LOVELY PROFESSIONAL UNIVERSITY

The Malicious Insiders Threat In The Cloud

A Dissertation Submitted

By

Atulay Mahajan

11007099

To

Department of CSE/IT

In partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology In

Software Engineering

Under the guidance of

Ms. Sangeeta Sharma

Asst. Professor, LPU

(May 2015)

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 dissertation and work has been done towards the detection and conception of strategies to solve these malicious insider threats.

Keywords: Cloud, Cloud Computing, Security, Malicious Insider, Insider Threat.

CERTIFICATE

This is to certify that **Atulay Mahajan** has completed M. Tech dissertation titled **“The Malicious Insiders Threat in the Cloud”** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M. Tech, Computer Science and Engineering.

Date: 5th May, 2015

Signature of Advisor

Sangeeta Sharma

UID - 15681

ACKNOWLEDGEMENT

A project cannot be said to be the work of an individual. Hence, 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 dissertation.

I am highly thankful to my mentor, **Ms. Sangeeta Sharma** for her active support, valuable time and advice, whole-hearted guidance, sincere cooperation and involvement during the whole process and in completion of this dissertation within the stipulated time.

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.

Atulay Mahajan

DECLARATION

I, Atulay Mahajan hereby declare that the dissertation proposal entitled, **“The Malicious Insiders Threat In The Cloud”** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: 5th May, 2015

Atulay Mahajan
Reg. No. 11007099

STRUCTURE OF REPORT

Chapter 1 - Introduction gives a brief history of cloud computing, its benefits, essential characteristics, models and introduction to the security paradigm to understand the problem definition.

Chapter 2 - Review of Literature gives a brief summary of the processes being followed by various authors in selecting, sorting and describing extracted information.

Chapter 3 - Present Work contains Objectives that tell what has been intended to solve in this dissertation. Research Methodology explains what methods are used and further provides the subject matter and the topics which have been studied and discussed, parameters for what will be talked about and what the dissertation covers.

Chapter 4 - Results & Discussions show and explain the end results of successful implementation.

TABLE OF CONTENTS

Content **Page No.**

LIST OF FIGURES

Content **Page No.**

Chapter 1
INTRODUCTION

1.1 History of Cloud Computing

Cloud Computing (CC) is a new term given to a technological evolution of distributed computing and grid computing. CC has been evolving over a period of time and many companies are finding it interesting to use. Without the development of ARPANET (Advance Research Projects Agency Network) by J.C.R.Licklider in 1960's and many other researchers who dreamt of improving the interconnection of systems, CC would never have come into existence. The advent of ARPANET, which helped to connect (for sharing, transferring, etc.) a group of computers [1], lead to the invention of Internet (where bridging the gap between systems became easy). This Internet helped to accelerate multifarious activities such as human interaction (social media, instant messaging, etc.), business needs of an organization (online shopping, financial services, etc.).

Further advancement in this area of Internet resulted in development of Applications Service Provision (ASP), grid and utility computing and cloud computing [1]. CC introduced a new paradigm which changed the traditional interconnection of systems to a pool of shared resources that can be accessed through internet.

1.2 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.” [15]

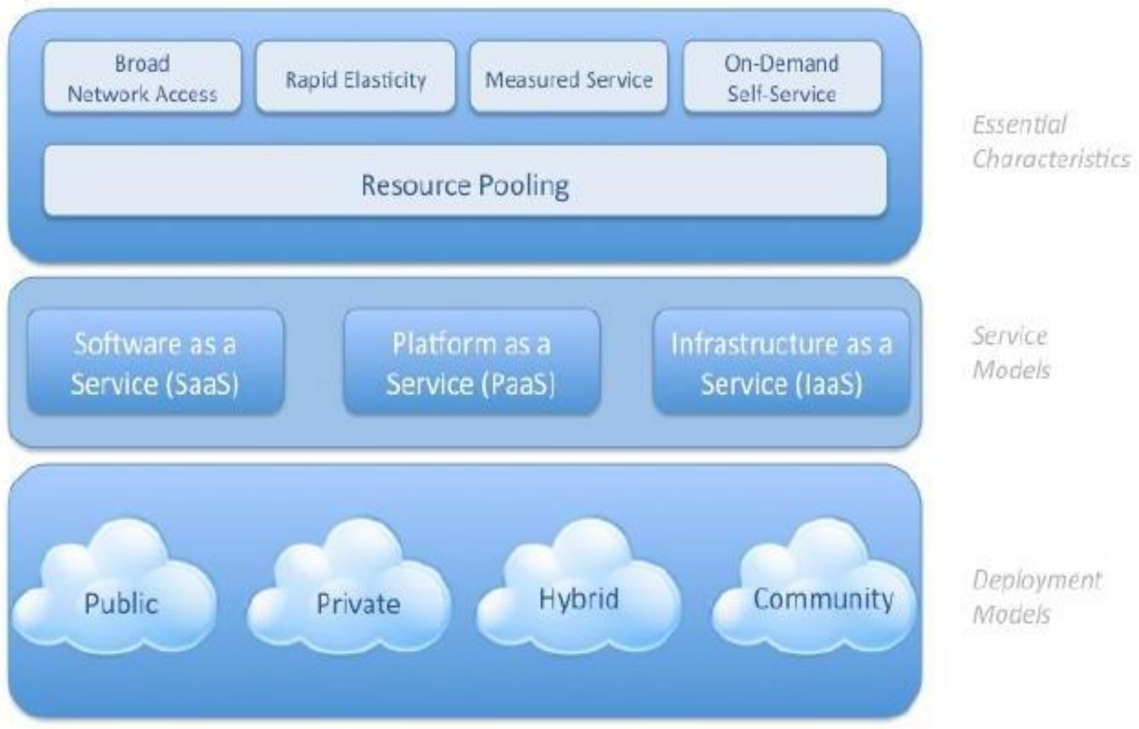


Figure 1 – “Visual Model of NIST Working Definition of Cloud Computing”.

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.

1.3 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.

1.4 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

1.5 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.

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.

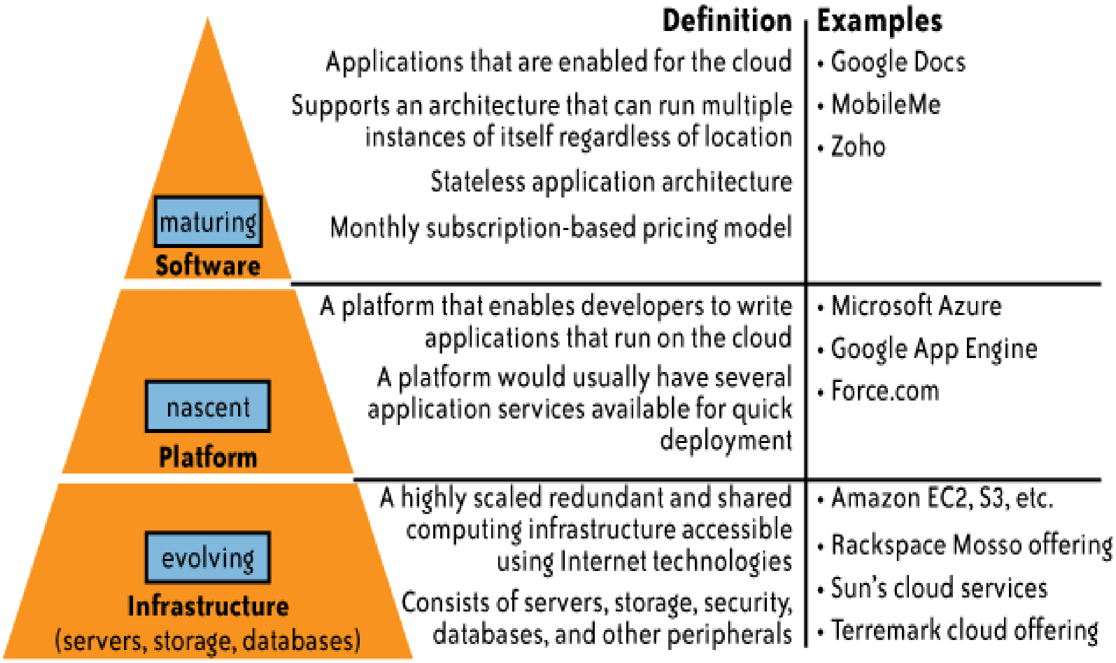
This platform consists of infrastructure software, and typically includes a database, middleware and development tools. A virtualized and clustered grid computing architecture is often the basis for this infrastructure software.

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.

.



	Definition	Examples
maturing Software	Applications that are enabled for the cloud Supports an architecture that can run multiple instances of itself regardless of location Stateless application architecture Monthly subscription-based pricing model	• Google Docs • MobileMe • Zoho
nascent Platform	A platform that enables developers to write applications that run on the cloud A platform would usually have several application services available for quick deployment	• Microsoft Azure • Google App Engine • Force.com
evolving Infrastructure (servers, storage, databases)	A highly scaled redundant and shared computing infrastructure accessible using Internet technologies Consists of servers, storage, security, databases, and other peripherals	• Amazon EC2, S3, etc. • Rackspace Mosso offering • Sun's cloud services • Terremark cloud offering

Figure 2 – Cloud Service Models

1.6 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 [15].

1.7 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. [19]

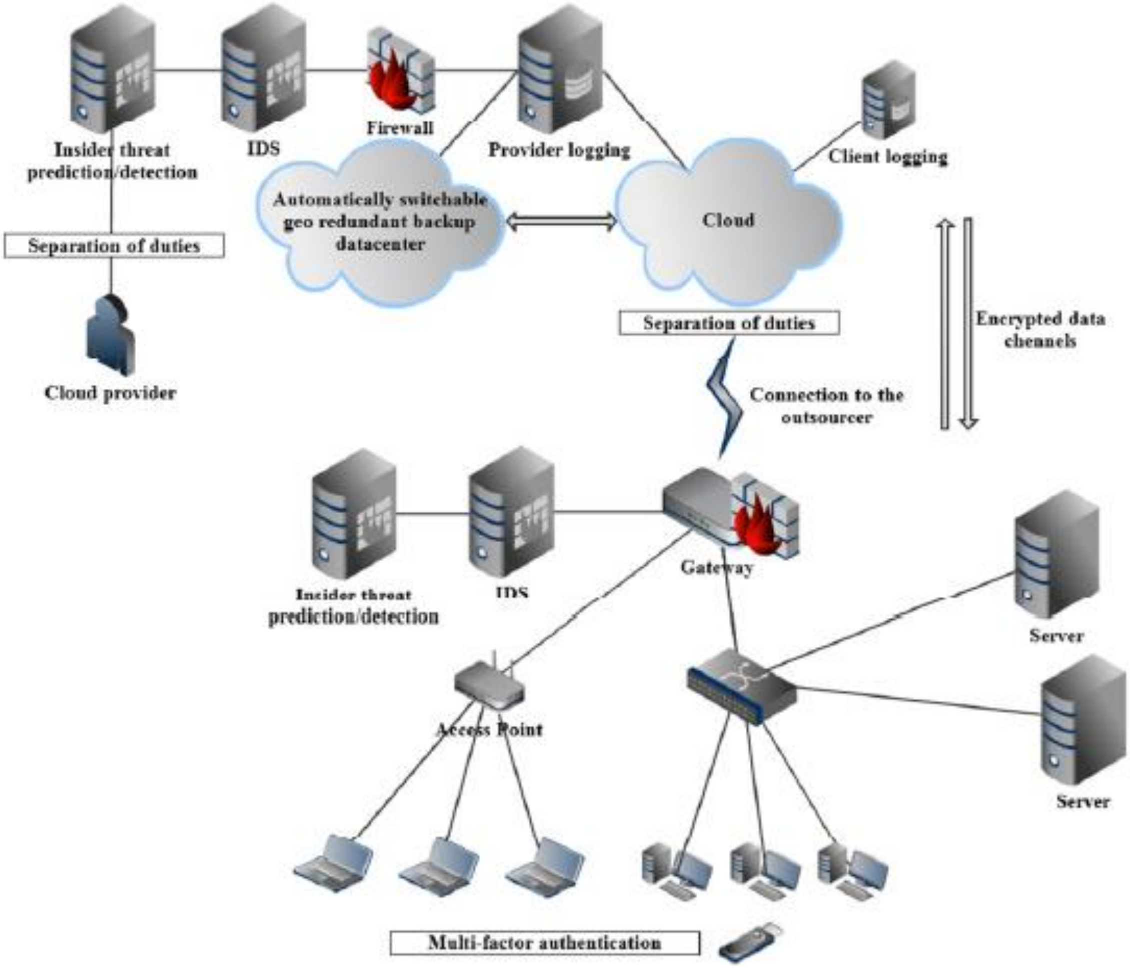

Insider threat prediction/detection
IDS
Firewall
Provider logging
Client logging
Automatically switchable geo redundant backup datacenter
Cloud
Separation of duties
Cloud provider
Separation of duties
Encrypted data chennels
Connection to the outsourcer
Insider threat prediction/detection
IDS
Gateway
Server
Access Point
Server
Multi-factor authentication

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

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.

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.

1.8 The Motives of A Malicious Insider

In reality, there are many different types of attackers with different reasons to attack users. Some examples are -

- 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.

Chapter 2

REVIEW OF LITERATURE

Collecting Data From Literature

To identify which areas of cloud computing security need more research, initially CC challenges are found 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 so as to develop appropriate mitigation strategies for the problem.

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.

Magklaras et al. [13] have presented the concept of an “insider threat specification language” that enables analytical description of the actions of a malevolent insider, so as to detect such actions and tie them to suspicious insiders.

Francisco Rocha [16] from School of Computing Science, Newcastle University used the technique of deploying integrity-protected virtual machine monitors (VMMs), a.k.a., hypervisors.

- Respect security design requirements.
- For the malicious insider threat ensure that the principle of least privilege is respected in the memory access model used for the management VM.

Also, he used trustworthy computing to provide integrity measurements of hypervisors to remote clients.

- Integrity measurement, cryptographic hash of software/binary code.
- Remote attestation enables a verifier to establish trust in an initially untrusted platform.

The shortcoming is that it only protects inter-vm communication; hence the rest of a virtual machine's memory is still vulnerable to attack.

Greitzer et al. [6] advocate a predictive model that identifies several weighted indicators of insider risk. They discuss development of a reasoning system to integrate multiple data sources and help analysts identify high-risk events.

William R Claycomb et al. [3] have discussed the common notion of a cloud insider as a rogue administrator of a service provider. They have presented two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer’s local resources. They also characterize a hierarchy of administrators within cloud service providers, give examples of attacks from real insider threat cases, and show how the nature of cloud systems architectures enables attacks to succeed.

Md. Tanzim Khorshed et al. [14] boast that cloud computing helps reduces cost of services and improves business outcomes. But to market this and popularize its use by IT user community, there are many security risks to be solved. They also mentioned that the cloud services pose an attractive target to cyber-attacks and criminal activities as these services have information from many organizations and individuals stored in their repositories.

The authors perform a survey in cloud computing to find out gaps and security concerns and mentions five common types of attacks:

i. Denial of service: In this type of attack the attacker prevents the legitimate user from accessing his resources,

ii. Malicious insider attacks: This type of attack the attacker is an insider. This person can easily gain access to sensitive user information namely: passwords, cryptographic keys, etc.

iii. Cross virtual machine side channel attacks: Is the type of attack in which attacker resides in the same physical hardware as that of the target virtual machine and gains access to his sensitive information,

iv. Phishing attacks: In this type of attacks the attacker sends links to the target user through email or instant messages. These links look as if they were sent by a trusted party but through this links the attacker can gain access to user sensitive information,

v. Attacks targeting shared memory: The shared memory between the user and the attacker is used to perform unwanted, unauthorized actions.

They proposed a method for automatic identification of these attacks, tested its effectiveness by simulating attacks in a real, actual cloud setup. The design of this model, they say, is based on machine learning models. Various models are considered and a support vector machine (SVM) is able to detect maximum attacks.

In the end, the authors conclude that their results are outcomes of simulation and express that there can be difference in depth, volume and intensity of attacks in simulation as compared to an actual environment. This leaves us an impression that the method proposed still needs real world experimentation and hence, the attacks mentioned in this paper are still a threat in CC environment.

Miltiadis Kandias et al. [11] deal with the insider threat in the cloud environment. An insider attack in the cloud is easier to perform and has far greater impact than an attack in a traditional infrastructure. At the same time, detection and identification of the physical entity that performed the attack remains challenging. They address the problem in a holistic way by differentiating between the two possible scenarios –

i. "Defending against a malicious insider working for the cloud provider", and
ii. "Defending against an insider working for an organization which chooses to outsource parts or the whole IT infrastructure into the cloud."

They identify the potential problems for each scenario and propose the appropriate countermeasures, for both the cloud clients and providers, for each insider scenario in an effort to mitigate the problem. Solving the insider threat requires a large number of countermeasures, to be implemented by both cloud providers and clients.

Popovi and Hocenski [12] discussed security issues, requirements and challenges that cloud service providers (CSP) need to address in cloud engineering:

i. Security issues describe the problems encountered during implementation of cloud computing (CC).
ii. Security standards provide some security templates, which are mandatory for cloud service providers. The Open Visualization Format (OVF) is a standard for creating new business models that help the company to sell a product on premises, on demand, or in a hybrid deployment model.
iii. Security management models are designed based on the security standards and best practices.

Maggi and Zanero [7] addressed countermeasures (anti-viruses, intrusion detection systems) developed to mitigate well-known security threats. The focus is mainly on anomaly-based approaches which are mostly suited for modern protection tools and not for intrusion detectors. The pattern-based changes (example: from thin client connected to the main frame or powerful workstations connecting to thin clients) are observed, which cause some simultaneous changes in work environment and new problems to security of CC.

Subashini and Kavitha [17] dealt with the security risks faced in the CC. They provided empirical evidence on security risks and issues encountered during deployment of service delivery models in an organization. The service models are placed in cloud and the empirical validation was made in order to justify the safety of the environment. Security was the main issue while there were also complications with data protection and data privacy in a continuous manner that affected the market.

Eystein Mathisen [5] discusses some key security issues of cloud computing (policy, software and hardware security) and techniques implemented to reduce the risk. The author expresses that usage of CC will increase in near future and more companies will share their information to cloud servers, which could attract large groups of hackers. He also says that in future there are possibilities for interoperability and data lock-in issues, which can be reduced by using open standards from the time of CC adoption. The author concluded by saying that security is always addressed late while adopting CC and also mentioned that security standards are still missing for CC. If an organization wishes to shift to CC but is reluctant due to lack of proper measures or standards, it can refer to Open Cloud Manifesto which is the largest initiative surrounding open standards. These standards are restrictive and so most companies do not wish to follow the Open Cloud Manifesto standards.

Iliana Iankoulova et al. [9] have performed a systematic review to identify which security requirements need to be further researched. To find that, the authors used an existing model with 9 sub-factors namely: access control, attack/harm detection, non-repudiation, integrity, security auditing, physical protection, privacy and confidentiality, recovery and prosecution to categorize their findings. From this review, they found that nonrepudiation, physical protection, recovery and prosecution are the least researched in security areas. Integrity, access control and security auditing are the most popular areas. A surprising finding in their review is that privacy and confidentiality had been observed only in 7% publications. In addition to security requirements, solutions to these identified challenges were also mentioned.

Bishop and Gates [2] 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 [18].

Ertaul et al. [4] mentioned CC's features like reduced total cost of ownership, scalability and competitive differentiation. They claim CC also minimizes complexity and provides faster and easier acquisition of services to customers. Virtualization is the technique used to deal with quality of service (QOS). Usage of CC is considered to be unsafe in an organization. For dealing with this type of situation, they investigated a few major security issues with CC and also existing countermeasures to those security challenges. Advantages for implementing CC from a different point of view are also discussed. They also stated that some standards are required in CC for security.

Farhan Bashir Shaikh et al. [8] include information regarding vulnerable security threats from 11 articles. The authors tabulated their findings i.e., problem discussed and technique used to solve the problem in their paper. But in the end, they conclude expressing that cloud computing from user perspective is suffering from numerous security threats. This, they say, is the only worth mentioning disadvantage in CC.

They also list out the following as key concerns in their point of view:

i. Users' authentication: User authentication process must be improvised to ensure that malicious users do not get access to powerful computing systems in CC.

ii. Leakage of data or Data loss: Data can be at risk if an unauthorized person gains access to shared pool of resources and deletes or modifies data. This risk can increase further if there exists no backup for that data.

iii. Clients' trust: There must be strong authentication practices implemented to ensure that the clients' data is being protected from unauthorized access.

iv. Malicious users handling: Malicious users can be attackers using cloud services with a malicious intent or an insider who has gained the trust of company but works to gain access to sensitive information stored in cloud.

v. Hijacking of sessions: These kinds of attacks happen when a legitimate user is prone to phishing or insecure application interfaces that can be exploited by attackers. Through this kind of attacks, attackers gain user credentials and hijack legitimate users sessions.

vi. Wrong usage of CC and its services: Cloud computing service providers give access to try their cloud services for a limited period of time for free. Some users utilize this trial period to misuse the resources obtained through CC service provider.

Chapter 3
PRESENT WORK

3.1 Problem Formulation

This dissertation 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.

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. Hence, it is worthwhile to formulate a security strategy which will enable the Cloud providers and customers alike to fight against the threat of malicious insider.

3.2 Objectives of Dissertation

Since an insider attack in the cloud is easier to perform and has far greater impact than an attack in any traditional infrastructure, hence this dissertation aims to identify the various malicious insider threats faced during cloud computing, focusing specifically on the Rogue Administrator Threat and thus, aims to find the solutions for the challenges that still do not have proper mitigation strategies identified through the literature review.

The steps being done are mentioned below-

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

3.3 Research Methodology

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. 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.

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

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.

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".

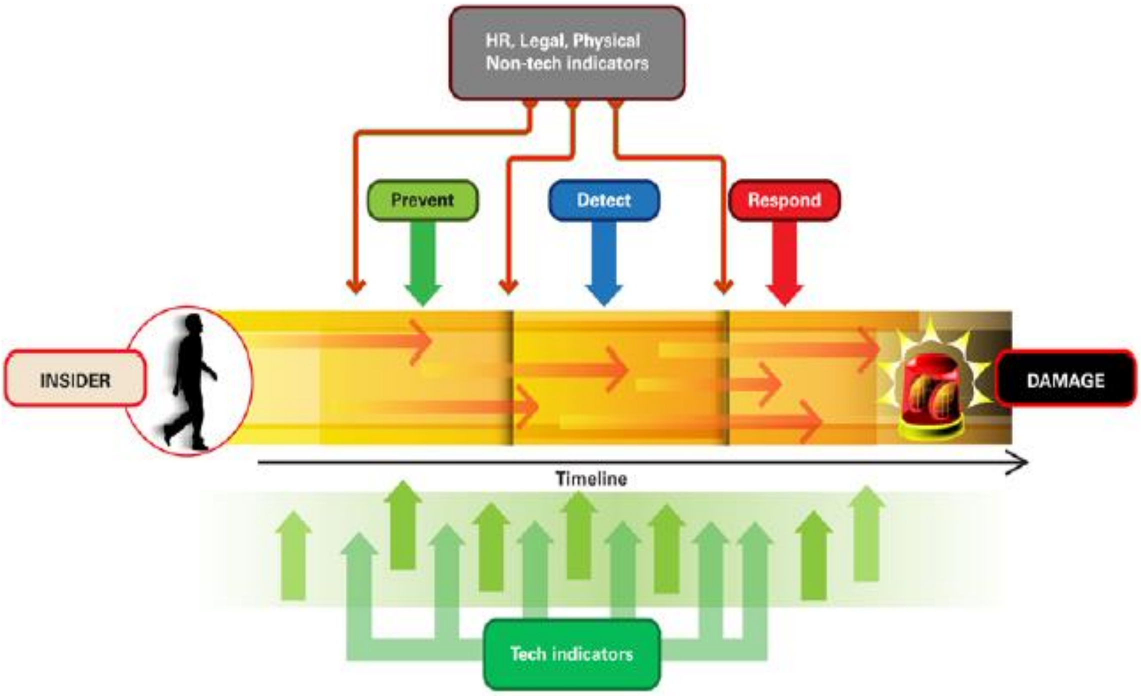


Figure 4 - Opportunities for prevention, detection, and response for an insider attack.

Problem To Be Solved

In the existing works, the Malicious Insider (MI) attack techniques are only basically and abstractly described. Without the proof of concept, the MI attacks are just theoretical threats. Therefore, we need a different kind of solution for solving the malicious insider threats.

Hence, the objective of this dissertation is to show that how we can stop any malicious insider from stealing confidential data of the cloud user.

For understanding my proposed solution, we first need to understand the term "**Rogue Administrator**". The rogue administrator employed by a cloud provider is a cloud-related insider. 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 to consider is IT sabotage, where an employee seeks 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.

Here, a cloud environment has been deployed in which the threat of Rogue Administrator would be detected by performing the attacks stated below and solutions have been provided so as to prevent further stealing of the users' data. The attacks here show that how 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.

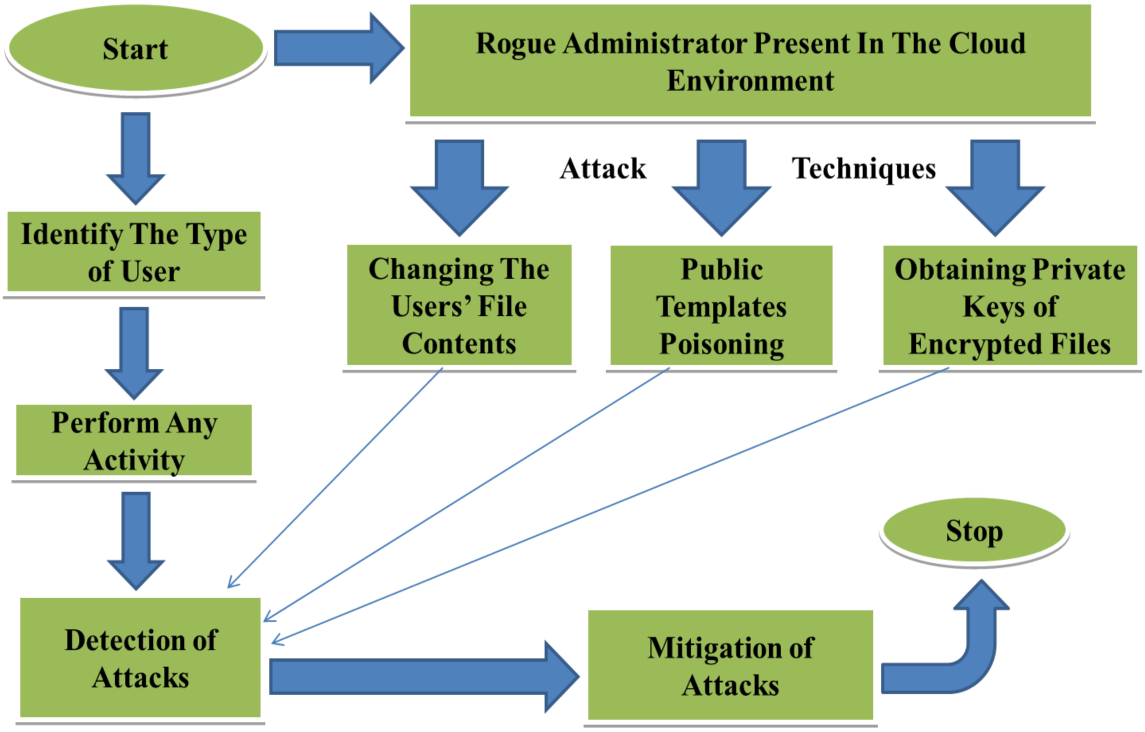

Start
Rogue Administrator Present In The Cloud Environment
Attack
Techniques
Identify The Type of User
Changing The Users' File Contents
Public Templates Poisoning
Obtaining Private Keys of Encrypted Files
Perform Any Activity
Stop
Detection of Attacks
Mitigation of Attacks

Figure 5 - Flowchart Showing How A Malicious Insider (Rogue Administrator) Can Get Confidential Information of Cloud Users.

Performed Attacks

So, in this dissertation, I have provided the proof of concepts, showing three different types of attacks and then providing their mitigation techniques too. The attacks are –

i. **Changing The Contents of Users' Files,**

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

iii. **Public Templates Poisoning.**

Now, starting with the **first attack technique**, I have deployed a virtual cloud environment in which the user can upload a file to his/her private cloud and if any malicious insider, in our case, the rogue administrator makes any changes to the file, 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.

Proceeding towards the **second attack technique**, the user also has the option of encrypting his/her files using AES algorithm which provides added security. The user can upload the file, 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.

<u>Proposed Solution</u>

I have created a virtual cloud environment in which the cloud is deployed locally in the system itself. The three types of attacks shown above can be used by any malicious insider to gain access to the users' data. These 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 using Cloud Sim v 3.0.3.

There are 2 types of users of the system – administrator and users. The cloud server has a mode of encryption using **AES (Advanced Encryption Standard)** in which a private key is used for authentication and establishing secure channels with the clients.

I have used the concept of **OTP (One Time Password)** to tackle the problem of Rogue Administrator as a malicious insider. Also, the malicious insider would not be able to access the users' data as a cloud-based rogue administrator would have access to the encrypted data, but not the associated keys, and a local rogue administrator would have access to the locally-stored keys, but not the encrypted data.

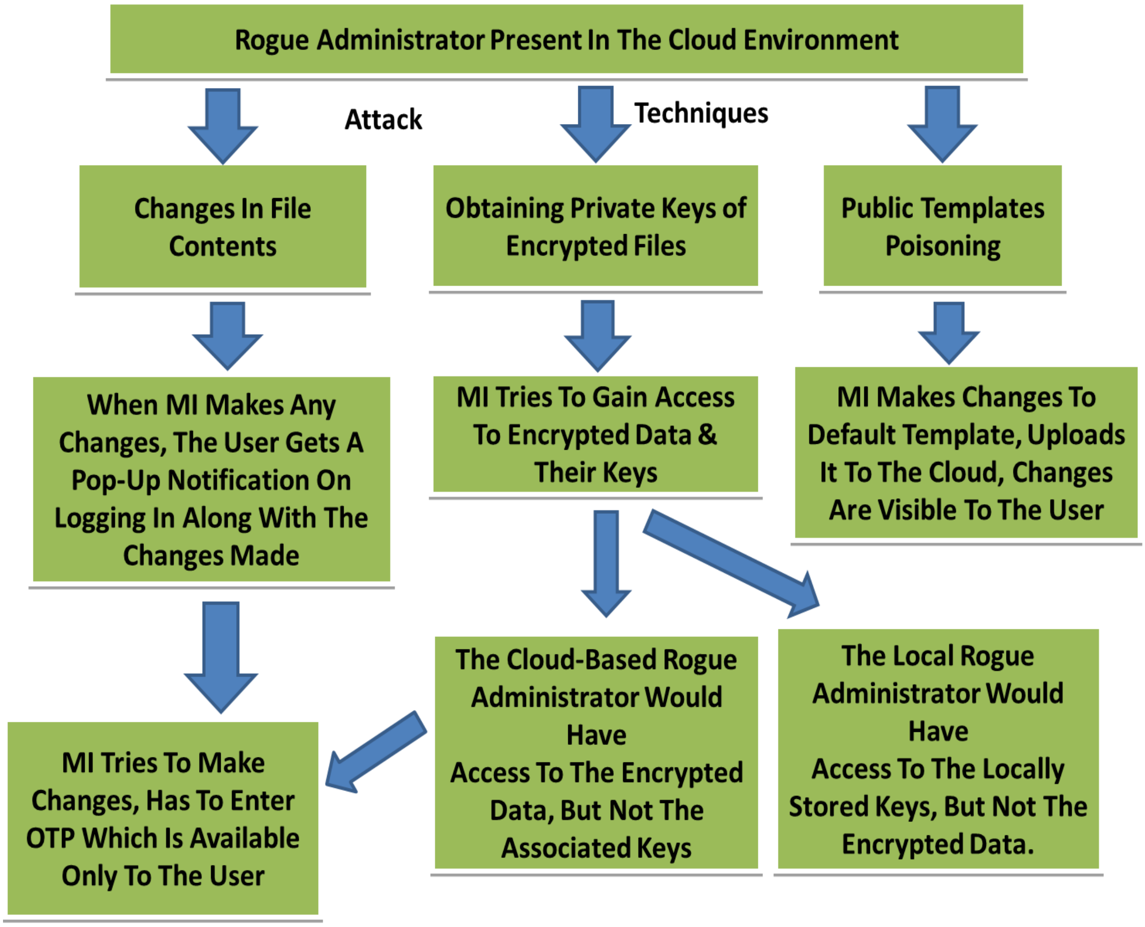

Rogue Administrator Present In The Cloud Environment
Attack
Techniques
Changes In File Contents
Obtaining Private Keys of Encrypted Files
Public Templates Poisoning
When MI Makes Any Changes, The User Gets A Pop-Up Notification On Logging In Along With The Changes Made
MI Tries To Gain Access To Encrypted Data & Their Keys
MI Makes Changes To Default Template, Uploads It To The Cloud, Changes Are Visible To The User
MI Tries To Make Changes, Has To Enter OTP Which Is Available Only To The User
The Cloud-Based Rogue Administrator Would Have Access To The Encrypted Data, But Not The Associated Keys
The Local Rogue Administrator Would Have Access To The Locally Stored Keys, But Not The Encrypted Data.

Figure 6 - Flowchart Showing How The Malicious Insider (Rogue Administrator) Threat Can Be Mitigated Using My Proposed Solution.

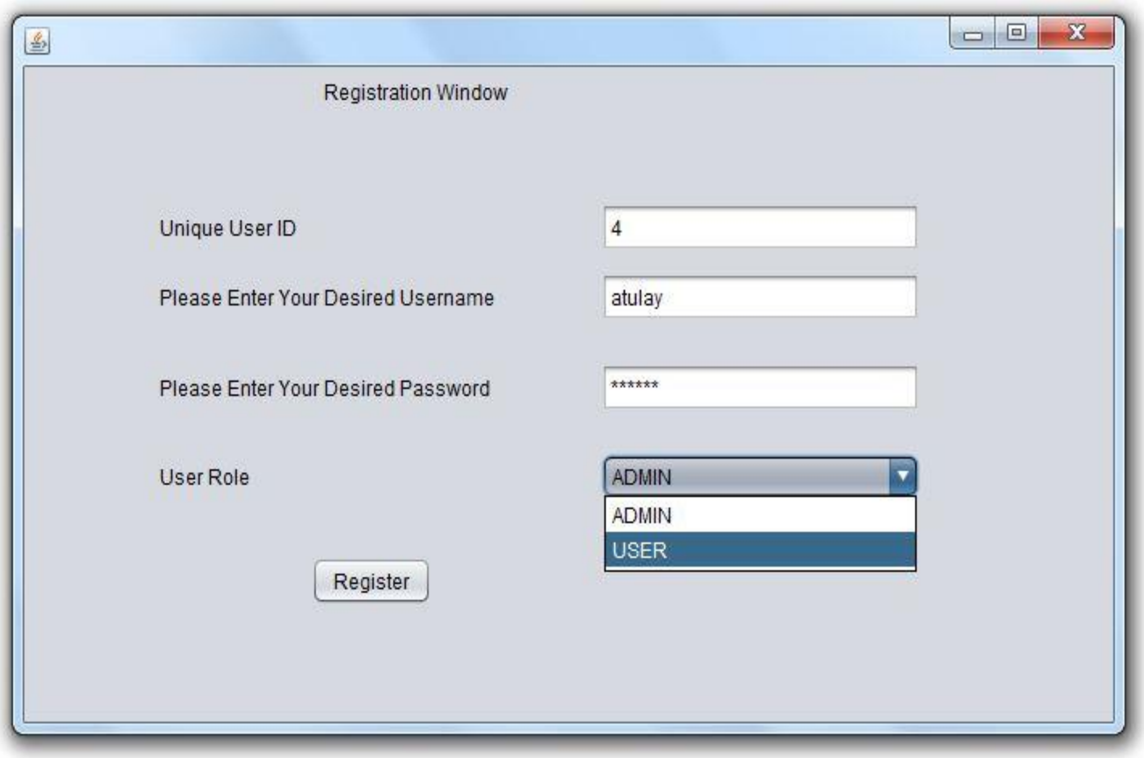
Chapter 4

RESULTS AND DISCUSSIONS

In this chapter, I have presented the attacks being performed by a malicious insider who has root access to the management of the servers that compose the cloud.

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 presented my proposed solutions in the form of my implementation snapshots.

Firstly, we will register a user. So, here is the Registration Window for the user in this Cloud Interface.



Registration Window

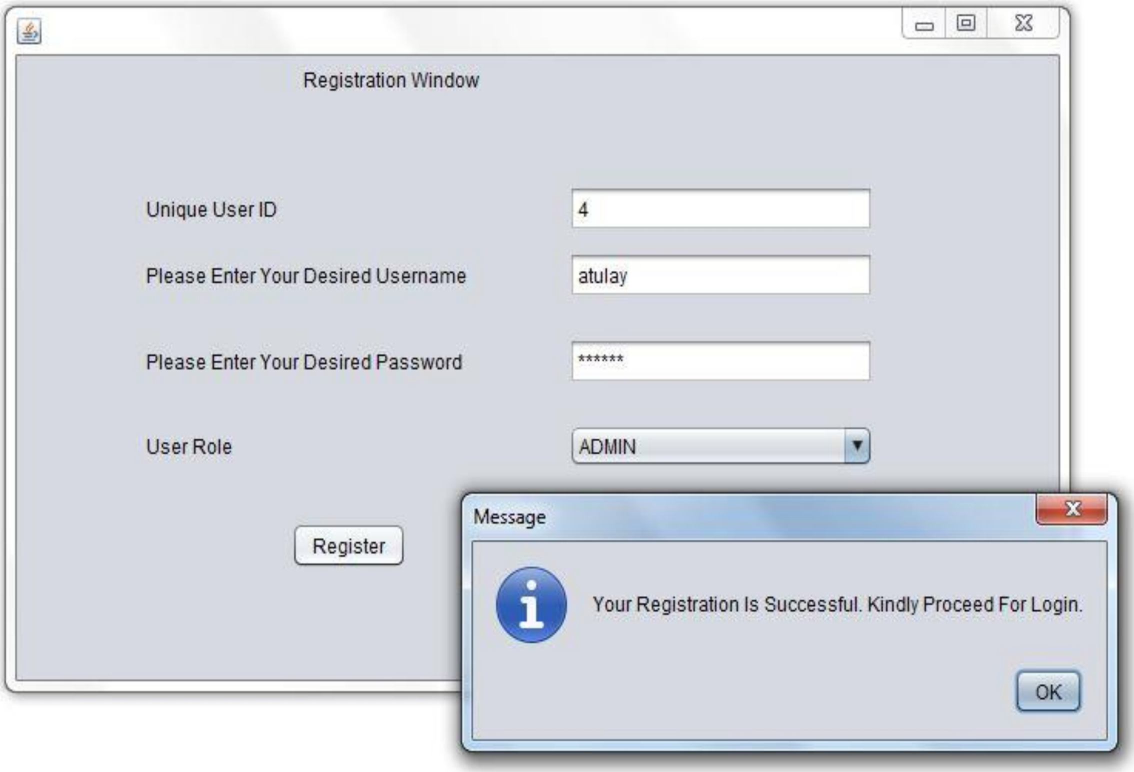
Unique User ID: 4

Please Enter Your Desired Username: atulay

Please Enter Your Desired Password: ******

User Role: ADMIN

Figure 7 - Registration Window.



Registration Window

Unique User ID: 4

Please Enter Your Desired Username: atulay

Please Enter Your Desired Password: ******

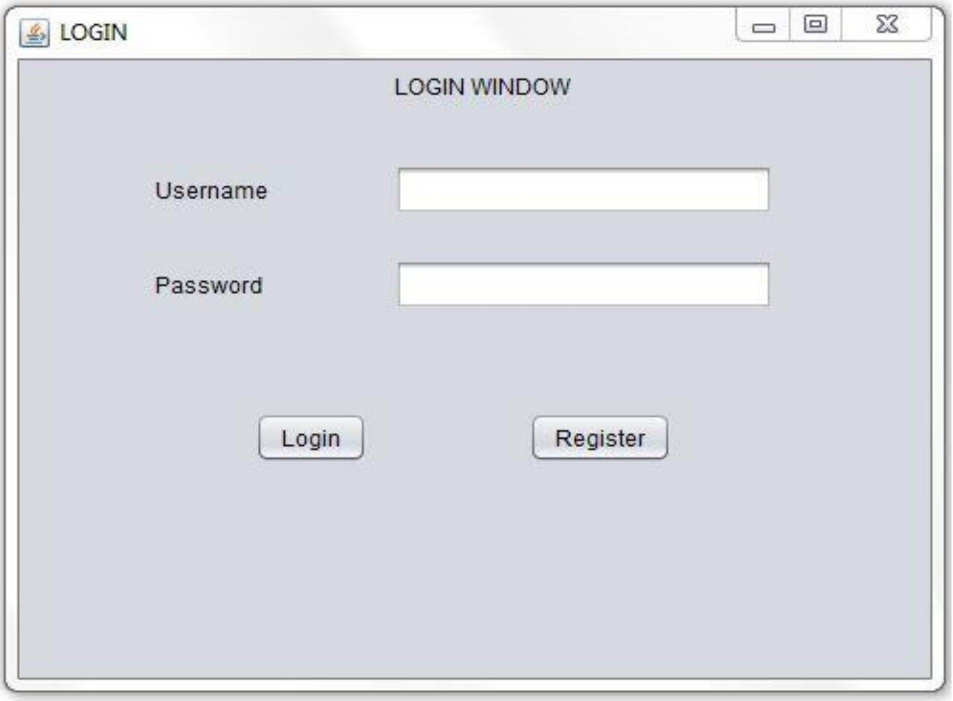
User Role: ADMIN

Message

Your Registration Is Successful. Kindly Proceed For Login.

Figure 8 - Registration Successful.

After Registration, we will head towards the login window to gain access to the interface.



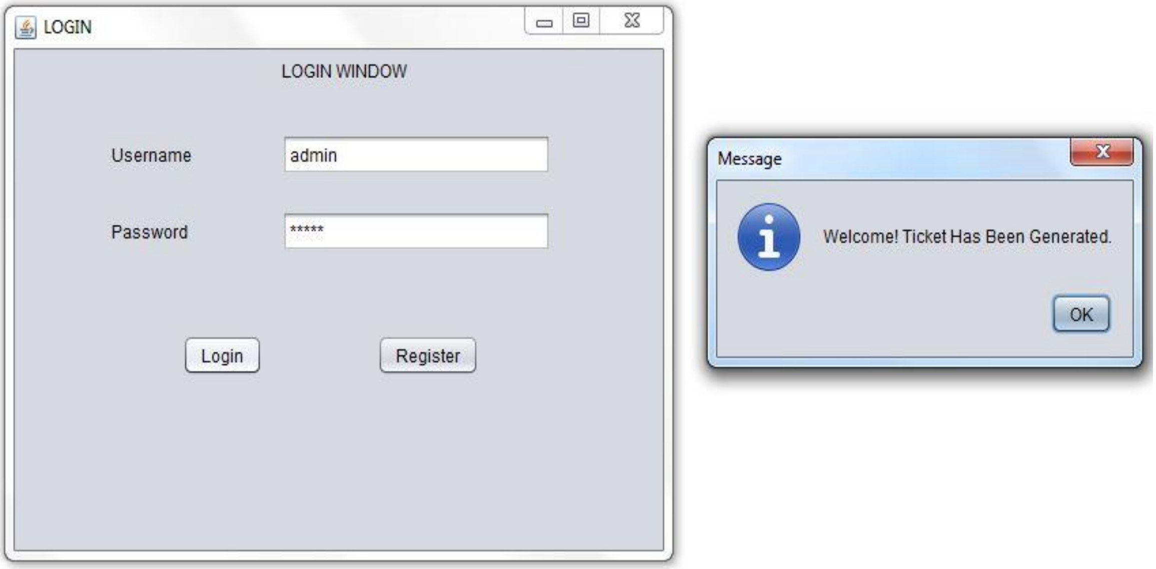
LOGIN

LOGIN WINDOW

Username:

Password:

Figure 9 - Login Window.

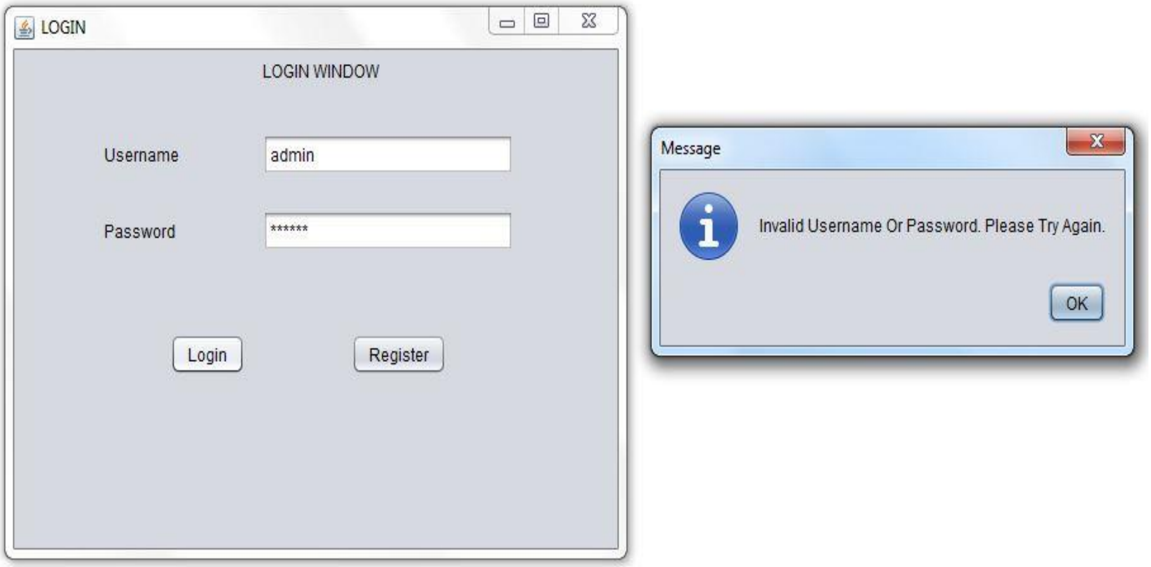


Username admin

Password *****

Welcome! Ticket Has Been Generated.

Figure 10 - Login Successful.



Username admin

Password ******

Invalid Username Or Password. Please Try Again.

Figure 11 - Login Failed.

Now, we have logged in as an administrator. Since the administrator has root level access, so the panel has option of uploading files, viewing files, viewing the list of users as well as their files.

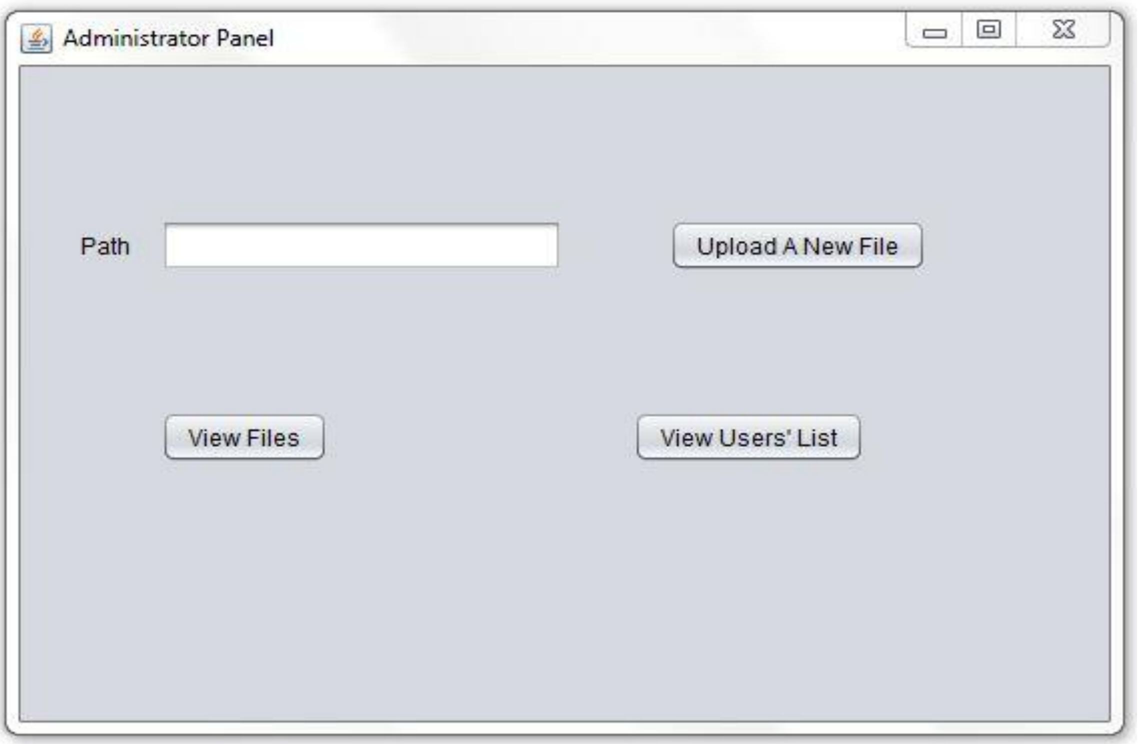
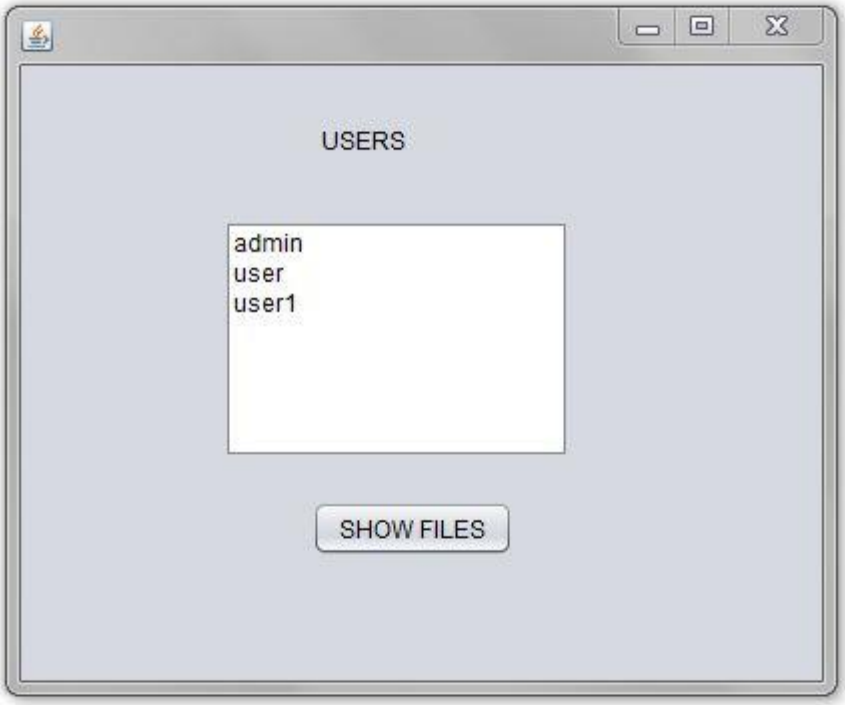


Figure 12 - Administrator Panel.

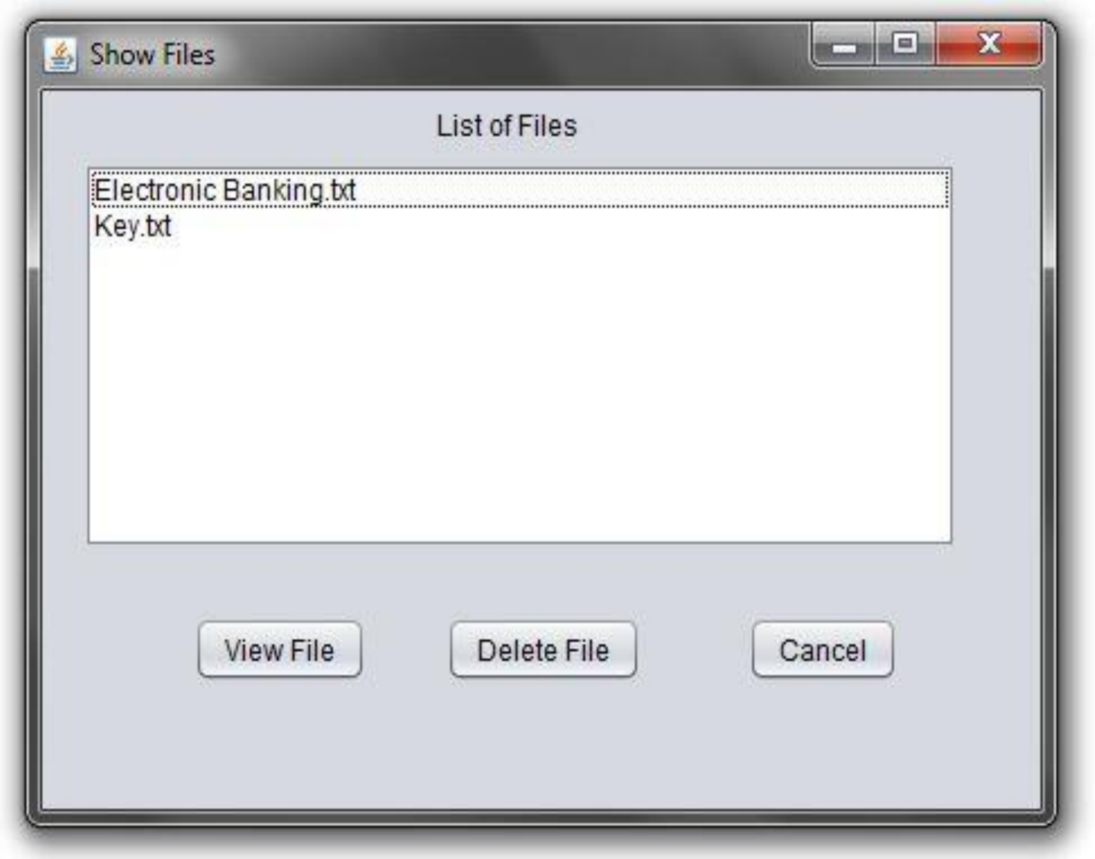
To view the list of all registered users (including administrator), click on View Users' List.



admin
user
user1

Figure 13 - List of Users.

Also, the administrator can view and delete individual user's files too. There is an option of viewing as well as deleting.



Electronic Banking.txt
Key.txt

Figure 14 - List of Files.

Now, I have shown the **User Panel**.

The users have the privilege to upload file, either in normal mode or in encrypted mode.

When uploaded normally, the user can view it without any password.

When encrypted, a key file is generated for viewing the file which can be accessed by the local administrator but he would be unable to access the data.

Similarly, the cloud based administrator would be able to access the encrypted files but not their associated keys.

For gaining access to the files, the user has to do a secure login by entering the OTP sent to his/her registered email ID.

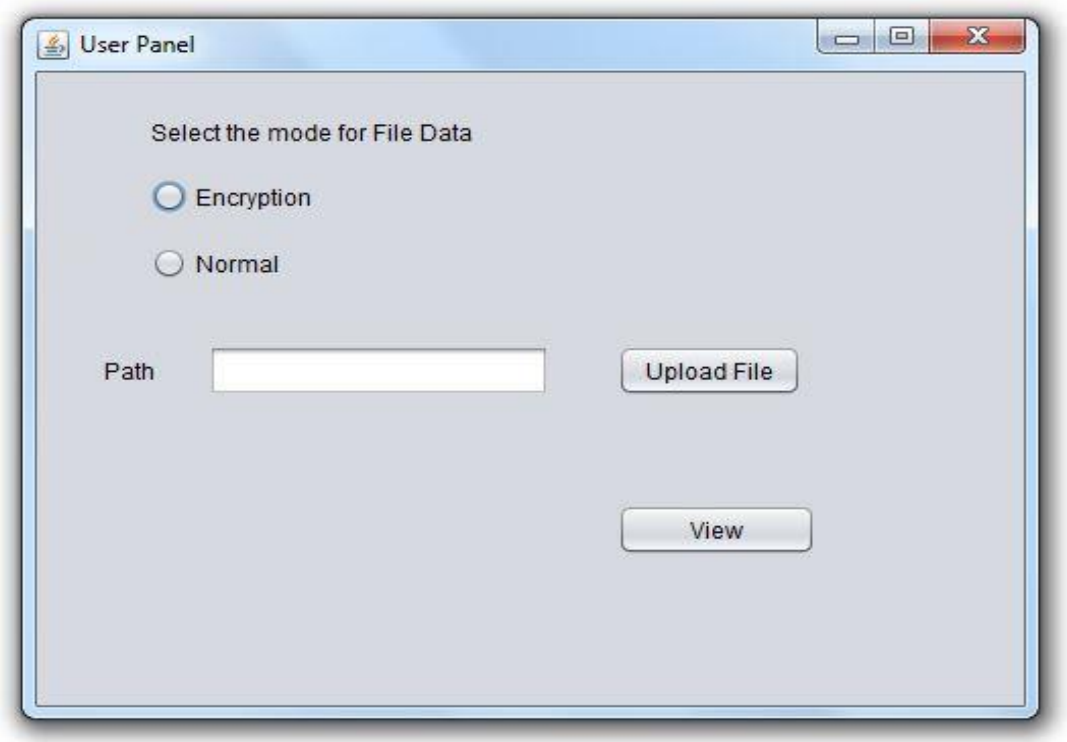
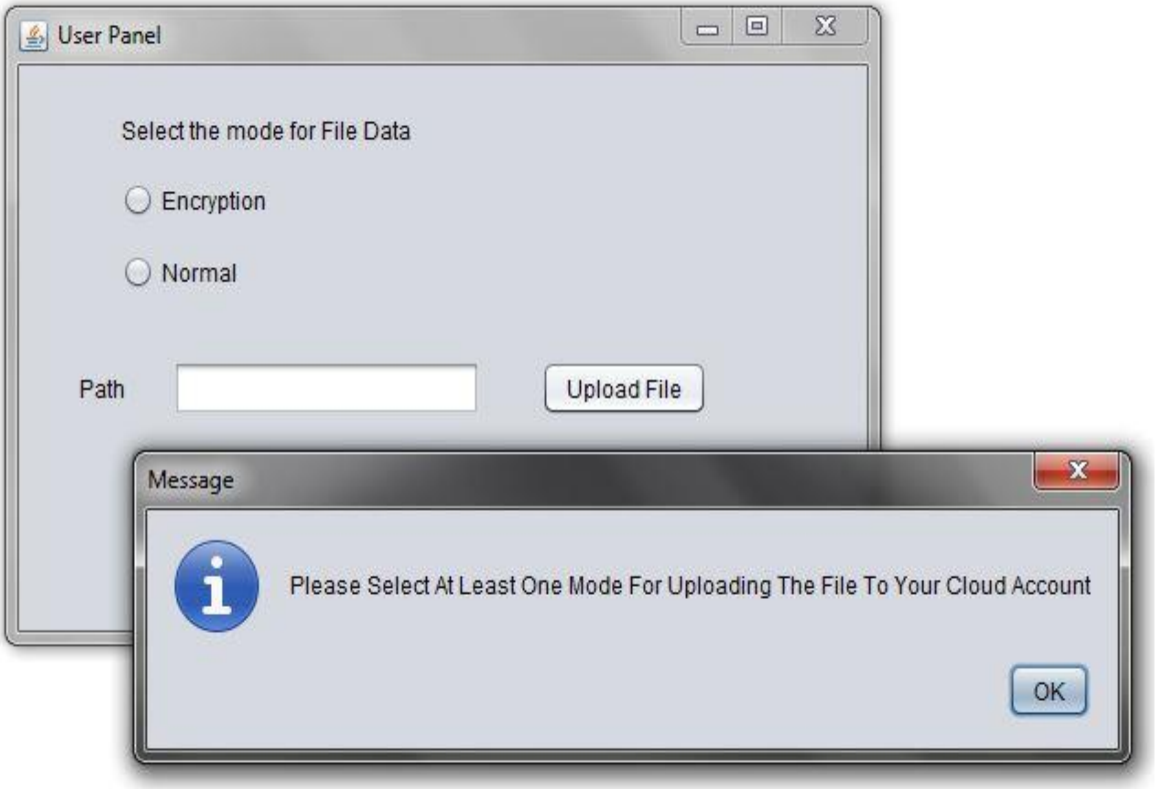
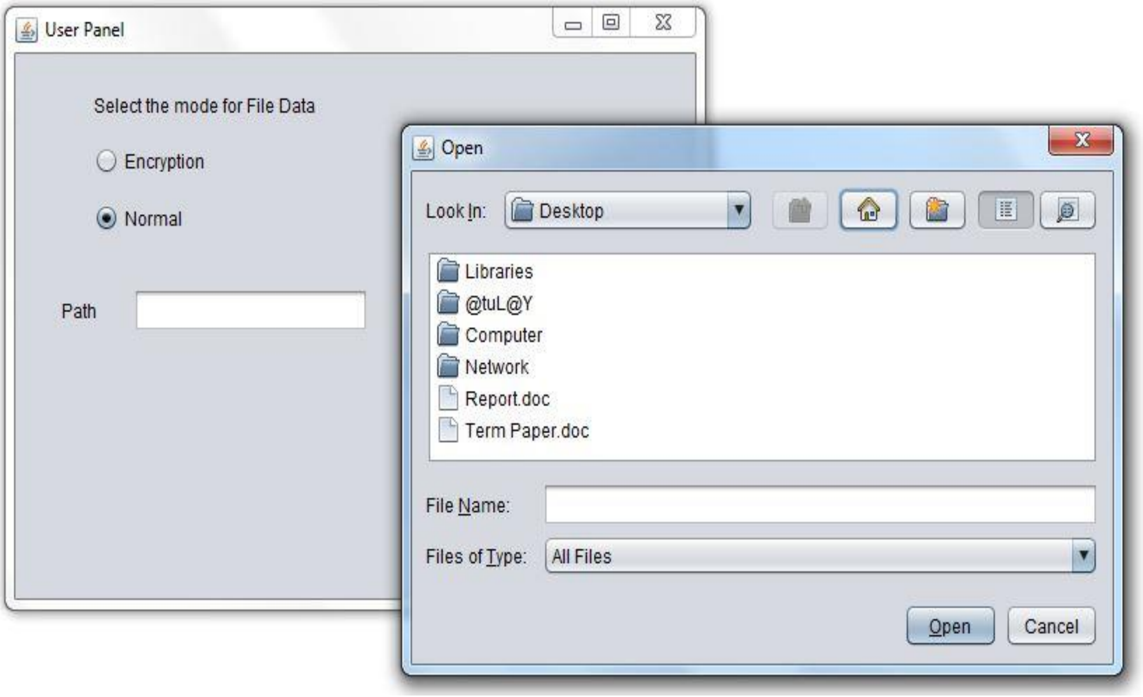


Figure 15 - User Panel.



Please Select At Least One Mode For Uploading The File To Your Cloud Account

Figure 16 - Upload Mode For A User.



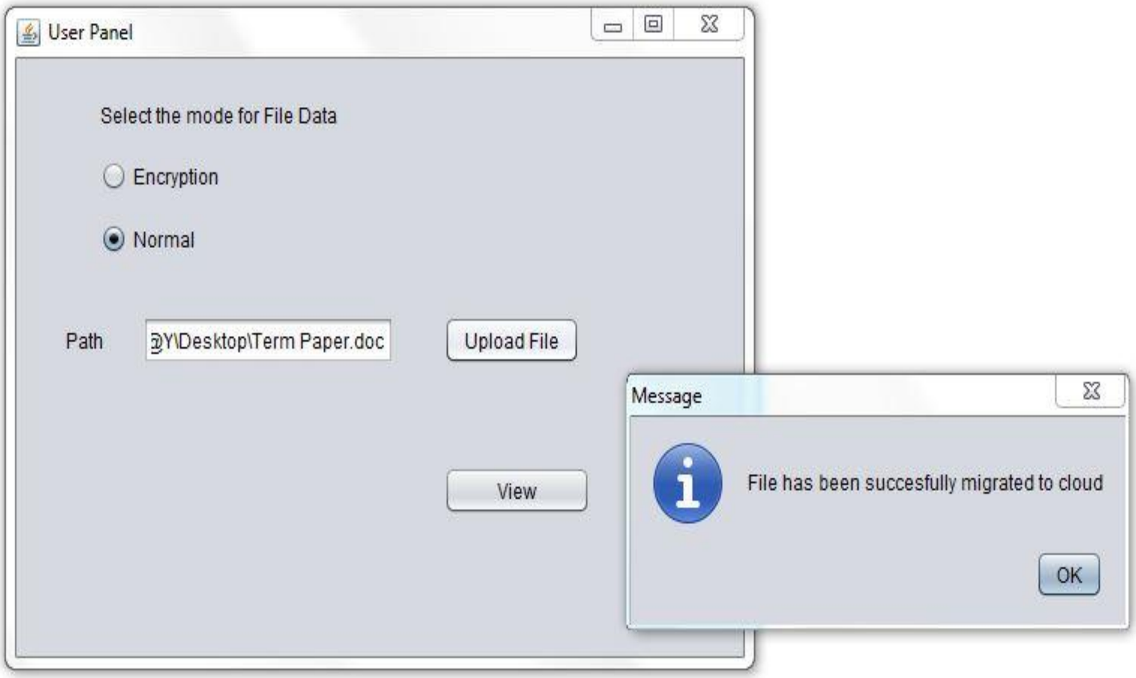
Select the mode for File Data

○ Encryption

● Normal

Path

Figure 17 - Normal Upload Mode For A User.



Select the mode for File Data

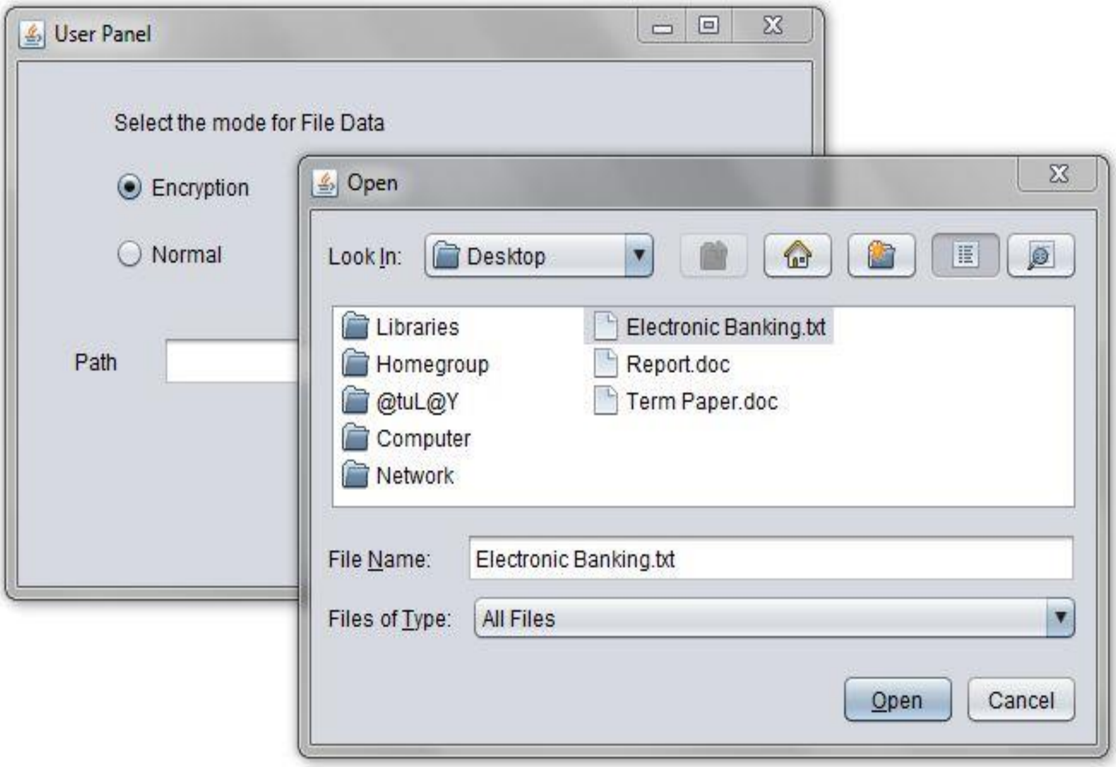
○ Encryption

● Normal

Path @Y\Desktop\Term Paper.doc

File has been succesfully migrated to cloud

Figure 18 - Normal Upload Complete.



User Panel

Select the mode for File Data

● Encryption

○ Normal

Path

Open

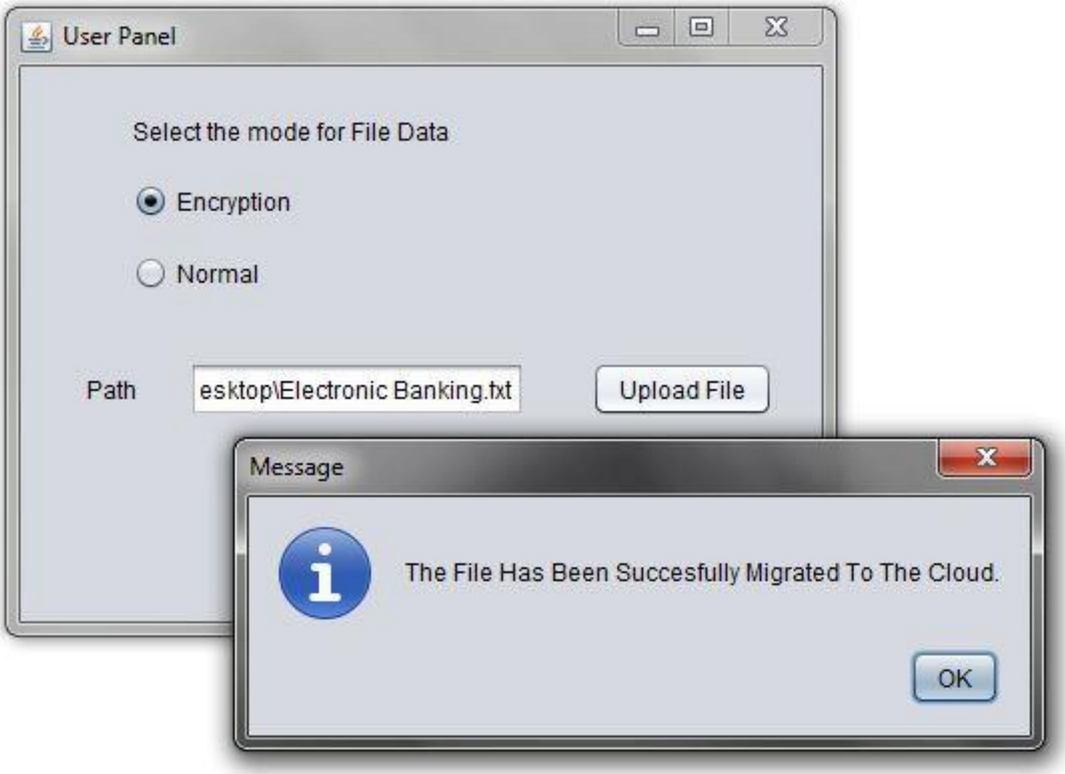
Look In: Desktop

Libraries
Homegroup
@tuL@Y
Computer
Network
Electronic Banking.txt
Report.doc
Term Paper.doc

File Name: Electronic Banking.txt

Files of Type: All Files

Figure 19 - Encryption Mode Upload For A User.



User Panel

Select the mode for File Data

● Encryption

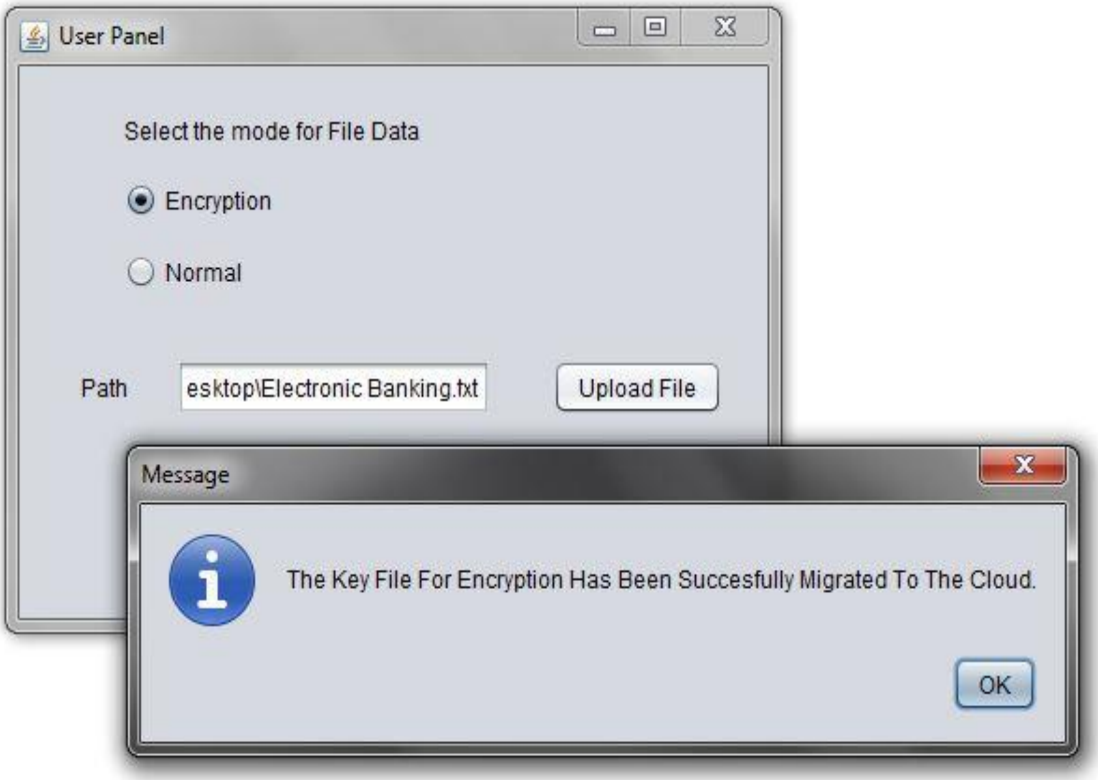
○ Normal

Path: esktop\Electronic Banking.txt

Message

The File Has Been Succesfully Migrated To The Cloud.

Figure 20 - Encryption Mode Upload Complete.



User Panel

Select the mode for File Data

● Encryption

○ Normal

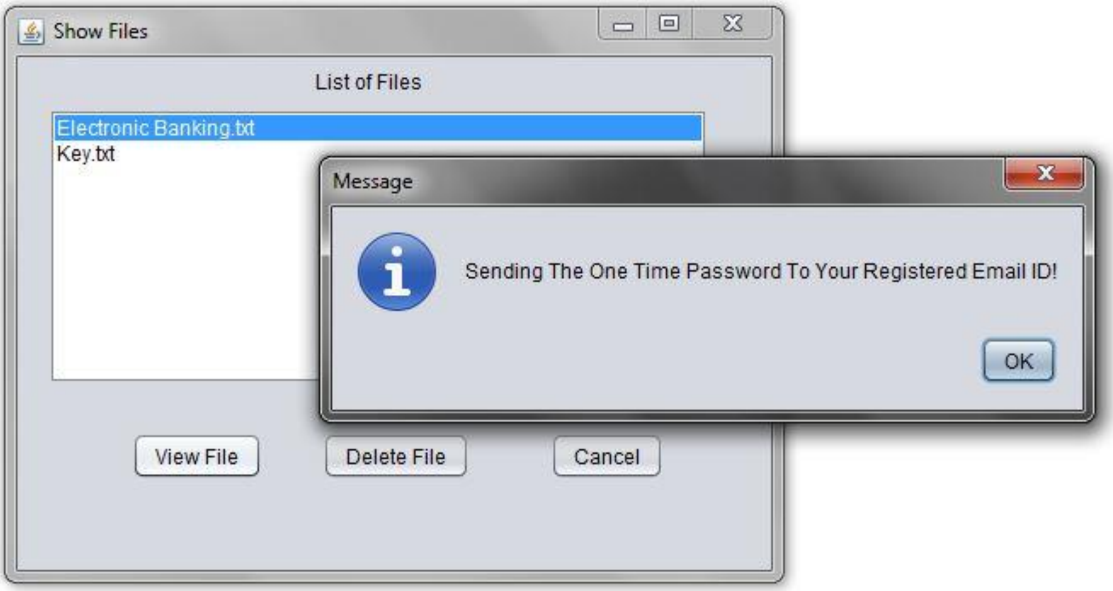
Path esktop\Electronic Banking.txt

Message

The Key File For Encryption Has Been Succesfully Migrated To The Cloud.

Figure 21 - Associated Key Upload Successful.

When the user wants to view his/her file, he/she has to click on View File which opens a pop-up for sending an OTP to the registered email ID.



Show Files

List of Files

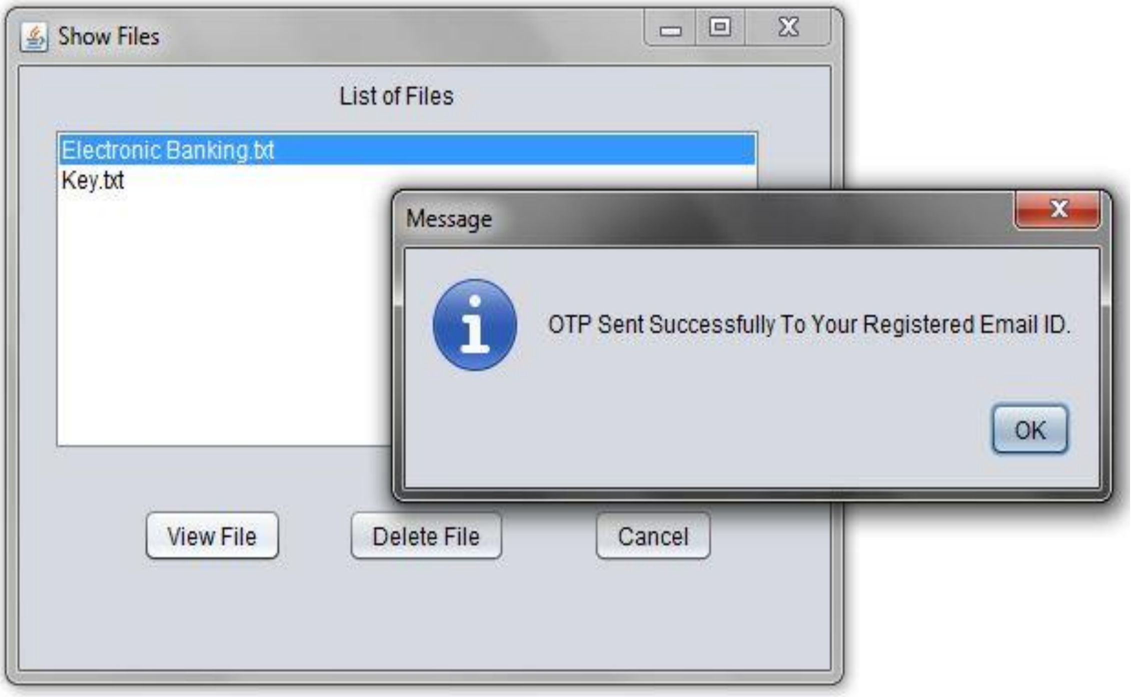
Electronic Banking.txt
Key.txt

Message

Sending The One Time Password To Your Registered Email ID!

Figure 22 - Sending OTP.

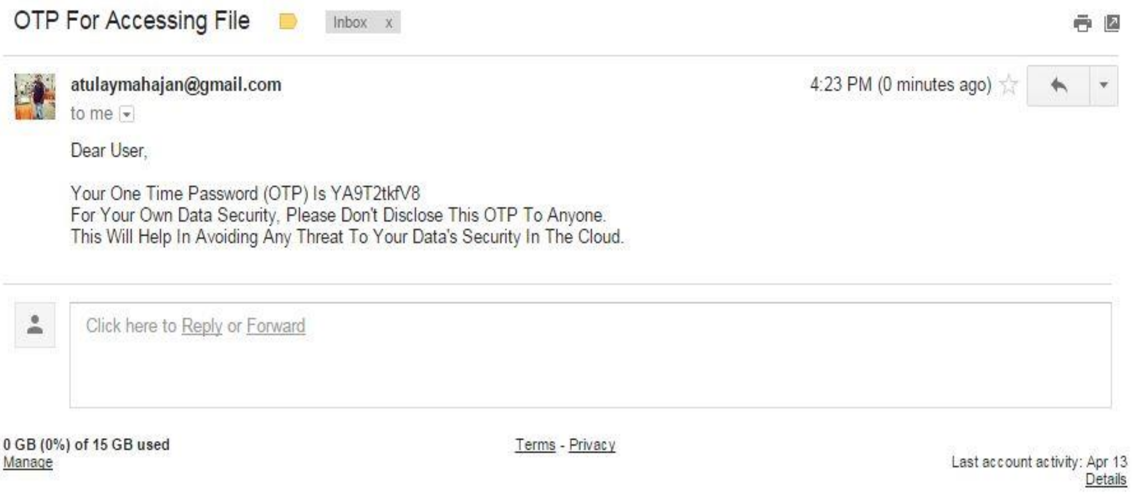
After the OTP is sent, the user gets a confirmation.



OTP Sent Successfully To Your Registered Email ID.

Figure 23 - OTP Sent Successfully.

I have designed my code to send an OTP to the user's registered email address.



OTP For Accessing File

atulaymahajan@gmail.com

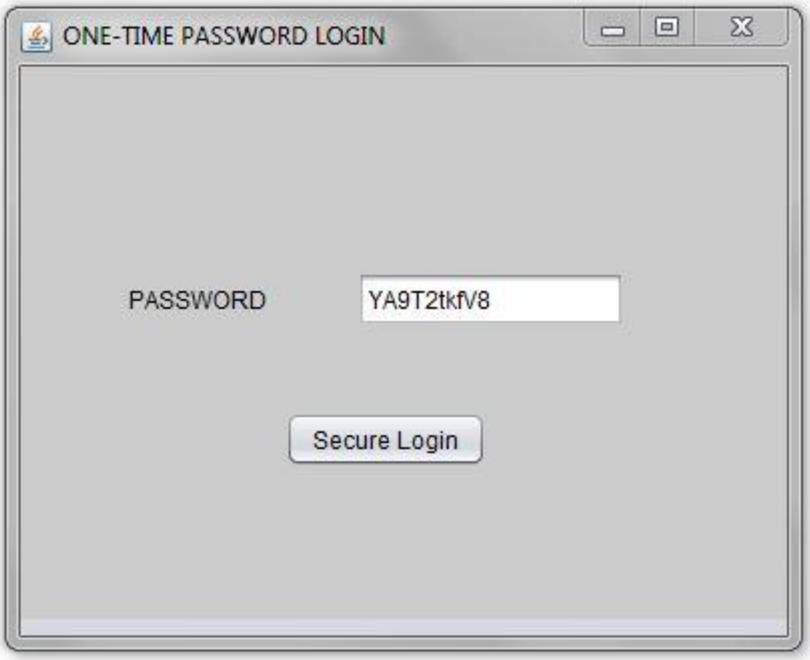
4:23 PM (0 minutes ago)

Dear User,

Your One Time Password (OTP) Is YA9T2tkfV8
For Your Own Data Security, Please Don't Disclose This OTP To Anyone.
This Will Help In Avoiding Any Threat To Your Data's Security In The Cloud.

Figure 24 - OTP In Gmail.

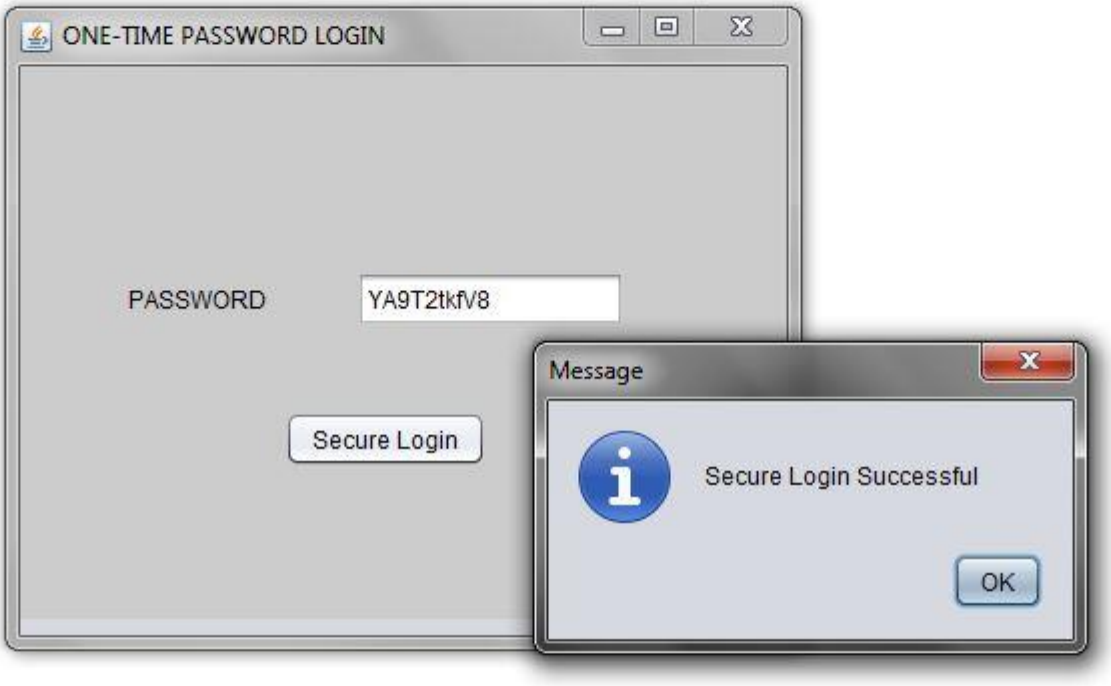
After getting the OTP in the registered email address, the user has to enter it in a pop-up.



PASSWORD YA9T2tkfV8

Figure 25 - Enter OTP.

After entering the OTP, click on secure login to gain access to the file.

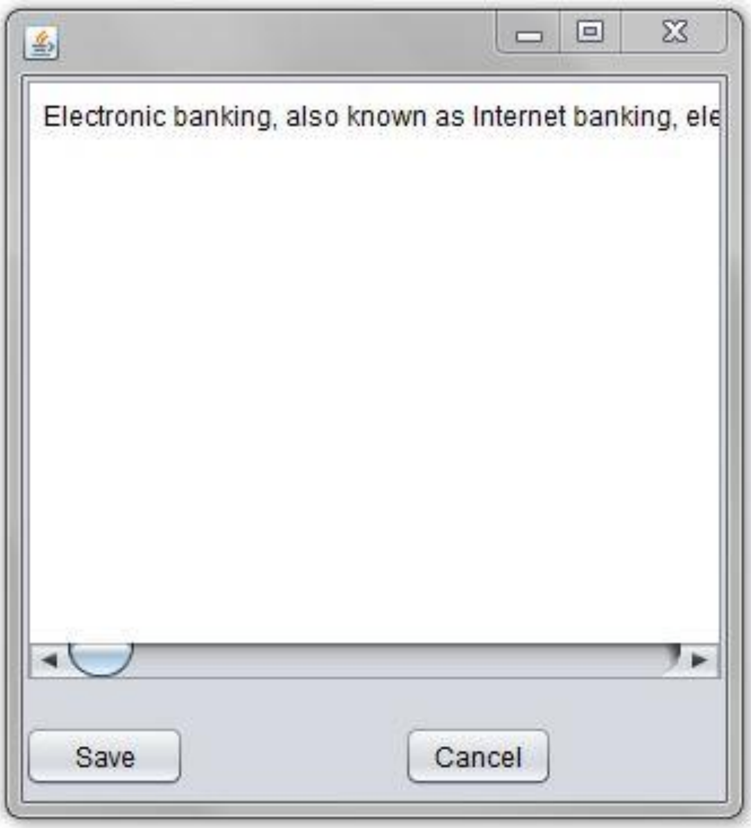


PASSWORD YA9T2tkfV8

Secure Login Successful

Figure 26 - OTP Verified Successfully.

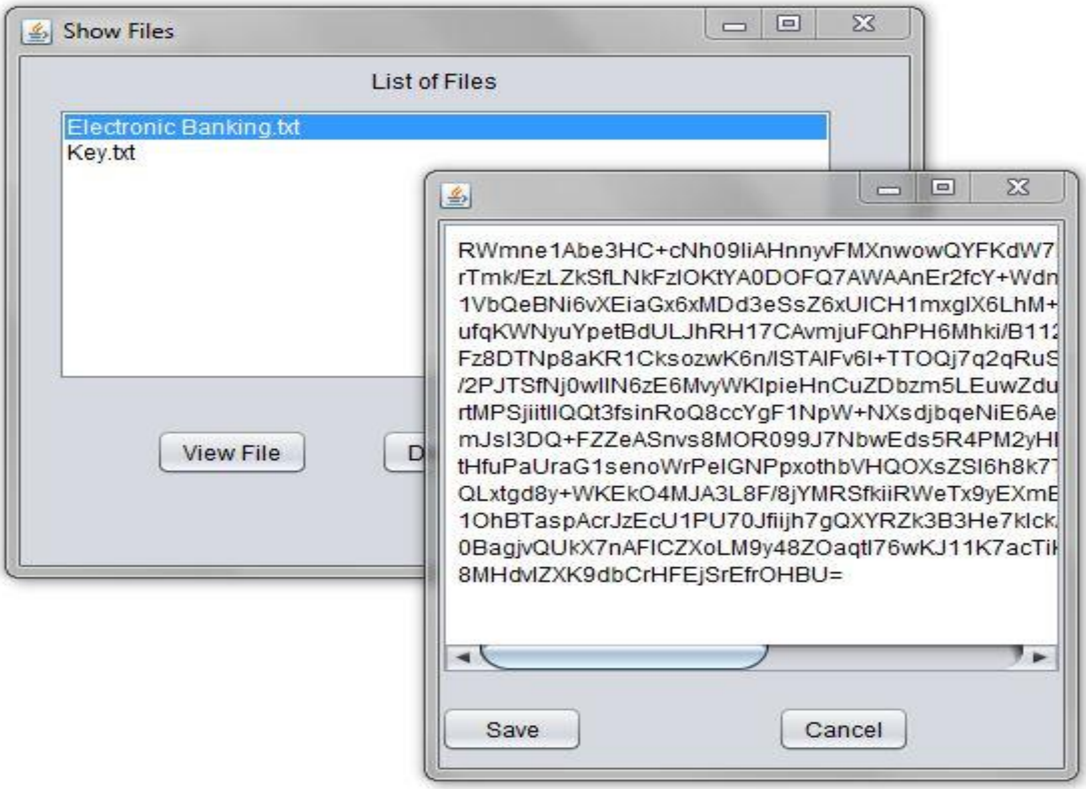
After Successful Secure Login, the user can access his/her data without the fear of any Malicious Insider.



Electronic banking, also known as Internet banking, ele

Figure 27 - Viewing File After Decryption.

If any user tries to access the file without decryption, it will appear as random characters which cannot be understood by anyone as a private key is needed for decryption.



RWmne1Abe3HC+cNh09IiAHnnyvFMXnwowQYFKdW7
rTmk/EzLZkSfLNkFzIOKtYA0DOFQ7AWAAnEr2fcY+Wdn
1VbQeBNi6vXEiaGx6xMDd3eSsZ6xUICH1mxgIX6LhM+
ufqKWNyuYpetBdULJhRH17CAvmjuFQhPH6Mhki/B11
Fz8DTNp8aKR1CksozwK6n/ISTAIFv6I+TTOQj7q2qRu
/2PJTSfNj0wIIN6zE6MvyWKIpieHnCuZDbzm5LEuwZdu
rtMPSjiitIIQQt3fsinRoQ8ccYgF1NpW+NXsdjbqeNiE6Ae
mJsI3DQ+FZZeASnvs8MOR099J7NbwEds5R4PM2yH
tHfuPaUraG1senoWrPeIGNPpxothbVHQOXsZSI6h8k7
QLxtgd8y+WKEkO4MJA3L8F/8jYMRSfkiiRWeTx9yEXm
1OhBTaspAcrJzEcU1PU70Jfiijh7gQXYRZk3B3He7kIck
0BagjvQUkX7nAFICZXoLM9y48ZOaqtI76wKJ11K7acTi
8MHdvIZXK9dbCrHFEjSrEfrOHBU=

Figure 28 - Viewing File Without Decryption.

Chapter 5

CONCLUSION AND FUTURE SCOPE

Conclusion

Cloud Computing is a promising paradigm with growing acceptance, but there is still much work to be done if we want to achieve holistic security in the cloud. This dissertation demonstrated that an insider can violate data confidentiality without the need of high technical skills. It also discussed the benefits of my current proposed solution for the problem.

Malicious activity from within the Cloud provider system is tough to observe when there are collusion and collaboration between multiple insiders and outsiders within the Cloud environment.

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.

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.

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.

Future Scope

Future research on cloud-related insider threats should focus on identifying and addressing unique vulnerabilities posed by the use of cloud computing services. Hence, my future work will focus on detailed implementation and analysis of insider threat prediction and detection models for the cloud along with ways for the service providers to offer security as a service within the cloud.

Furthermore, the implementation will enable us to measure the effectiveness of the countermeasures proposed in above chapters in practice, and enhance/modify them accordingly.

Chapter 6

LIST OF REFERENCES/ BIBLIOGRAPHY

[1] B.R. Kandukuri, VR Paturi, and A. Rakshit. Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on, pages 517-520, 2009.

[2] 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.

[3] 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.

[4] Ertaul, Levent, Sarika Singhal, and Gökay Saldamli. "Security Challenges in Cloud Computing." In Security and Management, pp. 36-42. 2010.

[5] Eystein Mathisen. Security challenges and solutions in cloud computing. In Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, pages 208-212, 2011.

[6] 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.

[7] F. Maggi and S. Zanero. Rethinking security in a cloudy world. Technical report, Technical report, Dipartimento di Elettronica e Informazione, Politecnico di Milano, 2010.

[8] F.B. Shaikh and S. Haider. Security threats in cloud computing. In Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pages 214-219, December 2011.

[9] Iliana Iankoulova and Maya Daneva. Cloud computing security requirements: A systematic review. In Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on, pages 1-7, 2012.

[10] Insider Threats In The Cloud. http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=105

[11] 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.

[12] Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges. In MIPRO, 2010 Proceedings of the 33rd International Convention, pages 344-349, 2010.

[13] 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.

[14] Md. Tanzim Khorshed, A. B. M. Ali, and Saleh A. Wasimi. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 2012.

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

[16] 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.

[17] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1):1{11, January 2011.

[18] 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.

[19] Top threats to cloud computing: Cloud security alliance. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf