Approaches for Mitigating Insider Attacks in Cloud Infrastructure

Divya Vadlamudi, Pushpitha.M, Sarika.G, Tejaswini.N

Abstract— Now-a-days Enterprises and individuals make use of cloud services which offers them a lot of advantages from the features of cloud computing like pay-as-you-use, elastic scalability and others. By the use of Internet Cloud Consumers can be able to get the cloud services. But there are few concerns in adopting the cloud-based services for individual's daily work. The main concern is lack of security to the cloud consumer's data and computations performed by the consumer. Another main concern is threats from the malicious insiders like insider attacks and also from the unauthorized users like outsiders. In the current paper we have gone through different approaches for detection and prevention insider attacks.

Keywords: Cloud Computing, Insider attacks, Outsiders

1. INTRODUCTION

Cloud Computing allows users to utilize many services such as providing Software, Platform and Infrastructure at low of cost by the interaction of cloud provider. It also offers many features such as large storage , where users can able to store a large amount of data Cloud computing also provides Shared resources, virtualized servers, so many IT sectors and individuals wants to use it [1].Cloud computing makes use of networks of servers at low-cost to establish special connections to data. But some security concerns are preventing wide adoption of cloud. Some of the issues are breaching of data, Hijacking of Accounts, Threat from insiders, injecting the malware, Abusing of Cloud facilities, Shared Vulnerabilities, Data loss [2]. These factors will cause damage the integrity and confidentiality of the data present in cloud.

Deployment models are partitioned based upon the accessibility of the cloud [3]. They are

1. Private Cloud: The assets and frameworks that provide the administration are observed inside the organization or association that uses them in private cloud. The association is the supervisor for organization of the frameworks which are utilized to provide with administration. Moreover association is likely in charge of all the products or customer apps that are introduced on the end-user framework.

Revised Version Manuscript Received on March 08, 2019.

Divya Vadlamudi, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. (E-mail: divya.movva@kluniversity.in)

Pushpitha.M, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. (E-Mail: pushpithamodugula@gmail.com)

Sarika.G, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. (E-Mail: g.sara200@gmail.com)

Tejaswini.N, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. (E-Mail: tejashwini.1024@gmail.com)

2. Public Cloud: public cloud allows services accessible by public easily. Because of its openness this type of cloud might be less secure. In general society administration had shown every one of the frameworks and resources that give the administration are housed at an outside administration supplier.

3. Community Cloud: These are semi-open clouds that are distributed by independents from select group of institutions which are gathered together. The associations would prefer not to utilize an open cloud i.e. public cloud which is interested in each one. They need more security than what an open cloud offers.

4. Hybrid Cloud: This cloud is the mixture of two or more deployment models. A hybrid cloud may acquaint more many-sided quality with nature, yet it additionally permits more adaptability in satisfying an organizations destination.

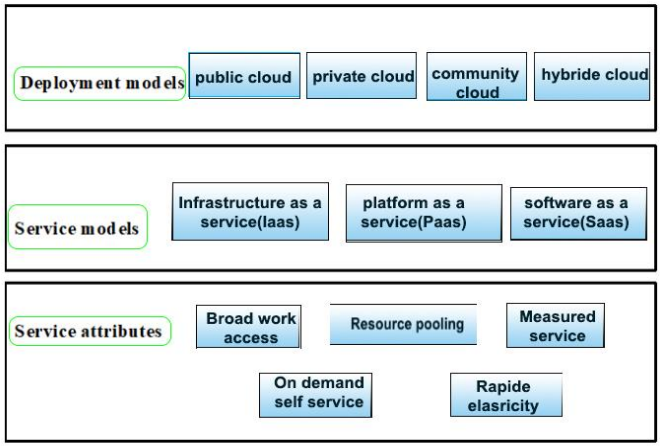

Figure 1: Cloud architecture by NIST

Service models in Cloud are [4]:

1. Infrastructure as a Service (IaaS)

It allows customers to obtain storage, machines and framework. IaaS administrator handles the entire framework and the users are responsible for entire parts of the organization. These also include working framework, apps and user associations with framework.

2. Software as a Service (SaaS)

It facilitates users with working environment which includes apps, administration, and user interface for particular software. In SaaS, the application is provided to the customer with a customer interface, and the user's function begins and

ends with entering and managing its data and customer collaboration. Everything beginning from the application to the foundation is the seller's obligation. SaaS requires continuous internet connection to use the software from any desired location.

3. Platform as a Service (PaaS)

PaaS provides users with virtual machines, frameworks, applications and control structures. The customer can pass on their applications to the cloud base or utilize applications that are modified by utilizing devices which are supported by PaaS administration provider.

The paper is ordered as follows: Section II covers concept of insider attacks and section III explains about some approaches for the insider attacks mitigation. After discussing the various approaches we have compared all these approaches. In Section IV we concluded our paper with a finding.

2. INSIDER ATTACKS

Insiders are members within the organization working in any group, who have an authorized access to the systems and networks and are intended to misuse the computer systems [5].In some cases these are also referred as an Threat from the insiders. A Threat is considered as an action which might result in the ruin of organization and even may prone to attacks. Therefore this insider attack is designed to harm the organization by the medium of employees who are having authorized access to the information system [6]. Individuals who became insiders, will exhibit certain personality characteristics intentionally or unintentionally, which may differ from one person to the other persons. There is a scenario in which individual will disclose some similar actions without the intention of performing an insider attack. If organizations will able to identify these features or behavioral actions then there is a chance to reduce insider attack.

The Organizations must identify the people who display these attributes and screen them intently. It is likewise fundamental that the organization guarantees its workers comprehend that these kinds of practices and activities can be lead to gain information by insiders. There are many different features which may distinguish insider attackers from normal employees. Insiders are the ones who can access the company's system they may be a workers, contract holders, consultancy agents. Insiders may also act as a third-party holder. [7]. Insiders no need to work for the company currently. An insider is the one who had a deep knowledge in security and operation on the systems. Andrews et al. states that “Mostly all insiders use local resources such as Operating systems, installed applications, networks in order to carry out their purposes". So there is no need to break the organization systems.

There are two categories of insider attacks adversarial insiders and Unintentional insiders

The actions which are submitted by antagonistic insiders were the process corruption and unapproved declaration of delicate data. Insiders still utilize hacker automated tools on the Internet in order to perform malicious acts which incorporate the establishment of data and over-burdening of the system or frameworks, using informal community locales to enroll different insiders [8]. Finally, we need to know that the workers who are working from outside other than the workplace for them the companies will provide mobile access so that they can increase their productivity which will lead prone to attacks. Without any malicious intent the unintentional insiders creates threats to the organization. This is what will make it different from unintentional insiders from adversarial insiders. But still the unintentional insiders cause harm to the organization which lead to increase in the probability to harm secrecy, Integrity and accessibility of organization’s data. Lack of knowledge about organizations procedures or sometimes being neglect can lead to the destruction of organization.

An insider is the person having access to the organization assets and insider attack is an attack made by the people who have access credentials to the company’s network and system. They can do anything with the data which is stored in data centres. The main problem is giving access to the insiders by which they can access/modify the sensitive information. The risk of insider threat is with the employees who have access credentials which may lead huge damage of client’s data present in the cloud. To minimize this problem the cloud provider must give the access to only a few members of peoples like who are working for the same organization and even it is easy to detect and correct threats by monitor minimum people instead of more number of the employees who are having legal access [9]. By these we can reduce the loss of data confidentiality and integrity of the consumers.

Chances for detection of insider attacks

It is fact, that insiders are having legal access and more knowledge about company's data which is resided in the data centers. The insider without ensuring the security policies of the company/organization it is difficult to detect or analyze them and there is a less chance to catch the insider. In the case which insider has intentionally compromised the firewall and performing malicious things by bypassing the security policies, there is high chance of the insider detection and the organization can tighten the security measures and countermeasure to prevent their data. The insider can perform attacks on what he/she has actual access. Here the chance of being caught is very low and also difficult.

3. LITERATURE SURVEY

In this section primary requirement of the security providence like confidentiality, integrity are examined in all the approaches.

Table 1: Comparison of different approaches for preventing insider attacks

	Confidentiality	Integrity	Software	Hardware	Insider threat detection	Insider threat prevention
Spintzner[10]	✖	✖	✔	✖	✔	✖
Gene L.Tang et al[11]	✔	✔	✔	✔	✔	#
Miltiadis et al[12]	✔	✔	✔	✔	✔	#
Khan et al[13]	✔	✔	✔	✔	✔	✔

✔-Yes ✖-No #-Partial

Spitzner [10] presented many ways for the insider attack detection by making use of honeypots. Honeypots are resources of the information system to attract malicious users. To confine the endeavors made by outsiders to infiltrate into company's network, De-Militarized Zones (DMZ) contains these honeypots broadly established in them. He also affirmed the usage of certain types of honeypots namely, honeynets and honeytokens. Honeytoken is "data that the client isn't approved to have or data that is wrong". This data would then be able to guide the insider to detect whether insider target was malicious or not by using more advanced honeypot and a decision can be controlled by examining the insider's association with the honeypot and ensure that the honeypot looks practical to the insider so as to achieve such communication that will be utilized to collect data.

Even though honeypots provide good detection of insider attacks they also suffer from some shortcomings. The honeypots performance decreases when the malicious insider does not collaborate with the honeypot or honeytoken, in the case if their identity is found or detected by the insider. The second one is, if malicious attacker finds the existence of honeypot, he or she can infuse fake or flawed data which makes the insider threat detection complicate.

Gene L.Tang [11] et al presented various strategies for detection and prevention of insider threats using trusted computing. Trusted computing is the set of rules specified in TCG (Trusted computing group) with motive providing computer and other computing devices more secure through dedicated hardware. The strategy for detecting insider attack is performed by Monitoring the System Log. This method can detect the attack in two cases when the attack is performed out by the malicious insider or after the attack is done by the insider.

Techniques for Preventing Insider Attacks utilizing Trusted Computing (TC) include a couple of methods like Use of setup management practices to recognize logic bombs and malevolent code, Data Protection from Stealing, Providing security for Remote Access. But these methods are not highly implemented due to high cost concern

Miltiadis et al [12] discussed the problem by dividing insider threat into two possible cases, one is a malicious insider who is the employee working at the side of cloud provider, and another one an insider working for an organization which adapted cloud services to deploy their infrastructure. Strict detachment of obligations, in which no individual will have more control than what they require to satisfy their job, and access of data on a need to know premise to representatives are other known mitigation systems. He also proposed many countermeasures that should be performed by cloud provider and cloud consumer to reduce the intensity of insider threat.

Khan et al [13]. proposed methodology prevents the sensitive data computation from the insider attacks which are likely to be performed by the cloud administrator. The proposed technique achieves confidentiality and integrity of user information computation in IaaS cloud. The idea of this method depends on a Trusted Virtual Machine Monitor (TVMM) and a remote verification. The platform is attestated by the trusted party with PCR hash value. The service provider records and attestates the node controller (NC) using the TPM remote attestation property with a remote trusted party. This is how the trusted parties used for building trust between the customer and the provider in cloud.It also has a secure VM launch protocol to help the launch of customer VM on just those Node Controllers which satisfy requirements of confidentiality and integrity. In another protocol which is proposed for the purpose of computing sensitive data which is organized as Piece of Application Logic, which is executed in the Flicker protection. So the delicate data can only be viewed by the client PAL in the Flicker session. Data is operated there in full separation from remaining system. By this client data confidentiality is achieved and is prevented from the malicious insider.

The Table 3.1 demonstrates the aim of survey is to give confidentiality and integrity of data together with trusted method to mitigate the insider attacks. Khan et al approach which is the integration of both software and hardware that works well for the prevention of the insider attacks in cloud infrastructure. This approach majorly uses the hardware support for mitigation of insider attack.

4. METHODOLOGY AND PROCESS TO OBTAIN RESULT

The mechanism proposed makes use of an algorithm which uses the concept of the watermarking. This algorithm secures the information that cloud client has stored in the cloud. The algorithm is embedded in the security module which is discussed below.

Security Module: Security module is connected to the entire framework to shield information from various assaults which are uniquely planned from the insiders like cloud provider and system administrators who are authorized.

Algorithm: Algorithm here used is Digital Watermarking based

Notation:

WD : To be watermarked Data;
$\overline{WD}$: Watermarked Data;
SK : Session key;
Alg : Watermarking algorithm;
PK_c : Private Key of client;
pk_c : Public key of client;
PK_{app} ; Private Key of cloud app
pk_{app} : Public Key of cloud app.

Pseudo code:

D← (Data) //Send the data to generate Watermark
$\overline{WD}$ ← encode (WD, SK, D) //To embed a watermark
ic← PK_c(hash ($\overline{WD}$)) //For the check of non-repudiation & integrity
S← pk_{app} (SK) // Encrypt SK with public key of cloud application
Client $\overline{WD,S,ic}$ Cloud app

Cloud application:

Cloud application verifies signature and apply the integrity check using $\overline{WD}$, ic,pk_c
Flicker ($\overline{WD}$, S) // application initiated flicker session
SK ← PK_{app} (S) // Obtain session key SK to decode $\overline{WD}$
WM ← decode ($\overline{WD}$, SK) // Obtain embedded watermark WM
Obtain required Data //Original information

The following algorithm steps ensure that all the sensitive information that is used by the application in cloud is retrieved and processed by the cloud app without any insider action which leads to the destruction or the disclosure of the information.

5. CONCLUSION

Cloud computing facilitates service to user over network. The major problem in adapting of cloud is Insider attacks. Insider attacks negatively effects the reputation of the cloud. To avoid insider attacks and other effects of insiders various approaches are implemented. So in this paper we have studied some of the methodologies for identification and prevention of insider threat proposed by various researches. The approaches are compared on the basis of various parameters for the further research.

REFERENCES

1. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications. 2011 Jan 1;34(1):1-1.
2. https://www.incapsula.com/blog/top-10-cloud-security-concerns.html.
3. Peng J, Zhang X, Lei Z, Zhang B, Zhang W, Li Q. Comparison of several cloud computing platforms. InSecond International Symposium on Information Science and Engineering (ISISE 2009) 2009 Dec 1 (pp. 23-27). IEEE.
4. Ren K, Wang C, Wang Q. Security challenges for the public cloud. IEEE Internet Computing. 2012 Jan;16(1):69-73.
5. Bhadauria R, Chaki R, Chaki N, Sanyal S. A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388. 2011 Sep 25.
6. Cummings A, Lewellen T, McIntire D, Moore AP, Trzeciak R. Insider threat study: Illicit cyber activity involving fraud in the US financial services sector. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST; 2012 Jul.
7. McCormac A, Parsons K, Butavicius M. Preventing and profiling malicious insider attacks. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMAND CONTROL COMMUNICATIONS AND INTELLIGENCE DIV; 2012 Apr.
8. Zeadally S, Yu B, Jeong DH, Liang L. Detecting insider threats: Solutions and trends. Information security journal: A global perspective. 2012 Jan 1;21(4):183-92.
9. Ohta K, Okamoto T. Multi-signature schemes secure against active insider attacks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 1999 Jan 25;82(1):21-31.
10. Spitzner, Lance. "Honeypots: Catching the insider threat." Computer Security Applications Conference, 2003. Proceedings. 19th Annual. IEEE, 2003.
11. Tang GL. Trusted computing: addressing insider threats to the banking and financial sector.
12. Kandias, Miltiadis, Nikos Virvilis, and Dimitris Gritzalis. "The insider threat in cloud computing." International Workshop on Critical Information Infrastructures Security. Springer, Berlin, Heidelberg, 2011.
13. Khan, Imran, et al. "A Protocol for Preventing Insider Attacks in Untrusted Infrastructure-as-a-Service Clouds." IEEE Transactions on Cloud Computing (2016).