International Journal of Electrical and Computer Engineering (IJECE)
Vol. 5, No. 1, February 2015, pp. 136~141
ISSN: 2088-8708

Mitigation of Insider Attacks through Multi-Cloud

T. Gunasekhar, K. Thirupathi Rao, V Krishna Reddy, P. Sai kiran, B. Thirumala Rao
Dept of CSE, K L University. Andhra Pradesh, India
Email: tgunasekhar@kluniversity.in[1], kthirupathirao@kluniversity.in[2]

Article Info

Article history:

Received Sep 16, 2014
Revised Nov 7, 2014
Accepted Dec 5, 2014

Keyword:

Attacks
Confidential
Insider
Intellectual Property
sabotage

ABSTRACT

The malicious insider can be an employees, user and/or third party business partner. In cloud environment, clients may store sensitive data about their organization in cloud data centers. The cloud service provider should ensure integrity, security, access control and confidentiality about the stored data at cloud data centers. The malicious insiders can perform stealing on sensitive data at cloud storage and at organizations. Most of the organizations ignoring the insider attack because it is harder to detect and mitigate. This is a major emerging problem at the cloud data centers as well as in organizations. In this paper, we proposed a method that ensures security, integrity, access control and confidentiality on sensitive data of cloud clients by employing multi cloud service providers. The organization should encrypt the sensitive data with their security policy and procedures and store the encrypted data in trusted cloud. The keys which are used during encryption process are again encrypted and stored in another cloud area. So that organization contains only keys for keys of encrypted data. The Administrator of organization also does not know what data kept in cloud area and if he accesses the data, easily caught during the auditing. Hence, the only authorized used can access the data and use it and we can mitigate insider attacks by providing restricted privileges.

Corresponding Author:

T. Gunasekhar,
Research Scholar,
Department of Computer Science and Engineering,
K L University,
Greenfields, Vaddeswaram, Guntur District, Andhra Pradesh 522502, India
Email: tgunasekhar@gmail.com

1. INTRODUCTION

According to the CERT definition of insider threat "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" [1]. An insider attack can be defined as an intentional misuse of computer system which has potential data about an organization. According to this definition attacker can be employee, contractor and/or third party business partners. The damages of insider threat are: IT sabotages, theft of confidential information, trade secrets and Intellectual property (IP). 85% of reported fraud is committed by people within the organization [1]. A typical organization loses approximately 5% of its annual revenue to insider fraud and 330 cases of insider fraud identified during 2010.Such that every organization needs secure management of sensitive data and Intellectual property. In cloud environment most of insider threat can be done by cloud insiders such that they should provide robust security algorithm on client data [2]. In this paper we provide a prototype for securing data at data centers as well as at organizational databases.

2. THE INSIDER THREAT

The organizations or cloud providers can recruit participants by word of mouth and advertisements, then participants were can be assigned with terms and conditions. Each condition describes the scenario of the same task to be complete but they provide role that manipulate their "intent" [3].

TYPES OF INSIDER THREAT

Based on the levels of access privileges, the insider threat can be broadly categorized in to four types:

- Pure insider
- Insider associate
- Insider affiliate
- Outside affiliate

Each has its own level of access credentials and with different motives.

Pure Insider (Employee)

An employee has all access rights and typically they can have badge or keys to their organization data centers. In fact the employees might well about logical and physical structure of sensitive data because they have every right to access data and company cannot restrict the employees during work hours. So, employees are most danger about to insider threats and the insider threats are possibly by employees of that company only. The elevated insider is an insider who as auxiliary privileges from normal employees. The system administrators or root administrators, who have full power on central data, these kinds of employees may have additional access to do their job but in some cases they will get more access than they required. In most often to reduce the insider threats, the companies need to strict the people by providing the limited and accurate access to information systems. The pure insiders can be restricted to insider attacks via three key aspects. One that with limited access privileges that should effect on their general duties. By doing so we can prevent and easily detect the insider who made malicious activities over sensitive information. Here, the key is controlling and limited access. Second key is fall under the behavior of insiders. In general someone committed to insider attacks, their behavior pattern might be different from as usual. Such persons openly speak badly about company and/or resources those are assigned to them. They usually very angry about organization and unhappy about workloads and, they are ready to leave the company. The third factor of the pure insiders is money. The general employees could not commit to insider attacks, if the workload and financial problems getting as issue they might be tempted to do attacks. If someone offers lump sum to employees to make all the problems away from them, they might commit to perform insider attacks.

Insider Associate

Insider associates are not employees but they have some sort of access in terms of physical instead of network of company. The insider associate might have limited access to physical elements instead of company network. Security guards, cleaners and contractor and/or business partners are fit under this category of employees. After working hours some of the employees may leave their sensitive data on their desk, the insider associate may copy that data and made some malicious activity on data. Here, the problem is that a main key was maintained at central location that can be used by anyone to gain access to office place. Some of the insider affiliates sophisticated about computer resources and they made copy of sensitive data. It is some kind of insider attack. To prevent such type of attacks, the general employees could be aware of these types of attacks. The employees should understand that the people have auxiliary access privileges and they should lock systems and secure sensitive data before they leave the company.

Insider Affiliate

The insider affiliates are not employees like pure insiders and insiders. The pure insiders and insider affiliates has reason to access company resources but insider affiliates do not. The insider affiliate is friend, spouse, and/or third party client of that organization. In some occasions, the friends of employees may visits to them; they can get access using the employee credentials through the remote access. When they get engaged with some work, the insider affiliates might theft sensitive information from the employee desk. This is a simple problem but it may leads to insider attacks. If suppose, the spouse want to use laptop of employee; the employee might give credential to insider affiliate. She can modify, delete or copy the sensitive data from laptop and it leads to insider data loss or threat. It seems to be very simple problem but result of it shows how danger it is. In order to prevent insider attack from insider affiliates, the employees should educate with policies and procedures of company.

Outside Affiliate

Outside affiliates are not a part of company and they don't have legitimate access to companies' resources. Unprotected wireless network is a best example. The outside attacker may access the network

without any access privileges. So, outsiders are free to use and he can do whatever he want. It is an obvious problem in companies and companies should aware of such type of attacks. The companies should upgrade security policies and procedures. These attacks are easy to identify or detect.

In some scenario participants may fallen on hard financial period among them, the malicious employees or participants can accept a new and higher paying job, which is offered by new company or competitor but they want bring the inside information of old organization. All the participants after completed formalities and pre-study questionnaires and then they will receive necessary components with their respective scenario. The participants play their role on working hours over specified days to complete their tasks. The resources were configured to monitor both network and host based behavior at all the times. When the participants completed they should return resources to the research leads. In addition to this normal behavior, the malicious participants more likely to relieve their jobs into data gathering periods i.e., more logoffs and more logons and indirect data access. Malicious participants also avoided by searching for detailed data by accessing project sites and relevant shared data directories.

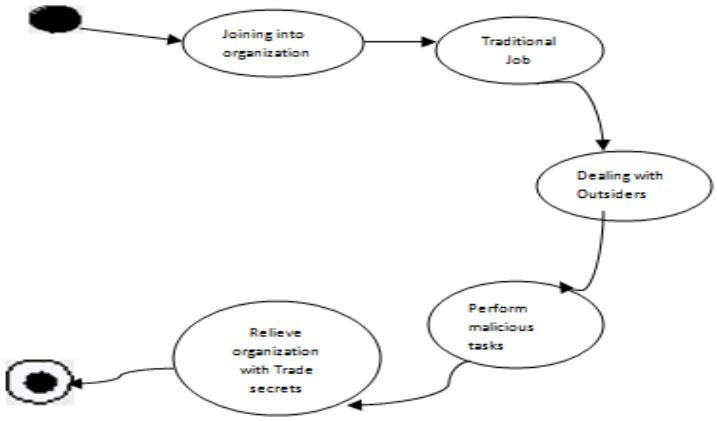

Figure 1. States of Insiders

Figure 1 shows this relationship, and gives a summary of example attacks and/or vulnerabilities each level of administrator could exploit.

Insider Threats in CSP

The insiders in this scenario are: cloud provider and cloud clients, the malicious administrator working for the cloud provider and cloud clients may miss use their privileges to destroy the cloud data [3]. The malicious insiders may theft intellectual property of other employees and use those credentials to destroy or steal the information systems in cloud data centers. The result of these attacks in cloud data centers will vary from data breaches to data steal of the infected systems and data centers. Detecting such an indirect access is challenging task. All common cloud services like PaaS, SaaS and, IaaS are equally likely insider attacks as long as the insider has privileges to access datacenters and /or cloud management systems [2] [4]. Hence, cloud computing paradigm could be utilized in order to outsource vast parts of the infrastructure instead of specific services, such as web hosting or application hosting. The following section will demonstrate the generic model view of an insider attacks in cloud era.

3. GENERIC MODEL

The generic model of cloud environment provides facilities for clients to store their sensitive data, software as service (software is provided as service from cloud provider), platform as service (platform is provided as service) [6] [7] and infrastructure as service. In general the organizations want to use cloud services in a secure manner instead of purchase products [10]. Due to the security concerns the organizations want to keep their data in secure manner such that data can be encrypted by using cryptography algorithms and store it in cloud data centers. The encryption mechanism needs key management to process information; this is trivial task of clients. The figure 2 depicts generic version of cloud based organization. Here, the administrators of organization and cloud service providers have valid privileges to access the cloud information, which is stored at cloud data centers [5].

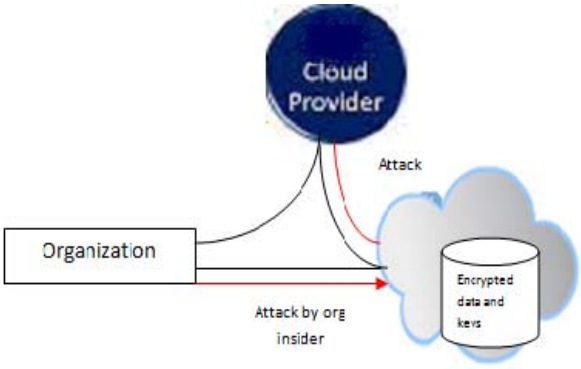

Figure 2. Generic model

But the insider may have malicious intent about the stored data and they might perform unusual operations on sensitive data. In such an environment cloud provider has access privileges to cloud data center, the insiders of cloud may perform harmful activities on clients by using the cryptographic keys of relevant data [10]. The organizations suffer from generic model whenever they lost intellectual properties and privileges. Hence the generic model is weak potentiality to secure clients information system.

4. PROPOSED MODEL

Our proposed secure cloud model includes the same components as the generic model discussed in the earlier section, with additional security features such as firewalls and algorithm. The operation of this algorithm described in more in detail in below.

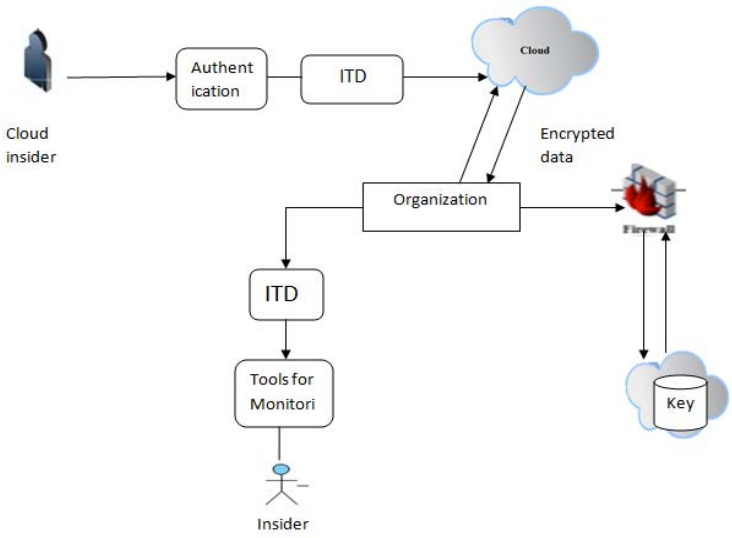

Figure 3. Proposed Model

Another important aspect here is that multiple clouds are utilized to keep their data as secure. In one of the cloud data center the encrypted information stored and another cloud can be used to store the keys of the cryptography algorithm. In order to encrypt the information we need strong cryptography algorithm such that it might be have keys i.e., public key and/or private key. In the generic model cloud provider have an authorized access to cloud data centers by this they can perform malicious tasks on stored data. The generic model is not secure because encrypted information and keys are stored in same cloud data centers. If one cloud insiders gained access; they can perform nontraditional tasks on entire data system as a legitimate user. The proposed model vanquishes these issues by using heterogeneous clouds.
The following will elaborate about the process of methodology,

1. In order to maintain Sensitive data in secure manner, it should be encrypted with strong cryptography algorithm.
2. Store sensitive encrypted data in cloud with secure mutual agreement among cloud provider and company.
3. Keys that are used while encrypting data are stored on another cloud by accounting security policies of cloud service provider.
4. Provide digital certificates to the insiders of cloud provider as well as insiders of organizations to authorize the right persons.
5. Establish network monitoring and audition tools to detect unintended behavior of insiders.
6. Through this model we can provide at most security to the stored data.

By exploitation of this framework the organizations can conserve their sensitive data from the irrupt access.

5. CONCLUSION

We identified two types of insider threat in cloud computing. The first is the one who works for the cloud provider. They could cause great deal of information damage in both the provider and its customers. The second is the one who works for the organization that decides to outsource. We described and documented the differences between the traditional insider and the malicious insider in cloud. The proposed model ensures security on key server, sensitive data and, other information systems in cloud data centers as well as in organizations.

According to the Internet threat resource center, twenty four percent of data breaches that reported from financial institutions in during 2008 and twenty percent of government information breaches and, sixteen percent of private business data breaches were caused by insider attacks**.** 50 percent of government websites vulnerable, those have no security mechanisms.

Even though this framework provides security on stored data, there are some concerns about key management and side channel attacks are possible. Our research continues on side channel attacks in order to prevent such attacks.

REFERENCES

[1] www.cert.com/insider-threat.
[2] Miltiadis Kandias, Nikos Virvilis, Dimitris Gritzalis., "The insider threat in cloud computing", *Information Security & Critical Infrastructure Protection Research Laboratory*, 2012.
[3] Theoharidou M., Kokolakis S., Karyda M., Kiountouzis E., "The insider threat to Information Systems and the effectiveness of ISO 17799", *Computers & Security*, Vol. 24, No. 6, pp. 472-484, 2005.
[4] Bishop M., Gates C., "*Defining the Insider Threat*", in Proc. of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, Tennessee, Vol. 288, 2008.
[5] Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., Zaharia M., "*Above the Clouds: A Berkeley View of Cloud Computing*", UCB/EECS-2009-28, Univ. of California at Berkley, USA, 2009.
[6] Ruby K., Shaw E, Post J., "The insider threat to information systems: The psychology of the dangerous insider", *Security Awareness Bulletin*, Vol. 2, pp. 1-10, 1988.
[7] Kandias M., Mylonas A., Theoharidou M., Gritzalis D., "*Exploitation of auctions for outsourcing security-critical projects*", In: Proc. Of the 16th IEEE Symposium on Computers and Communications (ISCC '11), Greece, 2011.
[8] Anderson J., "*Computer security threat monitoring and surveillance*", Technical Report. Anderson Company, Pennsylvania, 1980.
[9] Schultz E., "A framework for understanding and predicting insider attacks", *Computers & Security*, Vol. 21, No. 6, pp. 526-531, 2002.
[10] Thompson P., "*Weak models for insider threat detection*", in Proc. of the Defense and Security Symposium, Florida, 2004.
[11] Bradford P., Hu N., "*A layered approach to insider threat detection and proactive forensics*", in Proc. of the 21st Annual Computer Security Applications Conference, 2005.

BIOGRAPHIES OF AUTHORS

T. Gunasekhar received his Bachelor of Technology and Master of Technology from Jawaharlal Nehru Technological University Anantapur in 2011 and 2013 respectively. He is pursuing PhD in K L University in computer science and engineering stream. His area of research is cloud computing, Computer networks and Network security.

Dr. K.Thirupathi Rao, M.Tech., Ph.D., working as Professor and Head of the Department in Computer Science and Engineering department at KL University, Guntur Dist., A.P., India. His research interest includes Cloud computing, Operating systems and Computer Networks. He has published large number of technical papers in National & International Conferences and in National & International Journals. At present he is serving as Program Committee Member (PC) of various International Conferences. He is Chief Technical Advisory Board Member, Chief Editor, Editor and Technical Reviewer of many International Journals. He obtained his doctoral degree for the topic related to scheduling in the area of cloud computing. He is having good number of publications in reputed international journals and guiding 8 research scholars in the area of cloud computing.