

An Authentication Model for Cloud Computing Application

By

Rafal Adeeb AL-Khashab

Supervisor

Prof. Dr. Alaa H Al-Hamami

This Thesis is submitted in Partial Fulfillment of the Requirements
for The Master`s Degree of Science in Computer Science

Department of Computer Science

College of Computer Sciences and Informatics

Amman Arab University

نموذج للتحقق في تطبيقات حوسبة السحابة

أعداد

رفل أديب الخشاب

أشرف

الأستاذ الدكتور علاء الحمامي

قدمت هذه الرسالة لأستكمال متطلبات الحصول على درجة الماجستير في
الحاسب الالى

قسم علوم الحاسوب

كلية الدراسات الحاسوبية العليا

جامعة عمان العربية

AUTHORIZATION

I, the undersigned “Rafal Adeeb AL-Khashab” authorize Amman Arab University to provide copies of this thesis to libraries, institutions and any other parties upon their request.

Name: Rafal Adeeb AL-Khashab.

Signature: 

Data: 30/11/2013.



iii

Resolution of the Discussion Committee

This dissertation titled "An Authentication Model for Cloud Computing Application ", has been defended and approved on.

Discussion committee Title Signature

Discussion committee Member	Title	Signature
Prof. Dr. Alaa H. Al-Hamami	Chair and Supervisor	<i>Alahamami</i>
Dr. Ahmad M. Al-Odat	Member	<i>Podat</i>
Dr. Venus W. Samawi	Member	<i>WWS</i>



IV

DEDICATION

I dedicate this thesis to:

My parents,

My sisters,

My supervisor Prof. Dr. Alaa Al-Hamami,

My favorite friends,

My lecturers and all staff of Amman Arab University

For their love and support

ACKNOWLEDGMENT

I want to thank ALLAH for his blessings that help me achieve my dream. I would like to thank my supervisor Prof. Dr. Alaa Al-Hamami who supported and helped me to complete this thesis. I would like to thank him because he was always available when I needed his help. Also, I would thank everyone who contributed to the elaboration of this thesis.

TABLE OF CONTENTS

DEDICATION	V
ACKNOWLEDGMENT	VI
TABLE OF CONTENTS.....	VII
LIST OF ABBREVIATIONS	IX
LIST OF FIGURES.....	X
Abstract.....	XIII
Abstract(Arabic).....	XIV
CHAPTER ONE INTRODUCTION.....	1
1.1Introduction	2
1.2 Security Issue in Cloud Computing	5
1.3 The Characteristics of Cloud Computing	8
1.4 Cloud Computing Service Model (Architectural Layers of Cloud Computing)	12
1.5 Cloud Computing Deployment Model	15
1.6 Cloud Security Problem	19
1.7Contribution.....	20
1.8 Thesis Organization	20

CHAPTER TWO Literature Review	22
2.1 Introduction	23
2.2 Statement of the problem	23
2.3 Literature Review	26
CHAPTER THREE THEORETICAL DESIGN	43
3.1 Introduction	44
3.2 Authentication procedure	46
CHAPTER FOUR THE EXPERIMENTAL WORKS	63
4.1 Introductions	64
4.2 Execution authentication procedure	64
4.3 Execution privacy:-	74
CHAPTER FIVE CONCLUSION AND FUTURE WORK	81
5-1 Introduction	82
5.2 Conclusion	82
5.3 Future work	83
REFERENCE	85

LIST OF ABBREVIATIONS

Abbreviations	Meaning
ABE	Attribute-Based Encryption
CaaS	Cloud Communication as a Service
CAM	Consolidated Authentication Model
DaaS	Database as a Service
DDoS	Distributed Denial of Service
DoS	Denial of Service
GPS	Global Positioning System (Navigation System)
IaaS	Infrastructure as a Service
IDS	Intrusion Detection Systems
IT	Information Technology
KDCs	Key Distribution Centers
MaaS	Monitoring as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
TaaS	Testing as a Service
VMs	Virtual Machines
VPC	Virtual Private Cloud

LIST OF FIGURES

Figure Number	Figure Name	Page
CHAPTER ONE		
Figure (1-1)	Main Concepts of Cloud Computing	2
Figure (1-2)	Types of Cloud Service Model	13
Figure (1-3)	Types of Cloud Deployment Model	15
CHAPTER TWO		
Figure (2-1)	Cloud Authentication	25
Figure (2-2)	Cloud Mechanism	26
CHAPTER THREE		
Figure (3-1)	The Proposed Cloud Model	47
Figure (3-2)	Password Encryption	49
Figure (3-3)	Image Encryption	52
Figure (3-4)	Password Decryption	55
Figure (3-5)	Image Display	57
Figure (3-6)	Generate Password	61

CHAPTER FOUR		
Figure (4-1)	Main Interface in Application	67
Figure (4-2)	New Account Interface	68
Figure (4-3)	Sec-user Table	69
Figure (4-4)	Successful Registration	69
Figure (4-5)	Third Party Table	70
Figure (4-6)	Installation Stages of Application	70
Figure (4-7)	Backup Stages	71
Figure (4-8)	Cloud Application	71
Figure (4-9)	Log-in Interface	73
Figure (4-10)	Notice to the User	73
Figure (4-11)	Display Images	74
Figure (4-12)	Notice Email	75
Figure (4-13)	User Email	75
Figure (4-14)	Cloud Interface	76
Figure (4-15)	Cloud Details	76
Figure (4-16)	Files Interface	77
Figure (4-17)	Backup History Interface	77
Figure (4-18)	Share File Interface	78
Figure (4-19)	Stages of Hide Folder	79
Figure (4-20)	Stages of Open the Folder Hidden	80
Figure (4-21)	Share Files Type	80

Figure (4-22)	Stages of Hidden Link	81
Figure (4-23)	Stages of Retrieve Hidden Link	82

Abstract

Recently cloud computing is considered the next generation in world of the internet. The word cloud computing means different things to different people, but there is a common definition used by people as the away to deliver service and data rather than as a product, the data owners can remotely store and access their data in the cloud anytime and anywhere.

The concept of cloud computing is a model for sharing resources like serves, storage, network, and application, Cloud computing made service available for customer in open environment. Thus, it is important to provide authentication to communicate through cloud. Cloud users feeling that their data will be secured and available to them.

In this study, the researcher designed successful implementation of cloud authentication; when the users used the internet and before any communication across a network they need to be authenticated with the cloud. A third party is responsible to check if the user is authorized or not, after that, it gives identification to the user for safety access to the cloud.

In this thesis, the researcher used multiple password mechanism by generating new password every log-in instead of using single password. In other words, they generated multiple passwords from one password to provide more security for the user, application, and cloud. The proposed model has been implemented on the personal cloud due to its basic structure for the other clouds deployment.

الملخص

أصبحت الحوسبة السحابية في الأونة الأخيرة هي الجيل الجديد في عالم الانترنت، حيث تعني عدد من المفاهيم التي تختلف بالاعتماد على مستخدميها، وبالرغم من ذلك فأنهم يتفقون على مفهوم أساسي وهو ان الحوسبة السحابية هي طريق لتوصيل الخدمات والبيانات الى المستخدمين اكثر من كونها منتج، وان مالكي هذه البيانات بإمكانهم القيام بتخزينها والوصول اليها في اوقات واماكن مختلفة.

ان المفهوم العام للحوسبة السحابية هو عبارة عن نموذج مشاركة المصادر مابين المستخدمين مثل الخدمات، مواقع الخزن، مصادر الانترنت والتطبيقات، وتكون جميع هذه المصادر متاحة للمستخدمين كخدمة سحابية متوفرة في البيئة المفتوحة. لذلك فمن الضروري توفير الوثوقية للاتصال الذي يحدث من خلال السحابة، وجعل جميع مستخدميها يشعرون بأن بياناتهم متوفرة ومؤمنة في وقت واحد.

لقد قمنا بهذه الرسالة بتصميم تطبيق ناجح، عندما تكون هناك حاجة للتحقق من المستخدمين للسحابة قبل تحقيق أي اتصال خلال الشبكة. حيث يقوم الطرف الثالث، الذي يكون مسؤول عن عملية الاتصال مابين المستخدمين والحوسبة، بالتأكد من وثوقية الشخص المستخدم وأعطائه صلاحية الدخول اليها.

ومن أجل زيادة أمانة الاتصال مع الحوسبة السحابية، فقد استخدمنا ميكانيكية توليد عدد من كلمات السر بدلا من كلمة سر واحدة، واستخدام واحدة من هذه الكلمات في كل عملية دخول بدلا من استخدام كلمة سر واحدة لجميع عمليات الدخول. وقد تم اختيار الحوسبة الشخصية لأختبار تطبيق الرسالة عليها من خلال اعتبارها الهيكل الاساسي لبقية انواع نشر الحوسبة.

CHAPTER ONE

INTRODUCTION



1.1 Introduction

The cloud computing concept gets all attention of all Internet users. This concept is not a new idea. It is a combination of several concepts from virtualization, distributed application design, grid computing, utility computing and clustering. The cloud computing is a set of multiple resources (hardware and software) that is available through the internet and managed by the provider. The customers get all or some of these resources according to the used cloud system. The main concepts of cloud computing declared in Figure (1-1).

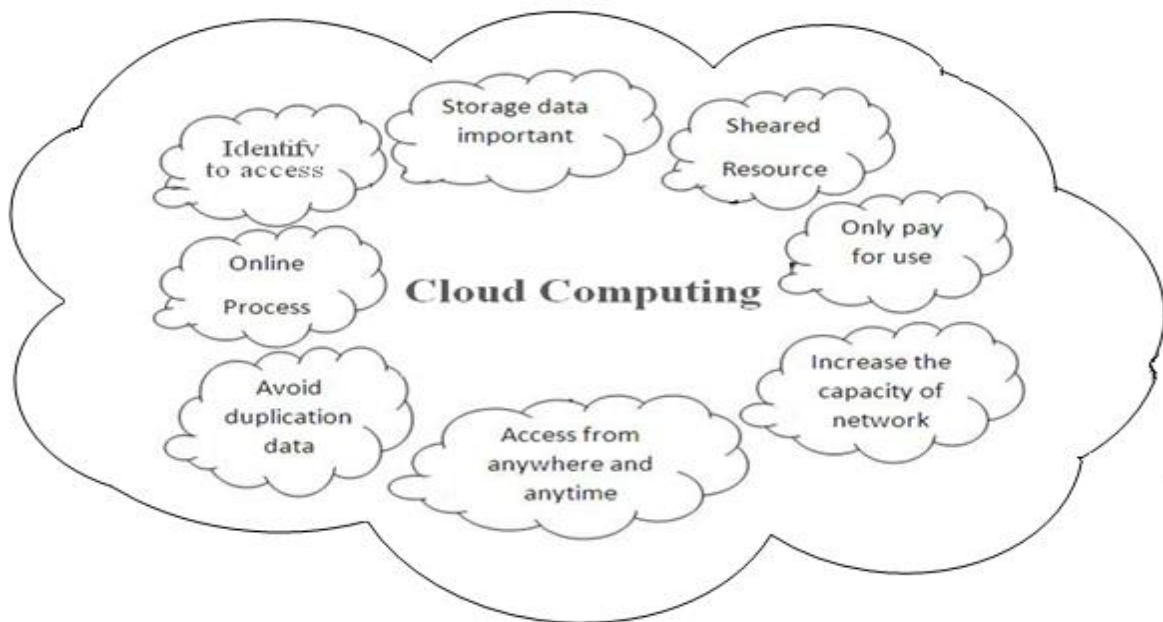


Figure (1-1) ... Main Concepts of Cloud Computing

The organization pays for the access of cloud computing services; these services are present to customer according to the client need, the storage space, processing capabilities, the number of the clients allowed them to work, and other factors. The main idea of the cloud is how the customers satisfied their requirements and pay only for the actual used without needing any details about process.

Cloud computing is a way to increase the capacity of a network without investing in new infrastructure, training new personnel, or licensing new software [1].

Cloud computing can be able to rent a server or a thousand of servers and run a geophysical modeling application to provide useful service to any customer. It can store and secure amounts of data that accessed only by authorized applications and users. It is the ability to use the applications on the internet that store and protect data while providing a service. Also, it gives the ability to use other web services to integrate photos, maps, and Global Positioning System (GPS) information to create a mash up in customer's web browsers [2].

Cloud computing helps for avoid duplication of data to a certain extent. Large organizations (who do not use cloud computing) spread over many countries may need to have some information available at anytime to their offices. The only way to achieve this without setting up a costly, centralized server is to have copies of the required information at many servers throughout their offices.

This duplication of data can be avoided by using cloud computing. If the organizations use public cloud services, or even have a private cloud system of their own, then all the information would be present only at the cloud and everyone would be able to access the data easily [3].

Cloud computing allows providers to develop, deploy and run applications that can easily grow in capacity, work rapidly, and never fail without any concerns on the properties and the locations of the underlying infrastructures [4].

Cloud vendors effectively sell computation and storage resources as goods, some cloud vendors and third parties sell higher-level resources, such as the Google Application platform, relational database management system (DBMSs) or the Sales Force application. The customer controls the virtual machine's capacity (computational and storage) by sending the cloud vendor a service request to add or subtract resources as needed. The time to gain or release capacity (for small fractions of the provider's inventory) is typically measured in minutes, not months [5].

Cloud computing is not just about technology. It represents the fundamental change in which how information technology is provisioned and used. Before adopting the cloud computing, enterprises have to consider its benefits, risks, and effects on their organization and customer. Persons who are interrelated with the networking environment, cloud computing is a preferable platform for them. Therefore, in recent days providing security has become a major challenging issue in cloud computing [6, 7].

1.2 Security Issue in Cloud Computing

Security issue refers to the protection of data, network, computer programs, computer power, and other elements of computerized information system. Security problem is getting complicated because users do not need to be an expert to launch an ordinary attack, thus, the security trends mainly to prevent or at least minimize the attacks [8].

Any security model defines through subjects and objects, as well as in the cloud computing environment, the security defines through subjects such as users of the cloud, attacker trying to gain control, the cloud controller, cluster controllers, node controllers, and process running on various node controllers as well as the system itself, and defines through objects such as files, programs, resources, etc. that available in the cloud system [9].

Cloud computing is like any new technology. It has some risk in the cloud environment. Resources are shared among all servers, users, and individuals. As a result, the data stored in the cloud become available to all. Therefore, data of an individual can be handled by all other users of the cloud. Thus the data or files become more vulnerable to attack. As a result, it is very easy for an intruder to access, misuse, and destroy the original form of data and an intruder can also interrupt the communication [7].

We should focus on security issue when any user is using the cloud services or two users are sharing the same cloud services. Number of security issues associated with cloud computing but these issues fall into two broad categories:

Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service through the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and their clients' data and applications are protected. While the customer must ensure that the provider has taken the proper security measures to protect their information [10].

Security is a key concept while considering the move to the cloud applications that have very sensitive and confidential information which would be better off being behind the corporate firewall. Technical mechanisms of data security in the cloud are still evolving and still the top most inhibitor of cloud adoption [11].

Thus before migration to the cloud, one should focus on some important attacks on cloud computing [10, 12]:-

- **Denial of Service (DoS) Attacks: -**

A large cloud services provider is a large target and more attractive for those who wish to cause maximum distribution through attacks such as distributed Denial of Service because it is shared by many users, which makes DoS attacks much more damaging.

- **Zombie Attacks: -**

Throughout the Internet, an attacker tries to get the attention of the victim by sending requests from innocent hosts in the network. These types of hosts are called zombies. In the Cloud computing, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood a large number of requests through zombies.

This type of attack can affect the cloud service because it will cause Denial of Service (DoS) or Distributed Denial of Service (DDoS) to the servers.

- **Backdoor Channel Attacks: -**

It is a passive attack. It allows hackers to gain remote access to the compromised system. Using backdoor channels, hackers can be able to control victim's resources and can make it a zombie for attempting a DDoS attack. It can also be used to discover the confidential data of the victim.

- **Side Channel Attacks: -**

Cloud system is responsible for service request; this type of attack tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. If the attacker succeeds to do this, then the attacker will send valid requests that are redirected to the malicious services automatically.

- **Authentication Attacks: -**

Authentication is a weak point in hosted and virtual services and it is frequently targeted. There are many different ways to authenticate the users; for example, based on what a person knows to allow the user to enter the cloud application. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

- **Man-in-the-Middle Attacks: -**

This attack is commonly taking place when different cloud users across the cloud communicate with each other or share the resources from the cloud environment. This attack is carried out when an attacker places himself between the two users and tries to hack the information during the transmission. Anytime, attackers can place themselves in the communication path. There is the possibility that they can intercept and modify their communications.

- **Phishing Attacks: -**

Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. In cloud, it may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the cloud.

In the area of cloud computing, different security models and algorithms are applied. In this thesis, the focus was on authentication attacks to show users that their information is secured and they have authority to know who access their information in the cloud and require strong authentication between application components so that is transmitted only to authorized parties.

1.3 The Characteristics of Cloud Computing

Cloud computing has several characteristics such as:

1- Reducing The Running Time & Responding Time :-

For the applications that cloud is essential for running batch jobs, cloud computing makes it straightforward to use 1000 servers to accomplish a task

in 1/1000 of the time that a single server would require and reduce the time to setup, install and configure the applications in the organization [2].

2- Reducing The Cost :-

The most important characteristic in cloud computing is reducing the cost and that has several directions [13]:-

- Reducing the hardware cost: - getting the whole works done in the cloud without purchasing high cost equipment's for the organizations that having thousands of employees, who only need a terminal to connect to the cloud in order to perform most of the computation.
- Reducing the software costs: - The proprietary software is no longer needed to be purchased. The amount gets paid to the cloud's provider as when it is needed to use the high cost software instead of buying it. Also reduces the software cost which is needed to run and manage any organization's server.
- Maintenance and upgrading cost: - It is possible for the employers to quickly remove the associated computer costs when the number of employees is reduced. It is easy to migrate, or upgrade the current operating system, hardware, etc. with a new one, because the organization only needs to pay for the services which they want to upgrade instead of investing again and purchasing the high cost software and hardware.

3- Independence Device and Location :-

One of the benefits of cloud computing is that, although the organization is not aware of the physical location of the data and what device to use, but they view the data to be presented in one location. Independence device and location enables the users to access the systems using a web browser regardless of their location or what device they are using. The portability of the application is that the users can use it from home, work, or at client locations. These characteristics are enabling the employees to access the data from anywhere they are in [13, 14].

4- Resource Pooling :-

Resources such as network bandwidth, virtual machines, memory, processing power, storage capacity, etc. are pooled together to serve the multiple customers who are using a multi-tenant model with different physical and virtual resources that are dynamically assigned and reassigned according to the consumer demand [14, 15].

5- Reliability :-

Reliability is improved if multiple redundant sites are used, which makes the cloud designed is suitable for business continuity and disaster recovery. When the user use the cloud computing, the data will be stored in the cloud and the user do not need to think of their data [1].

6- Performance :-

Performance is monitored consistent and loosely coupled architectures are constructed using web services as the system interface [1].

7- Maintenance :-

Maintenance of cloud computing application is easier, because they do not need to be installed on each computer users and can be accessed from different places [1].

8- Back – Up Facility:-

Cloud computing provides an automatic data backed – up facility as opposed to a desktop computer or notebook computer does set to automatically save the important data on the server [13].

9- Reduces the Risks of Theft :-

Since the data exists in the cloud, any company's resources or other computing equipment is stolen, then there will be less chances of losing the company's proprietary and sensitive data, and it will also reduce the chances of greater financial impact [13].

10- Availability and Collaboration:-

If the user gets services from the cloud using internet then he/she is not responsible for the underlying infrastructure of the service. For example, if the system is properly working or any system is failed completely or faulty, every concern is managed by cloud itself by its distribution nature so user gets a quality service.

If a company has all its important data or computation on the cloud, then it is very easy to access the data from anywhere if you have only a computer terminal and it is connected with the Internet. Similarly it also allows the

participant to share and work on the same instance of the data. It is easy for the organization to expand its branches [13].

11- **On-Demand Self-Service:-**

Customers can automatically provision computing capabilities and resources on their own when is needed without necessitating any human intervention [15].

12- **Elasticity and Scalability:-**

The cloud is elastic. This means that resource allocation can get bigger or smaller depending on demand. Elasticity enables scalability, so the cloud can scale upward for peak demand and downward for lighter demand. Scalability also means that an application can scale when adding users and application requirements change [15].

1.4 Cloud Computing Service Model (Architectural Layers of Cloud Computing)

Cloud computing providers provide a variety of services to the customers, in practice, cloud service providers tend to offer services that can be grouped into three categories :- software as a service, platform as a service, and infrastructure as a service, as shown in Figure (1-2).

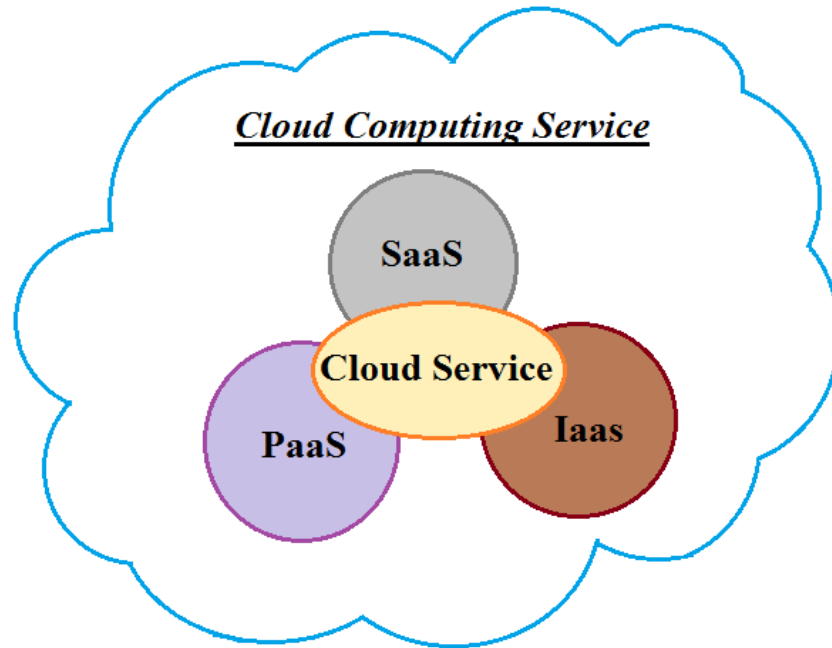


Figure (1-2) ... Types of cloud service model

1.4.1 Software as a Service (SaaS):-

The capability has been provided the consumer to use a provider's application that runs on a cloud infrastructure, a single instance of the application runs on the cloud services and multiple end users or client organization.

SaaS delivers special-purpose software that is remotely accessible by the consumers through the internet, the consumer's dose not mange or control the underlying cloud infrastructure including network, servers, operating system, storage, or even individual application capabilities [14, 16, 17].

1.4.2 Platform as a Service (PaaS):-

The capability has provided the consumer to deploy onto the cloud's consumer-created infrastructure or acquired application created using programming language, libraries, services and tools supported by the provider.

PaaS encapsulates a layer of software and providers. It has services that can be used to build higher-level services. The consumer does not manage or control underlying cloud infrastructure including network, servers, operating system, or storage, but a user has controlled over the deployed application and possibly configuration setting for the application-hosting environment [14,16,17].

1.4.3 Infrastructure as a Service (IaaS):-

The capability has provided the consumer to supply the processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating system and applications. IaaS delivers basic storage and compute capabilities as standardized services over the network. The consumer dose not manage or controls the underlying cloud infrastructure but has controlled over operating system, storage, and deployed applications, and possibly limited control of select networking components [14, 16, 17].

1.5 Cloud Computing Deployment Model

Cloud computing services and technology are deployed over different types of delivery model when moving from standard enterprise application deployment model to one based on cloud computing. These types based on the characteristics and purpose. IT organization can choose to deploy application on public, private, virtual private, personal, community or hybrid clouds as shown in Figure(1-3). Companies may make a number of consideration with regard to which cloud computing model they choose to employ, and they might use more than one model to solve different problems [2,18] .

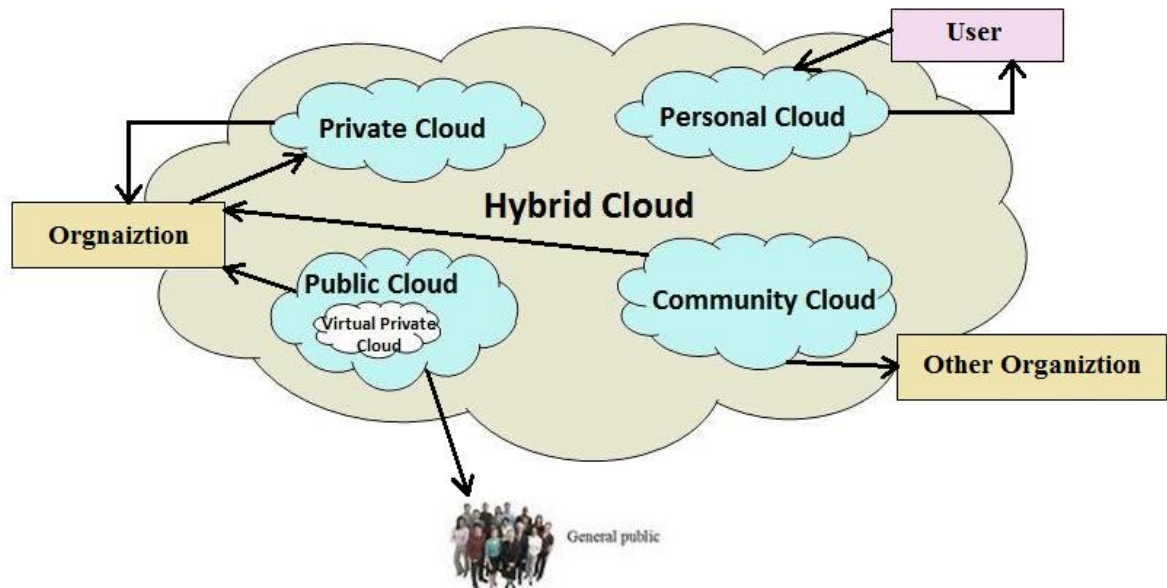


Figure (1-3) ... Types of cloud deployment model

1.5.1 - Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It owned, managed and operated by service provider (business, academic, government organization or some combination of item).

The resources, such as storage and application, from different customers are likely to be mixed together on the cloud's servers, storage system, and network. These resources are made available to multiple customers by a service provider through internet. This type of cloud is typically low-cost or pay-on-demand and has highly scalable services [2,14,18].

1.5.2- Private Cloud

The cloud's infrastructure is provisioned for exclusive use by a single organization comprising multiple customers; it can be built, managed and operated by the company's own IT organization, by a cloud provider (third party), or some combination of them. Private cloud are built for the exclusive use of one client, this model gives companies high level of security, quality of service and control over how application or data are deployed on it [2,14,18].

1.5.3- Community Cloud

The cloud's infrastructure is provisioned for exclusive use and it is controlled and shared by several organization and support a specific community that has shared interests, such as mission, policy and security requirements.

It may be owned, managed and operated by one or more of the organization in the community, a third party or some combination of them, and it may exist on or off premises, and the members of the community share the access to the data and application in the community cloud [2, 14,18].

1.5.4- Hybrid Cloud

The cloud`s infrastructure is a combine of two or more distinct cloud`s infrastructure like public, private and community. That remains unique entities, but is bound together by standardized or proprietary technology that enables data and application portability. The application with less stringent security, legal, compliance and service level requirements can be outsourced to the public cloud, while keeping business-critical services and data in a secured and controlled private cloud.

Hybrid clouds introduce the complexity of determining how to distribute applications across both public and private. Among the issues that need to be considered is the relationship between the data and processing resources. If the data is small, or the application is stateless, a hybrid cloud can be much more successful than if large amounts of the data must be transferred into a public cloud for a small amount of processing [2, 14, 18].

1.5.5 - Virtual Private Cloud

The cloud`s infrastructure is provisioned for exclusive use in specific portion of public cloud infrastructure; this cloud is virtually partitioned rather than completely physically separated from the larger cloud. The main idea of this Virtual Private Cloud (VPC) definition is really that the VPC is not

completely physically separated from the larger cloud and some physical infrastructure sharing remains.

The service providers in this cloud utilize public cloud resources and infrastructure to create infrastructure which is physically separated, it would simply be called private or semi-private virtual cloud, and it owned, managed and operated by a public cloud vender.

Virtual private cloud was introduced specifically for those customers interested in taking advantage of the benefits of cloud computing but who have concerns over certain aspects of the cloud. Common concerns involve privacy, security and the loss of control over proprietary data. In response to this customer need, many public cloud vendors designed a VPC offering a part of a vendor's public infrastructure but having dedicated cloud servers, virtual networks, cloud storage and private IP addresses, reserved for a VPC customer.

The VPC is on demand configurable pool of shared computing resources in a public cloud, isolated between the tenants of the public cloud and not shared with any other customer. The isolation between tenants of a public cloud is performed via access control mechanism [18,19,20].

1.5.6 Personal Cloud

The cloud's infrastructure is provisioned for personal use, this cloud help any user to access the digital files located in home can be used from any device, anytime and anywhere.

It can be owned, managed and operated by the user who creates the personal cloud, and only the user who owns the cloud can access to this

cloud's serves and responsibility who is looking to own files and maintain on it. But it is also possible to grant permission to others such as family and friends.

In this thesis, we use the personal cloud because this type provides each user with independent virtual network and can store any type and any size of a file online in centralized location, releases space on PCs, smart phones and tablets. The files can be accessed from any device that is connected to the internet.

The personal cloud allows user to backup data automatically in a safe, secure and nearby location without having to wonder whether third parties have access to own private and personal information or not [21, 22, 23]. In this research, we are interested in personal cloud computing. We will tackle the security problem (especially the authentication problem) in personal cloud computing

1.6 Cloud Security Problem

Cloud computing is one of the most important topics today in the field of information technology. It means a virtualization of resource that maintains and manages itself, and enabling the remote access from known or unknown device at any time.

The security issue is considered one of the main concepts in every growing field. The security problem of cloud computing is a hot research topic. Although cloud computing has many benefits, it is still not safe from threats and vulnerabilities that prevent the users from trusting it.

Authentication is used to distinguish between authorized user and unauthorized one. The authentication problem is one of the challenges in cloud computing, so we need to propose a generic authentication model to detect and prevent unauthorized access that occurred through communication between the user and cloud.

1.7 Contribution

We choose subject cloud computing as a next generation in internet world and presenting explanation about cloud like concepts, characteristic, type service and deployment model.

Also discuss the problem that users feel worried and afraid to the migration process to the cloud, this problem called authentication. Therefore in this thesis we try to design a model to provide authentication for the user.

We determine the personal cloud as cloud deployment model, to experience thesis model, then present some idea to provide data privacy inside this cloud.

1.8 Thesis Organization

This thesis contains five chapters, **in chapter one**, we summarized the main concepts of cloud computing, security issue of cloud and discussed different type of attacks on it, important Characteristics, service and deployment model and we declare which type of cloud deployment model and attacks we will focus on it.

In chapter two, we discuss the main security problem from our perspective in the cloud between the user and the cloud, and choose a personal cloud type of the cloud computing to test the problem and its solution on it. And present a summary of related work associated with cloud computing in general, and with this thesis in specific.

In chapter three, we present a model for how to solve the problem of trust between the user and the cloud, also we present the main components and algorithms in this model, and we explain each algorithm by flow charts.

In chapter four, this chapter explains the main interface of the proposed model, the model includes two procedures, authentication procedure and privacy procedure, and we present these procedures by explaining the model design by interfaces.

In chapter five, we summarized conclusion about our model, and propose some ideas for future work dealing with this thesis.

CHAPTER TWO

Literature Review



2.1 Introduction

Cloud computing can use one or thousands of servers. It can store data and applications that are accessible only by authorized user. In this chapter we will explain the main problem from our perspective in the cloud computing, and we will present summary of related work associated with this thesis.

2.2 Statement of the problem

There are many benefits of cloud computing, but the main benefit is portability of the user's application that can be accessed from anywhere and anytime, and the dependence of cloud architecture on shares resources. Therefore the security issues has become a major challenge in cloud computing, the security concepts of various kinds like service availability, distributed processing, traffic handling, alter data and application, access control and protection share resource depends on the authentication.

In this thesis, we are dealing with personal cloud which is the basic of the other type of deployment cloud computing, so the security of the personal cloud is the core for the other types of cloud computing deployment models. The malicious, hacker and other threats are considering the major cause of lacking security of the personal cloud due to centralized location and remotes access to cloud.

According to attacks, a centralized location can be an easier target than several goals and remote access that is insecure technology which offers a boundary of options for attackers to infiltrate enterprises.

The biggest concern is attackers will use remote connection as a jumping point to get deeper into an organization.

There are many service providers for personal cloud storage. In this research, we are interested in using **justcloud** by the link (<http://www.justcloud.com/>) service provider to construct our personal cloud storage. Justcloud as cloud storage provider comes with its own interesting features. These features are:

- Free Account Available for limited time, with minimum cost after testing.
- Unlimited Storage for Videos, Music and any type of Files
- Free iPad, iPhone, Android, Blackberry Apps
- Windows, Mac and Linux Compatible
- Anywhere File Access, Anytime
- Unlimited File Sharing
- Sync Multiple Computers
- Full Computer Restore
- Drag & Drop

We focus on authentication, which refers to any mechanism by which a system allows or denies the access to the data and keep them stored at cloud sites that are accessible only by the users who own the data. The complexity of this mechanism is increased when data is distributed over a wide ranged area or greater number of devices and users. Improve authentication in the cloud will be due to control by third party over all users and clouds; it is responsible for monitor communication between users and clouds, as shown in Figure (2-1).



Figure (2-1) ... Cloud Authentication

The authentication mechanisms in identification and access control is achieved by three methods: the first method refers to the identification of a human by their physical characteristics called biometric such as DNA, fingerprints, retinas and irises, voice patterns, facial patterns and hand measurements. The second method can be defined between two parties. One of these parties is determined which method to identify authorized user like ATM card, smart card and mobile phone.

The third method is one of the widely used mechanisms to authenticate authorized user. In this method the user is able to select something and he/she is the only one who knows that information like password, PIN and pattern.

In this thesis we use the password to identify authorized user. This method is weak because when the user reuses the same password in multiple log-ins it can be easily broken by hackers, on the other hand using multiple passwords will increase security but at the same time these individuals in general facing difficulties in remembering multiple passwords. So we need an accurate method to provide high security and easy use to user, as shown in Figure (2-2).

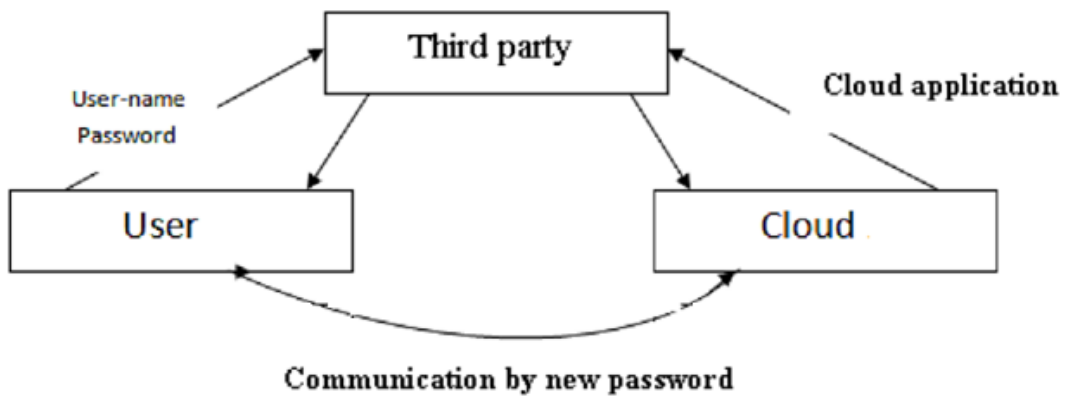


Figure (2-2) ... Cloud Mechanism

2.3 Literature Review

Cloud computing is a new technology that is going to be a big change in the network world, the significant security concerns that need to be addressed when moving application and service to the cloud. A lot of research has been focused on this area, so we present a brief of related work that falls within this area:-

- **Atesh Kumar & et al [1]**

With the rise of phenomenon of cloud computing, an innumerable terms, concepts and approaches have emerged. This paper is a brief survey of cloud computing, also various elements of cloud and present efforts to clear the basic concepts of cloud computing with simple example of them.

This paper discussed the applications, characteristics, deployments models and layers of cloud computing and its security issues evolved from information security point of view. Also included a wide set of controls, technologies and policies used to protect the associated infrastructure, application and data of cloud computing.

- **Kawser Wazed Nafi & et al [7]**

This paper explains the cloud computing platform gives people the chosen for sharing resources, services and information among the people of the whole world. And it is declared in private cloud model, the information is shared among the persons who are in that cloud.

This paper proposed new security structure for cloud computing platform. This structure includes AES file encryption system, RSA system for secure communication and MD5 hashing for hiding information. This model ensures security for whole cloud computing structure.

In proposed system, an intruder cannot easily get information and upload the files because he needs to take control over all the servers, which is quite difficult. The model, though it is developed in a cloud environment, individual servers' operation has got priority here. So, decision taking is easy for each server, like authenticate user, give access to a file etc.

- **Neeraj Bhargava& et al [24]**

The authors in this paper declare the cloud computing as a basic requirement today, everybody who uses the cloud wants to secure their data from natural disaster. The application framework of Cloud provides wings to the Distributed Computing, now client not only save data to the server but can also use the computing resources of the server over the Cloud.

It is a new phase of Information Technology, where companies are competition by offering free cloud storage with attractive interface. The Cloud itself has distinguish meaning when integrate it with the Internet as a bridge, so any computer from the Internet can access the cloud. The authors in this paper expanded the type of service model in cloud computing to Cloud Software as a Service (SAAS), Cloud Platform as a Service (PAAS), Cloud Infrastructure as a Service (IAAS), Cloud Communication as a Service (CAAS), Cloud Monitoring as a Service (MAAS) and Cloud Database as a Service (DAAS).

This paper mainly focuses on the performance analysis of the Cloud Computing, the overall performance of Cloud Computing depends on “How light the interface?” & “How is the availability of resources at the server?” And it discusses core application areas of Cloud Computing and concludes that performance to data center affects by distance and number of users.

- **Shruti N. Pardeshi [25]**

The author in this paper declares software testing in general as a process used for evaluating an attributes or capability of program and makes sure that it meets the requirements, and it is an activity conducted for finding errors in software. It also verifies and validate whether the program is working correctly or not.

Now-a-days testing becomes very important activity in terms of exposure as well in terms of security, performance and usability. If we consider hardware and software licenses, the testing is too expensive task for user.

As cloud computing providing anything as a service, it gives idea about testing as a service through which customer can save the cost of maintenance and up gradation. This paper discussed this idea about the cloud computing along with its very important service which is testing, testing as a service is interesting and hot topic in the research field.

This paper described the necessity of Testing as a Service (TaaS) and proposed new TaaS architecture, and introduced the idea for future that include more number of testing techniques in support of TaaS and validate TaaS platform by considering the security issue. And it gives a proper solution with the various testing required with the different criteria of software development.

- **Abdelmajid Hassan Mansour Emam[26]**

This paper discussed the cloud computing is a new computing paradigm that changes the way of information technology is provided and used, but achieving acceptable level of information security issues are an important aspect and a key factor in the cloud.

This paper firstly lists some of the different security issues of the cloud computing, and then proposes additional security mechanism of Authentication and Authorization which very important for a large distributed system like a cloud system, it is usually ensures that only authorized persons may use the resources in the role of identity and authorizations management.

There should always be a specific security analysis for the data or applications that are to be mapped to any, so the proposed scheme ensure that only the registered user with exact Emil ID may Authorized to access the requested service by using his Mail-ID as an additional form authentication and authorization.

- **Lamminthang Singsit& et al [27]**

This paper discussed many advantages that offered by Cloud computing, such as data ubiquity, flexibility of access, better performance and low startup cost. The main challenge in this advantage is the owner's loss of control of his/her data. Thus it is very important that the security gaps be identified and addressed, secure access control policies, data integrity check and the data privacy technique to hide the data from the service provider needs to be implemented.

Simply encrypting the data is inefficient and is vulnerable to attacks when the access control policies change. Several techniques have been proposed to address these issues. This paper presents a novel and efficient solution that employs two layers of encryption of the data and an encrypted data object containing the second access key. The proposed technique provides a way for data confidentiality and privacy.

Key update problems are addressed by using three keys, A_x , B_x , and K_x . The keys, B_x and K_x are used to encrypt data at the owner site and service provider side respectively to protect the data from both unauthorized. Service Provider is also prevented from reading the data as data owner encrypts it before storing. The key, A_x , is used to encrypt the key, K_x , which is used as a token for access anonymity. To access the outsourced data, a user presents the key, A_x to the Service Provider for authentication.

- **Huiming Yu & et al [28]**

In this paper cloud computing services including data storage service, cloud computing operating system and software as a service introduced, it is discussed different types of challenges that dealing with cloud computing security, such as data privacy and security are discussed especially for users with sensitive data that would be detrimental to the client if it were stolen. And external threats when attacker that exploits vulnerabilities in services provided to a consumer, it can be characterized by attacks that occur outside a consumer's domain.

This paper explained the security technologies that developed to enhance cloud computing security. Cisco Secure Data Center Framework provided multiple security layers to enhance cloud computing security,

the Cisco has developed this framework with three consideration, the first one is traditional security issues of information assurance such as data access control and encryption, the second consideration is control that means directly manage how and where data and application are deployed and used, the third consideration is service-level management which include contracting and enforcement of service level agreements between different parties.

- **La'Quata Sumter [29]**

The authors in this paper identifying whether there is a need for some type of security capture device/ measure on the cloud, which will allow users to know whether their information is secure and safe without comprising by threats and attacks.

This paper would focus on the security measures of cloud computing and this is a critical issue for successful cloud. It focused on two questions: (1) is the cloud computing a security threat to users' information? (2) How will the customer be able to know that their information is secure? To address the above questions, this paper designed a cloud computing lab to identify if there is a need for a capture device on the cloud, which will allow users to know that their information is secure and safe from threats and attacks.

- **Nithiavathy. R& et al [30]**

This paper studied the problem of data security in data storage in cloud servers and it focus about Cloud computing has been the genuine solution to the rising storage costs of IT Enterprises. The data outsourced to the cloud would help in reducing the maintenance.

The user's data are moved from cloud to large data centers, which are located remotely which does not have control over it.

Hence there is a security breach which has to be resolved. To address this issue, this paper proposed an effective method to achieve secure and dependable cloud storage by using distributed storage integrity auditing mechanism, which incorporate homomorphic token and distributed erasure-coded data for dynamically storing data.

The proposed design in this paper use erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. This design allows the user with lightweight communication and computation cost, to maintain reliable cloud storage correctness, and to locate the misbehaving server in which the data are frequently changing in cloud.

- **Mr. Venkata Sreedhar& et al [31]**

Cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the devices used to access these services and applications do not require any special applications, So it is easy to see why the enablers are paving the way for massive adoption of the cloud.

Secure delivery of data has always been the main issue for IT Executives when it comes to cloud adoption, and The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point.

The enterprises will be better off with a long term vision for technology, people, information, legality and security to leverage capabilities offered by cloud computing. The shift into the cloud computing should be planned and it should be done gradually over a period of time.

This paper illustrates Cloud Computing architecture, working and service models and exemplifies homomorphic encryption as a solution for dealing with these serious security concerns for accessing the cloud data, homomorphic encryption schemes which allow the transformation of cipher texts $C(m)$ of message m , to cipher texts $C(f(m))$ of a computation/function of message m , without disclosing the message.

- **Swati P. Ramteke&et al [32]**

This paper focus on privacy data and access control in cloud computing, when moving to the cloud should protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effectual data utilization, a very challenging task.

It is also focuses on proposing deployment architecture of Intrusion Detection Systems in the Cloud, and it discusses and list several existing threats for a Cloud infrastructure and motivated to use Intrusion Detection Systems (IDS) and its management in the Cloud.

This paper proposed a new model for data storage and access in clouds, the model scheme avoids storing multiple encrypted copies of same data. Model designed for secure data storage, cloud stores encrypted data (without being able to decrypt them), and the main innovation of proposed model is addition of Key Distribution Centers (KDCs).

Also this paper proposed a solution which removes the trusted central authority, and protects the user's privacy by preventing the authorities from pooling their information on particular users, thus making Attribute-Based Encryption (ABE) algorithm more usable in practice.

This paper discusses and list several existing threats for a Cloud infrastructure and motivated to use Intrusion Detection Systems (IDS) and its management in the Cloud. The IDS handles large flow of data packets, analyze them and generate reports efficiently by integrating knowledge and behavior analysis to detect intrusions. This IDS integrates knowledge and behavior analysis to increases a cloud's security.

- **G. Murugaboopathi& et al [33]**

This paper highlights the basic concept of cloud computing and some of the security measures which have been taken into consideration till now and study of various security challenges in cloud computing. Also includes various ways which can be implemented for the betterment of cloud computing.

It discussed few reasons which are basically advantage of the cloud computing has become a main concepts on which multiple organizations are working (e.g. Dell, IBM, Sun, Microsoft, Amazon etc.). It is out of reach for most of the organizations and/or individuals to purchase all the required hardware/software resources.

So, using the resources available on the cloud one can perform required task by paying the applicable amount. But, always with popularity security issues come into picture and in this case security involves privacy and consistency of user data, durability of systems, protection from hacking and specially protection of contents which are vulnerable to potential threats.

So, cloud computing must be launched with a strong security system so, that both service provider and user can be benefited. This paper is a study of various security issues in cloud computing and attempts provided solutions to various cloud security challenges.

- **Tanupriya Choudhury & et al [34]**

This paper declared the cloud computing as a recent trending in IT that moves computing and data away from desktop and portable PCs into large data centers. The cloud storage is a relatively basic and widely applied service which can provide users with stable, massive data storage space. A cloud computing provider or cloud computing service provider owns and operates live cloud computing systems to deliver service to third parties.

This paper shows that the architecture of current cloud computing system is central structured one; all the data nodes must be indexed by a master server which may become bottle neck of the system. In this paper, the proposed new cloud storage decentralized architecture (no centralization is there, that's why it's designed in Peer to peer) and designed a prototype system. And it proposed system designed cloud based environment where request and response is taking place between client and chunk servers through Gateway.

- **Jaejung Kim & et al [35]**

This paper declare due to increasing needs of Internet access through smart phones and smart pads, it is essential to have service provider systems, which allows to access services through a variety of devices. In particular, this system is required to protect credential and personal information saved in each

device, is need a more efficient and secure Consolidated Authentication Model (CAM) in order to authenticate a user and devices.

The paper purpose is to suggest a safe and convenient user authentication model that mobile device users can effortlessly use credentials in cloud computing environments. Also it discuss the security and privacy issues of the current user authentication model that are not able to provide credential roaming in cloud computing environments due to the absence of securely available credential protocol in consolidated user authentication method. In order to solve this problem, the paper proposed the secure CAM architecture so that one credential is applicable to various mobile devices in cloud computing environments.

The paper designed the secure CAM architecture in cloud computing environments, which not only provides more flexible authentication framework but also leads to safer credential management in operating various mobile devices such as smart phone, smart pad, etc. and it define framework architecture, credential profile, protocol framework for consolidated authentication mechanism in order to provide an appropriate user authentication model for a cloud computing environments.

- **Josef Spillner& et al [36]**

This paper declares the consumption of online services and cloud computing offerings is on the rise, largely due to compelling advantages over traditional local applications. From a user perspective, these include zero-maintenance of software, the always-on nature of such services, smashups of different applications and the networking effect with other users.

This paper discussed the need for personal cloud control centers and introduced a suitable architecture based on a custom model of cloud elements and activities. Also it proposed a model in two points (1) a user-centric model of cloud elements beyond the conventional including activities across trust zones, and (2) a personal control console for all individual and collaborative user activities in the cloud.

The model in this paper needs focus to increase maintenance of software and attempt to prevent data replication strategies harmfully and determine which data should be replicated.

- **Idilio Drago & et al [37]**

This paper explains the personal cloud storage services are gaining popularity. With a rush of providers to enter the market and an increasing offer of cheap storage space, it is to be expected that cloud storage will soon generate a high amount of Internet traffic.

Very little is known about the architecture and the performance of such systems, and the workload they have to face. This understanding is essential for designing efficient cloud storage systems and predicting their impact on the network.

This paper presents a characterization of Dropbox, the leading solution in personal cloud storage in the datasets. The contributions are threefold: Firstly, this paper first to study Dropbox, which we show to be the most widely-used cloud storage system. Secondly, the paper characterizes the workload users in different environments generate to the system, highlighting how this reflects on network traffic.

Lastly, paper results show possible performance bottlenecks caused by both the current system architecture and the storage protocol. This is exacerbated for users connected far from storage data-centers.

The main advantage in Dropbox protocol is nearly seamless file sharing service, so this paper needs to explain different level of security in dealing with Dropbox and how protect file sharing.

- **SANG-HO NA & et al [38]**

This paper discusses the personal cloud is integrated and federate cloud services and total manage user data. This paper proposes definition of personal information and discusses potential threats through data (Personal Information) flow in personal cloud service.

This paper discusses key function and requirements to guarantee anonymity of user and providing user identifiable information to service provider at the same time. Also define Given Information (PIgiven)which means user information that is voluntarily given, when we join some services, to service providers such as name, id, email address, etc. and Generated Information (PIgen)which means when customer use service, the system generate some user related information for serving or managing. Usually system, for example, generates user activity log file, collect user related information, and store in system.

Finally, this paper proposes simplified privacy evaluation model. And upon the model, the paper discuss which function is needed for privacy preserving in personal cloud and how can we provide anonymity to user.

This paper needs analyze Given Information and Generated Information, how dealing with this information between user and system, and how to keep the information in both security and privacy.

- **Beom Heyn Kim & et al [39]**

This paper declares the people today have more personal data in digital formats than ever before; the average person accumulates gigabytes of digital photos, bills, receipts, e-mails and documents into their personal “digital repository”. As a result, people moved to fill this need by offering both free and paid online storage in the cloud.

Cloud providers store user data on highly reliable systems, which protects the data against both failures in the cloud provider and failures of the user's devices.

This paper focus on unity, it is designed to store personal data across a set of clients running on devices that are owned and administered by the same user, so we assume that all the clients trust each other and execute the Unity protocol correctly.

Unity provides secure and durable storage for personal data that does not depend on the security or availability of a central service. Instead, Unity exploits the trend towards users having more personal computing devices and the increasing amounts of storage available on those devices.

The Unity model in this paper assumes that failures are rare, but this may not be the case with a large number of cheap devices, so this model need to enhance Unity to tolerate failures and how to deal with failure if it happens.

- **Adishesu Hari& et al [40]**

This paper introduce the notion of a Personal Cloud, the Personal Cloud provides an ideal solution for the secure sharing of compute and storage resources across peers in a resource and application agnostic manner, and facilitates new computational paradigms such as datacenter-less, distributed virtual clouds.

This paper provided and implemented solutions for the challenges of managing a Personal Cloud, such as IP address sharing, bandwidth sharing and isolation from local home network traffic. And also propose and implement a provably optimal solution to the resource management problem, allowing peers to share VMs across their individual

Many challenges still exist and involved in moving from the prototype to the operational stage. One open research issue (applicable for any cloud deployment not just the Personal Cloud) is securing the cloud user from the cloud provider.

It is important to create a secure, tamperproof environment for the VMs in the Personal Cloud which prevents the hosting provider from snooping on the contents of the VMs' memory, storage or network traffic.

This paper declare key aspect of the Personal Cloud is the matchmaking or resource sharing aspect, in which individual users express the number of VMs they are willing to host in their Personal Cloud, and the number of VMs they wish to use in other Personal Clouds. And it assumes that the matchmaking algorithm runs in a central entity called the Matchmaker to which individual Personal Clouds submit their individual requests and offers.

We present in this chapter the previous work are dealing with this thesis, they are discussed cloud computing in general, and declare the main challenges in the cloud like security, privacy and authentication.

All literature review are explained that the main problem in all challenges is how to prevent unauthorized user from access to the cloud computing, but did not present a particular method to protection of cloud and how prevent user from access to the cloud.

In this thesis, we proposed method to check the user authority, and present method to the user for secure access to own data and application in the cloud, and then we offer some ideas to the user for how to maintain the data privacy in the cloud.

CHAPTER THREE

THEORETICAL DESIGN



3.1 Introduction

Cloud computing is one of the most rapid growing in information technology, because it enables users to store their data and applications in the cloud and access them wherever and whenever by using any device. So, the cloud authentication is the main problem in new cloud environment and there are many concerns from organizations and individuals about how authentication can be managed.

Password authentication is a common approach to the system security. It is widely used to authenticate an authorized user because user is usually accomplished by employing usernames and passwords when using web browser to access the cloud. The security is reduced when users reuse the same password for different clouds or for different log-in in the same cloud, at the same time; we know that people generally have difficulty in remembering multiple passwords.

In this thesis, we will propose a more efficient security model for cloud computing that helps users to freely choose single password for multiple uses in the cloud. The process in this thesis is generating new password every log-in instead of single password. In other words, it is generating multiple passwords from one password.

The proposed model includes three main components:-

- 1- Cloud user: - the individual user can store his/her data and applications in the cloud, also can access them from anywhere and anytime.

- 2- Third party: - A person who manages cloud server and provide authentication method between user and cloud.
- 3- Cloud application: - It is the application that allows user to enter cloud computing and have full control over cloud.

The model process occurs in third party section which has a list of users-names and users-passwords. When user log-in his/her user-name and password, the model makes sure if the user authorized or not, then third party combine between user-password and counter which calculates the user access times, and generates new password that will be resent to both user and cloud for communication.

The proposed framework for cloud computing model is consisting of two procedures:-

- 1- Authentication procedure.
- 2- Privacy procedure.

Figure (3-1) shows the proposed cloud model and the main steps in each procedure.

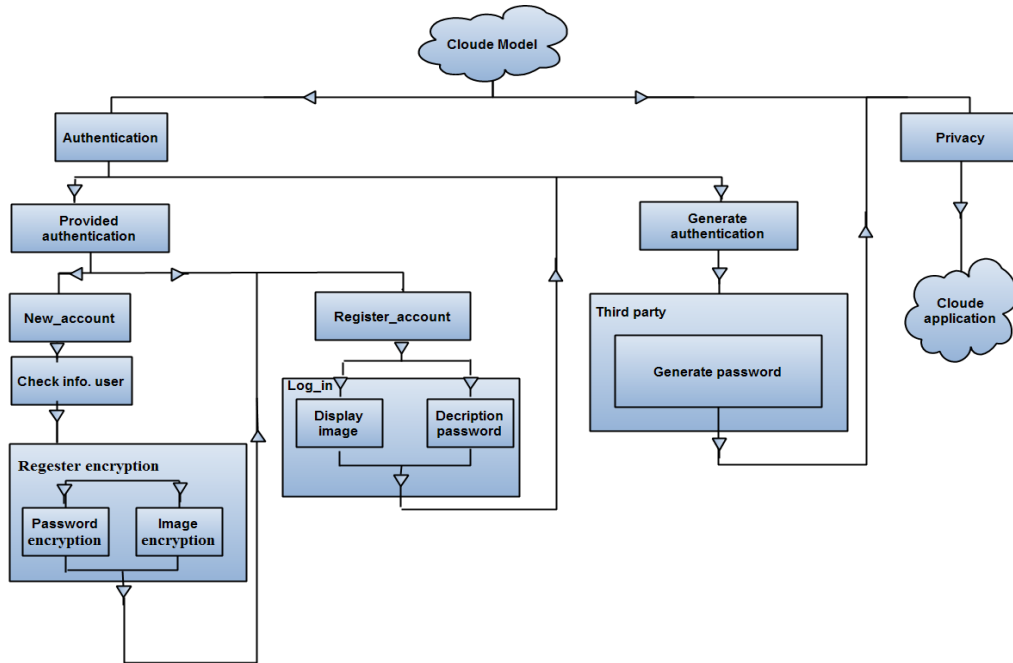


Figure (3-1) ... The proposed Cloud Model

3.2 Authentication procedure

It is the first procedure used to provide authentication between user and cloud, this procedure includes:-

- Provided authentication.
- Generate authentication.

3.2.1 Provided authentication:-

The provided authentication is designed to prove the entered user to the model is authorized, it is including two stages:-

- New-user stage.
- Registered user stage.

3.2.1.1 New user stage:-

The first stage include new-account interface, when the user used the cloud application at the first time, this stage include:-

A. User Identification

User registered information and the system will check his/her information, new-account interface includes:-

- Username field: -the user name is registered and the system check the database if it is registered or not.
- Password field: - the user password is registered and the system checks the strength of the password.
- Confirm field: - user password is reregistered and the system checks confirm field with password field if they are the same or not.
- Email field: - the user email is registered and the system checks the correctness of the email.
- Image: - user selected personal image from personal computer gallery.

B. Register algorithm

User registrations process that includes two algorithms:-

- **Password Encryption algorithm:-**

When the user registers a password in the new-account interface, this algorithm used to encrypt user password and saves it in the database. The model uses this algorithm to protect password from hacker in the database as shown in Figure (3-2).

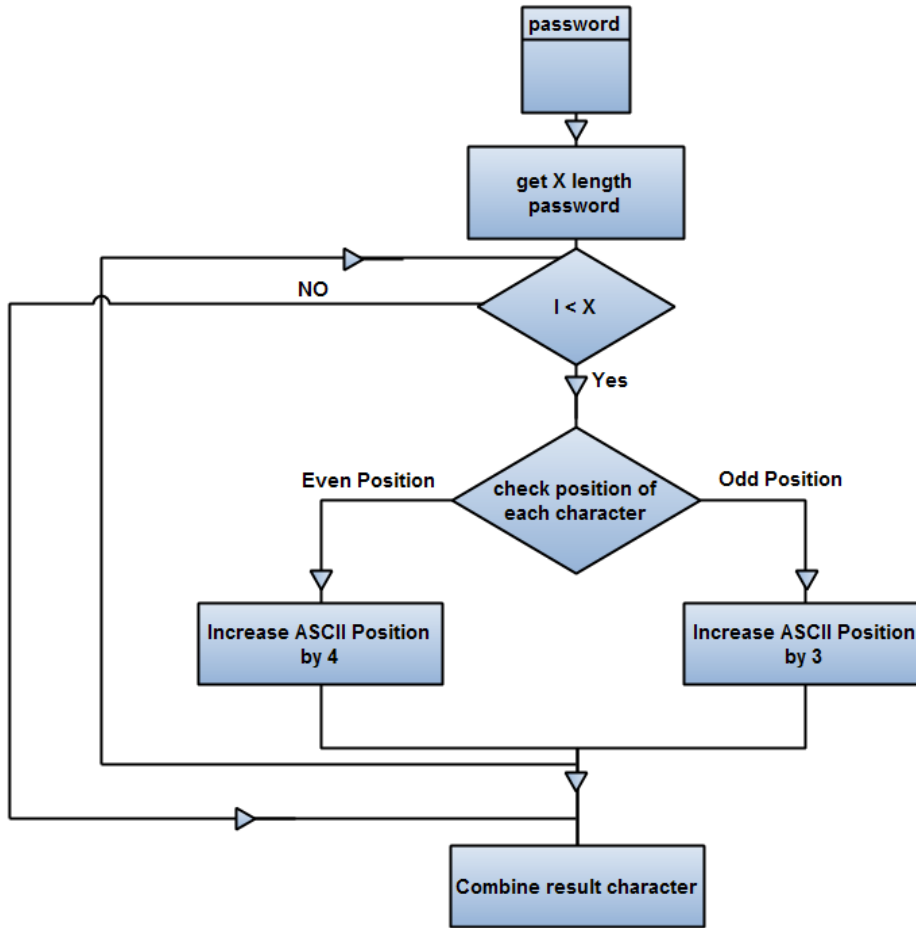


Figure (3-2) ... Password Encryption

Algorithm: Password Encryption (M, N)

// - Input: - password.

- The function of this algorithm is to use the password of the registered user in input and result encryption password in output.
- Segment password in to m, $m = \{m_1, m_2, \dots, m_x\}$.
- Output:- password //

$M \leftarrow$ password

$X \leftarrow$ length of password

Start loop

$i \leftarrow 1$ to X

If i is even Then

$N[i] \leftarrow m[i] + 4$

Else

$N[i] \leftarrow m[i] + 3$

End if

End loop

Return (N).

Example:-

- Variables:-

M= rafal	X=5	i=1 to 5
----------	-----	----------

- Operation:-

i	M[i]	ASCII (M[i])	ASCII (N[i])	N[i]
1	r	18	18+3=21	u
2	a	1	1+4=5	e

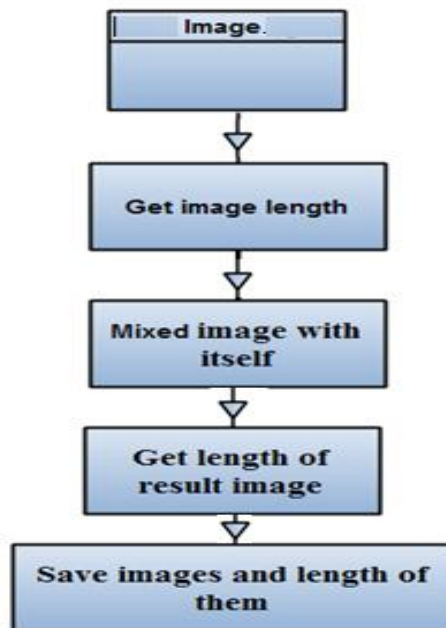
3	f	6	6+3=9	i
4	a	1	1+4=5	e
5	l	12	12+3=15	o

- Result:- ueieo

Return (ueieo).

- **Image Encryption algorithm:-**

When the user register his/her own image in the new-account interface, this algorithm used to encrypt user image and saves it in the database. The model uses this algorithm to increase authentication and defines authorized



user as shown in Figure (3-3).

Figure (3-3) ... Image Encryption

Algorithm: Image Encryption (M, N):-

// - Input: - image.

- The function of this algorithm is to use the image of the registered user in input and result encryption image in output, and save two images and length of them in the database.

- Output:- image //

M ← image

// appends M to M to construct a file with 2 copies of the original image

N ← combine (M, M)

Return (N).

Example:-

Variable:-



Operation:-

Appending two copies of the original image using the oracle command

dbms_lob.append (M, M)



Result:-

3.2.1.2 Registered user stage:-

The second stage include log-in interface to enter user-name and password, the model check them with user-name and password saving in the DB.

If the user is correctly registered, the model will execute the two algorithms:-

- Password Decryption algorithm.
- Image Display algorithm.

If the user is not found, the model gives the user three attempts. If the result is not correct then model will block the access.

- **Password Decryption algorithm :-**

This algorithm is used to decrypt password from database and compare it with password in the interface which is entered by the user, the model uses

this algorithm to check information user as shown in Figure (3-4).

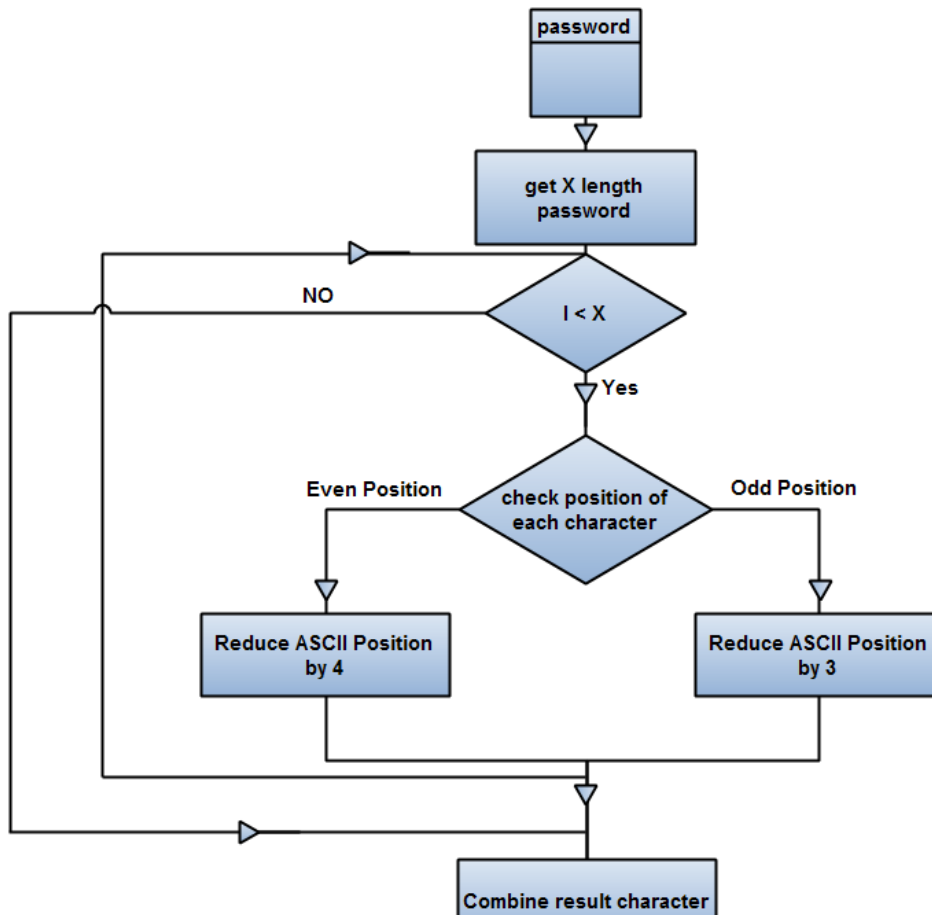


Figure (3-4) ... Password Decryption

Algorithm: Password Decryption (M, N):-

// - Input: - password.

- The function of this algorithm is to use the encrypted password from database in input and result plain password in output.
- Segment password in to m, $m = \{m_1, m_2, \dots, m_n\}$.
- Output:- password //

$M \leftarrow$ encrypted password

$X \leftarrow$ length of password

Start loop

$I \leftarrow 1$ to X

If i is even Then

$N[i] \leftarrow m[i] - 4$

Else

$N[i] \leftarrow m[i] + 3$

End if

End loop

Return (N)>

Example:-

- Variables:-

M= ueieo	X=5	i=1 to 5
----------	-----	----------

- Operation:-

i	M[i]	ASCII (M[i])	ASCII (N[i])	N[i]
1	u	21	21-3=18	r
2	e	5	5-4=1	a
3	i	9	9-3=6	f
4	e	5	5-4=1	a
5	o	15	15+3=12	l

-

Result:- rafal

Return (rafal).

- **Image Display Algorithm :-**

When the model gets sure of the user password, this algorithm is used to show six images in different sequence in the interface log-in and the user determines the correct image. The model compares between the image that is selected by the owner of the account with image saved in the database to the same owner. The model uses this algorithm to amplify user authentication as shown in Figure (3-5).

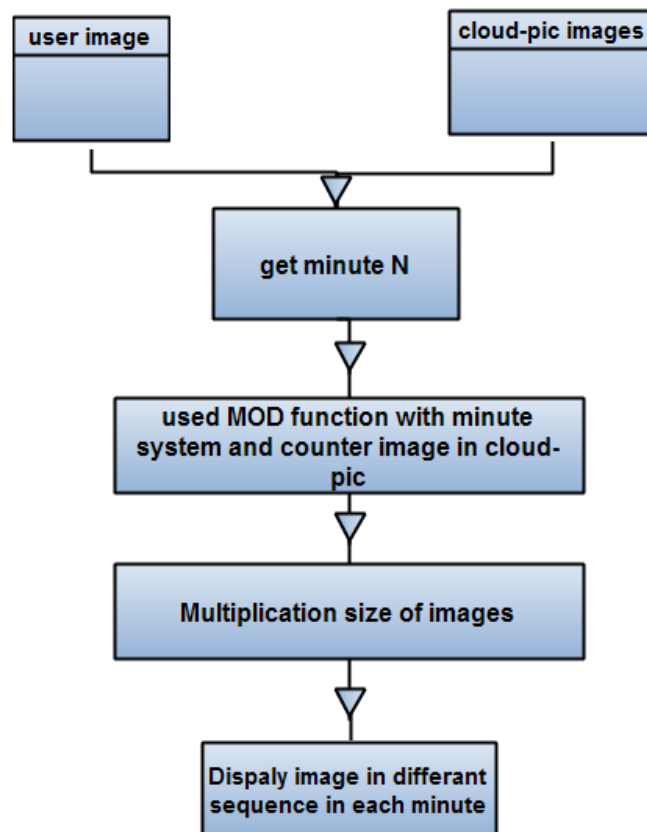


Figure (3-5) ...Image Display

Algorithm: Images Display (M, N):-

// - Input: - images.

- The function of this algorithm is to use five images from cloud-pic and user image in input, and displays these six images in output to the access person.
- Used minute system and counter of images in cloud-pic.
- Output:- images //

M ← images

L ← cloud-pic images

Y ← minute system

Start loop

I ← 1 to 3

Vseq ← Y mod counters (L)

Z[i] ← Vseq (L)

End loop

X ← multiplication size (Z)

N ← X with user image

Return (N)

Example:-

- Variables:-

M	
L	
Y	minute system

- Operation:-

Change the sequence of images using the oracle command

$$(seq = Y \text{ mod counter } (L))$$

- Result:-



3.2.2 Generate Authentication:-

Generate authentications an internal stage in our model, third party is responsible for this stage, and it is controlling two processes:-

- The first process accomplish the previous stages to prove authentication, the third party is receiving the correct image which is selected by the user, and draw back the user image from third- party table which is saved when user registered. And compares between two images, to check the authority of user.
- The second process is designed to generate new authentication to increase trust between user and cloud by generates multiple passwords from one password to each log-in cloud. This process include generate-password algorithm.

- **Generate password algorithm:-**

This algorithm used to generate password for each log-in cloud with counter is selected by third party and resend new password to the user and the cloud as shown in Figure (3-6).

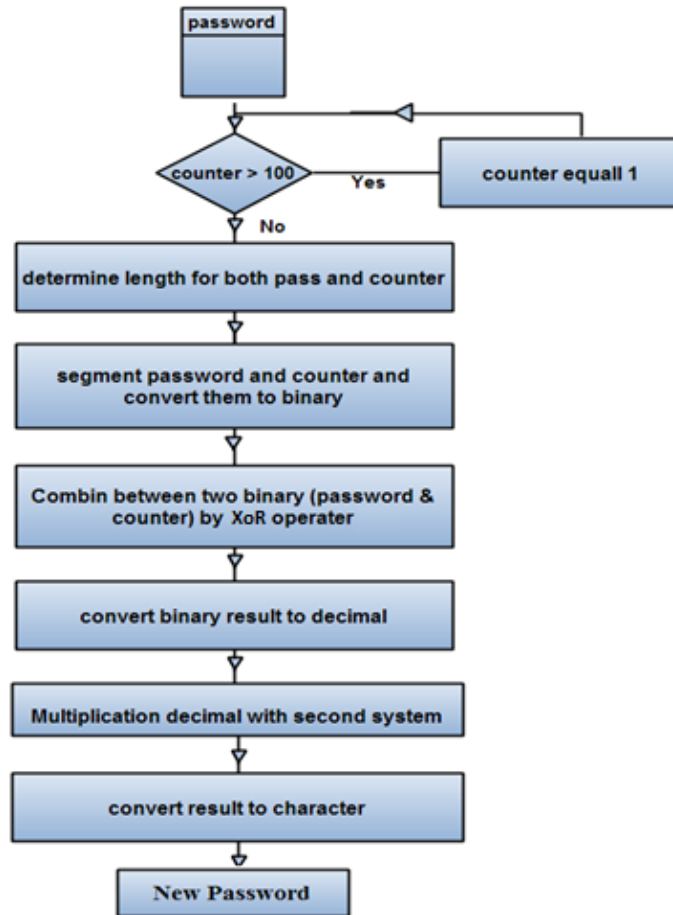


Figure (3-6) ... Generate Password

Algorithm: Generate Password (M, N):-

// - Input: - password.

- The function of this algorithm is to use the original password that is registered by user in input and new password in output.
- Counter from (1 to 100).
- Convert password to numbers and segment it in to p , $p = \{p_1, p_2, \dots, p_x\}$.
- Segment counter in to c , $c = \{c_1, c_2, \dots, c_y\}$.
- Output:- password //

```

M ← password
  Z ← counter

  X ← password length

  Y ← counter length

  J ← 1

  If Z greater than (100) Then
    Z ← 1

  Else

    Start loop
      I ← 1 to X

      Binp[i] ← binary (pi)

      Binc[i] ← binary (cj)

      J ← J + 1

      L ← Binp XoR Binc

      Dec[i] ← decimal (L)

      If J greater than (y) Then
        J ← 1

      End if

    End loop

  End loop

```

Sec ← Dec * second system

N ← convert (Sec) to character

Return (N)

Example:-

- Variable:-

M= ueieo	Z=20	X=5	Y=2	J=1	S(Initial second system)=4
----------	------	-----	-----	-----	----------------------------

- Operation:-

i	M[i]	A=Ascii(M[i])	B=Binp[i]	Z[i]	C=(A XOR B)	Dec(c)	Dec×S	char	N
1	u	21	10101	2	10111	23	23*4=92	92 mod 26=14	n
2	e	5	00101	0	00101	5	5*4=20	20	t
3	i	9	01001	2	01011	11	11*4=44	44 mod 26=18	r
4	e	5	00101	0	00101	5	5*5=25	25	y
5	o	15	01111	2	01101	13	13*5=65	65 mod 26=13	m

- Result:- ntrym.

Return (ntrym).

3.3 Privacy

The log-in cloud is the last stage. This stage includes main interface between user and cloud. When user enters user- name and new password in

cloud interface, it permits user to full control to all data and application found in the cloud.

In this thesis, we use one of the cloud computing service providers. The service provider cloud is called just cloud; many of the process are occurred in this service provider and declared it in chapter four.

CHAPTER FOUR

THE EXPERIMENTAL WORKS



4.1 Introductions

The biggest challenge in cloud computing application is to provide authentication to organizations and individuals users. There are many alternatives to provide authentication. The proposed model attempts to use easy and transparent method, at the same time, it is strong method to protect user from different threats.

Chapter four shows the proposed model for cloud computing and explain its two main procedures:-

- Authentication procedure: - the first procedure is designed to prove and generate authentication, all stages in this procedure are accrued outside the cloud computing.
- Privacy procedure: - the second procedure is designed for ensuring privacy and protects data and application in the cloud computing, all stages in this procedure are accrued inside the cloud computing.

4.2 Execution authentication procedure

The specific user processes in the authentication procedure are occurred between the user and the cloud, this procedure includes:-

- Prove authentication.
- Generate authentication.

4.2.1 Execution prove authentication

The prove authentication is designed to define the user is authorized or not, it is including two stages:-

- New-user stage.
- Registered user stage.

4.2.1.1 Execution new user stage

The user registered new account in the application cloud. When users use this application in the first time, the first interface appears to the user in the application as shown in Figure (4-1).

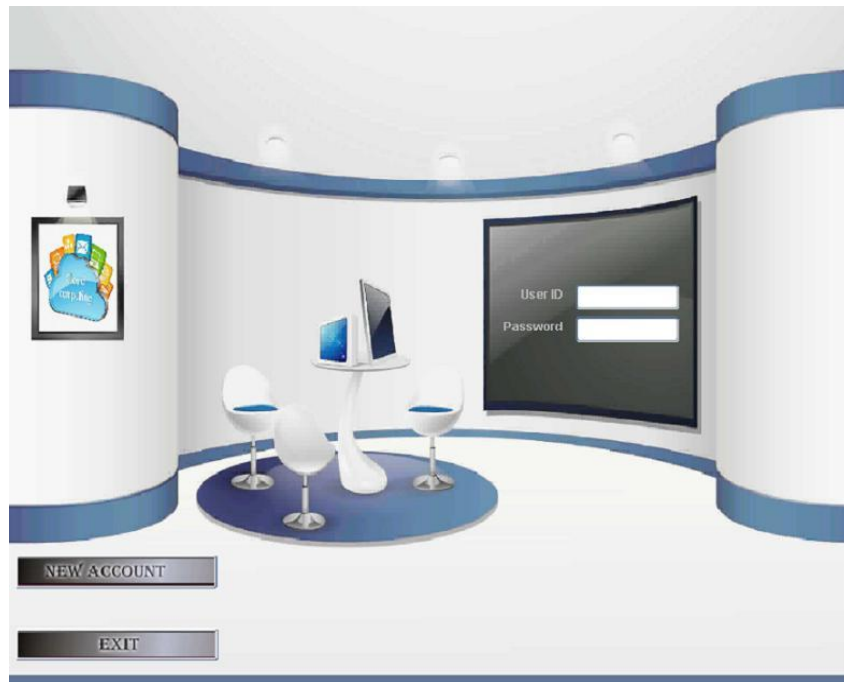


Figure (4-1) ... Main Interface in Application

If the user does not have an account in the application, the user choose the new account button then registered all the required information and upload the image of his/her own as shown in Figure (4-2).



Figure (4-2) ... New Account Interface

After the user is registered his/her information and upload the belonging image, the model will make sure that the information is correct, and make sure if the user is already registered in the model or not by search the user in the sec-user table.

The model is encrypt password and user`s image by password encryption algorithm and image encryption algorithm, then store all the information in the sec-user table as shown in Figure (4-3).

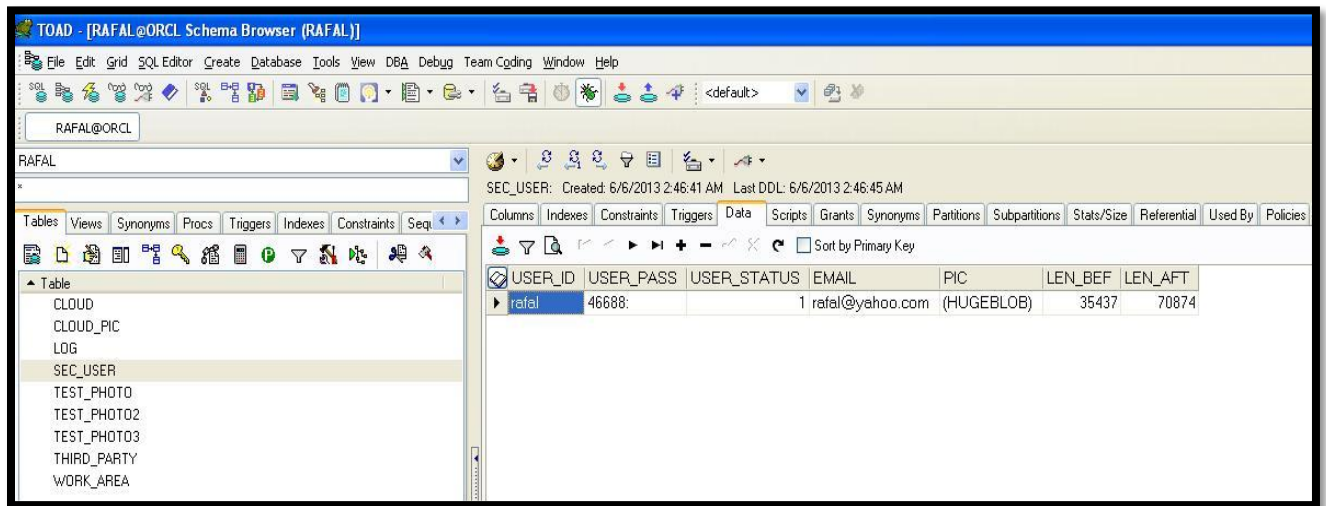


Figure (4-3) ... Sec-user Table

The model is displaying message to inform the user that the registration is successes as shown in Figure (4-4).

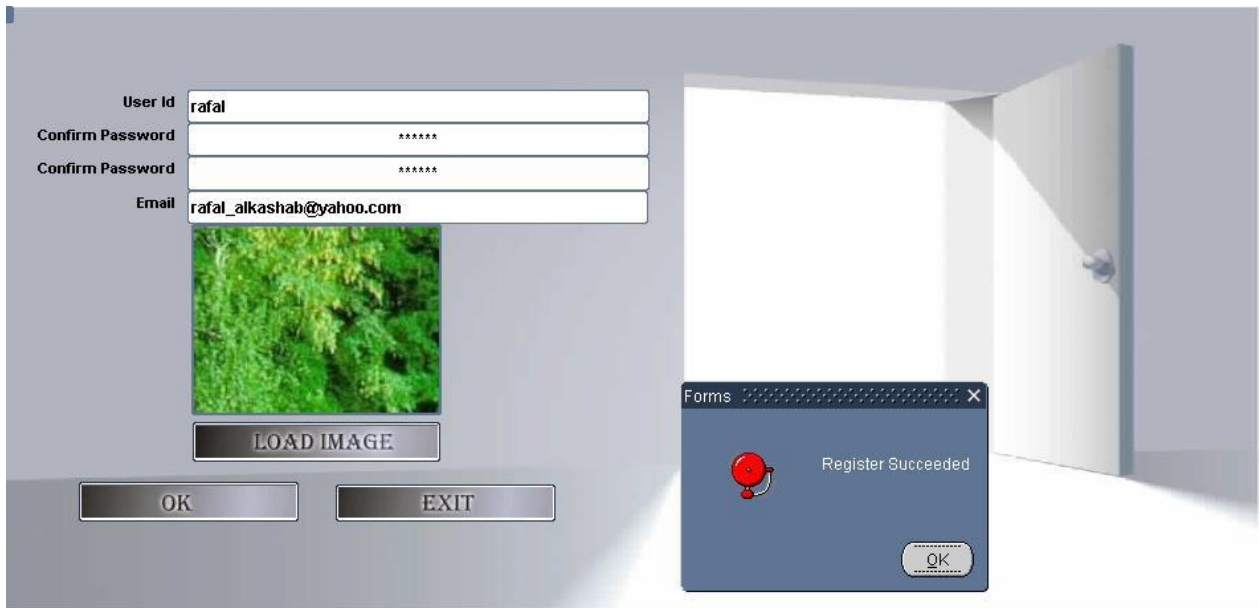
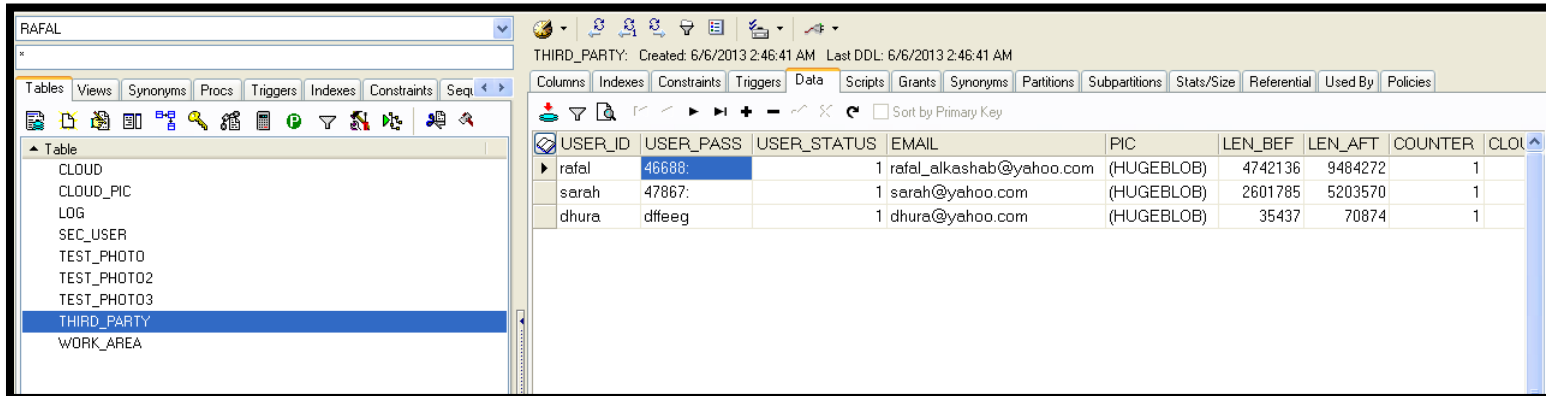


Figure (4-4) ... Successful Registration

At the same time the model is send a copy of all information to the third party table to be used later for comparison as shown in Figure (4-5).



The screenshot shows a database management interface for a table named THIRD_PARTY. The table has columns: USER_ID, USER_PASS, USER_STATUS, EMAIL, PIC, LEN_BEf, LEN_AfT, COUNTER, and CLO. The data rows are:

USER_ID	USER_PASS	USER_STATUS	EMAIL	PIC	LEN_BEf	LEN_AfT	COUNTER	CLO
rafal	46688:	1	rafal_alkashab@yahoo.com	(HUGEBLOB)	4742136	9484272	1	
sarah	47867:	1	sarah@yahoo.com	(HUGEBLOB)	2601785	5203570	1	
dhura	dfeeg	1	dhura@yahoo.com	(HUGEBLOB)	35437	70874	1	

Figure (4-5) ... Third Party Table

After completing user registration, the user will install application cloud computing, installation stages of the application as shown in Figure (4-6).

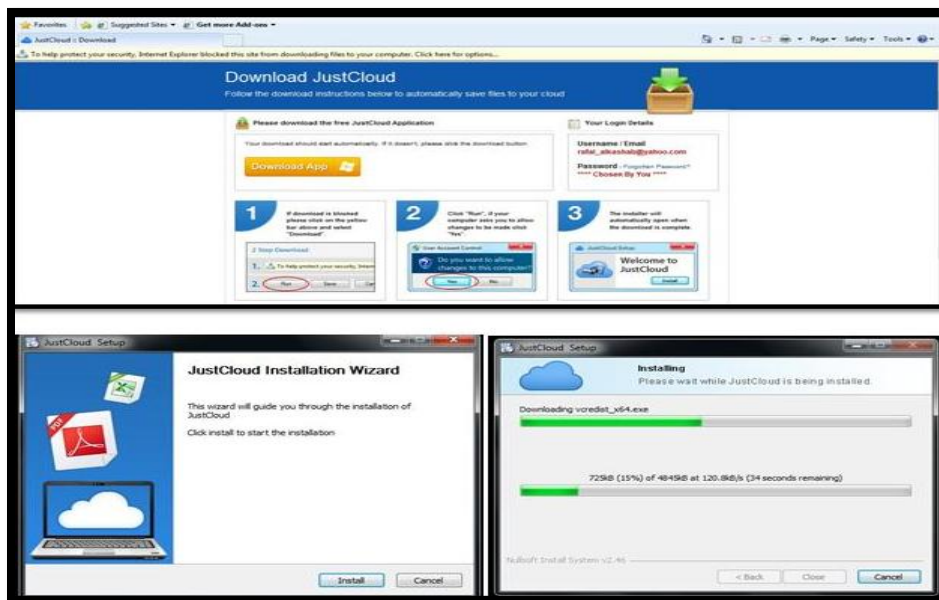


Figure (4-6) ... Installation Stages of Application

The application becomes direct backup from personal computer, the backup may be general and the cloud make copy for all data in the computer, or backup may be custom and select which folder copy to the cloud as shown in Figure (4-7).



Figure (4-7) ... Backup Stages

At the end of installation and backup stages, the cloud application existing in the desktop computer and the user can use this application anytime and only form the computer is install the application as shown in Figure (4-8).



Figure (4-8) ... Cloud Application

The cloud application includes:-

- Backup: - this field includes loading of all new data are exist in the computer.
- Drag & Drop: - this field include loading of specific new data exist in the computer.
- My File: - When user click on this field is going to cloud computing and appear all data are stored in the cloud.
- Restore: - This field shows the data in cloud computing, the user select required data to replay from cloud to computer. For example, if the data is deleted from computer.
- Sync Folder: - this field is open folder on the desktop computer contains the files that loading to the cloud.
- Settings: - this field includes cloud application settings, like: language, backup reports and computer name.
- Help: - this field include just cloud support center.

4.2.1.2 Execution registered user stage

The user can use the cloud anytime and from anywhere. The first interface appear to the user when use the cloud is log-in interface and the user is recorded the required information. Figure (4-9) shows the interface.



Figure (4-9) ... Log-in Interface

When the user registers user-name and password, the user will press enter, the model display a message for the user notice to choose the correct image as shown in Figure (4-10).

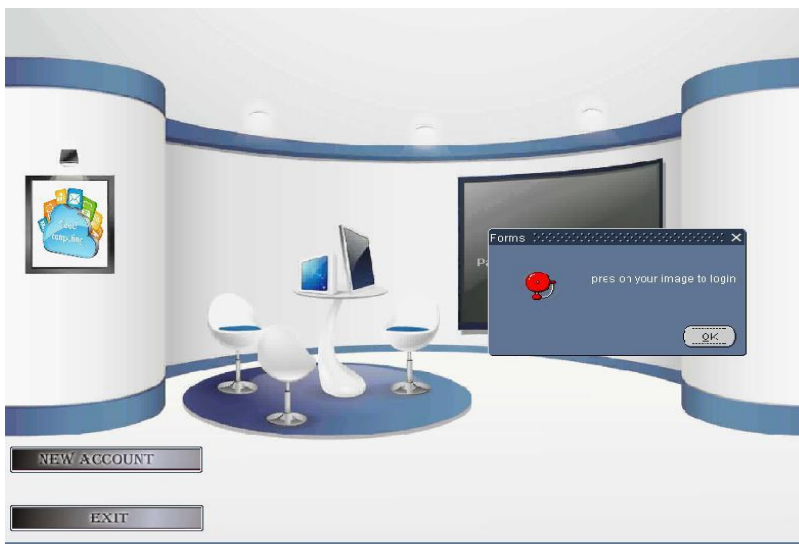


Figure (4-10) ... Notice to the User

Six images are displayed to the user, five images taken at random from cloud table as well as the correct user image as shown in Figure (4-11).



Figure (4-11) ... Display Images

4.2.2 Execution generate authentication:-

When the user chooses the correct image, all the process is transmitted to the third party. The third party makes a comparison between the selected image by the user in the log-in interface with the saved image in the third party table, to determine the user is authorization.

If the user is authorized, the third party generate new password from original password by using generate-password algorithm, and it is display a notice to the user by sending email contains the new password as shown in Figure (4-12).



Figure (4-12) ... Notice Email

In each log-in cloud, the user receives email contain the generated password and the link of the user's cloud, in this case only the authorized user knows the new password. The user used “user-name” and “new password” to log-in the cloud, as shown in Figure (4-13).

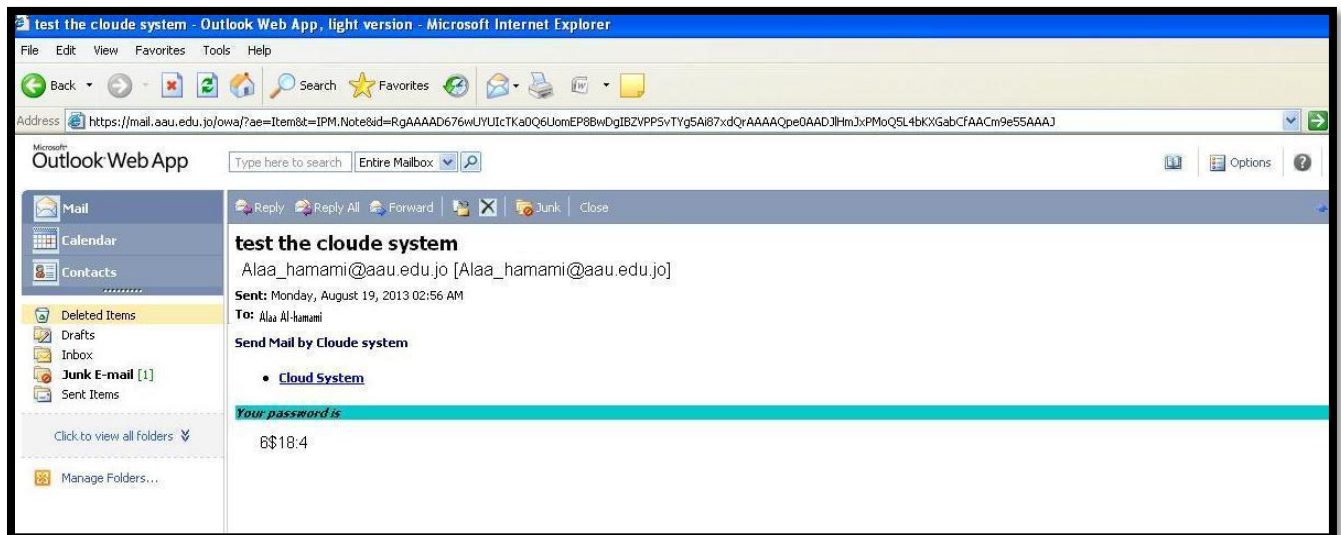


Figure (4-13) ... User Email

4.3 Execution privacy:-

The user will register log-in in the cloud by using “user-name” and “new password” as shown in Figure (4-14).



Figure (4-14) ... Cloud Interface

The main interface in the cloud computing shows all details of files to the user, Figure (4-15) shows the Cloud Details.

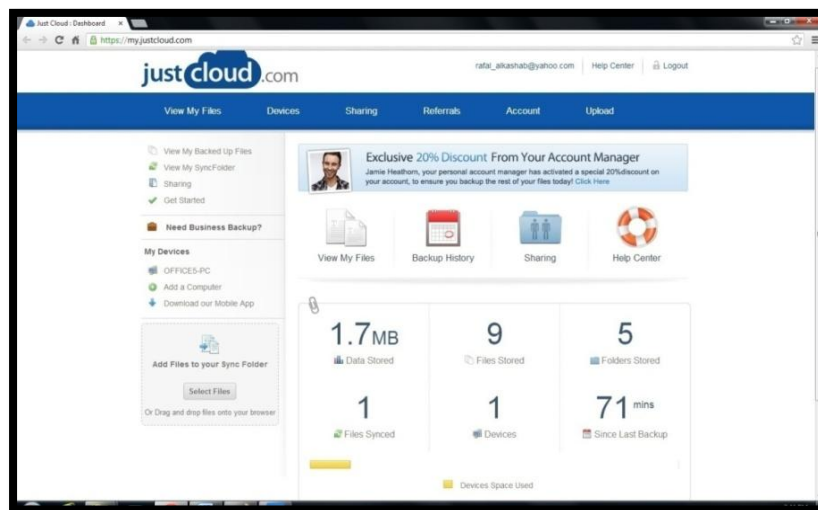


Figure (4-15) ... Cloud Details

This interface include:-

- View My File:- this fields include all files are loading to the cloud as shown in Figure (4-16).

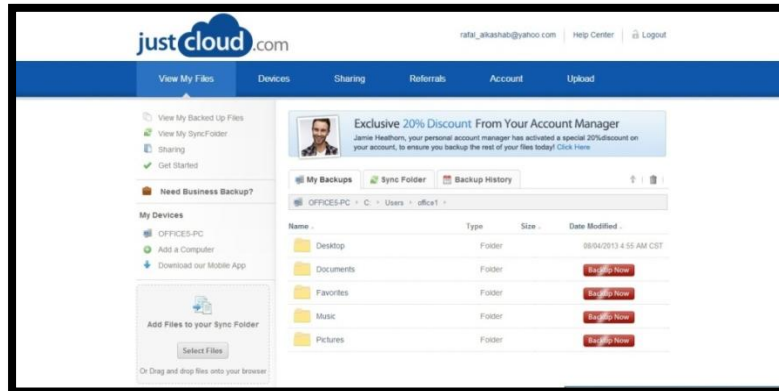


Figure (4-16) ... Files Interface

- Backup History: - this field includes date, time and from any computer the user make backup as shown in Figure (4-17).

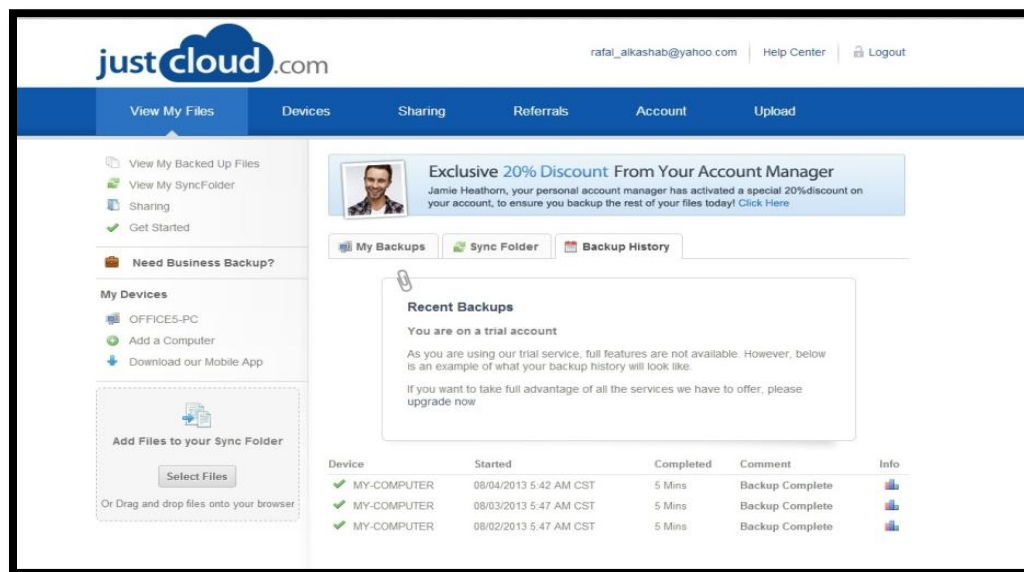


Figure (4-17) ... Backup History Interface

- Sharing: - this field includes share files with other users. When the user clicks on share file button, all files on the cloud will display to the user and the user selects which file is sharing as shown in Figure (4-18).

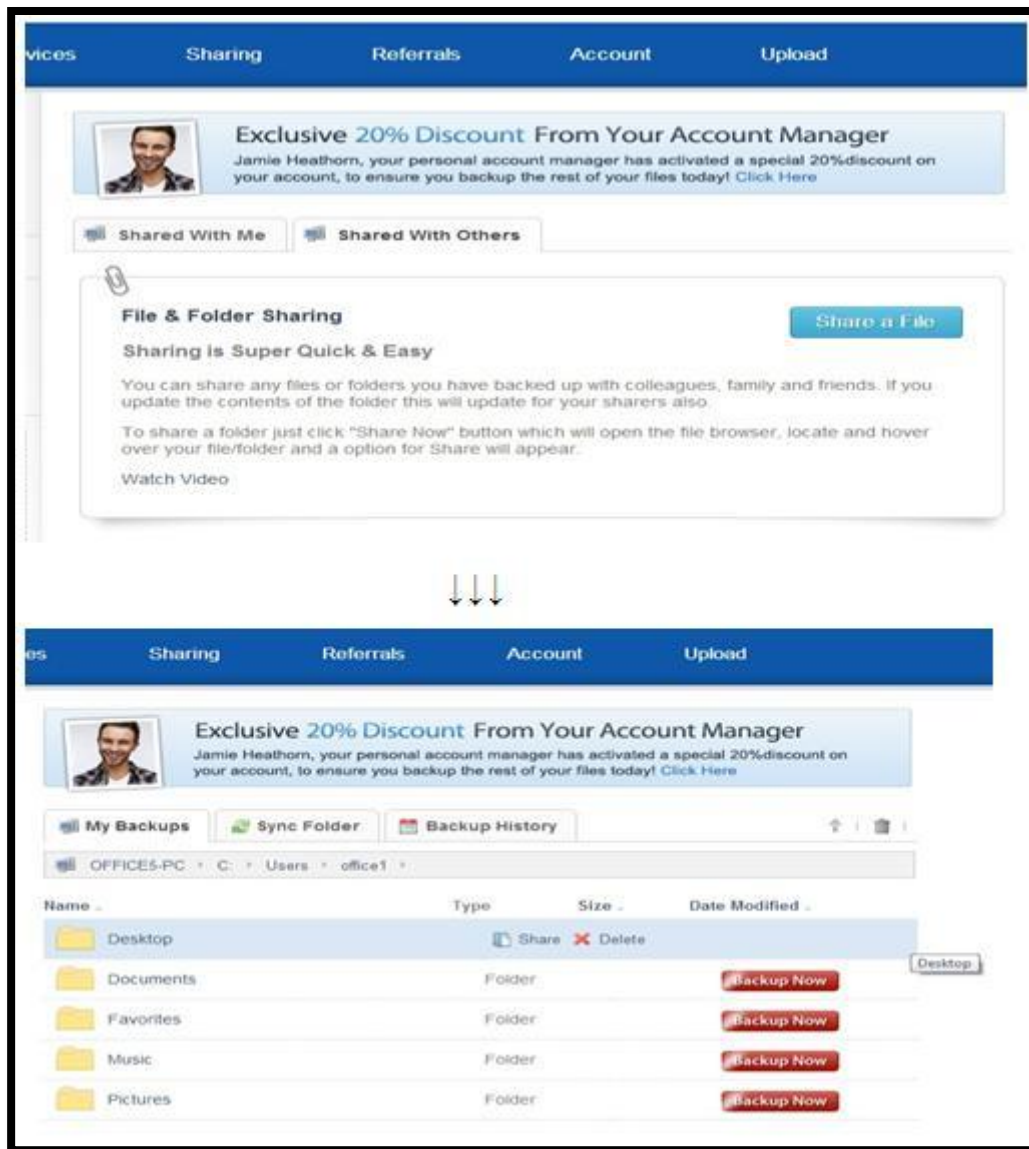


Figure (4-18) ... Share File Interface

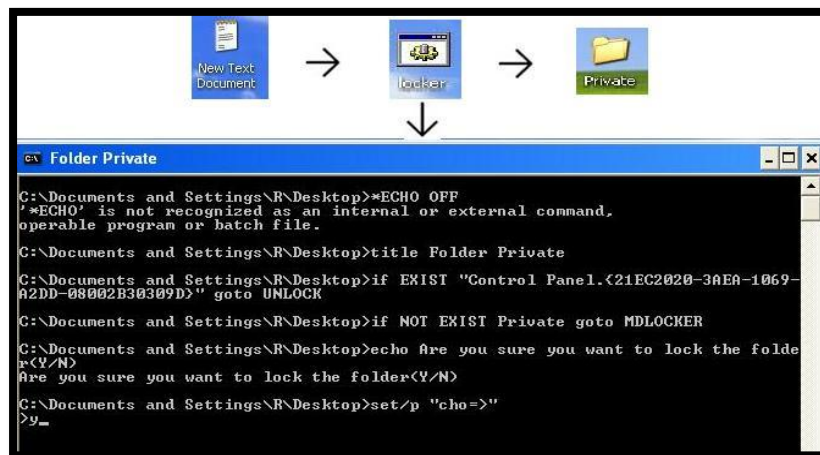
In this thesis, we provide privacy for two types of files:-

- Privacy of Backup files.
- Privacy of sharing files.

4.3.1 Execution privacy of backup files:-

We provide privacy of backup files by using methods to closing important folder before loading to the cloud, when the user needs to show this folder in the cloud must know which methods are used to close folder.

The proposed model uses password method to close folder by writing a set of DOS coding, and written required password in this code in TXT. The TXT is saved as (locker.bat). When click on the locker icon will display the private folder; the cloud user puts all secret files in this folder and hides this folder from appearing by click on the locker icon. Stages of this method appear in Figure (4-19).



The user loads the locker to the cloud embedded secret file. When the user likes to display this file, he/she will click on locker icon to display private folder as shown in Figure (4-20).

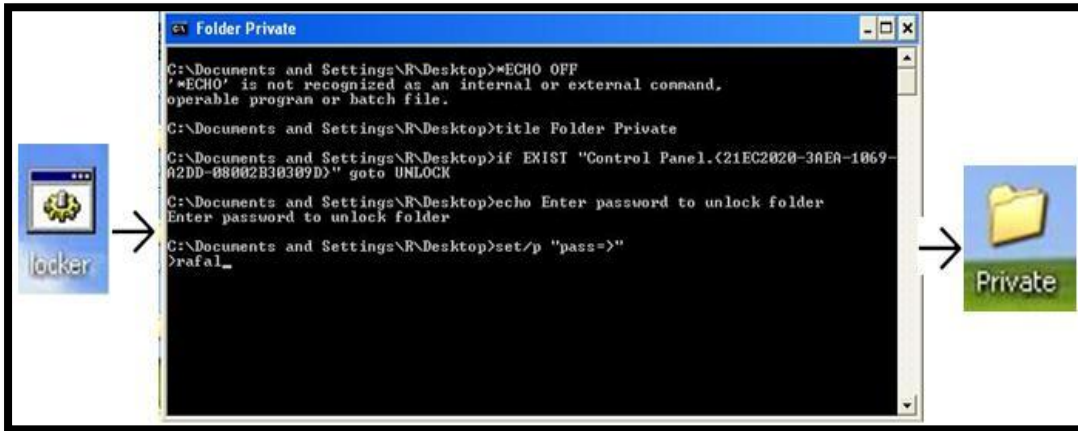


Figure (4-20) ... Stages of Open the Folder Hidden

4.3.2 Execution privacy of sharing files:-

After the user determines which folder should be share of the user will choose the type of sharing files as shown in Figure (4-21).

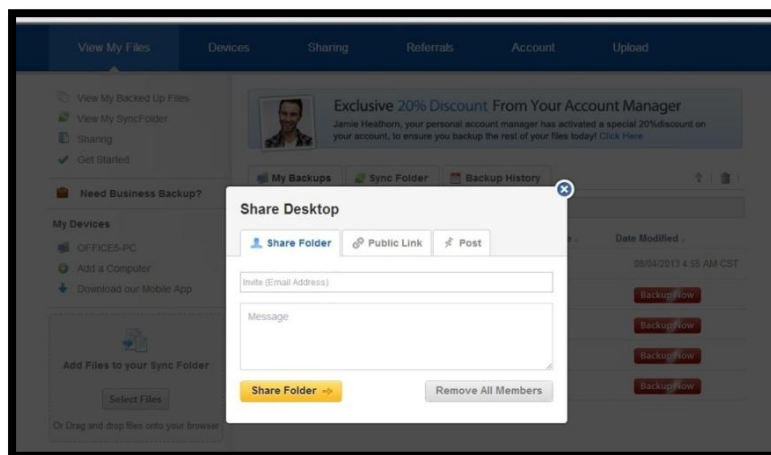


Figure (4-21) ... Share Files Type

The sharing files in cloud computing with other users include:-

- Share folder: - Share file with only one user by sending the link sharing file to the user's email.
- Public link: - put the link of sharing file in public link and any user can show this file.
- Post: - share file by social media like Facebook and Twitter.

The previous type is deployment files by link; we provide privacy of this like by hidden link in to picture or statement as shown in Figure (4-22).

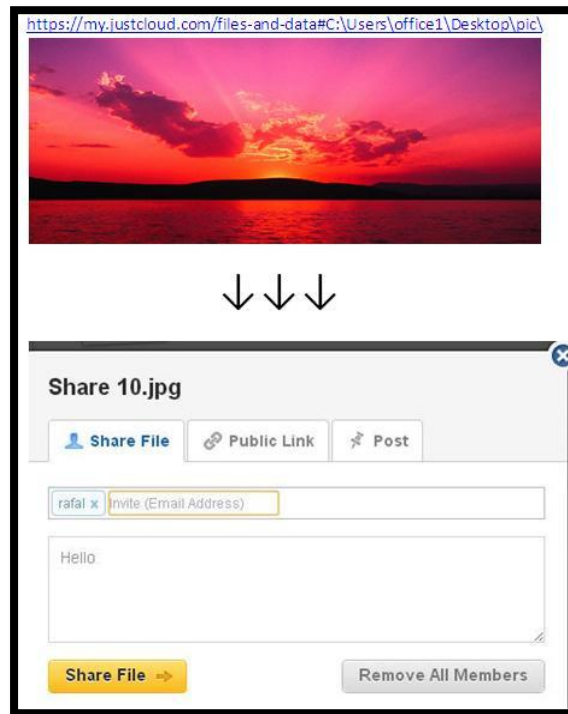


Figure (4-22) ... Stages of Hidden Link

The user sent this picture or statement to the other user, so only the other user is know the hidden link to show the shared file. Figure (4-23) shows an example.

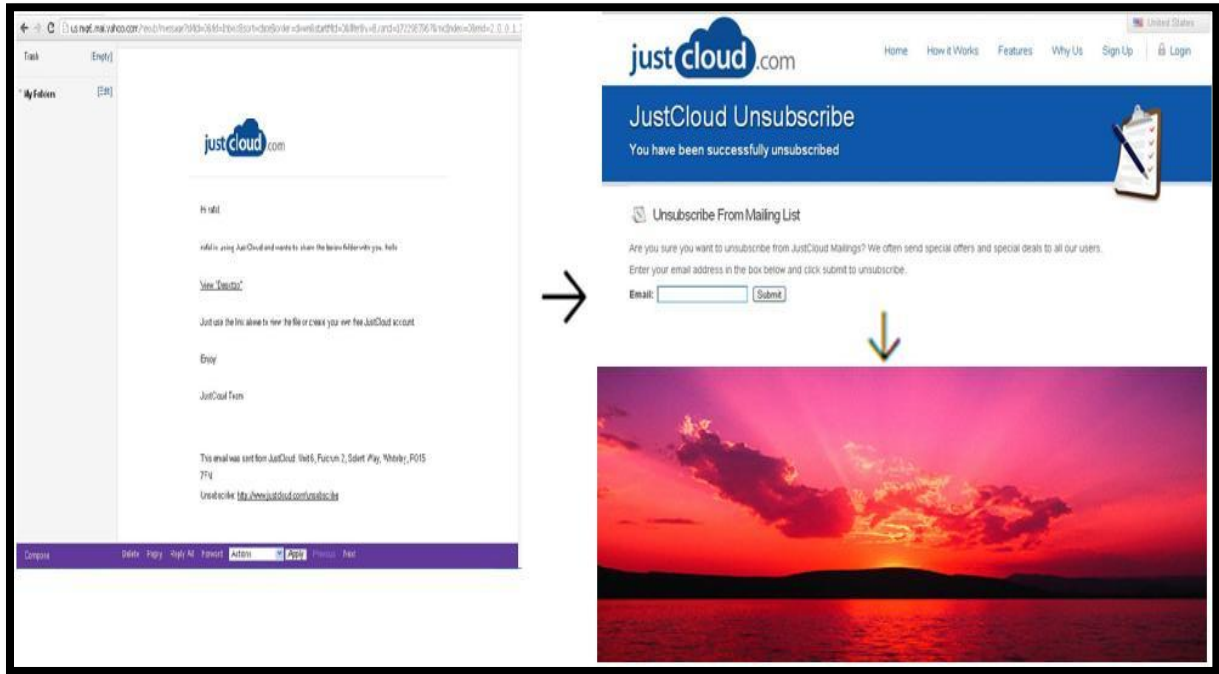


Figure (4-23) ... Stages of Retrieve Hidden Link

CHAPTER FIVE

CONCLUSION AND FUTURE WORK



5-1 Introduction

The cloud computing is a new field in information technology and it is available to organization and individuals. Many researchers are written in this field, and try to declare concepts, advantages and disadvantages dealing with it.

The main problem in the cloud computing is authentication for the users to trust using the cloud. In this thesis we designed a model to achieve cloud authentication and present some ideas for cloud privacy.

In this chapter, we present summarized details of the implemented model in conclusion, and offer some suggestions in future work to develop ideas that presented in the thesis.

5.2 Conclusion

The concept of cloud computing is still unclear to many. Therefore in this thesis we tried to clear the basic concepts of cloud computing such as general meaning of cloud, security issue related it, characteristic, deployment and service model.

While the cloud computing has several benefits, migration to the cloud needs allows users to know that their information is secured and safe from threats and attacks on the cloud. In this thesis we made efforts to provide authentication to show cloud users that their information is secure and they have authority to know who access his information in the cloud.

When we designed the proposed model, we focused on two points, the first point is to prove authentication through image as determined by user, this image is used to proof if the cloud user is authorized or not.

The second point is to generate authentication through using multiple password technique in the cloud; it is a new research field which is gaining interest from cloud users because the probability of brute force attack for breaking the password can be reduced when increase generated multiple passwords from single password.

After the user has access to the cloud computing, we offered some ideas to provide data privacy inside the cloud, and suggested methods to execute these ideas in future work.

5.3 Future work

At the end of the thesis, we offer some suggestion for future work to provide more trust between user and cloud, this suggestion is summarized in:-

1. The possibility of adding one of the biometric authentication types to the identification of humans by their characteristics in addition to the image like finger print and Iris recognition, to more identification of the user.
2. To provide more security for the generated password, the third party can send the new password to the authorized user by the Mobile phone instead of the email. Mobile phone will be used more securely by the user and could be used anywhere and anytime.

3. It is possible to achieve the ideas that presented in privacy session in this thesis by:-
 - Before Backup to the cloud, determine specific part in the cloud by the user, and the user is upload all important data and application to this part. Then identify privilege of the part cloud to determine which users can access to this part, and determine type of privilege to authorized users from administrator like show, alter, add and delete.
 - Before sharing any link in the cloud with other users, the link is hidden in the text or image by one type of the steganography like Least Significant Bit. Then share text or image with the users, so only authorized user knows which steganography method is used through seeing the link.
4. It is possible to enhance the implemented model according to the characteristics of the new deployments model by adding more features and expanding the model.

REFERENCE



[1] Kumar, A.,Ranjan, A.,Gangwar, U. , “An understanding Approach towards Cloud Computing”, International Journal of Emerging Technology and Advanced Engineering, volume 2, issue 9, (2012).

[2] Sun Microsystems, “Introduction to Cloud Computing Architecture”, Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA 1st Edition, White Paper, (2009).

[3] Chowdhury, C.R., Chatterjee, A., Sardar, A., Agarwal, S.,Nath, A., “A Comprehensive study on Cloud Green Computing: To Reduce Carbon Footprints Using Clouds”, International Journal of Advanced Computer Research, Volume 3, Issue 8,(2013).

[4] Dwivedi, S.K., Kushwaha, D.S., Ankit, M., “Security Issues And Resource Planning In Cloud Computing”, International Journal Of Engineering And Computer Science, Volume 2, Issue 2, (2013).

[5] Mohana, R.S., Thangaraj, P., Kalaiselvi, S., Krishnakumar, B., “Cloud Computing for Biomedical Information Management”, International Journal of Scientific Engineering and Technology, Volume 2 Issue 4, (2013).

[6] Buyya, R. , Yeo, C. , Venugopal, S. , “Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities”, 10th IEEE International Conference on High Performance computing and Communication, (2008).

[7]Nafi, K.W., Kar, T.S., Hoque, S.A., Hashem, M.M., “ A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”, International Journal of Advanced Computer Science and Applications, Volume 3, (2012).

[8] Turban, E., King, D., Lee, J., Liang, T., Turban, D., “Electronic Commerce 2012: A Managerial and social networks perspective”, Pearson, United States of America, 7th edition, (2012).

[9] Dhage, S.N., Meshram, B.B, Rawat, R., Padawe, S., Paingaokar, M., Misra, A., “Intrusion Detection System in Cloud Computing Environment”, International Conference and Workshop on Emerging Trends in Technology, (2011).

[10] Munir, K., Palaniappan, S., “SECURE CLOUD ARCHITECTURE”, Advanced Computing: An International Journal (ACIJ), Volume 4, (2013).

[11] Subashini, S., Kavitha, V., “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Application, volume 34, issue 1, (2010).

[12] “10 Security Concerns for Cloud Computing”, Global Knowledge Training LLC. All rights reserved (2010).

[13] Ullah, S., Xuefeng, Z., “Cloud Computing Research Challenges”, 5th IEEE International Conference on BioMedical Engineering and Informatics, (2012).

[14] Rawat, S.S, prof. Sharma, N., “A New Way to Save Energy and Cost-Cloud Computing”, International Journal of Emerging Technology and Advanced Engineering, volume 2, issue 3, (March 2012).

[15] Massadeh, S.A., Mesleh, M.A., “Cloud Computing in Higher Education in Jordan”, World of Computer Science and Information Technology Journal (WCSIT), volume 3, (2013).

[16] Kaur, N., Gagandeep, S., Kaur, M., “A Cloud Computing Against Unified Ontology”, International Journal of Computer & Technology, volume 3, no. 2, (October 2012).

[17] Tiwari, P., Dr. Mishra, B., “Cloud Computing Security Issues, Challenges and Solution”, International Journal of Emerging Technology and Advanced Engineering, volume 2, issue 8, (August 2012).

[18] Boampong, P., Wahsheh, L., “Different Facets of Security in the Cloud”, Proceedings of the 15th Communications and Networking Simulation Symposium, (2012).

[19] <http://www.techopedia.com/definition/26814/virtual-private-cloud-vpc> , accessed by 15/3/2013.

[20] <http://www.neovise.com/defining-virtual-private-cloud-vpc>, accessed by 18/3/2013.

[21] “the coming personal cloud: cloud storage for the rest of US”, Iomega an EMC company, white paper, (2010), http://iomega.com/resources/pdf/pdf_30.pdf, accessed by 1/4/2013.

[22] Srinivasan, J., Wei, W., Ma, X., Yu, T., “EMFS: Email-based Personal Cloud Storage”, 6thIEEE International Conference on Networking, Architecture, and Storage, (2011).

[23] Ardissono, L., Goy, A., Petrone, G., Segnan, M., “From Service Clouds to User-centric Personal Clouds”, IEEE International Conference on Cloud Computing, (2012).

[24] Bhargava, N., Bhargava, R., Mathuria, M., Daima R., “Performance Analysis of Cloud Computing for Distributed Client”, International Journal of Computer Science and Mobile Computing, volume 2, Issue 6, (2013).

[25] Pardeshi, S., P., “Study on Testing as a Service on Cloud”, International Journal of Advanced Computer Research, Volume 3, No. 1, Issue 8, (2013).

[26] Emam, A., H., M., “Additional Authentication and Authorization using Registered Email-ID for Cloud Computing”, International Journal of Soft Computing and Engineering, Volume 3, Issue 2, (2013).

[27] Singhit, L., Ashok, M., “Ensuring Data Privacy and Access Anonymity using Cryptographic Techniques in Cloud Computing”, International Journal of Computer Trends and Technology, volume 4, Issue 5, (2013).

[28] Yu, H., Powell, N., Stembridge, D., Yuan, X., “Cloud Computing and Security Challenges”, 50th Annual Southeast Regional Conference, page 298-302, (2012).

[29] Sumter, L., “Cloud Computing: Security Risk”, 48thAnnual Southeast Regional Conference, No. 112, (2010).

[30] Nithiavathy, R., Suresh, J., “Verification of Data Reliability and Secure Service for Dynamic Data in Cloud Storage”, International Journal of Advanced Computer Research, Volume 3, No. 1, Issue 8, (2013).

[31] Ventrapragada, V., S., Ravuri, D., Jyothi, G., “A Study on Cloud Computing and its Security Issues”, International Journal of Computer Science and Network, Volume 2, Issue 1,(2013).

[32] Ramteke, S., P., Karemore, P., S., Golait, S., S., “Privacy Preserving & Access Control to Intrusion Detection in Cloud System”, International Journal of Innovative Research in Computer and Communication Engineering, Volume1, Issue 1, (2013).

[33] Murugaboopathi, G., Chandravathy, C., Kumar, P., V., “Study on Cloud Computing and Security Approaches”, International Journal of Soft Computing and Engineering, Volume 3, Issue 1, (2013).

[34] Choudhury, T., Vashisht, V., Srivastava, H., “A Secure Decentralized Cloud Computing Environment over Peer to Peer”, International Journal of Computer Science and Mobile Computing, Volume 2, Issue 4, (2013).

[35] Kim, J., Hong, S., “A Consolidated Authentication Model in Cloud Computing Environments”, International Journal of Multimedia and Ubiquitous Engineering, Volume 7, No. 3, (2012).

[36] Spillner, J., Schill, A., “ π Control: A Personal Cloud Control Centre”, arxiv, Volume1, (2012).

[37] Drago, I., Mellia, M., Munafò, M., “Inside Dropbox: Understanding Personal Cloud Storage Services”, Proceedings of the 2012 ACM conference on Internet measurement conference, (2012).

[38] NA, S., HUH, E., “Privacy Evaluation Model for Personal Cloud Service”, Mathematical Methods for Information Science and Economics, (2012).

[39] Kim, B., H., Huang, W., Lie, D., “Unity: Secure and Durable Personal Cloud Storage”, Proceedings of the 2012 ACM Workshop on Cloud computing security workshop, (2012).

[40] Hari, A., Viswanathan, R., “The Personal Cloud— Design, Architecture and Matchmaking Algorithms for Resource Management”, 6th IEEE International Conference on Networking, Architecture, and Storage, (2011).

