Ministry of Higher Education

and Scientific Research

University of Diyala- College of Science

Department of Computer Science

Improving Security , Management, Sharing In Cloud Computing

A Thesis

Submitted to the Department of Computer Science\ College of Science\ University of Diyala in a Partial Fulfillment of the Requirements for the Degree of Master in Computer Science

By

Rasha Rokan Ismail

Supervised by

Asst. Prof. Dr. Taha M. Hassan

2020 AC ***1440AH***

وزارة التعليم العالي والبحث العلمي

جامعة ديالى

كلية العلوم

قسم علوم الحاسوب

تحسين الأمن ،الادارة ،المشاركة في الحوسبة السحابية

الرسالة

مقدمة الى قسم علوم الحاسوب/ كلية العلوم /جامعة ديالى كجزء من متطلبات نيل درجة الماجستير في إختصاص علوم الحاسوب

من قبــل

رشا روكان إسماعيل

بإشراف

أ.م.د طه محمد حسن

1440هـ **2020 م**

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].

Key management concerned with generating keys for all users including the new ones that may join later. If all group members use a single key, the users should be more careful with key management. Frequent changes in membership should be handled by key management as it may result into high computation overhead if not properly handled. Rekeying represents a simple solution. So, when a new user is added, the group generates a new key, re-encrypts the data and distributes the keys again to all the members. On the other hand, when a member leaves the

group, same procedure of rekeying is performed by the group the to avoid the departing users from using the current key to access data illegally. But, and in case of frequent changes to the group membership, this may result an increased overhead. Regardless, there is always a threat from malicious authorized users within the group who may attempt to access and tamper the data. In case of a single symmetric key, if users of the group hold the entire key, it may prove to be a serious threat if any of the authorized users turn malicious. Though data is encrypted, it is thus necessary to handle key management efficiently to provide secure data sharing in cloud storage [6][7][8].

1.2 Related Works

Several works are related to the aim of this thesis, 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 Diffie-Hellman 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.
5) In 2017 Darpalli Nithya ,etal , [13], a key conveyance with no correspondence channel was proposed, where the clients able to know their private key from their gathering supervisor in secured method. AES Algorithm used for the systems of information encryption and decoding while ring mark is utilized for circulating the key between the gathering individuals.
6) In 2018, (Ghadge and U bale) [14], proposed a secure manner for distributing keys without utilizing any protected communication channel, and the user is capable of safely getting the private keys

from group administrators (managers). Only users in the gathering are able to use the cloud. A fine-grained access control and anti-collusion attack are provided by the system. Files are stored on many clouds in various groups using a hybrid cloud. A secure revocation is also supported by the system.

7) In 2018, (vishal salunke et al.) [15], proposed a system takes the advantage of the balanced radically symmetrical incomplete block vogue symmetric balanced incomplete block design (SBIBD), they have a tendency to gift a unique block design depending on a protocol of key agreement, which provides multiple participants, that can flexibly expand how many participants in associate degree passing cloud surroundings the block style structure supported the planned cluster information sharing model. The protocol of key agreement is employed to come up with a typical conference key for a number of participants to guarantee that the protection of their later communications and this protocol is applied in CC for supporting secure and economical information sharing. They have a tendency to project a block style primarily based on key agreement protocol within which, TPA realize malicious user from the cluster and take away from cluster we've got an inclination to gift general formulas for generating the common conference
8) In 2018, (Khandale and Varpe) [16], the data sharing freely to a group of users helps to increase the efficiency of work and to ensure data sharing within the group as well as from difficult external sources. To solve this problem, the symmetric / asymmetric block symmetric balanced incomplete block design

symmetric balanced incomplete block design (SBI BD) is designed for the main security, so the user is unable to have access to data where the shared conference key K was created using the SB BID scheme for many users. The algorithms used in this system are the DES and Blowfish algorithm in order to improve system performance greatly.

9) In 2018, (Devi et al.) [17], two layers of encryption information that are run by a lower encryption layer are highlighted, the information owner encrypts the bottom layer, and the third party encrypts the top layer on the owner's test information. owner. The owner sends a key to legitimate clients for encryption and decryption. This ensures that only a large client has access to information. The algorithm used is hash.
10) In 2018 Shen, Jian, et al, [18], presented a safe and fault-tolerant keyagreement for group data sharing in a cloud storage scheme. This techeques depended on SBIBD and group signature . A common conference key can be effecintly generated by the proposed approaach, the key can be used to support secure group data sharing and safegurd the security of the outsourced data in the cloud at the same time. It should be noted that this paper has presented algorithms to construct the SBIBD and its mathematical descriptions.Additionally,efficient access control and authentication services have been achieved regarding the technique of group signature. This scheme can also support the traceability of user's identity in an anonymous environment.

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 Thesis

The goal of this thesis 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, security and identity verification Authorized users. 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. Digital signature is different for each user and for each file uploaded, modified or updated by user (owner, client) or TPA in the system. Therefore, the logistic map and Chebyshev map algorithms are used to enhances the strength of the system being used in TPA to generate different keys.

1.5 Outline Of Thesis

In addition to this chapter, this thesis 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, types of key management scheme and solution to the security manners. In addition, the need of secret sharing schemes, secret sharing schemes, problems with existing secret sharing schemes, cryptography, types of cryptography model, logistic map and Chebyshev map are explained in this chapter.
- **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.