Reliable Re- Encryption and De- Duplicating data in Cloud Environment

Purnima Mandrekar[1], Priyanka Tarange[2]

Department of Computer Engineering, MCT's Rajiv Gandhi Institute of Technology, Mumbai University, India.

---***---

Abstract - *As there are always enhancements in the technologies, the need for sharing the resources and data has also considerably increased. After sharing these data online, security of data is very important and also saving the memory space of the cloud is also essential at the same time. In our proposed system, the concept of re–encryption and de- duplication of data is used.*

***Key Words*: cloud environment, encryption, re-encryption, de- duplication, and decryption.**

1.INTRODUCTION

Cloud infrastructures can be classified into private or public cloud infrastructure. In private cloud infrastructure, it is managed and owned by the customer (owner). It means that the customer (owner) has full control over his own private cloud and he may or may not grant permissions to the one he suspects as unauthorized user. In public cloud infrastructure, it is owned and managed by the cloud service provider (CSP). It means that the customer (owner) does not have full control over the data. Now a days, many people are using the cloud storage for storing their data permanently on cloud without having a fear of losing the data from the computers, laptops, mobile phones etc. Even though many people are using cloud infrastructure, it lacks some of the important features like the cloud accepts duplicate data, same name of the file with same size and same type but after the user has uploaded it into the cloud it automatically renames it as document (2), which consumes much space in the cloud.

1.1 Reliable Re-encryption

The server checks whether the document uploaded on the cloud is a single copy, then the server encrypts the document which has to be shared to other users and generates a key so that the document which is shared to the users can view the document by entering the key of the document. The owner shares that document individually or in a group. If user leaves the group and already a link has been shared in that group, that user has also the access to the document, so in order to be secured of leaking of any confidential information re-encryption of the document is done based on time-stamp. So that the document will also be safe and nobody will try to hamper the document even if he/she knows the key to open and view the document.

1.2 De-duplication

Now a days, sharing of resources and data has increased considerably. After sharing these data online the data has to be secured. The owner uploads a document online on the cloud. At the server end, it will apply de- duplication algorithm and will generate a unique serial number for the document. This unique serial number is used for verifying whether already the same name of the document exists in the cloud or not. If there exists a document with a same name and the owner is trying to upload it once again, then that document will not be uploaded and will show an alert message that the document already exists, which saves lot of space of the cloud because of repeated documents which is being uploaded by the users unknowingly and also saves the data which is used for downloading the document and the owner can share the link of the document among the valid authorized users.

1.3 Cloud Environment

Cloud computing is the computing based on the internet. Where in the previously, people used to download the application or program on their physical computer or server but now because of cloud computing people can access virtually to the same kind of applications through the internet without downloading and running it on their physical computer or server. Following are the things we can do with the cloud:

- Create new apps and services
- Store, backup, recover data
- Host websites and blogs
- Stream audio and video
- Deliver software on demand

Cloud Computing makes all the services available as and when required by any kind of user. The computing resources includes hard disk, databases etc. To access these resources from the cloud, they don't need to make any large scale capital expenditures. Organization need to "pay per use" i.e. organization need to pay only as much for the computing infrastructure as they use. The billing model of cloud computing is similar to the electricity payment that we do on the basis of usage.

2. RECENT WORKS

As the cloud computing technology is developing, large amount of data is stored in the cloud. Since the data uploaded in the cloud is not that much secure, in which there is a lack of de- duplication of data and re- encryption. If we are sharing a document to some person, if the document is confidential then that document can be shared to multiple people who are not authorized, in which there can be loss of confidentiality. Our proposed system is based on time based re-encryption of data in which there is a major drawback, the data can be updated by the owner only.

3. PROPOSED SYSTEM

In the fig.1, our proposed system, there are two modules: first is the owner (sender) and second is the user (receiver). For the owner (sender): The owner uploads a document online on the cloud. At the server end, it will apply de- duplication algorithm and will generate a unique serial number for the document.

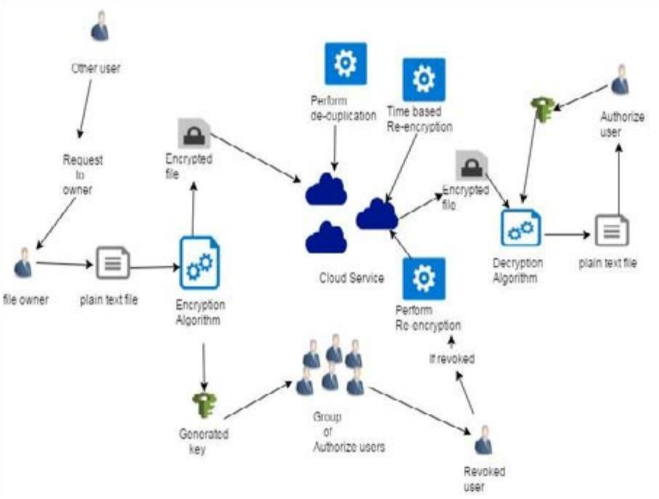

Fig -1: Overview of the Proposed System.

This unique serial number is used for verifying whether already the same name of the document exists in the cloud or not. If there exists a document with a same name and the owner is trying to upload it once again, then that document will not be uploaded and will show an alert message that the document already exists, which saves lot of space of the cloud because of repeated documents which is being uploaded by the users unknowingly and also saves the data which is used for downloading the document and the owner can share the link of the document among the valid authorized users.

After the server checks whether the document uploaded on the cloud is a single copy, then the server encrypts the document which has to be shared to other users and generates a key so that the document which is shared to the users can view the document by entering the key of the document. The owner shares that document individually or in a group. If user leaves the group and already a link has been shared in that group, that user has also the access to the document, so in order to be secured of leaking of any confidential information re- encryption of the document is done based on time- stamp. So that the document will also be safe and nobody will try to hamper the document even if he/she knows the key to open and view the document.

4. CONCLUSIONS

In this paper, we have proposed reliable re-encryption methods such as re-encryption of the data after the user has left the group or else the document has sent in a private mail to individual person, the document should not be misused by some other person (outside the organization or group). Even if the document is being forwarded by that person to another person who is not there in that organization, we can trace who has forwarded the document using the log file which is created using the hash function. We also have introduced data de-duplication of data using MD5 algorithm so that in the cloud there is only one copy of that document and if tried to upload the same document with the same name and size then it will not be uploaded as there is already a document existing in the cloud, which saves lots of space in the cloud and also data in order to download it. Hence we are providing more security to the data in the cloud and we can share confidential data in the cloud system with ease and rely on it.

5. FUTURE SCOPE

The further enhancements in this proposed project will be like OTP generation, the key would be received on mobile numbers as well as on the email id as per the choice of the user, the user can send documents to multiple people individually at the same time those who are not in any groups, time based re-encryption.

REFERENCES

[1] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang School of Information Science and Engineering, Central South University, “Reliable Re-encryption in Unreliable Clouds” Changsha, Hunan Province, P. R. China, 410083 Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA.

[2] IEEE 6th Control and System Graduate Research Colloquium, “A Reliable Data Protection Model based on Re-Encryption Concepts in Cloud Environments” Aug. 10 - 11, UiTM, Shah Alam, Malaysia, by Faraz Fatemi Moghaddam , Mostafa Vala.

[3] “Secure User Data in Cloud Computing Using Encryption Algorithms” Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[4] “Secure Auditing and De duplicating Data in Cloud” Jingwei Li, Jin Li, Dongqing Xie and Zhang Cai / IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.