International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

The Malicious Insiders Threat in the Cloud

Atulay Mahajan, Sangeeta Sharma

Lovely Professional University, atulaymahajan@gmail.com, 7837830737

Abstract — Cloud Computing, which once provided locally, has seen a technical and cultural shift of computing service provision to being provided remotely, and en masse, by third-party service providers. The data has now been placed under the protection of the service provider that was once placed under the security domain of the service user. Our data is no longer kept under our own watchful eyes as we have lost control over the protection of our own data at the hands of cloud service providers. While Cloud computing relieves various 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. Insider threat has become a serious security issue within the organizations. The problem of insider threats has been analyzed in this research paper and work has been done towards the detection and conception of strategies to solve these malicious insider threats.

Keywords — Cloud Computing, Cloud, Security, Insider, Malicious Insider, Insider Threat, Data Security, Iaas, Saas, Paas.

Introduction

→ Defining The Term Cloud Computing

Cloud computing is internet based where shared resources; software and information are provided to computers and other devices on-demand. Cloud computing is a new computing paradigm that attracted many users, businesses, and governments all over the world. Cloud computing, being the buzz word of the IT industry is the future of the computing. Cloud computing is the most demanded because of its performance, high availability and low cost.

According to the National Institute of Standards and Technology (NIST), Cloud computing has been defined as:
"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." [13]

The above definition clearly states that Cloud Computing helps in minimizing an organization's expenditure towards managing resources and also reduces the burden of maintaining software or hardware by its user. When burden of management, maintaining a software/hardware is reduced, the companies' expenditure and time spent towards infrastructure management is reduced and time saved can be utilized in doing some creative work. This is a huge advantage for users/organizations, which not only saves time but also boosts the performance of company by saving time spent on infrastructure.

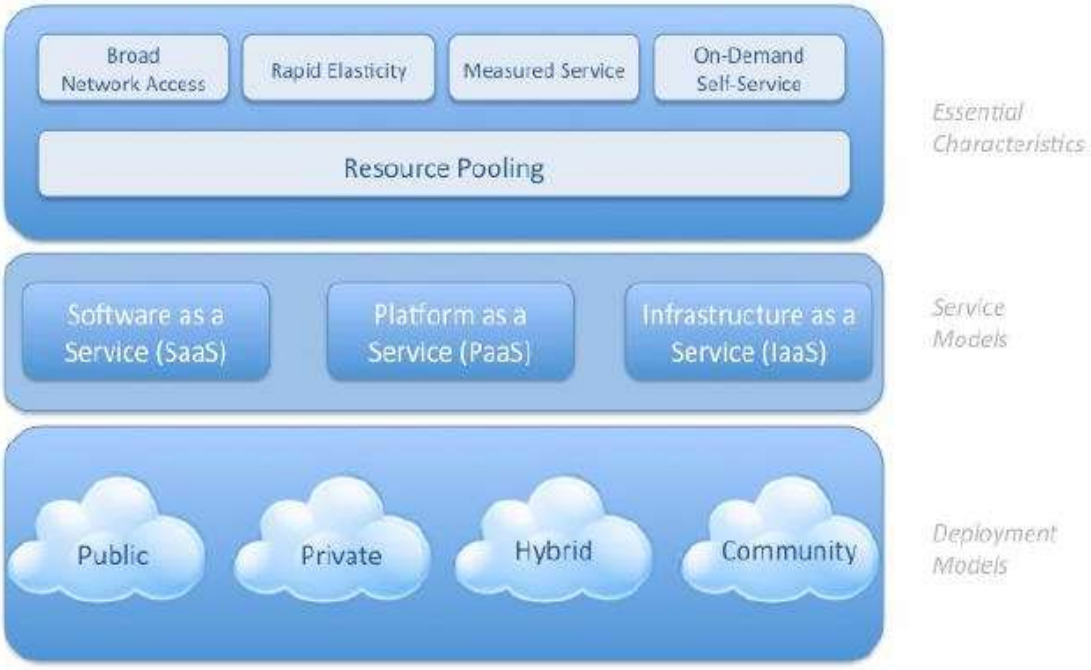

Figure 1 – "Visual Model of NIST Working Definition of Cloud Computing".

→ **Benefits of Cloud Computing**

Some common benefits of Cloud Computing are -

- Reduced Cost: Since cloud technology is implemented incrementally, it saves organizations total expenditure.
- Increased Storage: When compared to private computer systems, huge amounts of data can be stored than usual.
- Flexibility: Compared to traditional computing methods, cloud computing allows an entire organizational segment or portion of it to be outsourced.
- Greater mobility: Accessing information, whenever and wherever needed unlike traditional systems (storing data in personal computers and accessing only when near it).
- Shift of IT focus: Organizations can focus on innovation (i.e., implementing new products strategies in organization) rather than worrying about maintenance issues such as software updates or computing issues.

→ **Essential Characteristics**

A comprehensive list of the "essential characteristics" is given below –

1. On-demand self service
2. Broad network access
3. Rapid Elasticity
4. Pay-per-use
5. Connectivity
6. Resource pooling
7. Abstracted infrastructure
8. Little or no commitment

→ **Service Models**

- **Software as a Service (SaaS)**

A SaaS provider typically hosts and manages a given application in their own data centre and makes it available to multiple tenants and users over the Web. Some SaaS providers run on another cloud provider's PaaS or IaaS service offerings. Oracle CRM On Demand, Salesforce.com, and Netsuite are some of the well-known SaaS examples.

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. [11]

- **Platform as a Service (PaaS)**

Platform as a Service (PaaS) is an application development and deployment platform delivered as a service to developers over the Web. It facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet.

This platform consists of infrastructure software, and typically includes a database, middleware and development tools. A virtualized and clustered grid computing architecture is often the basis for this infrastructure software.

- **Infrastructure as a Service (IaaS)**

Infrastructure as a Service (IaaS) is the delivery of hardware (server, storage and network), and associated software (operating systems virtualization technology, file system), as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Unlike PaaS services, the IaaS provider does very little management other than keep the data centre operational and users must deploy and manage the software services themselves - just the way they would in their own data centre. Amazon Web Services Elastic Compute Cloud (EC2) and Secure Storage Service (S3) are examples of IaaS offerings.

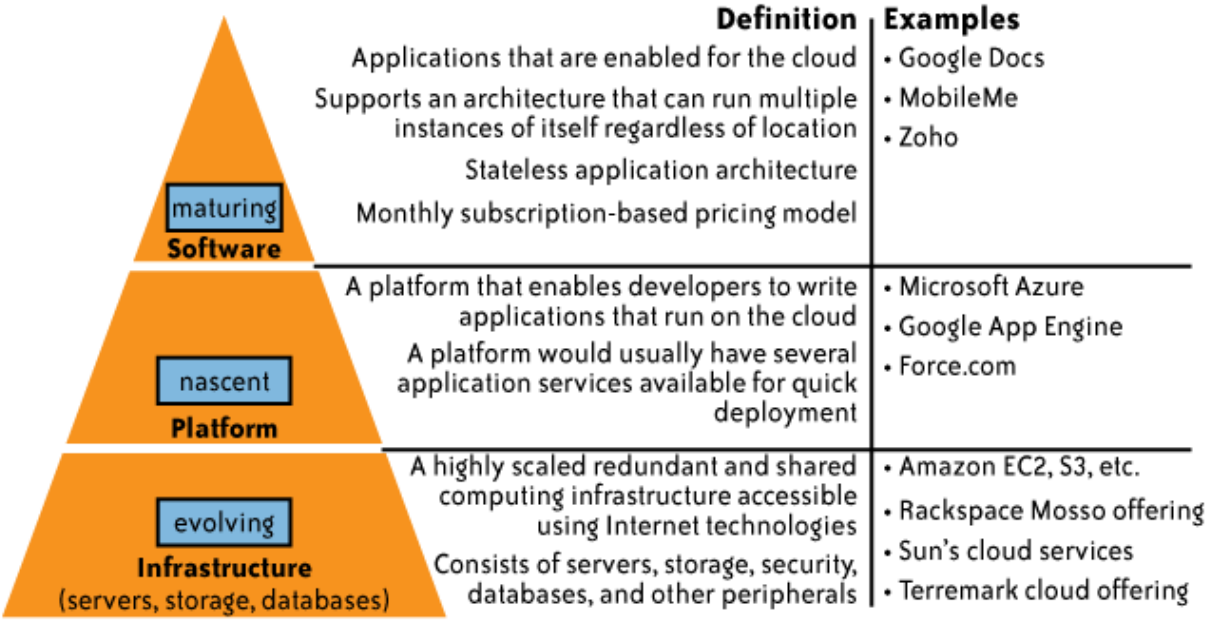

Figure 2 – Cloud Service Models

→ **Deployment Models**

Private cloud: In a private cloud, the infrastructure for implementing the cloud is controlled completely by a single organization (e.g., enterprise). Typically, private clouds are implemented in the enterprise's data centre and managed by internal resources. A private cloud maintains all corporate data in resources under the control of the legal and contractual umbrella of the organization.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: In a public cloud, external organizations provide the infrastructure and management required to implement the cloud. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Public clouds dramatically simplify implementation and are typically billed based on usage. This transfers the cost from a capital expenditure to an operational expense and can quickly be scaled to meet the organization's needs.

Hybrid cloud: The hybrid model may combine the best of the public and private cloud models that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

The Cloud Computing model offers the promise of massive cost savings combined with increased IT agility. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. Cloud computing is currently faced by barriers like security, interoperability, and portability which hamper its broader adoption [8].

→ **Importance of Security In Cloud Computing**

Security is one of the most important issues which hamper the growth of cloud. The idea of delivering important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment.

Regardless of the technical and operational countermeasures deployed in an infrastructure, defending against accidental or malicious human actions is difficult to do. The insider threat affects almost every infrastructure and remains an issue till date.

In the context of cloud computing, "a malicious insider with access to cloud resources can cause considerably more damage to the organization". Furthermore, as the attack can affect a large number of cloud users, the impact of such attack will be vital.

Malicious Insider Threat is #3 in the Cloud Security Alliance (CSA) top threats list. [14]

A malicious insider is an employee of the Cloud Service Provider who abuses his or her position for information gain or for other nefarious purposes e.g. a disgruntled employee. The threat of a malicious insider is well-known to most organizations.

This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. To complicate matters, there's usually very little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary - ranging from an amateur hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The extent of access granted could enable such an adversary to reap confidential data or gain complete control over the cloud services with little or no risk of detection. [15]

The impact that malicious insiders can have on an organization is substantial, given their level of access and ability to infiltrate organizations and assets. Brand damage, monetary impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that the consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat. [5]

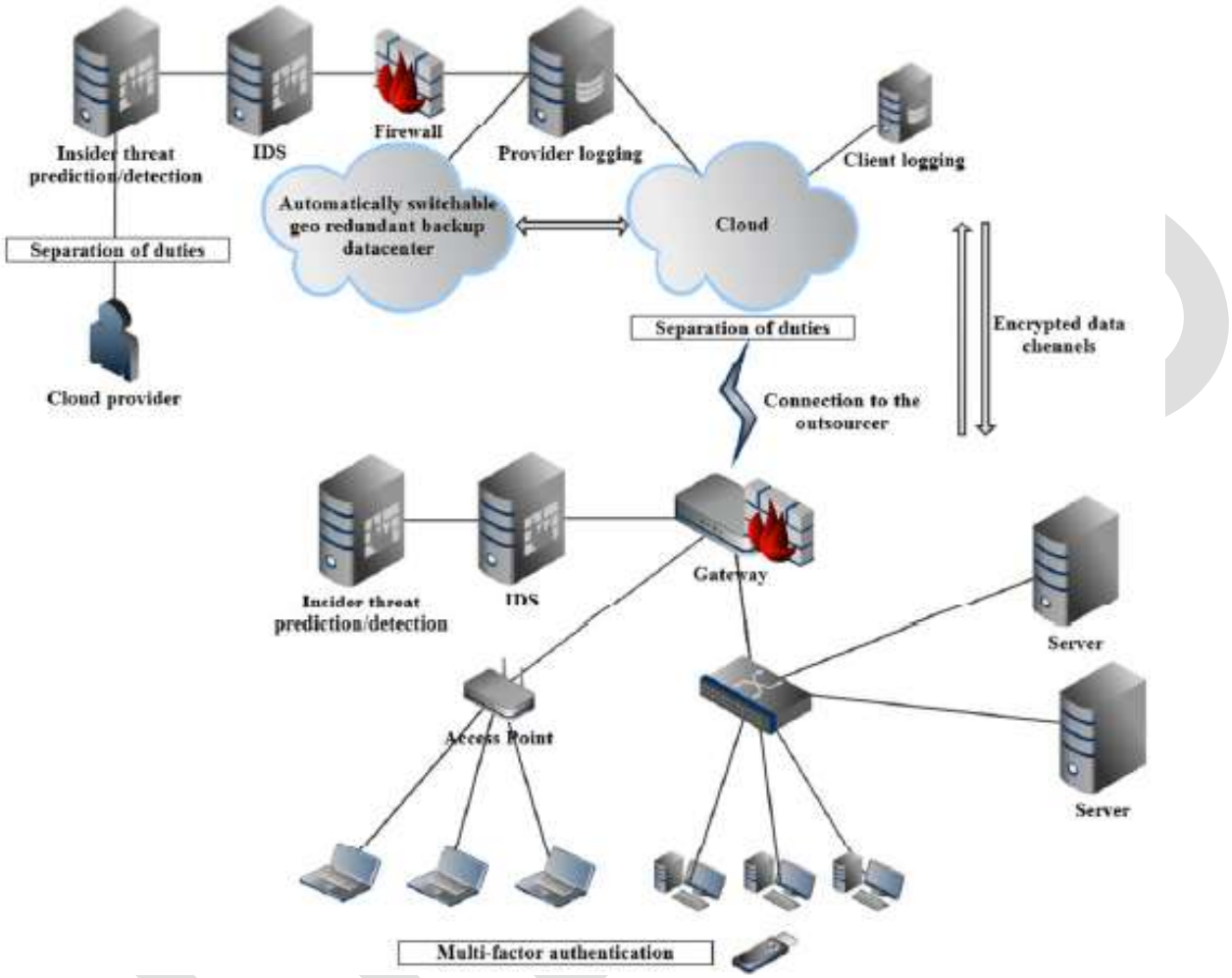

Figure 3 - Visualization of all security countermeasures versus insider threat.

→ **The Motives of A Malicious User**

In reality, there are many different types of attackers with different reasons to attack users. The following contains some examples.

- To steal valuable data - Hackers love to steal data as some data stored in the internet are valued millions of dollars. With access to valuable data, they can then generate revenue, for example, WikiLeaks.
- To cause controversy - Some attackers purely love the thrill and excitement of causing chaos and the internet, and similarly the Cloud, is one of the best mediums to target mainly because of the popularity of the internet as well as it being more likely to steal data over the internet in comparison to a personal computer system.
- To get revenge - Former workers who were recently stripped of their position at an organization may express their dissatisfaction by hacking the organization's network. When an organization makes use of the Cloud, this becomes all too easy for the former employee and there have been many cases of this happening in the real-world.

- To help - A hacker, in contrast, may also try to help an organization by identifying the security flaws in their system. A hacker may be confident enough to bypass the existing security protocol and implant his or her own mechanisms to expose the protocol.
- To prove intellect and gain prestige - Attackers may also want to show off their skills and gain prestige among their social skills if they were able to hack a large organization with solid security mechanisms. Some hackers make a career out of hacking organizations.
- Are just curious - Some hackers are curious to learn something about a company and/or organization. These kinds of hackers don't usually have malicious intent as they may not be aware of breaking security rules however it does not mean these hackers are less dangerous whatsoever.

Scope of The Research

This research paper focusses on the malicious 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]

A malicious insider could be, for example, an administrator of the cloud that goes rogue and as root access to the servers that compose the cloud. This type of attacker can violate data confidentiality without the need of high technical skills. A malicious insider can steal confidential data of the cloud user, so the user is mostly left with trusting the cloud provider. [9]

Malicious insider problem is through PaaS based services. If the service provider offers a platform that allows developers the ability to interact with user's data, i.e. Social Networking Applications, users may unknowingly allow access of all their data to these developers. [7]

The findings of this paper suggest that "all cloud types (IaaS, PaaS, SaaS) are equally affected by insider attacks as long as the insider has (or can gain) access to the datacenters or cloud management systems". Hence, it is worthwhile to formulate a security strategy which will enable the Cloud providers and customers alike to fight against this threat of malicious insider. [2]

Objectives of The Research

Since an insider attack in the cloud is easier to perform and has far greater impact than an attack in a traditional infrastructure, hence this paper aims to identify the various malicious insiders' threat faced during cloud computing and aims to find the solutions for the challenges that still do not have proper mitigation strategies identified through literature review.

So, basically I am performing the steps below-

1. Studying the malicious insider threat in the cloud,
2. Then detecting the malicious insiders present in a cloud, and hence,
3. Preventing those malicious insiders from doing any nefarious activity inside the cloud.

Research Methodology

Collecting Data From Literature

To identify which areas of cloud computing security need more research, initially CC challenges are found (this is done by searching the literature). Literature review is used to find all available data relevant to a particular research area, for collecting information to satisfy our questions. Based on the information gathered from literature review, an analysis was employed to develop general

explanations. This helped to identify the key concepts, terms and also resources used by other researchers. This data is used to develop alternative designs or find out need for further research.

Literature review using online databases involves a series of steps -

i. Identifying the keywords for the topic.
ii. Creating a list of possible search terms.
iii. Using search engines, electronic databases to find information.
iv. Modify the list of terms and repeat step iii.

Studying The Context of The Problem

In order to study the problem, it is suggested that it should be studied in two distinct contexts:

i. "Insider threat in the cloud provider": Where the insider is a malicious employee working for the cloud provider. He/she could cause great deal of damage to both the provider and its customers.
ii. "Insider threat in the cloud outsourcer": The insider is an employee of an organization which has outsourced part or whole of its infrastructure on the cloud.

Though responsibilities may be different, there are few elementary differences between a rogue administrator at the cloud provider and a rogue administrator within the customer organization; both insiders have root access to systems and data, and both may employ similar types of attacks to steal information. [4]

i. Insider Threat In The Cloud Provider

This is the worst-case scenario for both cloud providers and cloud clients, i.e. a malicious system administrator working for the cloud provider. Because of his/her business role in the cloud provider, the insider can use his/her authorized user rights to access sensitive data.

For example, an administrator responsible for performing regular backups of the systems where client resources are hosted (virtual machines, data stores), could exploit the fact that he/she has access to backups and thus, exfiltrate sensitive user data. Detecting such indirect access to data, can be a challenging task.

Depending on the insider's motives, the result of such an attack in a cloud infrastructure will vary from data leakage to severe corruption of the affected systems and data. Either way, the business impact for the provider will be significant.

Countermeasures

→ Client side
1. Confidentiality/Integrity
2. Availability

→ Provider Side
1. Separation of Duties
2. Logging
3. Legal Binding
4. Insider Detection Models

Table 1. Countermeasures

Countermeasures	Implemented by:
Cryptographic techniques	Client
Geo-redundant data centers	Client and Provider
Separation of duties	Provider
Logging and Auditing	Provider
Legal contracts	Provider
Insider detection models	Provider

Client: Client side countermeasures, Provider: Provider site countermeasures.

ii. Insider Threat In The Cloud Outsourcer

In this scenario, the insider is an employee of an organization, which has moved part (or the whole) IT infrastructure into the cloud.

Countermeasures

→ Provider Side

1. Anomaly detection
2. Separation of Duties
3. Multi-Factor Authentication

→ Client Side

1. Log Auditing
2. Host Based Intrusion Detection/ Prevention Systems (IDS/IPS)

Table 2. Countermeasures

Countermeasure	Implemented by:
Identity and Access management	Client and Provider
Multi factor authentication	Client and Provider
Log analysis and auditing	Client
IDS/IPS	Client
Insider prediction/detection models	Client

Client: Client side countermeasures, Provider: Provider site countermeasures.

We also have Socio-Technical Approaches and Predictive Models [10]. "A socio-technical approach to insider threats associated with cloud computing isn't directly applicable from the perspective of an organization concerned with the rogue administrator at the cloud provider, but it is helpful when looking for employees who exploit cloud weaknesses or use the cloud against the employer".

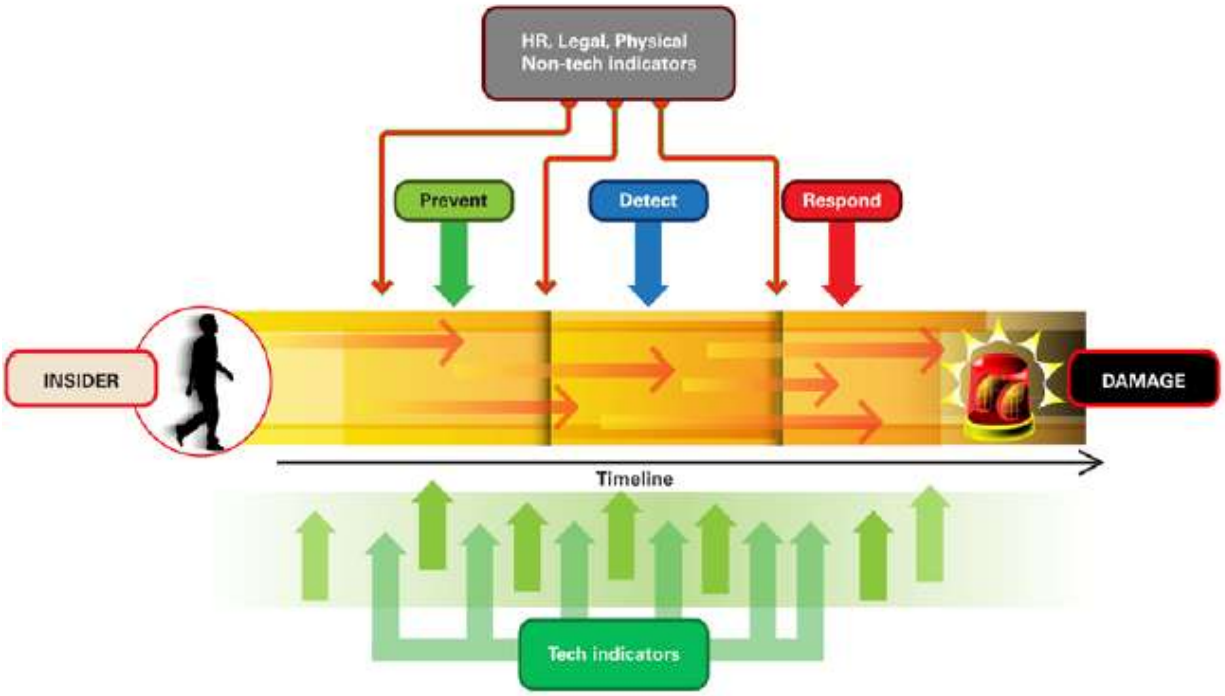

Figure 3 - Opportunities for prevention, detection, and response for an insider attack.

But we need a different kind of solution for solving the malicious insider threat. So, I have shown three different types of attacks and then provided their mitigation techniques too. The attacks are –

i. **Changing The Contents of Users' Files Without Their Knowledge,**

ii. **Obtaining The Private Keys of Users' Encrypted Files, and**

iii. **Web Template Poisoning.**

Detecting The Attacks

Starting with the **first attack technique**, I created a cloud environment in which the user can upload a file to his/her private cloud and since the administrator has access to all the users' files, he/she can become a malicious insider and make any type of change to the users' file(s) without their knowledge.

Proceeding towards the **second attack technique**, the users have the option of encrypting their files using AES algorithm which provides added security. The users can upload the file(s), either directly or by encrypting it with a private key. The key would also be stored on the cloud server itself, so any malicious insider who has root level access (administrator) can easily gain entry to the private key of users, decrypt the data and steal vital information or make any changes not intended by the owner of the files.

Finally, the **third attack technique** demonstrates the attack on public template. Employees who have access privilege to storage server or cloud management web interface (Web UI) can download the default public templates. Template poisoning attack assumes

the scenario when malicious insiders, who have enough privileges to access the storage server or Cloud management Web UI, download the template and deploy the downloaded template in his/her private storage with the attempt to poison the template. The poisoned template will be uploaded back into the Cloud. After the malicious insiders successfully uploaded the poisoned template, the users' data deployed from the poisoned template is vulnerable to the Malicious Insiders. [3]

The objective of this paper is to show that how a malicious insider can steal confidential data of the cloud user. A cloud environment has been developed in which the threat of Rogue Administrator has been detected by performing three attacks stated above and solutions have been provided below so as to prevent further stealing of the users' data. The attacks here show that a malicious insider can easily compromise passwords, files, and other confidential data. It is assumed that the attacks are performed by a malicious insider who has root access to the management of the servers that compose the cloud.

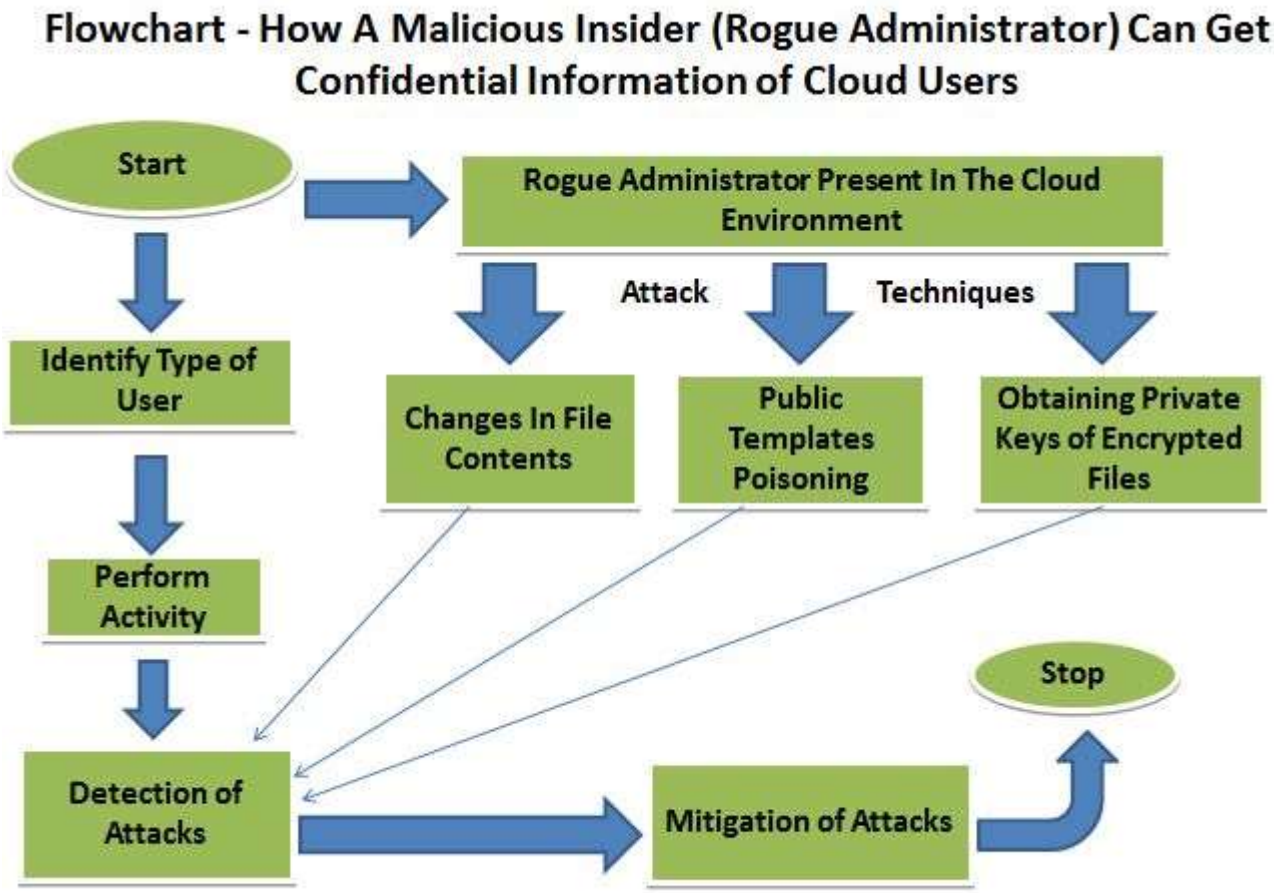

Figure 4 - Flowchart for solving the Malicious Insiders Threat.

No approach till now has offered a satisfactory path towards any solution for preventing or solving this type of threat. Therefore, in order to tackle the problem, I have created a virtual cloud environment in which the cloud is deployed locally in the system itself.

There are three types of attacks that a malicious insider can perform to access the user's data. The above stated attacks clearly demonstrate that it is currently possible to violate the confidentiality of the cloud user's data. The test environment was a single machine, with an Intel Core i7 Q740 Processor and 4 GB RAM. The machine had an emulated cloud infrastructure by using Cloud Sim v 3.0.3.There were 2 types of users of the system – administrator and users. The cloud server has a mode of encryption using AES

in which private key is used for authentication and establishing secure channels with the clients.

Mitigation Strategies & Results

For mitigating the **first type of attack**, the user will get a notification as a pop-up window that the file contents have been changed along with a pop-up showing the list of changes too. Hence, the attack can be easily detected by the cloud user and prevented further.

For the **second and third type of attack**, I have used the concept of OTP (One Time Password) to tackle the problem of Rogue Administrator as a malicious insider. As soon as the malicious insider tries to access some other users' data, the respective user will get a One-Time-Password (OTP) on their registered e-mail address which would prevent the malicious insider from accessing users' data. Also, a cloud-based rogue administrator would have access to the encrypted data, but not the associated private keys, and a local rogue administrator would have access to the locally-stored keys, but not the encrypted data.

Hence, after applying the above solutions, I aim to develop a way to prevent the malicious insider threat in the cloud.

Acknowledgment

A research is a combination of views and ideas, suggestions and contributions of many people. I take this opportunity to present my vote of thanks to all those who really acted as lightening pillars to enlighten my way to successful and satisfactory completion of this report. I am highly thankful to my mentor and co-author of this paper, **Ms. Sangeeta Sharma** for her active support, valuable time and advice, whole-hearted guidance, sincere cooperation and involvement during the whole process.
And last but not the least, I find no words to acknowledge the financial assistance & moral support rendered by my parents in making my efforts, a success. All this has become reality because of their blessings and above all, by the grace of Almighty God.

Conclusion

The cloud computing with such great offering such as storage, infrastructure and application designing capabilities on the go to the IT industry still fail to have proper standards for interoperability with other cloud service providers. This failure to provide concrete security standards, common underlying framework for data migration and global standards for cloud interoperability, make the leading technology "the cloud computing" still a vulnerable option for aspiring users. Malicious activity from within the Cloud provider system is tough to observe when there are collusion and collaboration between multiple insiders, insiders and outsiders within the Cloud environment.
Insider threats are a persistent and increasing problem. Insiders steadily continue to abuse organizational trust in other ways, such as using cloud services to carry out attacks. Organizations should know about vulnerabilities exposed by the utilization of cloud services and mindful of the availability of cloud services to employees within the organization.

Malicious insiders' attacks that exist in the Cloud system pose a critical threat to the organizations. With the flexibility of Cloud system, the malicious insiders can manipulate the privileges access the sensitive information remotely. [6]

In my opinion, if one is considering using the cloud, he/she should be certain to identify what information would be put out in the cloud and what one needs to make sure it is protected. Additionally, one should know the options in terms of what type of cloud would be best for one's needs, what type of provider would be most useful, and what are the reputation and responsibilities of the providers that one is considering before signing up. [12]

Therefore, by this paper, the suitable solutions to overcome this threat of malicious insider are briefly presented.

REFERENCES:

[1] Ilgun, Koral, Richard A. Kemmerer, and Phillip A. Porras. "State transition analysis: A rule-based intrusion detection approach." Software Engineering, IEEE Transactions on 21, no. 3 (1995): 181-199.

[2] Magklaras, G. B., S. M. Furnell, and Phillip J. Brooke. "Towards an insider threat prediction specification language." Information management & computer security 14, no. 4 (2006): 361-381.

[3] Rocha, Francisco, and Miguel Correia. "Lucy in the sky without diamonds: Stealing confidential data in the cloud." In Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on, pp. 129-134. IEEE, 2011.

[4] Claycomb, William R., and Alex Nicoll. "Insider threats to cloud computing: Directions for new research challenges." In Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual, pp. 387-394. IEEE, 2012.

[5] F. Greitzer, L. Kangas, C. Noonan, A. Dalton, and R. Hohimer,"Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats," in 45th Hawaii International Conference on System Science (HICSS), January 2012.

[6] Kandias, Miltiadis, Nikos Virvilis, and Dimitris Gritzalis. "The insider threat in Cloud computing." In Critical Information Infrastructure Security, pp. 93-103. Springer Berlin Heidelberg, 2013.

[7] Sundararajan, Sudharsan, Hari Narayanan, Vipin Pavithran, Kaladhar Vorungati, and Krishnashree Achuthan. "Preventing Insider attacks in the Cloud." InAdvances in Computing and Communications, pp. 488-500. Springer Berlin Heidelberg, 2011.

[8] Bamiah, Mervat Adib, and Sarfraz Nawaz Brohi. "Seven deadly threats and vulnerabilities in cloud computing." International Journal of Advanced Engineering Sciences and Technologies (IJAEST) 9, no. 1 (2011): 87-90.

[9] Ho, S. Mary, and Hwajung Lee. "A thief among us: the use of finite-state machines to dissect insider threat in cloud communications." Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, JoWUA 3, no. 1/2 (2012).

[10] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloud computing." In System Sciences (HICSS), 2011 44th Hawaii International Conference on, pp. 1-10. IEEE, 2011.

[11] Chou, Te-Shun. "Security threats on Cloud Computing vulnerabilities."International Journal of Computer Science & Information Technology 5, no. 3 (2013): 79-88.

[12] Mahajan, Harshal, and Nupur Giri. "Threats to Cloud Computing Security." InVESIT, International Technological Conference-2014 (I-TechCON). 2014.

[13] NIST Definition of Cloud Computing. http://www.nist.gov/itl/cloud

[14] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[15] http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=105