Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 129 (2014) 581 – 591

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[a*], Jemal Abawajy[b]

[a,b]School of Information Technology, Deakin University, Geelong Victoria 3217 Australia

Abstract

Insider attacks become a severe threat to organizations. The emergence of Cloud computing that provides computing as a utility has attracted organizations to store their sensitive data remotely by subscribing the virtual storage from Cloud service provider. While data outsourcing relieves the data owners from burden of local data storage maintenance and security, the steps of embracing Cloud storage service has led to security problems. With the services provided by Cloud service provider that can be extended from Cloud user to Private Cloud and expanded to Public Cloud, there are many possibilities that malicious insider attacks may occur to exploit the weaknesses of Cloud systems. Until now there are no perfect mitigation strategies that can be relied on to solve the threats. We describe the Cloud computing and security issues, discuss about malicious insiders attack in Cloud computing and analyses the existing mitigation strategies and techniques 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

Cloud Computing has gained significant acceptance because of the economic and technical benefits in delivering computing resources. Organizations and businesses can outsource their IT infrastructure into the Cloud and get benefits from rapid provisioning, scalability, and cost advantages. Organizations begin to adopt the advantages of flexibility, scalability, and management provided by Cloud computing

* Corresponding author.
E-mail address: zmohdyus@deakin.edu.au

doi:10.1016/j.sbspro.2014.03.716

platforms and services, and often consider security as one of their top concerns in Cloud environments. Although the benefits of Cloud Computing are distinct, security is a major constrain and numerous security risks and challenges have been identified.

A survey conducted by The Computer Security Institute (Richardson, 2008) indicated about 44% of all organisations experienced abuse of computer systems in 2008 which dropped to 30% in 2009; 42% reported loss of laptops both in 2008 as well as 2009; and 17% reported theft of customer data. The 2009 survey (Peter, 2009) also revealed 25% of the respondents felt that 60% of the financial losses were caused by insiders; unauthorised access or privileged access by insiders is 15%; and Internet access and e-mails abuse by insider are the fourth most rampant incident. Both the surveys indicate that insider threats are real and nearly rising to the level of an external threat.

Security is one of the major anxieties when planning to adopt the cloud. Proving the security of data in cloud is important to achieve users' trust on cloud providers. One of the most serious challenges, not only to cloud computing, but to data security in general, is the insider threat. The insider threat is one of the problems that concern organizations and individuals about cloud computing. Moving data to cloud raises the number of insiders, which may expose to insider attack. A malicious insider, such as a cloud administrator, can easily inspect the virtual machines of cloud users and retrieve sensitive information. 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 private cloud, public cloud and hybrid deployment of both. There will be communications and collaborations taking place between consumers, cloud provider, cloud users and so on that can encourage the collusion of malicious activities to exploit the vulnerabilities to compromise the organization asset.

Cloud computing offers some incredible benefits such as unlimited storage, access to quick processing power and the ability to easily share and process information. However, it does have several issues, and most of them are security related. Cloud systems must overcome many obstacles before it becomes widely accepted and adopted, but it can be utilized right now in the right conditions with some compromises. People can enjoy the full benefits of cloud computing if researcher can address the very real security concerns that appear with storing of sensitive information in databases scattered around the Internet.

The rest of the paper is structured as follows: Section 2.0 discusses the Cloud computing and security issues, Section 3.0 explains about the malicious insiders attack in Cloud computing, Section 4.0 discusses the analysis of existing mitigation strategies and techniques to reduce malicious insiders in the cloud computing, Section 5.0 conclude the discussion

2. Cloud Computing and Security Issues

A Cloud 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, et al., 2009). Cloud computing becomes a new paradigm for hosting and delivering services over the Internet. The benefits of Cloud computing are it 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. Cloud computing combines many computing

concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet.

Cloud systems are very economical and useful for businesses of all sizes Onwubiko (2010). Cloud computing is a technology that everyone would love to take full advantage of because it offers:

1. Limitless Flexibility: With access to millions of different databases, and the ability to combine them into customized services.
2. Better Reliability and Security: Users no longer need to worry about their hardware failure, or hardware being stolen.
3. Enhanced Collaboration: By enabling online sharing of information and applications, the Cloud offers users new ways of working together and cooperate.
4. Portability: Users can access their data from anywhere.
5. Simpler devices: With data stored and processed in the Cloud, users simply need an interface to access and use this data, play games, etc.
6. Unlimited Storage: Cloud offers a large expandable storage that can be upgraded when needed.
7. Access to quick processing power: Latest technology and infrastructure make the delivery of services faster.

There are three famous service models of Cloud computing as described below:

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.

The advent of Cloud computing technologies has created an environment in which all sorts of data can be easily accessed by almost anyone if it is not properly protected. But at the same time most companies and businesses are storing important and sensitive data like client names and contacts, transaction records in Cloud. This has led to the development of various data protection software, services and technology in Cloud so that the data stored in private, public and hybrid Cloud remains secure and safe. Both service providers and their clients lack of a consistent of knowledge and guidelines of collaborative insider attacks in the Cloud and this is seen as a major concern when customers plan to move to Cloud computing technology and services.

Although there are many benefits to adopting Cloud computing, there are also some limitations associated with it, which need to be observed. Security is the biggest issues in Cloud computing as it

offering storage service on a remote location that the consumers are generally need to trust the Cloud provider and unaware of what happens to their data. External data storage, dependency on the public Internet, lack of control, multi-tenancy and integration with internal security make Cloud computing exposes to risks.

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 certification before letting them access the data. From a security standpoint, this access control architecture is no longer applicable when we outsource data to the cloud. Because data users and cloud servers are not in the same trusted domain, the server might no longer be fully trusted as an omniscient reference monitor 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, et al., 2012).

The main security concerns of clients are loss of direct control of their data and being forced to trust a third party provider with confidential information. Among security threats in the cloud, insider threats such as malicious system administrators pose a serious risk to clients (Sundararajan, et al., 2011). The problem is challenging because the cloud provider's system administrators have elevated privileges for performing genuine system maintenance and administration tasks. An attack often posited by this insider is theft of sensitive information, resulting in loss of data confidentiality and/or integrity. The insider described by this threat may be motivated financially, a common motivator for theft of intellectual property or fraud. But another attack possibility that must be considered is IT sabotage, where employees seek to harm an employer's IT infrastructure. Some may dismiss this type of crime in cloud environments, where administrators work for the provider, not the customer organizations. However, this should not be entirely discounted. Even if it is unlikely an insider has a grudge against the victim organization, an insider's a 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 and compromisation by third parties, or of actions ordered by a subpoena (Bohli, et al., 2013).

There are two types of adversaries. The first type is the insider adversaries who can be employees that work for the cloud service provider or people who have gained access to infrastructure's internal network by social engineering or other means. They have control over the all servers, thus capable of changing any user's image or the legacy host on the hosting servers. The goal of the insider adversaries is to steal documents and applications from the user's VM. Furthermore, these adversaries would not expose their insider access with a simple deny of service attack (DoS). The second type is the outsider adversaries who reside outside the cloud infrastructure. In particular, we consider them the malicious users who have control over the VMs residing on the same physical server. This type of adversary is capable to using various VM Exit to exploit the software bugs in the hypervisor. As a result, both types of adversaries are

capable of gaining control of the host system and thus compromising the confidentiality, integrity and availability of legitimate user's VM. The goal of outsider adversaries is similar to the insider in that they want to compromise the confidentiality and integrity of the target user's VM. However, since it is relatively easy to gain access a guest VM, they are not concerned of being exposed and might launch DoS attack on neighbouring VMs (Ning, et al., 2012).

3. Malicious Insider Attacks

According to S.E. Institutes (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).

When insiders becoming malicious the organization should anticipate the risk of insider attacks to their data, their business partners and their long-term future. These attacks are arranged or executed by people that are trusted with varying levels of access to a company's systems and facilities, and who have intimate knowledge of the company's infrastructure, which an external attacker would take a significant period of time to develop.

An insider is an individual who is a present or former member of an organization, employee, contractor, partner, vendor or integrator, consultant and auditor, who is trusted, who formerly or currently has knowledge, credentials and granted with legitimate access and privileges to organization information systems and services in order to execute organization and business tasks. A malicious insider is an individual who is adversely, deliberately, intentionally and inevitably misuse his/her trusted position in an organization to abuse, exploit and violate the information systems and services to compromise confidentiality, integrity and availability of organizations' assets.

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 performed by malicious employees at the provider's or user's site. Malicious insider can steal the confidential data of cloud users. 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 involve various types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has increased 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 analyzed. 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 ensure that customers can continue to have 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, et al., 2012).

Cloud providers facilitate the users with various types of services including unlimited bandwidth and storage capacity. Some cloud service providers offer free limited trial periods that gives an opportunity for hackers to access the cloud immorally, their impact includes decoding and cracking of passwords, launching potential attack points and executing malicious commands. Spammers, malicious code authors and other cybercriminals can conduct their activities with relative impunity, as cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities. For example some cybercriminals use rich content applications such as flash files that enable them to hide their malicious code and utilize users' browsers to install malware.

As Cloud computing uses virtualization, cloud providers are dwelling the user's applications on virtual machines (VMs) within a shared infrastructure. The VMs are virtualized based on the physical hardware of cloud provider. In order to maintain the security of users, providers are isolating the VMs from each other so if any of them is malicious so that it will not affect the other VMs under the same provider. The VMs are managed by hypervisor in order to provide virtual memory as well as CPU scheduling policies to VMs. As the hypervisor is main source of managing a virtualized cloud platform, hackers are targeting it to access the VMs and the physical hardware, because hypervisor resides between VMs and hardware, so attack on hypervisor can damage the VMs and hardware. Strong isolation should be employed to ensure that VMs are not able to impact or access the operations of other users running under the same cloud service provider. Several vendors such as Xen and KVM are providing strong security mechanisms of securing the cloud hypervisors, but still it is identified that sometimes security of VMs is compromised**.**

4. Analysis of Mitigation Strategies

For the purpose of understanding the factors influencing online banking services towards customer service delivery, this paper proposes a conceptual model (see figure 1 below). This conceptual model is developed based on several previous studies related to electronic banking, behavioral factors, banking application, and customer service delivery.

5. Methodology

The idea of attack tree came from (Schneier, 1999) as early as 1999. Attack trees can be used for making security decisions. Based on varying attacks Attack Tree offers a formal, methodical way of describing the security of a system. The attacks against a system are represented in a tree structure, with the goal as the root node and different ways of achieving the goal as leaf nodes. Attack tree is as a formal methodology for analyzing the security of systems and subsystems. Attack Tree can assist organizations establish attack circumstances by analyzing system vulnerabilities and dependencies among these vulnerabilities. To detect insider attacks, several studies were based on the attack tree or attack graph. Chinchani, et al., (2005) proposed a model based on the attack tree and attack graph. Hui, et al., (2006) proposed the prediction model of Insider Threat Based on Multi-agents that consist of central agent, interactive agent, predicting agent, response agent and communication services agent. Their model is based on the agent and the distribute intrusion detection system (DIDS) with several advantages such as scalability. In the model, before the user can login into a system, a user must have a session with interactive agent. The interactive agents will generate the intended operations and submits them to central agents. The central agents will create the customized minimal attack tree and the information of tree structure will be stored in local rule database. Each user will be assigned the unique corresponding minimal attack tree. The rule database can be generated in run-time that is obviously different from traditional static rule database. Predicting agents will monitor users' operations and the probability of attacks based on the minimal attack tree. If an attack is detected, response agents will report the information to central agents. However, this requires that attack trees contain knowledge about the attacks.

Yaseen and Panda (2011) investigated the problem of the flow of information in a database that cause insider threat. The flow of information depends on dependencies between different data items at tables, records and attribute level of a relational database. There are six types of dependency relationships among data items as defined by the authors. Insiders may use their knowledge about dependencies to get unauthorized information. Insiders may infer unauthorized information by exploiting these dependencies between data items. A dependency relationship may involve a constraint. The authors classify such constraints into two types such as changing the value of an attribute and deleting or inserting records. The constraints show the values of data items that are stored in the knowledgebase of insiders. A change on the dependent data occurs only when the specified constraint is satisfied. Insider may be able to predict values of data items, which they may not be authorized to access by investigating constraints. Yaseen and Panda (2010) proposed Constraint and Dependency Graph (CDG), Dependency Matrix and Threat Prediction Graph to mitigate the problem. CDG is used to build knowledge graphs of insiders. The knowledge graph is build based on the Petri Nets a mathematical and graphical modelling tool using formula. The knowledge graph is created to represent the dependencies and constraints. The authors used CDG to show how insiders can follow dependencies to infer knowledge about data items. Changing the value of an attribute and deleting or inserting records produce constraints. Insertion or deletion in a table may affect other records in the same table. Therefore, a dependency matrix is used to show dependencies between different tables as well as the constraints on such dependencies. The dependency matrix constructs clusters of tables such as safe cluster and hot cluster. The safe cluster is a cluster of tables in which each table is independent, directly and transitively, from all other tables that belong to the same cluster. The hot cluster is a cluster of tables in which each table is directly dependent on all other tables that belongs to the same cluster. To predict the threat the authors construct the threat prediction graph (TPG) that consists of an attribute, the amount of information the insider has about and the threshold value. The threshold value is the amount of information that the insider is allowed to get about. To predict the threat three types of graphs has to be generated. In cloud computing scenario which involves VM that

has a huge processing of cloud user access, it might not be economical to have these processes in a real time. It might need a high speed of processing in the databases to capture all the transactions otherwise delays will occur and the transactions will be slow. Therefore, this approach is not adaptable in Cloud environment.

Yaseen and Panda (2011) investigated the problem of an insider's Knowledgebase in a database system. The Knowledgebase contains the values of data items accessed by an insider. These values may be combined with insensitive data items to infer sensitive information. Denying access to the data items would not solve the problem because the values are still exist in the insider's Knowledgebase. Values of data items in Knowledgebase have a lifetime. If other insiders update the values of the data items, the values will be different from the existing values in the insider's Knowledgebase that cause the lifetime of the data items expire. However, updating values of data items does not make their lifetime expire. Furthermore an insider's task may consist of several operations that involve many data items. Connection between data items may involve dependency relationship so that the access to data items needs to be performed in some order. Different order of access to data items will lead to different type of risks and vulnerability.

Yaseen and Panda (2011) proposed two methods for executing an insider's task: batch of transaction and transaction by transaction. Batch of transaction involves set of operations required for each task, various insiders and their tasks, and dependencies of data items between the operations. In this method, the authors determined which accesses the insider should get first depend on the level of risks. Unordered accesses to data item to complete a transaction will expose to vulnerability in the system. The access is based on dependency relationship between the data items. Different dependency has different impact on access to data items. Furthermore to minimize the risk the authors applied the lifetime to the data items. When other insiders update the values of data items the lifetime of the data items in Knowledgebase will expire. When the lifetime expired, insiders cannot infer the correct information based on from previous access. However if there is no other insider update the data item values the transaction will be delayed. Therefore, the insider will be granted an incorrect value of the risky data item. The incorrect but close enough value is provided to the insiders but still do not expose any sensitive data. This is done by using Neural Dependency and Inference Graph (NDIG).

In the latter way, insiders may submit the transactions one after another. The first approach could not be applied when the system does not know what insider plan to access. To solve the problem, accesses patterns of data items for each task of each insider can be extracted and stored. These patterns are used to construct the Task Graph that indicates the data items, the paths of possible accesses to those data items. It also shows the dependent and independent operations by insider in a task. This can predict the tasks of insiders and combine it with their knowledgebase can facilitate the prediction. Based on this model it is possible to enhance it to solve the problem of collaborative insider's threat in Cloud computing. This is because the model can detect multiple insiders operation by looking at the access to the data item. But the constraint is Cloud computing is a large system that generates a lot of data in real time. It is impossible to apply this solution in a multiple huge Cloud database that contains many data items. Thus, this model need to be improved and enhance to cater the insider's threat in the Cloud.

Chen, et al. (2006) addressed the problem of collusion attacks to electronic transactions in e-commerce system through the security protocol. The electronic transactions are exposed to internal threats and the transactions may be possibly intercepted and revealed by internal computer or network users. Security protocols are implemented to secure the transactions. However, the security protocols contain some flaws and collusion attacks may occur when there are extensions of message sharing among people in the organization. The collusion attacks usually involve of an attacker, a group of participants

and a threshold of the attack. The collusion attacks begin when the principals put their individual secrets together and jointly recover the secret. A malicious user who attempts to obtain unauthorised data by colluding with other principals might discover more secrets even though none of them previously knew this message individually. Chen, et al. (2006) proposed a framework to detect collusion attacks in security protocols. The framework consists of three steps: identify frequent k-item sets from the transaction database of principals; construct knowledge based inference rules, and; detect collusion attacks by matching frequent item sets with the knowledge base. Frequent Patterns (FP) tree algorithm is used to identify the frequent item sets from database transactions. A knowledge base is constructed that comprises the knowledge that is specific to the domain of application, including such things as facts in the domain, and rules that describe the relations or phenomena in the domain. The inference rules of knowledge base consist of the basic manipulation of secure messages in security protocols. The detection of collusion attacks is implemented by matching derived frequent item sets with knowledge bases. The intrinsic inference mechanisms of Prolog are used to manipulate the knowledge base and frequent item sets. This approach cannot be applied into the Cloud environment where there are many huge databases scattered, distributed and located at different sites of network. As Prolog rules are used for the knowledge representation, and the Prolog inference engine is used to derive conclusions, therefore the DBMS must periodically synchronize the scattered databases to make sure that they all have consistent data in order to identify frequent itemsets, construct knowledge and detect collusion.

Kohli, et al. (2011) addressed the problem of insider collusion threats to critical assets. Collusion threats occur when two or more employees accessing a system with different privileges collude. Insiders may collude with other insiders or with outsiders to attack, steal or damage the organization's assets. The collusion is done in a structured manner and has a defined objective. Unauthorized elevation of privileges may occur when one or more threat agents are insiders. The collusion threat might be even worse if it happens in Value webs where organizations collaborate with other organizations through cross-organizational networks that involved outsourcing, partnering, joint ventures and subcontracting. The collusion may involve other kind of threat agent called External Insider. It is very difficult to predict the attack vectors, motivation factors and the actors involved in the collusion. Collusion threats give more negative impact to organizations compare to individual threats. Kohli, et al. (2011) proposed an approach to identify the collusion threat. The approach is based on risk analysis that gives a realistic impression of the asset's security risks and assists in highlighting risks. The assessment of risk occurs after the identification of threats and vulnerabilities surrounding those assets. The authors highlight the problem of collusion in banking system transaction and classified the approach in two ways. The first scenario is where the collusion threats are not considered during threat identification. To complete a transaction each agent has physical or logical access to an asset. The access to critical asset is controlled by segregating a different limit of access for each of threat agent to accomplish a transaction. For each individual threat agent the risk of accessing the asset is low due to the segregation of duties for each level. The second scenario is where the risk is assessed after the consideration of colluding threat agents. By analysing the number of individuals having access to the asset, the number of collusion possible could be predicted. The higher the collusion possible number the severe risk could be expected. This approach can be adapted to banking system as the bank has a structured role-based access control system to determine the access rights that a user possesses within an application domain. In this system a role is defined by function and position, separation of duties within the organization from human resource database so that the access can be controlled internally. However cloud computing utilizes the virtual computing technology, data may be scattered in various virtual data centre rather than stay in the same physical location or even across the national borders. Therefore the approach is not adaptable in Cloud environment.

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 and 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

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

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

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I., (2009). "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," *Future Generation computer systems,* 25, 599-616.

Onwubiko, C., (2010). "Security issues to cloud computing," in *Cloud Computing*, N. Antonopoulos and L. Gillam, Eds., ed: Springer London, 271-288.

Kui, R., Cong, W., and Qian,W., (2012). "Security challenges for the public cloud," *Internet Computing, IEEE,* 16, 69-73.

Sundararajan, S., Narayanan, H., Pavithran, V., Vorungati, K., and Achuthan, K., (2011). "Preventing insider attacks in the cloud," in *Advances in Computing and Communications*. vol. 190, A. Abraham, J. Lloret Mauri, J. Buford, J. Suzuki, and S. Thampi, Eds., ed: Springer Berlin Heidelberg, 488-500.

Claycomb, W.R., and Nicoll, A., (2012). "Insider threats to cloud computing: directions for new research challenges," in *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual*, 387-394.

Bohli, J.M., Gruschka, N., Jensen, M., Iacono, L.L., and Marnau, N. (2012). "Security and privacy-enhancing multicloud architectures," *Dependable and Secure Computing, IEEE Transactions,* 10, 212-224.

Ning, Z., Ming, L, Wenjing, L., and Hou, Y.T. (2012). "mushi: toward multiple level security cloud with strong hardware level isolation," in *Military Communications Conference,* 1-6.

S. E. Institute. (2013). *The CERT insider threat center*. Available: http://www.cert.org/insider_threat/

Bishop, M., and Gates, C. (2008). "Defining the insider threat," 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.

Sibai, F.M., and Menasce, D., (2012). "Countering network-centric insider threats through self-protective autonomic rule generation," in *Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference,* 273-282.

Che Fauzi, A., Noraziah, A., Herawan, T., and Mohd. Zin, N., (2012). "On cloud computing security issues," in *Intelligent Information and Database Systems*. vol. 7197, J.-S. Pan, S.-M. Chen, and N. Nguyen, Eds., ed: Springer Berlin Heidelberg, 560-569.

Schneier, B. (1999). *Attack trees: modeling security threats*. Available: http://www.schneier.com/paper-attacktrees-ddj-ft.html

Chinchani, R., Iyer, A., Ngo, H.Q., and Upadhyaya, S., (2005). "A target-centric formal model for insider threat and more," in *International Conference on Dependable Systems and Networks*, 108-117.

Hui, W., Shufen, L., and Xinjia, Z., (2006). "A Prediction model of insider threat based on multi-agent," in *Pervasive Computing and Applications, 2006 1st International Symposium,* 273-278.

Yaseen, Q., and Panda, B., (2010). "Predicting and preventing insider threat in relational database systems," in *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*. vol. 6033, P. Samarati, M. Tunstall, J. Posegga, K. Markantonakis, and D. Sauveron, Eds., ed: Springer Berlin Heidelberg, 368-383.

Yaseen, Q., and Panda, B., (2011). "Enhanced insider threat detection model that increases data availability," in *Distributed Computing and Internet Technology*. vol. 6536, R. Natarajan and A. Ojo, Eds., ed: Springer Berlin Heidelberg, 267-277.

Chen, Q., Chen, Y.P., Zhang, S., and Zhang, C., (2006). "Detecting collusion attacks in security protocols," in *Frontiers of WWW Research and Development - APWeb*. 3841 in Zhou, X., Li, J., Shen, H., Kitsuregawa, M., and Zhang, Y., (2006). Eds., ed: Springer Berlin Heidelberg, 297-306.

Kohli, H, Lindskog, D., Zavarsky, P., and Ruhl, R., (2011). "An Enhanced threat identification approach for collusion threats," in *Security Measurements and Metrics (Metrisec), Third International Workshop.* 25-30.