new method based on multiple criteria linear programming and particle swarm optimization to enhance the accuracy of attacks detection. Multiple criteria linear programming is a classification method based on mathematical programming which has been showed a potential ability to solve real-life data mining problems.

5. Conclusion

Cloud computing rely on network and hence it contains various security threats and attacks during its computation, deployment and working. These threats or attacks can be insider or outsider attacks. In order to overcome these problem there are number of security solutions like encryption, efficient security policies, intrusion detection system, etc. In order to deal with certain passive attacks IDS provides a good solution. Different IDS techniques like anomaly based or knowledge based approach are used to design effective IDS. But still there exists a need for more efficient intrusion detection system that uses the benefits of both types of technique. An Intrusion Detection System should also contain some prevention schemes based on the knowledge gather during various attacks in cloud in history. It is clear from the study that attacks mainly passive attacks are very difficult to identify and hence a better and effective some hybrid IDS could be the solution for such problem.

References

[1] U. Oktay, O.K. Sahingoz et al, "Attack Types and Intrusion Detection System in Cloud Computing", Elsevier, 2013.

[2] Jabej J, Dr.B. Muthu Kumar, "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach", Science Direct, 2015.

[3] Nandita Sengupta, Ramya Chinnasamy "Contriving Hybrid DESCAST Algorithm for Cloud Security", Elsevier, 2015.

[4] Praveen Kumar Rajendran, B. Muthukumar, G.Nagarajan, "Hybrid Intrusion Detection System for Private Cloud: A Systematic Approach", Elsevier, 2015.

[5] El-Sayed M. El-Alfy, Feras N. Al-Obeidat, "A multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection", Elsevier , 2014.

[6] Nir Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution", Elsevier, 2012.

[7] Dimitrios Zissis , Dimitrios Lekka, "Addressing cloud computing security issues", Elsevier, 2012.

[8] Rong C et al., "Beyond lightning: A survey on security challenges in cloud computing." Elsevier, 2012.

[9] Kshetri,N., "Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy", Elsevier , 2012.

[10] Sandeep K. Sood, "A combined approach to ensure data security in cloud computing". Journal of Network and Computer Applications, 2012.

[11] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems, Vol.25 (2009) 599–616.

[12] Cong Wang, Qian Wang, and Kui Ren, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM, 2010.

[13] B.Sumitra, C.R. Pethuru, "A Survey of Cloud Authentication Attacks and solution Approaches", IJIRCCE, 2014.

[14] Issa M. Khalil, Abdallah Khreishah, "Cloud Computing Security: A Survey", ISSN 2073-431X, 2014.

[15] Irfan Gul, M. Hussain, "Distributed Cloud Intrusion Detection Model", IJAST, 2011.

[16] IR.Ramya, IIG.Kesavaraj, "A Survey on Denial of Service Attack in Cloud Computing Environment", IJARET, 2015.

[17] Kevin Sloan, "Security in a virtualised world", Amethyst Risk Management, Network Security, Elsevier , 2009.

[18] Dimitrios Zissis et al, " Addressing cloud computing security issues", Elsevier, 2012.

[19] Hassen Mohammed Alsafi , Wafaa Mustafa Abduallah, "IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment", IJCIT, 2014.

[20] Seyed Mojtaba Hosseini Bamakan, et al., "New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming", Elsevier, 2015.

Author Profile

Mr. Piyush Pareta pursed Bachelor of Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya bhopal in 2014. He is currently pursuing Master of Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal. and currently working as Software Developer in Department of Information Technology.