ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

A study on various attacks and Intrusion Detection Systems in Cloud

Miss. Prachi Tembhare[1], Dr. Neeraj shukla[2]

M.Tech (Computer Technology and Application), Gyan Ganga College of Technology, Jabalpur, (M.P), India[1]

Vice Principle, Computer Science and Engineering, Gyan Ganga College of Technology, Jabalpur, (M.P), India[2]

Abstract: Cloud computing is the most emerging technology today. It is providing solution to various resources either software or hardware to its users' on-demand in pay-as-you go strategy. Now-a-days every IT companies are focusing on adoption of this latest innovative computing trend. Using virtualization technique, network and storage, this computing provides number of services using shared pool of resources in distributed environment. Due to its advent over the Internet, this computing is also vulnerable to various attacks like Man-in-the middle attack, DoS attack, Session Hijacking, etc. and hence arises number of security concerns. This paper elaborates various security concerns and popular attacks in cloud. Beside this it also focus on various Intrusion Detection System available in cloud computing.

Keywords: cloud security, attacks, Intrusion Detection System (IDS), Denial of Service (DoS), Anomaly Based IDS, knowledge base IDS.

1. INTRODUCTION

Cloud computing is the most innovative technology today. This computing provides the solution of requirement of hardware or software resources to individual or any organization, community, industry, etc. It provides this solution by using its various pools of shared resources which is the heart of implementation and deployment of this computing. This computing contains three important components that are network, storage and servers. The operational model of cloud computing uses its intermediate shared servers; network either Private network or Internet and Storage working in distributed environment.

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". Hence this computing overall reduces the operational, functional, manageable, infrastructural and overall computational cost for its users. Besides these advantages, this computing is also prone to number of attacks due to its dependency over the network (i.e. Internet). The Internet works using various protocols like TCP, UDP, ICMP, HTTP, etc. which are vulnerable to number of attacks today. Hence there arises number of security concerns and its solution in cloud computing.

Security issues such as Availability, Privacy, Authentication, Integrity and Trust plays a vital role in deployment and adoption of this computing. The next section of this paper elaborates security issues, followed by popular attacks and various Intrusion Detection System approaches that are present in cloud comp security issues in cloud.

Cloud computing consists of various security concerns that must be carefully treated before using this distributed computing. In cloud various security aspects are present that directly influence its adoption by the user. Rather than user these security aspects are also in concern with the cloud service providers. The problem of Trust among each other, the authentication issues together with the privacy concern also with the availability of data, information or services are to carefully examined in cloud computing.

Privacy/Confidentiality

Confidentiality refers to the privacy of the data or applications. Only authorized parties or systems should have the ability to access protected data. The threat to confidentiality in cloud is due to the increased number of parties, devices and applications involved. There arises the risk of data compromise, as the data becomes accessible to an augmented number of parties. Data confidentiality is correlated to user authentication. Protecting a user's account from theft or unauthorized agent is the main issue. Privacy is the desire of a person to control the disclosure of personal information [1]. Organizations dealing with personal data are required to obey to a country's legal

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

framework that ensures appropriate private and confidentiality protection in cloud computing.

Integrity:

Another security issue in cloud computing deals is the integrity of data and information. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware [18]. Integrity is the protecting data from unauthorized access so that there should not exit any deletion, modification or fabrication on the data. The Cloud service provider must provide the surety that there exist no modification in the customers' data.

Availability

Availability means making accessible of services, hardware, software or platform upon demand by the authorized party [18]. It is the property of a system being available and usable upon demand by an authorized entity. In cloud computing, availability refers to data as well as software but also hardware being available to authorized users upon demand. The cloud service provider must guarantee that information and information processing is available to clients upon demand.

Trust:

Trust is the major concern that directly influences the cloud user. Both the service provider and the cloud user should have the reliability between each other to provide the smooth functionality of computation in cloud. Trust in a cloud environment depends heavily on the selected deployment model, as governance of data and applications is outsourced and delegated out of the owner's strict control [18]. In traditional architectures, trust was enforced by an efficient security policy, which addressed constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

Attacks in cloud:

Before developing or deploying any system for security in cloud, it is essential that the knowledge of some popular attacks must be known. The next part of this paper explains about some of the popular attacks that may be present in cloud computing. These attacks hinder some important security issues such as Authentication, Integration in cloud.

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.

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.

Side Channel Attack

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.

Man-in-the-Middle Attack:

MITM has become quite popular in the cloud computing. It is mainly present in SaaS environment of cloud. Here the attacker intercepts the communication channel established between legitimate users and modifies the communication between client and server without their knowledge [13]. Some examples of this attacks are Wrapping Attack, SSL attack, etc.

Session Hijacking:

Session hijacking is the attack in which is the Session ID issued to the authenticated users is not protected properly, which in turn can be used for spoofing identity [13]. Session side-jacking uses packet sniffing tools to capture a login sequence and thus gain access to the user's session key Encrypting the communication channel can prevent this type of Session hijacking attack.

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

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

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.

Anomaly based Intrusion Detection:
It flags 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.

2. 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 that 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.

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 misconfigurations through a third party IDS monitoring and advisory service.

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.

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.

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

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

detection [20]. 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.

3. 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", 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." Comput Electr Eng , 2012
[9] Kshetri,N., "Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy", 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 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] NIST National Institute of Standards and Technology .http://www.nist.gov/itl/cloud/upload/cloud-defv15. Pdf, 2011
[17] Kevin Sloan, "Security in a virtualised world", Amethyst Risk Management, Network Security, 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", 2014
[20] Seyed Mojtaba Hosseini Bamakan, et al., "New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming", Elsevier 2015
[21] IR.Ramya, IIG.Kesavaraj, "A Survey on Denial of Service Attack in Cloud Computing Environment", IJARET, 2015