Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 129 (2014) 611 – 618

Procedia
Social and Behavioral Sciences

ICIMTR 2013

International Conference on Innovation, Management and Technology Research, Malaysia, 22 – 23 September, 2013

Analysis of Insiders Attack Mitigation Strategies

Zulkefli Mohd Yusop and Jemal H. Abawajy

Parallel and Distributed Computing Lab,
School of Information Technology, Deakin University, Victoria, Australia.

Abstract

Insider threat has become a serious information security issues within organizations. In this paper, we analyze the problem of insider threats with emphases on the Cloud computing platform. Security is one of the major anxieties when planning to adopt the Cloud. This paper will contribute towards the conception of mitigation strategies that can be relied on to solve the malicious insider threats. While Cloud computing relieves organizations from the burden of the data management and storage costs, security in general and the malicious insider threats in particular is the main concern in cloud environments. We will analyses the existing mitigation strategies to reduce malicious insiders threats in Cloud computing.

Keywords: Cloud Computing, Insider Attacks, Malicious Insider Collusions, Mitigation Strategies, Cloud Computing Security, Data Security.

1. Introduction

Cybersecurity has recently received tremendous publicity in mass media with emphases on externally perpetrated attacks. Although the insider threat has remained the most consistent issue facing organisation, it has not received the attention it deserves. (Claycomb & Nicoll, 2012) defined malicious insider as “a current or former employee, contractor, or other business partner who has or had authorized access to an organizations network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organizations information or information systems.”

There is ample evidence that insider threats are real and rising to the level of an external threat. For example, (Richardson, 2008) indicated that about 44% of all organisations experienced abuse of computer systems, loss of laptops and theft of customer data. (Peters, 2009) also reported that 60% of financial

doi:10.1016/j.sbspro.2014.06.002

losses were caused by insiders. Table 1 shows four categories of malicious insider threats along with the percentage of respondents that view each threat as "major" as reported by Computer Economics (2010). The moderate level of concern about malicious insiders indicated in Table 1 is both in conflict with the number of incidents actually reported by these same organizations as well as the threat is less appreciated by the organisations.

Organisation Sizes	Unauthorised Confidential Data		Fraudulent Transactions	System Sabotage
	Access	Disclosure		
Small	29%	31%	24%	24%
Medium/Large	30%	38%	30%	26%

Table 1: Four categories of malicious insider threats

In this paper, we study the problem of insider threats within the domain of Cloud computing. Because of the economic and technical benefits it offers, Cloud computing has recently gained significant acceptance. Organizations can outsource their IT infrastructure to the Cloud and get benefits that include rapid provisioning, scalability, and cost advantages. Although, organizations appreciate the flexibility, scalability, and resource management provided by Cloud computing platforms, security in general and malicious insider threats in particular has been considered as one of the main concerns in embracing Cloud computing. Insider attacks are always identified as a high-impact risk as malicious insiders can affect the security of many users. Furthermore, this risk of insider attacks will be more serious and damaging when involving Cloud computing. Thus, securing Cloud computing against the insider threats is important to achieve Cloud users' trust. In this paper, we will analyse and discuss various Cloud specific insider threats. Using real insider attacks cases, we will show how the inherent Cloud architectures facilitate insider attacks to be successfully mounted.

The rest of the paper is structured as follows: Section 2 discusses the Cloud Computing and security issues. Section 3 explains the malicious insider attacks specific to Cloud computing. Section 4 discusses the analysis of the existing mitigation strategies and techniques to reduce malicious insiders in the Cloud Computing. Section 5 concludes the paper and presents future direction.

2. Cloud Computing and Security Issues

Cloud computing is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). Cloud Computing is a new paradigm for hosting and delivering services over the Internet. It merges many computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies that depend on the Internet. According to (Jianfeng & Zhibin, 2010), there are three service models of Cloud Computing:

a) Software as a Service (SaaS) – The capability provided to the consumer is to use the provider's application running on a Cloud infrastructure. In this model, software application is hosted as service and end users use the application on the web browser.
b) Platform as a Service (PaaS) – The capability provided to the consumer is to deploy onto the Cloud infrastructure his own applications without installing any platform or tools on their local machines. In this model, end-user creates, tests and upload application using tools and libraries hosted by the service provider.
.
c) Infrastructure as a Service (IaaS) – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. This

model involves hosting of hardware computing services like storage, hard drive, servers, and network components. Service provider is responsible for maintenance and managing all these resources.

Cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction (Brown, 2011).

Cloud systems are very economical and useful for businesses of all sizes (Onwubiko, 2010) as it offers: (i) limitless flexibility with access to millions of different databases, and the ability to combine them into customized services; (ii) better reliability and security since users no longer need to worry about their hardware failure or hardware being stolen; (iii) enhanced collaboration by enabling online sharing of information and applications, the Cloud offers users new ways of working together and cooperate; (iv) portability since users can access their data from anywhere; (v) simpler devices as the data is stored and processed in the Cloud, users simply need an interface to access and use this data, play games, etc.; (vi) unlimited storage since Cloud offers a large expandable storage that can be upgraded when needed; and (vii) access to quick processing power using the latest technology and infrastructure make the delivery of services faster.

Although there are many benefits to adopting Cloud Computing, there are also some limitations associated with it. Security is the biggest issues in Cloud computing. This is because Cloud offers storage service on a remote location and the consumers must trust the Cloud provider even though the consumers are unaware of what happens to their data (AlZain, Pardede, Soh, & Thom, 2012). External data storage, dependency on the public Internet, lack of control of the data and multi-tenancy collectively make Cloud computing risky to many security concerns.

As individuals and enterprises produce more and more data that must be stored and utilized (emails, personal health records, photo albums, fax documents, financial transactions, and so on), they are motivated to outsource their local complex data management systems to the Cloud owing to its greater flexibility and cost-efficiency. However, once users no longer physically possess their data, its confidentiality and integrity can be at risk. Traditionally, to control the distribution of privacy-sensitive data, users establish a trusted server to store data locally in clear, and then control that server to check whether requesting users present proper credential before being granted access to the data. From a security standpoint, this access control system is no longer applicable when data is housed on the Cloud. This is because the users and Cloud servers are located in different geographic locations and the server might no longer be fully trusted for defining and enforcing access control policies and managing user details. In the event of either server compromise or potential insider attacks, users' private data might even be exposed (Kui, Cong, & Qian, 2012). Loss of direct control of their data is the main security concerns for the clients. By moving their private data to the Cloud, users are forced to trust the Cloud service providers with the secure and proper management of their data.

Among security threats in the Cloud, insider threats such as malicious system administrators pose a serious risk to clients (Sundararajan, Narayanan, Pavithran, Vorungati, & Achuthan, 2011). The problem is challenging because the system administrators have elevated privileges for performing genuine system maintenance and administration tasks. An attack often posited by such insiders will always result in loss of data confidentiality and/or integrity. These insiders may be motivated financially. This is a common motivation for theft of intellectual property or fraud. Another attack possibility that must be considered is IT sabotage where employees seek to harm an employer's IT infrastructure. An insider's grudge against the Cloud provider could result in harm to a victim organization with the intention of damaging the Cloud provider's reputation (Claycomb & Nicoll, 2012).

An attacker that has access to the Cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the Cloud can also modify the functions and their input and output data. Even though in the majority of cases it may be legitimate to assume a Cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the Cloud provider, successful attacks by third parties, or of actions ordered by a subpoena (Bohli, Gruschka, Jensen, Iacono, & Marnau, 2013).

3. Malicious Insiders Attack

CERN (Institute, 2013) defines an insider threat as such "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." Bishop and Gates (2008) defined an insider based on violation of a security policy using legitimate access and violation of an access control policy by obtaining unauthorized access. In the first case, the insiders perform some actions that is opposing to the security policy using their legitimate access. When the insiders have legitimate access to the data or resources and use that eligibility to provide the information to someone who does not have access or to deny access to someone who does have access. In the second case, the insiders misuse their eligibility to extend their privileges that enable them to break both the access control and security policies. They are considered key and trusted assets and are eligible the highest possible privileges for the systems they own. Excessive and unnecessary privileges can lead system owners to act in the way they please with very little restrictions and accountability (Sibai & Menasce, 2012).

The malicious insiders can cause serious threats to an organization. They are well-trained and well-versed with the infrastructure, tools and equipment to operate their tasks. They are aware of missions, visions, standard operating procedures, rules and regulations, terms and conditions as well as policies of the organization. However, they can suddenly turn to be an adversary when they are not satisfied with the organization decision-making, their claims are not fulfilled, they are not fairly rewarded, and they are not well treated by the organization. They are more dangerous compared to external hacker because they could perform malicious action in a very structured way, smooth, faster, indistinctly that might severely impact the organization.

Insider attacks can be executed by malicious employees at the provider's or user's location. This threat can break the trust of Cloud users on provider. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may include diverse types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has grown due to lack of transparency in Cloud provider's processes and procedures. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analysed. Additionally, users have little visibility about the hiring practices of their provider that could open the door for an adversary, hackers or other Cloud intruders to steal confidential information or to take control over the Cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the Cloud services with little or no risk of detection. Malicious insider attacks can damage the financial value as well as brand reputation of an organization. Moving critical applications and sensitive data to a public and shared Cloud environment is a major concern for organization. That is because organization has lost control of the data and totally depends on Cloud provider data security and defence. To alleviate these concerns, a Cloud solution provider must guarantee that customers can remain to experience the same security and privacy controls over their applications and services by providing evidence to these customers that their organization and customers are secure (Che Fauzi, Noraziah, Herawan, & Mohd. Zin, 2012).

4. Analysis of Mitigation Strategies

Chen and Malin (2011) addressed the problem of managing sensitive information in Collaborative information systems (CIS) environment. They proposed a framework called Community-based Anomaly Detection System (CADS) to detect insider threats based on information recorded in the access logs of collaborative environments. CADS uses a formal statistical model to measure the deviation of users from the inferred communities to predict which users are anomalies by performing an analysis of CIS access logs and therefore learn the patterns of user behavior to detect anomalous insiders.

Chia-Mei, Guan, Yu-Zhi, and Ya-Hui (2012) investigated the problem of sequence of attack behaviour to compromise the system in Cloud. A malicious attacker may combine multiple security vulnerabilities and often adopts persistent attack approach consisting of a sequence of attack behaviors into an intelligent attack. A malicious insider or service hijacking may abuse Cloud Computing or attack one or more machines in the Cloud. These cause more serious damage than in a network environment where machines are distributed and independent. Therefore the authors proposed Hidden Markov model to detect such attacks by examining the stages of an attack plan and analyzing logs to identify attack sequences.

Jung-Ho, Min-Woo, Seon-Ho, and Tai-Myoung (2011) addressed the problem of insiders execute their authorization legitimately to leak information on network system. The insiders may use the privileges of a program and execute the program in abnormal ways so that they can achieve their attack goals. Therefore the authors applied attack tree and misuse monitor to reduce security violation by identifying the insider information, preventing insiders' abnormal activities, preventing resource misuse and manage security policy and updating the database.

Yaseen and Panda (2010) investigated the problem of malicious modifications by insiders in relational databases. Dependencies can be used by insiders to make changes to the unauthorized data. Insiders can study constraints on dependencies between tables, attributes and data items to modify data. Therefore hiding dependencies from insiders can prevent them from modifying the unauthorized data. However they still can find out the hidden dependencies by collaborating and sharing different dependencies information among them. Two methods have been developed to prevent modifications: cut algorithm and modification graph. The cut algorithm determines which dependencies should be hidden. Changes made by authorized and unauthorized insiders produce insiders' modification graphs. The modification graph generated by algorithms shows the authorized and unauthorized data items that insider can modify.

Parveen, Evans, Thuraisingham, Hamlen, and Khan (2011) addressed the problem of detecting insider threats in unbounded, evolving, and unlabeled large data stream. The authors proposed ensemble-based stream mining, unsupervised learning, and graph-based anomaly detection to the problem of insider threat detection as well as demonstrating that the ensemble-based approach is significantly more effective than traditional single-model methods.

Brdiczka et al. (2012) addressed the problem of detecting malicious insider behavior through monitoring network activity and the use of enterprise applications using graph analysis, dynamic tracking, and machine learning. These tools can accurately identify known attacks, but they are reactive, and may be eluded by previously unseen, adversarial behaviors. Therefore the authors proposed an approach that combines Structural Anomaly Detection (SA) from social and information networks and Psychological Profiling (PP) of individuals. Psychological model will determine individuals who have the motivation and capability to carry out an attack.

Nithiyanandam, Tamilselvan, Balaji, and Sivaguru (2012) proposed a framework consists of layers to monitor user activity for preventing insider malicious activities. The framework prevents insider abnormal activities on IS by monitoring the point of use activity. The framework monitors the data

transfer media's and check for resource misuse by insider by comparing the resource transferred with the database.

Approaches	Collusion Detection	Platform
(Yaseen & Panda, 2010)	Yes	Database
(Chen & Malin, 2011)	No	Database
(Chia-Mei et al., 2012)	No	Cloud
(Jung-Ho et al., 2011)	No	Network
(Parveen et al., 2011)	No	O/S
(Brdiczka et al., 2012)	No	Network
(Nithiyanandam et al., 2012)	No	Network

Table 1. Comparison of approaches for mitigating insider threats based on collusion and platform.

5. Conclusion

Malicious insiders' attacks that exist in the Cloud system attempting to exploit the weaknesses of the system pose a serious threat to organizations. With the flexibility of Cloud system the malicious insiders can manipulate the privileges to access the sensitive information remotely. Even worse, malicious activity from the inside Cloud provider system is hard to observe when there are collusion and collaboration between multiple insiders, insiders and outsiders within Cloud environment. And these could pose severe implications to data confidentiality, integrity and availability. However no approach has so far offered a satisfactory path towards a solution. Therefore this study will investigate the suitable mitigation strategies to overcome the problem.

References

AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012, 4-7 Jan. 2012). *Cloud Computing Security: From Single to Multi-clouds.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Bishop, Matt, & Gates, Carrie. (2008). *Defining the insider threat*. Paper presented at the Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, Oak Ridge, Tennessee.

Bohli, J. M., Gruschka, N., Jensen, M., Iacono, L. L., & Marnau, N. (2013). Security and Privacy-Enhancing Multicloud Architectures. *Dependable and Secure Computing, IEEE Transactions on, 10*(4), 212-224. doi: 10.1109/TDSC.2013.6

Brdiczka, O., Juan, Liu, Price, B., Jianqiang, Shen, Patil, A., Chow, R., . . . Ducheneaut, N. (2012, 24-25 May 2012). *Proactive Insider Threat Detection through Graph Learning and Psychological Context.* Paper presented at the Security and Privacy Workshops (SPW), 2012 IEEE Symposium on.

Brown, Evelyn. (2011). Final Version of NIST Cloud Computing Definition Published. Retrieved July 20, 2013, from http://www.nist.gov/itl/csd/cloud-102511.cfm

Buyya, Rajkumar, Yeo, Chee Shin, Venugopal, Srikumar, Broberg, James, & Brandic, Ivona. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems, 25*(6), 599-616.

Che Fauzi, AinulAzila, Noraziah, A., Herawan, Tutut, & Mohd. Zin, Noriyani. (2012). On Cloud Computing Security Issues. In J.-S. Pan, S.-M. Chen & N. Nguyen (Eds.), *Intelligent Information and Database Systems* (Vol. 7197, pp. 560-569): Springer Berlin Heidelberg.

Chen, You, & Malin, Bradley. (2011). *Detection of anomalous insiders in collaborative environments via relational analysis of access logs.* Paper presented at the Proceedings of the first ACM conference on Data and application security and privacy.

Chia-Mei, Chen, Guan, D. J., Yu-Zhi, Huang, & Ya-Hui, Ou. (2012, 9-10 Aug. 2012). *Attack Sequence Detection in Cloud Using Hidden Markov Model.* Paper presented at the Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on.

Claycomb, W. R., & Nicoll, A. (2012, 16-20 July 2012). *Insider Threats to Cloud Computing: Directions for New Research Challenges.* Paper presented at the Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual.

Institute, Software Engineering. (2013). The CERT Insider Threat Center. from http://www.cert.org/insider_threat/

Jianfeng, Yang, & Zhibin, Chen. (2010, 10-12 Dec. 2010). *Cloud Computing Research and Security Issues.* Paper presented at the Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on.

Jung-Ho, Eom, Min-Woo, Park, Seon-Ho, Park, & Tai-Myoung, Chung. (2011, 13-16 Feb. 2011). *A framework of defense system for prevention of insider's malicious behaviors.* Paper presented at the Advanced Communication Technology (ICACT), 2011 13th International Conference on.

Kui, Ren, Cong, Wang, & Qian, Wang. (2012). Security Challenges for the Public Cloud. *Internet Computing, IEEE, 16*(1), 69-73. doi: 10.1109/MIC.2012.14

Nithiyanandam, C., Tamilselvan, D., Balaji, S., & Sivaguru, V. (2012, 19-21 April 2012). *Advanced framework of defense system for prevetion of insider's malicious behaviors.* Paper presented at the Recent Trends In Information Technology (ICRTIT), 2012 International Conference on.

Onwubiko, Cyril. (2010). Security Issues to Cloud Computing. In N. Antonopoulos & L. Gillam (Eds.), *Cloud Computing* (pp. 271-288): Springer London.

Parveen, P., Evans, J., Thuraisingham, Bhavani, Hamlen, K. W., & Khan, L. (2011, 9-11 Oct. 2011). *Insider Threat Detection Using Stream Mining and Graph Mining.* Paper presented at the Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom).

Peters, Sarah. (2009). *2009 CSI Computer Crime and Security Survey*: Computer Security Institute.

Richardson, Robert. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.

Sibai, Faisal M., & Menasce, D. (2012, 20-22 June 2012). *Countering Network-Centric Insider Threats through Self-Protective Autonomic Rule Generation.* Paper presented at the Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on.

Sundararajan, Sudharsan, Narayanan, Hari, Pavithran, Vipin, Vorungati, Kaladhar, & Achuthan, Krishnashree. (2011). Preventing Insider Attacks in the Cloud. In A. Abraham, J. Lloret Mauri, J. Buford, J. Suzuki & S. Thampi (Eds.), *Advances in Computing and Communications* (Vol. 190, pp. 488-500): Springer Berlin Heidelberg.

Yaseen, Q., & Panda, B. (2010, 20-22 Aug. 2010). *Malicious Modification Attacks by Insiders in Relational Databases: Prediction and Prevention.* Paper presented at the Social Computing (SocialCom), 2010 IEEE Second International Conference on.