Ministry of Higher Education and Scientific Research
University of Diyala- College of Science
Department of Computer Science

Improving Security , Management, Sharing In Cloud Computing

By

Ahmed Mohamed Ahmed

And

Saif Nayef Nasser

Prof. Naji . Sahi

2021 1442

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيم

(إِنَّ اللَّهَ وَمَلائِكَتَهُ يُصَلُّونَ عَلَى النَّبِيِّ يَا أَيُّهَا الَّذِينَ آمَنُوا صَلُّوا عَلَيْهِ وَسَلِّمُوا تَسْلِيمًا)

صدق الله العظيم

[الأحزاب:56]

الإهداء

إلى صاحب السيرة العطرة، والفكر المُستنير؛

فلقد كان له الفضل الأوَّل في بلوغي التعليم العالي

(والدي الحبيب)،

إلى من وضعتني على طريق الحياة، وجعلتني رابط الجأش،

وراعتني حتى صرت كبيرًا

(أمي الغالية)،

إلى إخوتي؛ من كان لهم بالغ الأثر في كثير من العقبات والصعاب.

إلى جميع أساتذتي الكرام؛ ممن لم يتوانوا في مد يد العون لي

SUPERVISOR CERTIFICATION

I certify that the preparation of this project entitled

Secure data Sharing on cloud computing

Prepared by

Ahmed Mohamed Ahmed

Saif Nayef Nasser

Was made under my supervision in the Department of Computer Science/College of Science/University of Diyala and it is part of the requirements for obtaining a Bachelor's degree in Computer Science

Signature :

Name :

Date :

Abstract

The rapid growth of cloud computing is attributed to providence of storage and fixable cloud services according to the users' demands. The owner of data has no complete control on them, because data is being controlled by a third party (the provider of the cloud service).This simplifies the access to data from any place in the world with least cost and time and through any available device as computers, laptops, smart phones and so on, instead of using storage and programs on a local computer.

These services are provided according to the concept of (pay to be used) which made the cloud service providers subjected to more enemies and hackers that may use the cloud for financial purposes. This caused a weakness in the cloud in terms of security and privacy of data safety. Data security represents a difficult issue when the owner of data shares it with a second party named data share on cloud.

Many researchers have addressed this problem through encrypting that uses different methods to encrypt data to provide privacy and security of data storing and sharing over a cloud. A system model is proposed in this project to permit safe and secure data share over the cloud, this is done through adding a third trusted party that provides privacy, safe access to data and controls other parties who send and receive messages. This party also generates a set of (private, public and symmetric) keys in order to be used as an authenticity between the system entities and for files encryption/ decryption processes.

Chapter One

General Introduction

Chapter One

General Introduction

1.1 Introduction

It is possible to define cloud computing (CC) as a model for enabling ubiquitous, suitable and on-demand network access to a shared groping of configurable computing resources that can be provisioned and released rapidly with smallest efforts made by the user side and least interaction by the service provider. It has found its way into a large number of individuals and small organizations as the use of cloud storage has reduced the need to maintain any physical resources. The most commonly used are Amazon S3 and Google cloud [1]. A user has only to pay the fees to access the resources of the cloud storage. Due to this, data sharing has become easy for individuals as well as organizations. They are able to access their data from anywhere anytime without the fear of data loss. But, the use of CC comes with a variety of issues of its own like loss of control over data, security, privacy and confidentiality. Hence, there is a need to secure data not only from unauthorized users but also from the cloud provider. As the

resources are shared, the users need to manage the use of cloud storage to reduce these risks. They need to make sure that data stored on the cloud is accessed only by members of the group to reduce the risk of losing control over that data. Apart from this, the users also need to make sure that the data is being stored and shared securely in the cloud [2][3][4]. One of the widely used options to secure data is to encrypt data using cryptography which provides a wide range of methods to encrypt data and ensure its privacy and confidentiality. Encrypting data before uploading it to the cloud assures privacy from the cloud service provider well. Cryptographic methods involve key management, encryption and decryption processes [5].

1.2 Related Works

Several works are related to the aim of this project, present the security of identity access management and data security in cloud computing as follows:

1) In 2016 More and Chaudhari) [9], proposed a system to promote a safe and secure auditing system for using and possessing abilities like maintaining privacy, Public scrutiny, data integrity, and confidentiality. Consequently, this audit system has been improved by considering the whole of these needs. This system includes several entities: The owner of data, TPA, and cloud server. The owner of data proceeds different processes like dividing the file into blocks, encrypting these blocks, and creating their respective value and sequence create a signature on it. TPA plays a core role in the integrity examination of data by performing activities such as generate fragmentation. The value of encrypted blocks received from the cloud server, sequential and signed. Lately, compare both Signatures to check whether the data stored on the cloud is manipulated. Data integrity is achieved upon request Users. Cloud Server is utilized for saving encrypted data blocks. This audit system uses AES Encryption algorithm, SHA-2 to verify the integrity and signature of RSA to calculate the digital signature.
2) In 2017, (Barela et al.) [10], a key agreement protocol depending on the new cluster design is proposed, which supports multiple users in a flexible and secure manner, supports the schema data share model.

A key agreement protocol was utilized to create a common conference key to multiple users for ensuring information security. This protocol was performed on cloud computing for supporting efficient and secure data sharing. An agreement protocol based on the design of the cluster is proposed, where TPA finds a malicious user from a group, and delete it from the group a tendency to provide generic formulas to generate the K-key for many participants. The error tolerance feature in this protocol allows the sharing of cloud data in the cloud to meet various major attacks. Also, the Diffie-Hellman algorithm is used.

3) In 2017,(Shen et al.) [11], a new set based on design a protocol of key agreement is introduced that supports the sharing of group data in the cloud. Because of the definitions and mathematics structural descriptions a design, many users can participate in the protocol and general formulas for the key to the joint conference Participants are drawn. The protocol can support fault tolerance property, which makes the protocol more secure and practical, and provides more properties (for example, Hide identity, tracking, etc.) to make it applicable A variety of environments, The DiffieHellman algorithm is used.
4) In 2017, (Singh et al.)[12], the paper refers to the method of verifying the integrity of the information stored data in the cloud. In this technique after data encryption, hash is generated using hash function. On the client side, after decrypting the data, each hash is compared with the other hash set to verify the uniqueness of the data.

This verification is that the data has been changed, or the same as the original data stored by the client.

1.3 Problem Statement

The problem statement when Cloud services provider is untrusted third party which provides data storage facilities, computational facilities. Therefore, for taking responsibility-sharing data on the cloud we introduce entry called as **"Third Party Auditor (TPA) "** which is trusted the party and take responsibility of encrypting/decrypting the files, secret key management and send encrypted/decrypted files to entities users and Cloud services provider. This major problem of this work is to design a secure system with high strong secrecy keys.

1.4 The Aim Of project

The goal of this project is to design and implement a system based on Third Party Auditor (TPA) as a reliable party where a key center is generated and distributed to users in the system. And it has ability to manage keys, create secret keys of different lengths and provide a range of services including reliability, confidentiality, It also encrypts, decrypts and shares data between users and protects data sent between customers with a high degree of security through using three types of public, private and symmetric keys using digital signature.

1.5 Outline Of project

In addition to this chapter, this project contains the following chapters:

- **Chapter Two:** this chapter illustrates the general cloud computing principles, the deployment module, service module and cloud computing architecture. As well as detailing characteristic of cloud computing, security problems in CC, risks in CC, challenges of key management in the cloud,
- ➢ **Chapter Three** which presents a description of the proposed architecture system also displays the modules of the proposed system in detail. After that, it explains the proposed algorithms.
- **Chapter Four:** it illustrates the requirements of the proposed system and displays the results of the implementation of the proposed system.
- **Chapter Five:** this chapter gives useful conclusions and some important suggestions for future work.

Chapter Two

Theoretical Background

Chapter Two

Theoretical Background

2.1 Introduction

Cloud Computing(CC) is a kind of computing that contains a set of connected computing nodes, servers, software services, hardware, and applications that are provisioned dynamically to customers. Generally, services are either delivered over the Internet, on private networks or on both. The main goal is to provide secure, reliable and scalable services, platforms and infrastructures to the customers.

2.2 Cloud Computing Principles

The growth of CC attracted the focus of different communities like students, consumers, researchers, businesses and even governmental organizations. Resources and potentials of Information Technology (IT) are provided by CC (e.g. infrastructure, storages, communication, applications, collaboration) via services offered by cloud service provider (CSP). CC is a term of marketing which is also named utility computing transporting the service as infrastructure, platform and software as a service in pay-as-you-go model to users

who ask for it **[19].** The symbol of the cloud inspired the name "cloud", for it is commonly used to refer to internet. The "cloud computing" term refers to the use of a remote data center for the purpose of managing scalable, reliable, on-demand access to applications**.** In a more generic definition, cloud is define as the "data center hardware and software that provide services .The cloud computing denotes a collection of servers and computers that can be accessed by the public through the internet"

The cloud was defined by lots of experts, yet the NIST (National Institute of Standards and Technology) has presented the definition: "a model for enabling comfortable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, storage, servers, services and applications) that can be provisioned and released rapidly with the smallest management effort and minimal interaction by service provider", which is the generally accepted definition. It can be also known as a modern method of computing service over the internet in which dynamically scalable and often virtualized resources are provided **[10].**

2.3 Classification Of Cloud Computing

The service models can be deployed on one or more deployment models such as, public clouds, private clouds, community clouds and hybrid clouds .

2.3.1 Deployment Module

Different models are available, each of which enjoys various characteristics. All models characteristics are given below:

2.3.1.1Public Cloud

The most common A public cloud, or as also known an external cloud the most familiar shape of CC, in which services are made available to the general public in a pay- as-you-go manner. Individual users or enterprises can reach these services over the internet. Many enterprises as Amazon, Microsoft and Google accept and adopt the public cloud as many other. The availability of internet made it possible for anyone to reach the public could **[9].**

2.3.1.2Private Cloud

A Private Cloud, or internal cloud, infrastructure is owned or leased by a single enterprise, and it is operated solely for an organization that serves customers. Most of the private clouds are large companies or government departments. Table (2.1) presents a comparison between public and private clouds. A Private Cloud is available only to a group of people who belong to an organization **[8].**

Table (2.1): Public vs. Private Clouds

Attributes	**Public**	**Private**
Infrastructure Owner	Third party (Cloud provider)	Enterprise
Scalability	Unlimited and On-Demand	Limited to the installed Infrastructure
Cost	Lower cost	High cost including: space, cooling, energy and hardware cost
Performance	Unpredictable Guaranteed Performance	Guaranteed performance
Security	Concerns regarding data privacy	Highly secure

2.3.2.3Community Cloud

A community cloud is a semi-private cloud that is used by a defined group of enterprises with similar backgrounds and requirements that is able to share their infrastructures, thus their scale is increased while the cost is being shared **[7].**

2.4 Architecture of Cloud Computing

Cloud enables better approaches for offering items and administrations with inventive, specialized, and valuing opportunities. As per NIST's Cloud Computing Reference Architecture, cloud computing

impact and influence five large actors along with its security implications. This definition Actors according to NIST Cloud Computing Reference Architecture [3].

a. **Cloud Consumer:** an individual or a group of people that initiate and keep a business association with the supplier of cloud services, and require aid from that supplier.

b. **Cloud Provider:** An organization or an individual involved in providing the services of CC to those who are interested with it.
c. **Cloud Auditor:** an organization that is responsible for conducting an independent assessment for the CC in terms of effectiveness and security of the system.
d. **Cloud Broker:** a third-party person or organization serves as an intermediary between providers and consumers of a cloud. This party

is responsible for discussing terms and conditions of the contract for the purchase of cloud services.[4]

e. **Cloud Carrier:** An intermediary entity, person or organization that provides transport and connectivity of cloud services from cloud provider to cloud consumers.

A full reference architecture of a CC is presented in figure (2.1). An important notion is that the figure shows an end-to-end reference architecture that presents all seven layers of the Open Systems Interconnection (OSI) model, also includes the commercial, governance and business aspects. It is clear that cloud computing is a complex and comprehensive solution of many vulnerabilities [5].

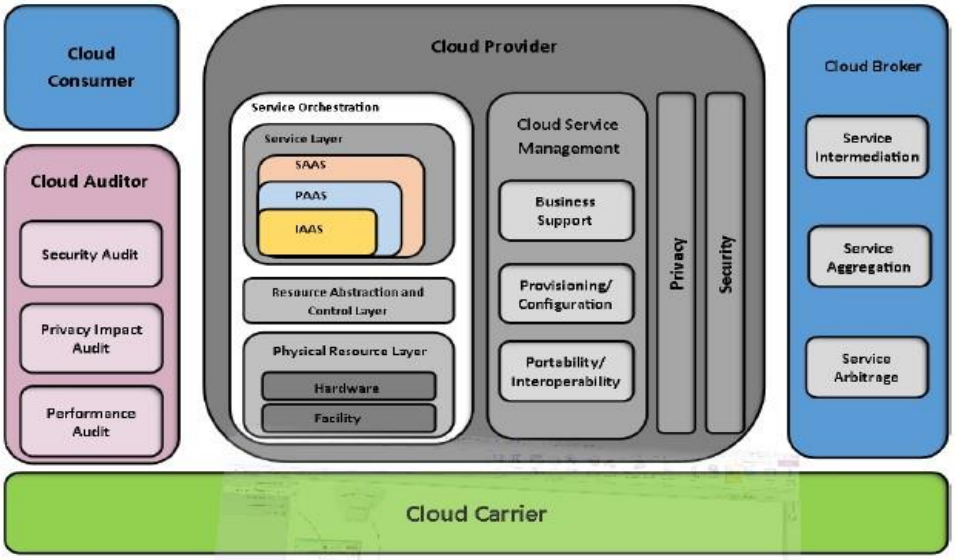


Figure 2.1: Architecture of Cloud Computing [3]

2.5 Characteristic of Cloud Computing

There are five main characteristics of CC defined by NIST as follows [6]:

1. **On-Demand:** CC customers can get the resources of computing by CSP as needed and on demand without the human interaction between customer and CSP. The customers can increase and decrease the resources that provided by CSP .
2. **Broad Network Access:** The customers of CC can access the services from any device that is connected to internet (such as tablets, laptops, mobile phones, and workstations) .[7]
3. **Resource Pooling:** CC resources are shared by multiple customers by use of a multi-tenant model. The customer generally has no control or knowledge over the exact location of the provided resources, but can be able to determine the location (such as state, country, or datacenter). Examples of resources include processing, memory, storage and network bandwidth.

4. **Rapid Elasticity:** By using rapid elasticity property the resources in cloud can be expanded or reduced quickly and efficiently depend on customer demand. This procedure will reduce the cost of cloud computing .

5. **Measured Service:** The amount of cloud resources used by the customer can be automatically and monitored.

The customer can use pay-per-use rather than paying for long-term licenses which are not related with the actual usage and the cloud must provide transparency for both customers and CSPs as well as monitored and controlled the resources used . And there are other common characteristics of cloud computing, they are[6] :

a) Low Cost Software.
b) Resilient Computing.
c) Homogeneity.
d) Geographic Distribution.
e) Advanced Security.
f) Service Orientation.
g) Massive Scale.
h) Virtualization.

2.6 Cryptography

The study of mathematical techniques related to aspects of information security such as entity authentication, data integrity, confidentiality, and data origin authentication is called cryptography. It deals with techniques of transmitting information in a secret manner to protect the information from unauthorized parties, even if the transmission

is done through an insecure channel. The basic types of cryptographic systems are: symmetric key (or secret key) algorithm, asymmetric key (or public key) algorithm and hash function [8].

2.7 Types of Cryptography Model

There are two basic schemes utilized to speed up the cryptographic transformations. The main scheme is to design faster (symmetric or asymmetric) cryptographic algorithms**.**

2.7.1 Asymmetric Cipher Model

It is also known as public-key encryption. One of the cryptosystem forms is asymmetric encryption in which different keys are used in encryption and decryption processes. One of the keys is private and the other is public. One of the keys is used for transforming plaintext into cipher text along with encryption algorithm, while the other key is used to restore the plaintext from the cipher text with the help of decryption algorithm [55].

2.7.2 Symmetric Model:

It is referred as conventional encryption. It is one of the cryptosystem forms in which same key is used for both encryption and decryption processes. Plaintext is turned into cipher text by the symmetric encryption through an encryption algorithm and a secret key. The plain text

is restored using same key and a decryption algorithm. Symmetric cipher is made of two wide categories: block cipher and stream ciphers[5].

2.8 Key Generation

Key generation is the process of generating keys for cryptography. The key is used to encrypt and decrypt data whatever the data is being encrypted or decrypted.

2.8.1 Chaotic maps:

a chaotic map is a map that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems.

2.8.1.1 The logistic map [6]:

It is a paradigmatic representation of chaotic mapping. Even if the logistic mapping is one dimension, however, the reaction of control is considered ideal. The logistic formula can be expressed as following:

$$x_{n+1} = \lambda x_n(1 - x_n)\ (n = 0,1,2, \dots) \quad (2.1)$$

In the equation, $\mathbf{X_n}$ is symbolized to the variable, also λ is an indication of system parameter whereas $\boldsymbol{\lambda \in (0,4]}$, $\boldsymbol{x_n \in [0,1]}$.

Chapter Three

Design and Implementation of the Proposed System

Chapter Three

Design and Implementation of the Proposed System

3.1 Introduction

The current chapter illustrates the proposed system model used for improving the security and sharing management in cloud computing, Finally, an explanation of the proposed system algorithm.

3.2 Proposed System Model

The proposed system model for safe data sharing on cloud computing with intension to provide data confidentiality and access control over shared data, it also removes the burden of key management and files by users. The system also supports dynamic changes of membership and enables clients to reach the data. they require even when the owner does not exist in the system.

3.3 The Entities in Proposed System

The Entities in Proposed System consist of three parts : CSP, Users (owner ,clients) and TPA. Following is a detailed explination for each:

1) **CSP:** Untrusted party provider store facilities and sharing data maintain access control list (ACL) assigned by users and based on that control access of encrypted store file .This list is sent by the owner, which includes a list of all clients who want to access some files stored in CSP

as shown in the table (3.1) as well as CSP will store a table containing all

the information about all owners who want to access certain files in the system and as shown in the table (3.2) and also maintains a list of all Files uploaded by the user as shown in the table (3.3) .A cloud storage server (CSS) is managed by cloud service provider (CSP) through which spaces is provided to the user to store data and compute it. The CSP, who controls the management of cloud servers (CS) and provides a paid storage space on its infrastructure to consumers. Servers are geographically distributed on vaious locations. The principle of the servers in the cloud computing is virtual servers because the location of the required service remains unknown for users.

Table (3.1) Access Control List

File ID	Client ID	Access Control

Table (3.2) Owner Information

Owner ID	File ID

Table (3.3) Last Update On File

File ID	Last Update by

2) **Users :** Users of the system is divided in two types:

a) **Owner:** person who wants to share own data to other persons and also wants to assign access rights to persons access control list (ACL) is

assigned by owner to CSP based on shared data. As shown in the table (3.1) that includes a list of (id) for each clients and a file that he wants to access by owner to CSP .

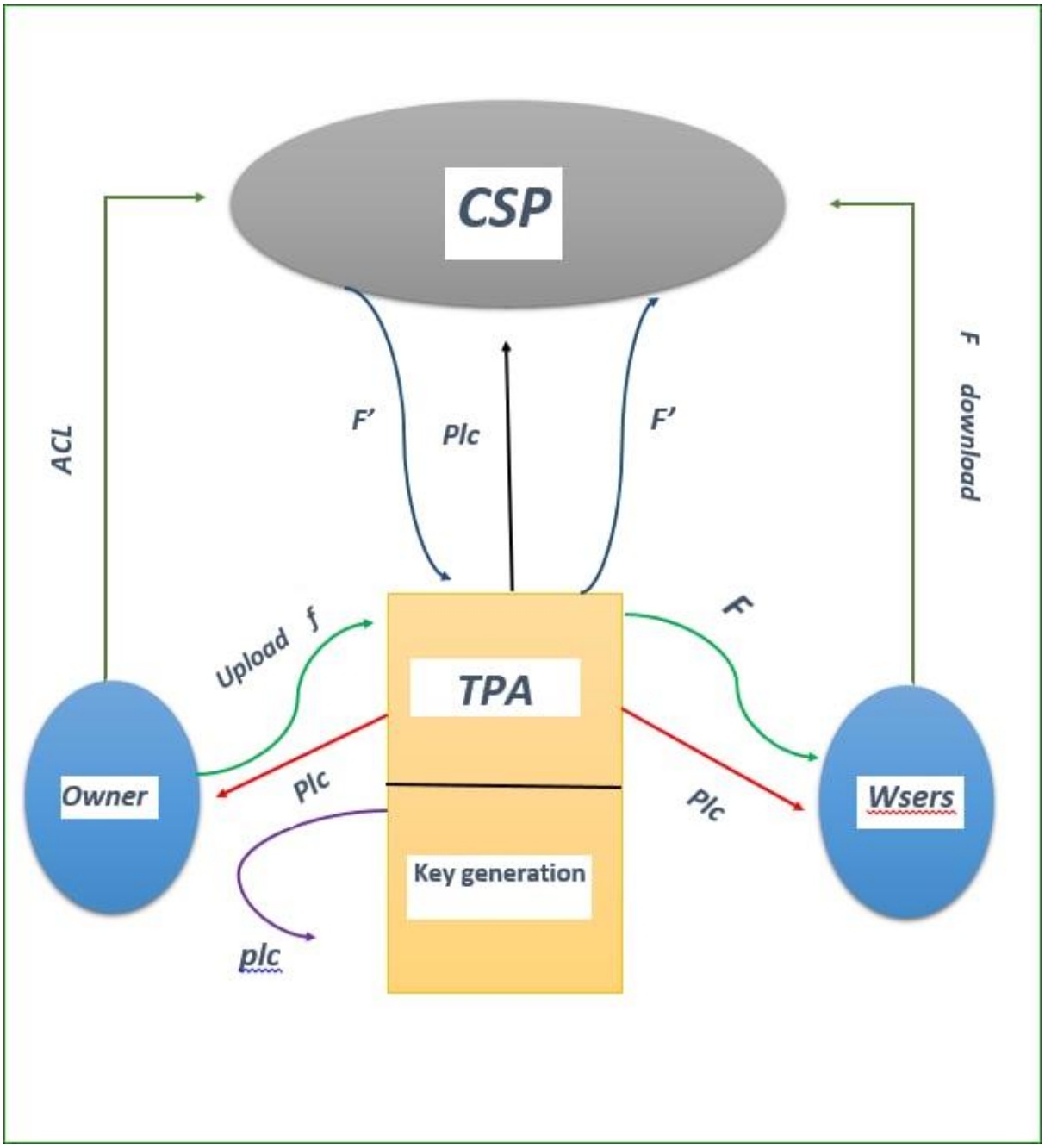
b) **Clients:** significant amounts of data are owned by clients, who want to stroe them on the cloud that relies on cloud storage server for data maintenance and computation. A clients are either organizations or individual consumers. and wishes to upload file and download file it into the CSP for ease of sharing or for cost saving. Can access and share data or downloaded or stored or lifted from the CSP through its registration system through which owner sends a list of all clients data within the system .

3) **TPA:** Trusted party that takes all responsibilities of key generation and management of the key encrypted / decrypted of shared files. Therefore, it is responsible for the generation and distribution of keys within the system, making it the main part in the design of the system where it provides security, confidentiality, reliability and credibility in the process of encryption and decryption of files uploaded to CSP. and management keys and sharing and maintain the confidentiality of users. used for authentication (digital signature) for each user within the system.where Encryption files uers into a form cannot be easily understood by untrusted CSP.i t is used for authentication (digital signature) for each user within the system by creating the private keys that it uses in the digital signature as

reliability varies from file to file and generating symmetric keys to encrypt files and send them to CSP so that the files cannot easily understand easily by CSP because it is untruest . And also decrypt file by symmetric key, show that in table (3.4).

Table (3.4) File Symmetric Key Information

File ID	Owner ID	Symmetric Key



3.4 Key Generation

The strength of any generation is based on undeniable quality of its output .

Indeed which any way the generator is designed, the product sequences must be strong . the proposed system required the generation of three types of keys: i.Public keys . ii. Private Keys . iii. Symmetric key .

3.4.1 Public keys

To generator public keys ,we use the **logistic map** $F(a,x_{n)}$ defined by the equation (2-1) .Figure (3.2) shows public keys generator

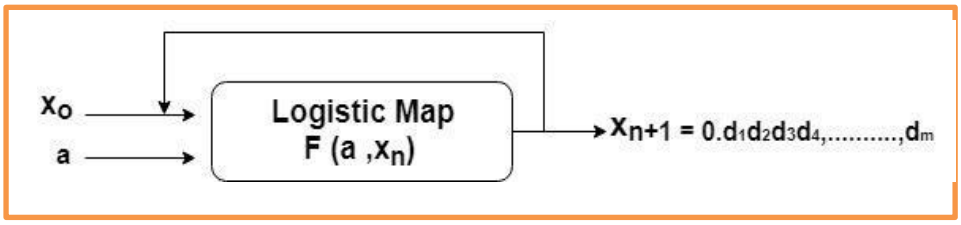


Figure (3.2) Public Keys Generator

Algorithm (3-1) Public Keys Generator

Input: logistic maps, a, x_o, m and k **Output :** Public keys and private key

Step 1: specify the number of Public keys required which equals to the numbers of users, let it is (m) .

Step 2: specify the length of Public key, let it is(k).

Step 3: using the logistic map (2.1), to generate (m) random numbers. **Step 4:** choose from the random numbers generated by the steps public keys with length (k).

The table (3.5) shows how to choose the public keys from the outputs of the logistic map, depending on the value of k.

Table (3-5) public key

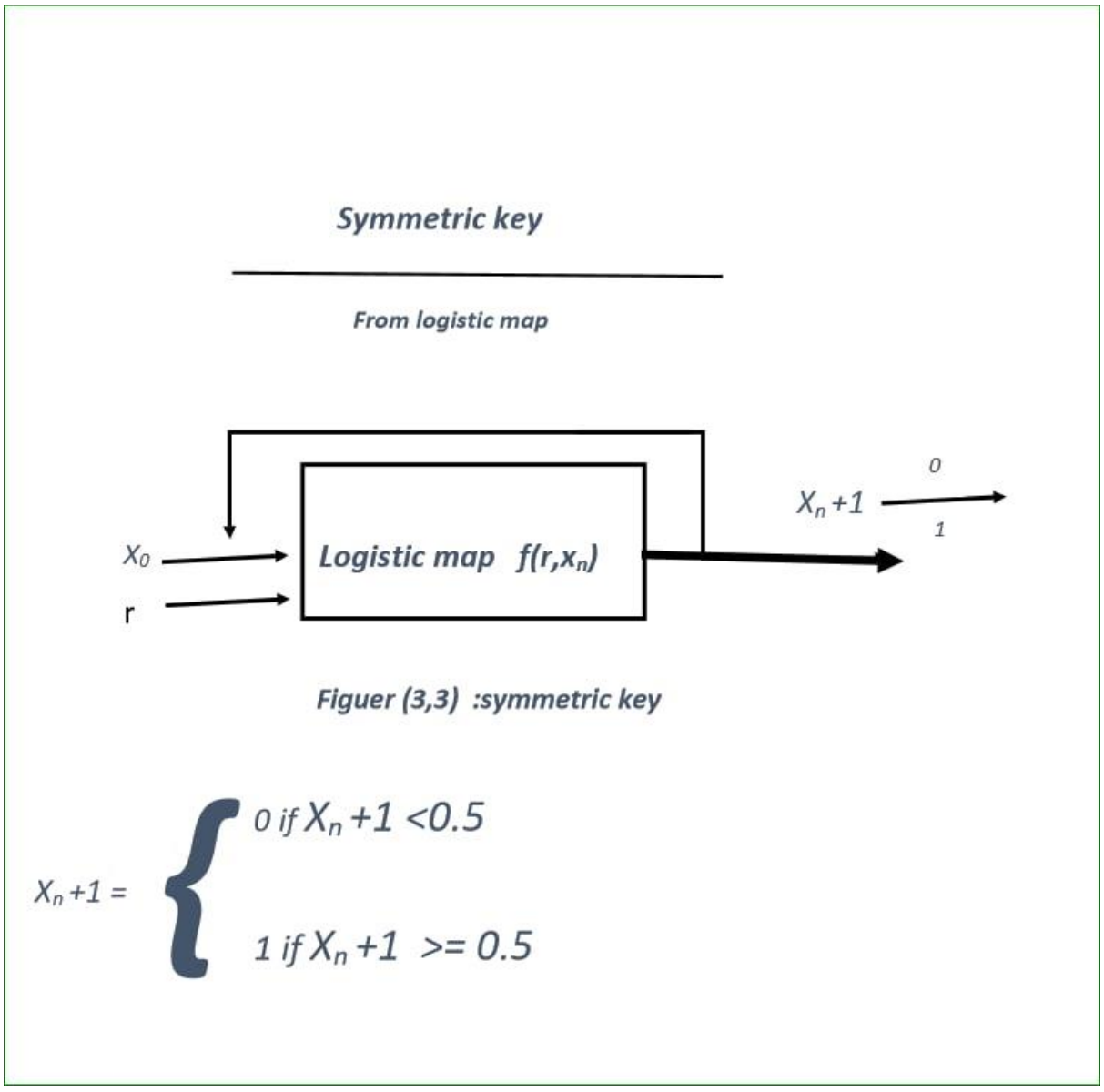
M	X_{n+1}	public keys		
		K=2	k=3	k=4
1	$0.d_{11}d_{12}d_{13}d_{14}$	$d_{11}d_{12}$	$d_{11}d_{12}d_{13}$	$d_{11}d_{12}d_{13}d_{14}$
2	$0.d_{21}d_{22}d_{23}d_{24}$	$d_{21}d_{22}$	$d_{21}d_{22}d_{23}$	$d_{21}d_{22}d_{23}d_{24}$.
.	.	.	.	
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
M	$0.d_{m1}d_{m2}d_{m3}d_{m4}$	$d_{m1}d_{m2}$	$d_{m1}d_{m2}d_{m3}$	$d_{m1}d_{m2}d_{m3}d_{m4}$

Where (m) the number of users' and (k) the length of public key because logistic map are highly sensitive to initial conditions (X_O) and (a) the public key can be changed for simplicity.

3.4.2 Private Keys

To generate private keys , we use the equations

(Pk*Pr)mod K=1



Figuer (3,3) :symmetric key

3.4.3 Symmetric Key

We choose two logistic maps which are **piecewise liner chaotic maps** as shown in the figure (3.3) .

The output obtained by the 1st logistic map is fed to the 2nd logistic map as the input (initial condition) and vice user .

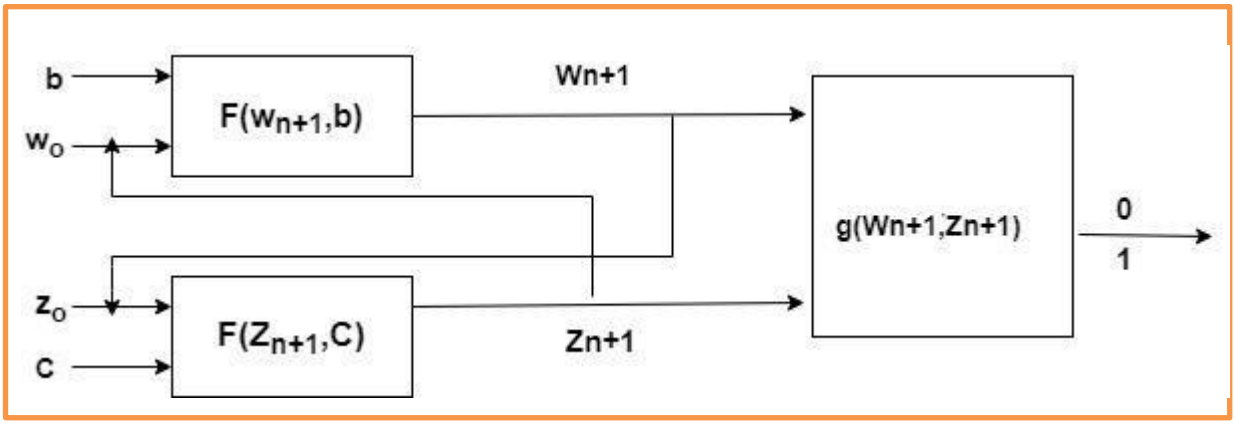


Figure (3.3) The Block Diagram of Random (K)

Where **g(Wn+1,Zn+1)**

0 **If Wn+1< Zn+1**

1 **other wise**

Decryption

3.5 Encryption / Decryption

To encrypte file (F), symmetric encryption is used with the symmetric key (k) generated in the system shown in the figure (3.3). equations (3.3) and (3.4) are used for encryption and decryption.

Encryption : $F' = F \oplus K$ **(3.3)**

Decryption : $F = F' \oplus K$ **(3.4)**

Where F′: cipher text file , F: plaintext , K: symmetric key and $\oplus$: XOR.

Chapter Four

Results and Analysis

Chapter Four Results and Analysis

4.1 Introduction

In this chapter, the implementation results obtained by the proposed system described in detail in Chapter 3 are summarized. The experimental results and tests of the system phases are also illustrated. Additionally, this chapter shows the performances evaluations of the security and integrity of information when a file is uploaded, downloaded or updated in cloud computing and verification system. It also contains a detailed depiction of the steps involved in application implementation.

4.2 Implementation Environment

The proposed system is implemented in Microsoft Visual Studio 2013 Visual Studio programming language (C# ,Asp.net) and the database (SQL server 2008 R2) using a laptop computer. The experiments were performed on an Intel (R) Core (TM) i5-4210U CPU M 380 @ 2.53 GHz, 64 bit Operating System and 8GB RAM. In the following sections, the detailed steps and implementation results will be explained for each step to accomplish the suggested system.

46

4.3 Datasets

The implementation and testing are applied on the database (SQL server 2008 R2), where Structured Query language, known as the SQL acronym, SQL Server 2008 is a strong system used for creating and managing relational database management systems (RDBMS). In most relational databases such as SQL Server, data can be reached through SQL Query Language or Structured Query Language, which allows users to query data as well as add, edit and delete database records. Detail on this language, in addition to dealing with data using C # database, Microsoft Reporting Services Reporting Services.

4.4 Proposed System Implementation

The following figure (4.1) shows the window and the main entities of the proposed system. The Proposed System implementation consists of Users Registration (Owners, Clients), CSP and TPA. The system implementation is explained in details.

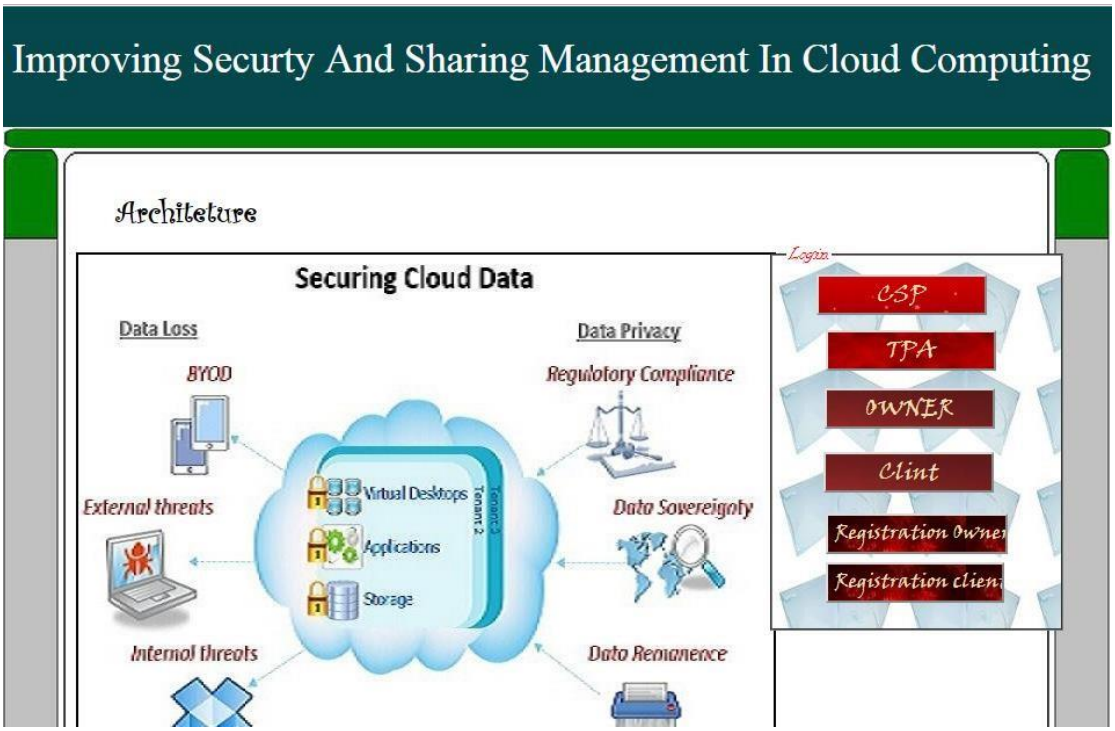


Figure (4.1) The Main Interface of The Proposed System,

4.4.1 Users Registration

The first stage of the implementation of the proposed system is registering the information of each user in recorded. This is performed through inserting user's information in the table made of several fields as (user name, password, E-mail, gender, date), these fields are requested. All fields are filled by the new user, except the last field, which is filled by the system that specifies the date on which the new user logged in the system. This phase helps identify the trusted users in order to allow them to access the cloud server. The registration module helps providing authentication and security for the new user. User authentication is required for each system to maintain security by not allowing unauthorized persons to access the cloud server. Each authorized user

will have a unique user ID/ password that allow him/ her to log in system as explained in figure (4.1). In the case the new user forgot to enter the required information in one of the fields, that user will not be a part of the system as shown in the figure (4.2). In addition, if entering the e-mail was incorrectly entered, the user will not receive the system registration as shown in figure (4.3). After the registration is completed correctly for the new user, a window will shown within the system, for each user in the system as shown in the figure (4.4). Figure (4.5) illustrates the correct final registration for new users who became members in the system.

Figure (4.2) Registration User

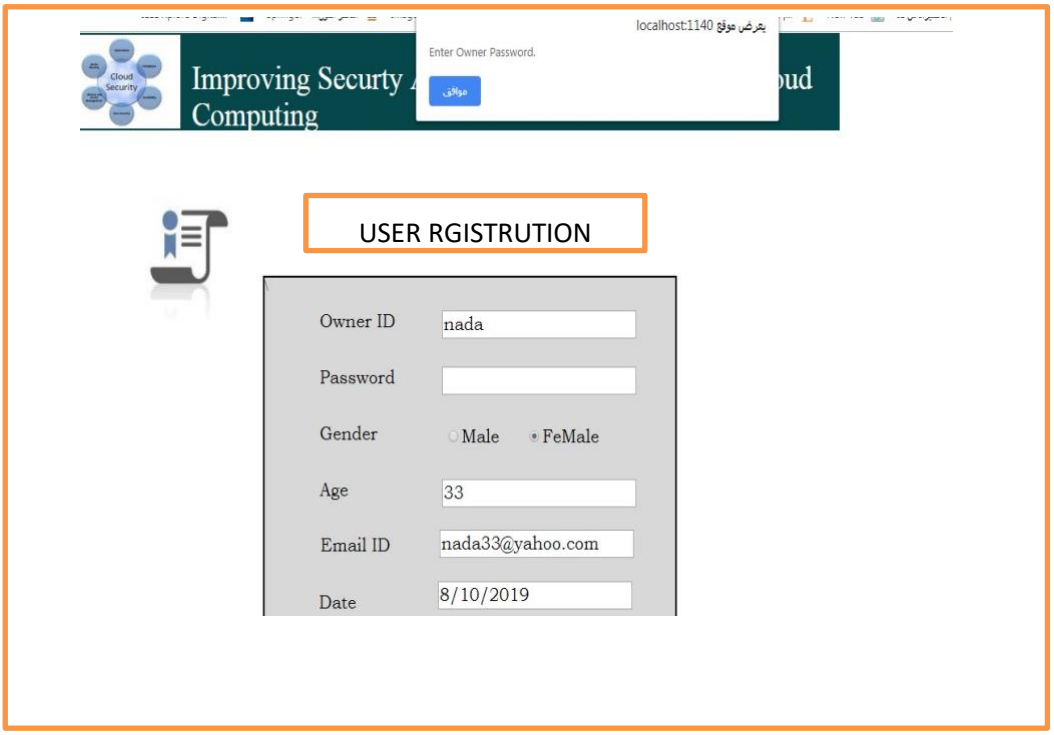


Figure (4.3) Registration User With Forget Field

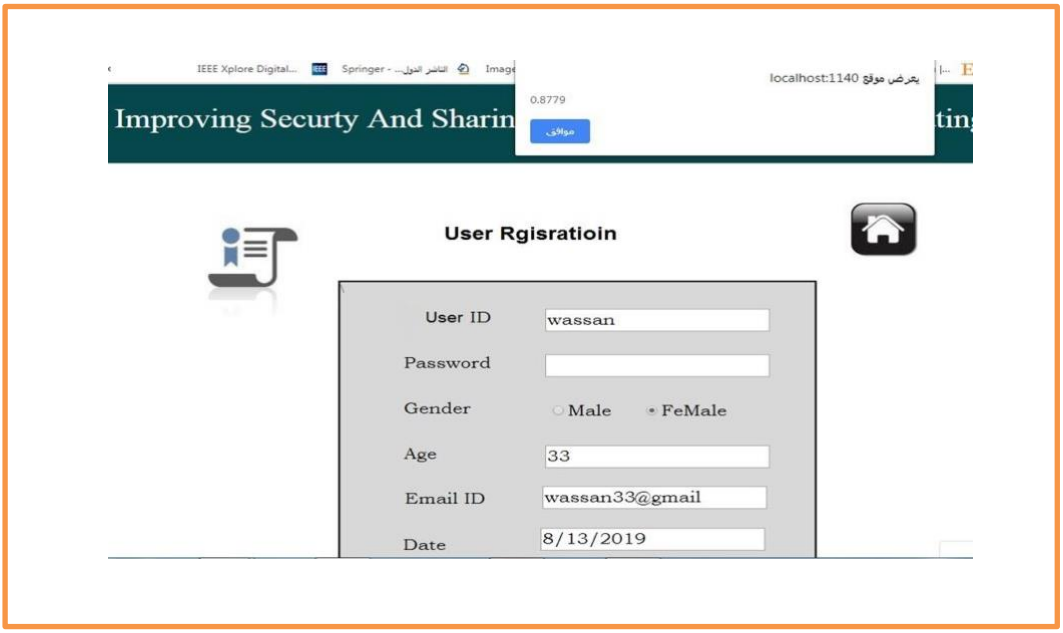


Figure (4.4) Registration User Insert Error Email

Figure (4.5): Correct Final Registration User

4.4.2 Third Party Auditor

TPA is the trusted third party among users, CSP. One of its priorities is to generate the keys for encryption, decryption and digital signature through the key generation center and its associated key as shown in the forms (Public, Private, and Symmetric) keys. It sends private keys to the owner and clients. The public keys are sent to CSP who keeps a copy to use when decrypting the encrypted signatures in order to verify the identity of the user. As for the symmetric keys, it keeps a table of its own for encryption and decryption as shown in table (3.5).

The following figure (4.2) shows the registrant main window of the TPA, which include the TPA Id and password to be entered. Figure (4.3) illustrates the main interface and duties, which will be presented in detail in this chapter.

Figure (4.6) TPA Window

Figure (4.7): General TPA Window

4.4.2 .1 Keys Generation Results

Three types of keys (public, private, and Symmetric) are generated by the key generation center directly linked to TPA Responsible for generating and distributing keys within the system, encryption and decryption of uploaded files, key management and file sharing between users and used for authentication and reliability (digital signature) for each user within the system as described below.

A- Public Keys Generation Results

Below is the results of generating public keys using the logistic map function when the input value for (x_o= 0.3216, a = 3,957, m = 50, k = 2, k = 3, k = 4) as shown in figure (4.8), which are declared for the whole system. When implementing the proposed system we will take (K =2).

Figure (4.8): Public Keys Implementation Result

B- Private Keys Generation Results

Below is the results of generating a private key depending on the public key that is shown in the figure (4.9) and the algorithm Chebyshev. Figure (4.8) shows the results of generating (50) entities .

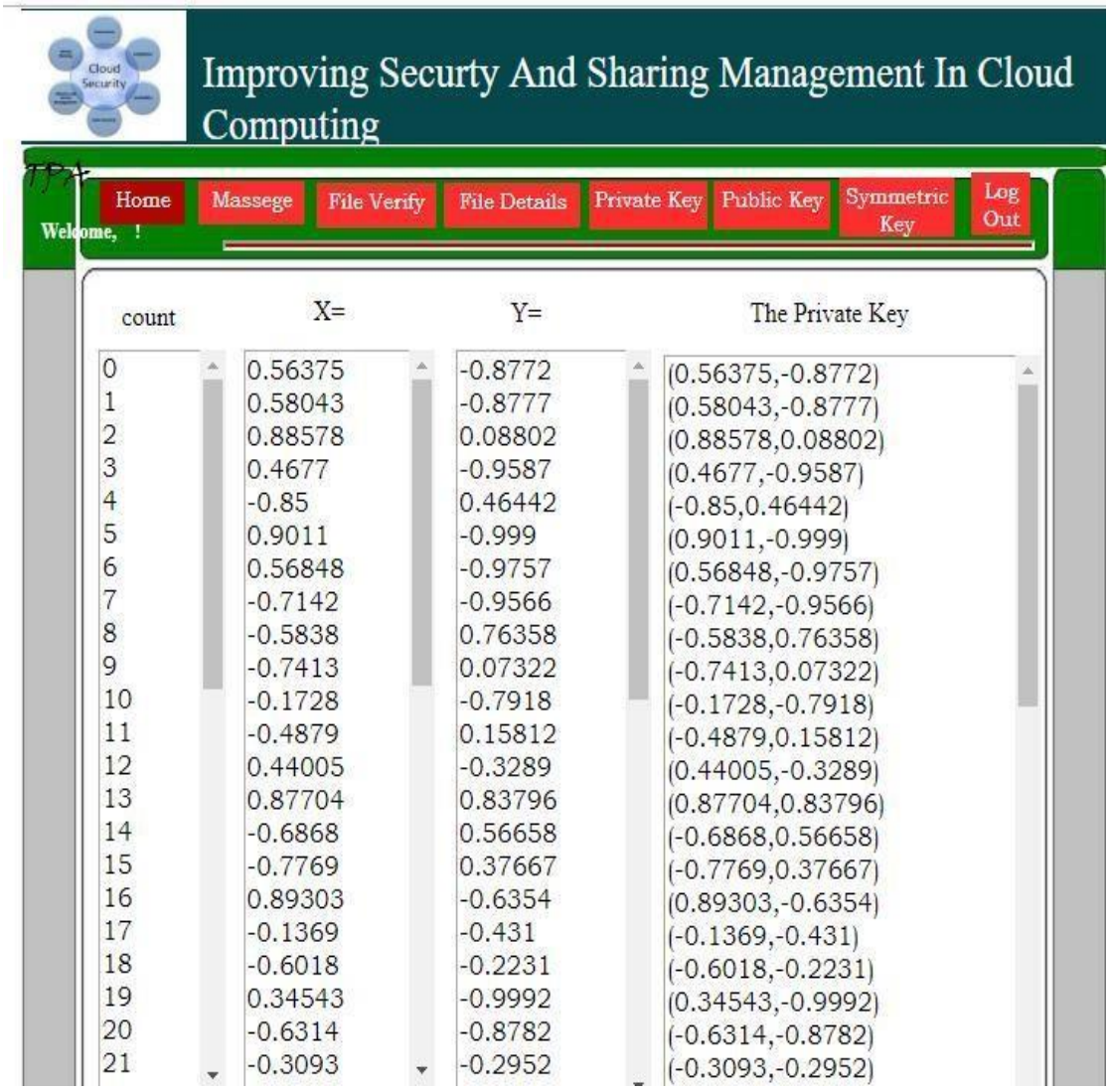


Figure (4.9) Private Keys Implementation Result

C- Keys Distributions

When keys are generated, TPA will distribute them to entities in the proposed system. Figure (4.10) below shows the final results containing the public and private keys when k=2, m=50.

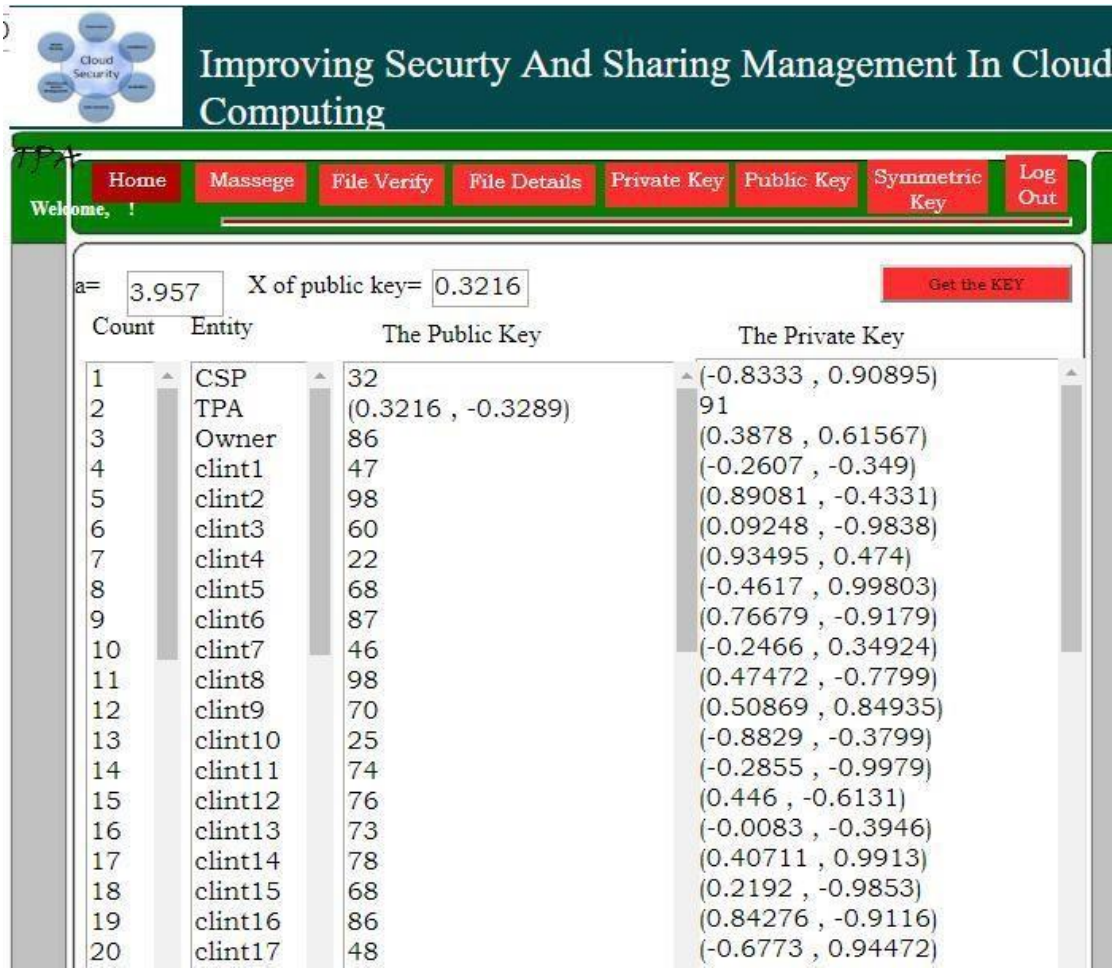


Figure (4.10) Keys Distributions

D- Symmetric Keys Generation Results

The results of implementing symmetric key generation using the system tow logistic map are shown in figure (3.3) as mentioned earlier in Chapter 3, they are used in the encryption and decryption of uploaded files in the cloud computing by TPA. The keys will be stored in the table (3.5) mentioned in chapter three belonging to TPA described below and as shown in the following figure below (4.11) based on (b=3.957 , w_o= 0.3216 ,c=2.57 ,z_o= 0.5216) The keys can be easily changed by changing

the inputs values only for(x_0)or(a),or both.

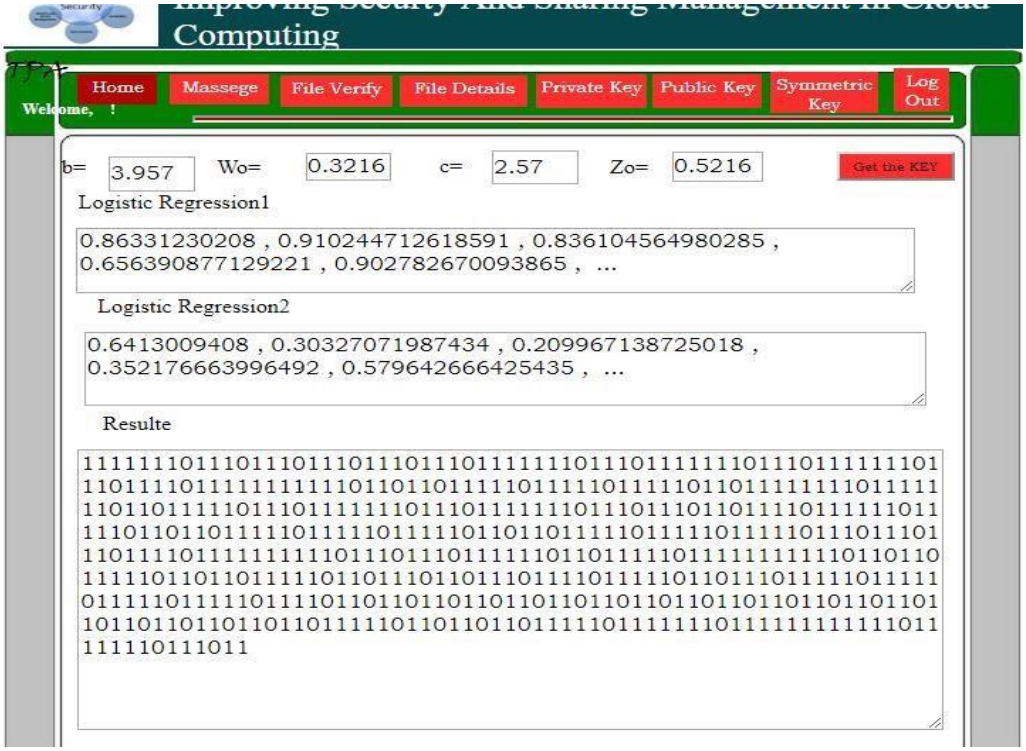


Figure (4.11) Implementation Result Of Symmetric Keys

66

4.4 .3 File Uploading

Uploading a file is achieved by an owner to CSP via TPA, figure (4.12) below with the results of uploading some files that include text and images.

4.4.3.1 Owner

The owner has a storage space inside the cloud, and this space is used by the customers who divide it and each section will belong to an owner. The following figure (4.5) shows the registrant main window of the owner, which includes the owner's Id and password that should be

References

References

[1] John W. Rittinghouse and James F. Ransome, **"Cloud Computing Implementation, Management, and Security",** CRC Press Taylor and Francis Group, LLC, 2010.

[2] Mahalakshmi, B., and G. Suseendran. **"An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions."** Data Management, Analytics and Innovation. Springer, Singapore, PP:467-482, 2019.

[3] Liu, Yuhong, et al. **"A survey of security and privacy challenges in cloud computing: solutions and future directions."** Journal of Computing Science and Engineering 9.3 (2015): 119-133.

[4] Aldossary, Sultan, and William Allen. **"Data security, privacy, availability and integrity in cloud computing: issues and current solutions ",** International Journal of Advanced Computer Science and Applications 7.4 (2016): 485-498.

[5] Parra-Royon, Manuel, and Jose M. Benítez. **"Delivering Data Mining Services in Cloud Computing "**,IEEE World Congress on Services (SERVICES). Vol. 2642 , 2019.

[6] []S. More and S. Chaudhari, **"Third Party Public Auditing scheme for Cloud Storage",** ELSEVIER Procedia - Procedia Comput. Sci., vol. 79, pp. 69–76, 2016.

(7). R. Barela, S. Govindwagh, and V. Rajaramwalunj, **"Secure Key Agreement Model for Group Data Sharing in Cloud Computing ",** International Journal for Scientific Research & Development ,vol. 5, no. 07, pp. 407–410, 2017.

[8] Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, **"Block Design-based Key Agreement for Group Data Sharing in Cloud Computing",** *IEEE Trans. Dependable Secur. Comput.*, vol. 5971, no. c, pp. 1–15, 2017.

[9] Singh, P. Sharma, and D. Arora, **"Data Integrity Check in Cloud Computing using Hash Function"**, nternational Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 1974–1978, 2017. [13] D. Nithya, **"A Novel Approach to Secure Data Sharing Scheme for Dynamic Members through Different Secure Methods",** International Journal for Modern Trends in Science and Technology ISSN: 2455-3778 , pp. 24–29, Volume: 03, Issue No: 11, November 2017.

[10] K.," **A Trusted Storage System for The Cloud**", MSc Thesis, Kentucky: College of Engineering at the University of Kentucky, 2010.

((إقرار المشرف))

اشهد بأن اعداد هذا المشروع الموسوم

تأمين تبادل البيانات على الحوسبة السحابية

والمعد من قبل الطلاب

احمد محمد احمد

سيف نايف ناصر

قد تم تحت أشرافي في قسم علوم الحاسوب / كلية العلوم/جامعة ديالى وهي جزء من متطلبات نيـــــــل شهادة البكالوريوس في اختصاص علوم الحاسوب

التوقيع:

الاسم:

المرتبة العلمية :

التاريخ :