IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.
www.ijiset.com
ISSN 2348 - 7968

Advanced Re-Encryption Technique and Verification Process in Cloud Computing

Shridhar.B[1] Pavan Gujjar Panduranga Rao[2]

[1]CSE ,Viswesvaraya Technological University, Rajiv Gandhi Institute of Technology,Bangalore, Karnataka ,India

[2]Research Scholar ,Dept.of CSSE , Andhra University ,Vishakhapatanam,Andhra Pradesh, India

Abstract— Cloud Computing is one of the latest and an ever growing technology.Cloud Computing provides the service over the internet . In the traditional approach there is no verification of the data in the cloud server if the data is modified and no notifications are sent to the data owner if the file is modified.Authentication of the users is not done properly or it is insecure.The better approach is that the data at the cloud server is verified and notification messages are sent to the data owner. Before uploading the data to the cloud server based on the file size and amount of space acquired by the file the verification is done at the cloud server. In this paper re-encrypting technique is implemented so that once after the data owner encrypts the data then the cloud server re-encryption technique is implemented.Re-encryption technique is performed in order to provide security for the data from the cloud server. The data is highly secure, data is confidential from the cloud server, communication costs are reduced and data integrity is achieved.

Keywords— Cloud Computing, Re-encryption, Authorized Users, Verification,Revocation Tracking,Data Security

I. INTRODUCTION

Cloud Computing provides storage space for the data. The services that the cloud provides are security and privacy[1]. Cloud sourcing will be playing the vital role in the next generation of cloud implementation. A public cloud is a shared cloud computing infrastructure that anyone can access. Public cloud services are available to clients from third-party service providers via to the Internet.

Cloud Computing is one of the ever growing technology. In cloud computing the data in the untrusted clouds is not secure. If the data is modified in the cloud server then the integrity of the data is lost in the cloud server. The data that is uploaded is not confidential enough. In proposed work the re-encryption technique is implemented so that for the data high security is provided.Verification of the file is done at the cloud server and notification are sent back to the data owner[4].

Cloud Server re-encryption achieves the task of data security and the data is highly secure in the cloud. More security is provided to the data that is uploaded to the cloud. Access control [1] duties responsibilities is delegated to the cloud.It is difficult for the data owner to manage the new keys and to perform re-encryption on the data.If the revoked users tries to attack the file then the data owner should get the data from the cloud server and private communication channels[1] must be established to distribute the new keys to the users and performing re-encryption.If the revoked users tries to modify the data in the cloud server a notification is sent to the data owner that the data in the cloud server is [5] modified or the file that has been uploaded is not safe. Thus it minimizes the communication and computation costs for the data owners. In the proposed system a Re-Encryption Technique is introduced to provide data security, data confidentiality and to achieve data integrity. Authentication is achieved by allowing only the authorized users to access the data from the cloud.

The major drawbacks [1] in the existing approach:

1. The Verfication of the file at the cloud server is not tracked and if some one tries to modify the file at the cloud server notifications are not sent to the data owner.

2. Revoked users are not traced and blocked by the cloud server.

3. The load on the data owner is increased if the revoked user attacks the file because the data owner has to get the data from the cloud server to perform re-encryption and new keys has to be re-distributed to the users.

4. If the data is not higly confidential there is no extra protection on the data that is uploaded to the cloud server.

5. Data Integrity is not achieved since protection on the data is very less.

ISSN 2348 - 7968

6. Authentication of the users is not done properly.Validation of the users is done with the help of username and password.

In this paper the major chanllening task is to verify the file that is modified at the cloud server and to keep track of the file that is modified at the cloud server.The revoked users are tracked and blocked automatically by the cloud server. Then the unauthorized users should be blocked or should not be allowed to access the data. In this paper re-encryption technique is introduced to provide the more security for the data. The data owner and the remote users roles are created by the cloud administrators in order to reduce the overload of the data owners.

The challenging issue is to monitor the attackers and to keep track of revoked[5] users. Another task is to protect the data by performing re-encryption on the owner and the cloud encrypted data. This is helpful if the data is highly confidential. Privacy of the users is taken in to account and only the authorized users are allowed to access or download the data to the cloud. Cloud Admin issues the token and maintains the keys of the users.

The advantages of using proposed system is:

1. The public Data Auditing is done by the cloud administrator so that he can keep track of the data that is modified at the cloud server and immediate notifications are sent to the data owner such as file is not safe or the data is modified at the cloud server.

2. If the attackers are trying to access the data they are traced by the cloud server and they are automatically blocked.

3. Remote Users have to provide two secret keys in order to get the data from the cloud server this allows only the authorized users to access the data and Data Confidentiality is achieved

4. Data is higly secure since multi-layer encryption is performed on the owners data.

5. The Costs are reduced by [1] re-encryption since there is no need to establish private communication channels to re-distribute the new keys to the users.

6. Two-step verification [9] is implemented so that authentication is done thoroughly.

II. RELATED WORKS

In the outsourced databases model the data management is outsourced to third party service providers. Third party service providers will allow its clients to update, create, store, access and modify their outsourced databases [1]. It assures authenticity and data integrity for outsourced databases. It does not allow the querier to change the data and only the authenticated users are allowed to modify the data. It incurs low computation and communication costs. The disadvantages with this approach is that there is no automatic blocking of the cloud server attackers in cloud computing. Data is stored in the untrusted cloud servers.

The cloud provides the services that are an attractive way of deployment model which consists of applications like Microsoft office word, MS-access. Compared to desktop applications the cloud services allows multiple users to edit shared state concurrently and in real time, while being globally accessible, highly scalable and available [4]. Various benefits come by fully trusting the cloud service providers with sensitive data. A framework is proposed to build a variety of collaborative applications in untrusted cloud servers. The attacker details are not dynamic instead it is maintaining the log files to store the attacker details and viewing using data mining concepts which is time consuming job and it has less security.

The Key challenging issue in cloud computing is to provide security and privacy for the data that we store in the cloud. Encryption methods in cloud computing provides the security for the data [7].Traditional encryption techniques is not enough to secure the data. In this approach encryption are performed using symmetric keys. Efforts are made to minimize the key that needs to be distributed. The limitations with this approach is that if the data owner is not having a copy of the data then the data owner should download the data from the cloud server and decrypt the data and encrypt the data with the new symmetric keys. The Privacy of the users is not taken in to consideration.

III. AUTHENTICATION AND DATA SECURITY

Data confidentiality is achieved since the owner encrypts the data and the cloud server cannot modify the data at the cloud server and it assures only the authorized users are allowed to access the data.Since Multi-layer encryption is peformed to the data.The data is higly secure in the cloud storage area.The two-step verification process is implemented so that user is authenticated twice.With the help of Re-encryption technique the data is more secure since the data is encrypted twice.Data Confidentiality is achieved by allowing only the authorized users are allowed to access the data.The two-step verification process is implemented so that only the authenticated users are allowed to access the data.first with the help of the password and the second step verification code is sent to the mobile of the authorized users[9].

IV. ARCHITECTURE

A. Data Owner

Data owner encrypts the data and uploads the data to the cloud server. Data that is uploaded in the untrusted cloud servers is not secure so that the data owner encrypts the data before uploading the data to the cloud server by assuring data confidentiality from the cloud server.

Data Owner can view the privileges that have been provided by the Cloud Admin such as file upload, File deletion, Account notification and Audit logs. Data Owner will come to know the privileges that he has having accordingly he can upload the file, delete the file and audit logs. Current date and time when the data is uploaded to the cloud server details are maintained by the log files. Privileges to the data owner are provided by the cloud administrators.

If the data is tampered in the cloud server or attackers tries to modify the file in the cloud automatic notification is sent to the data owner. The file is safe or not will be verified by the data owners. If the file is modified at the cloud server side then the automatic notifications is sent to the data owners. Data owner will send the metadata to the cloud admin after uploading the file to the cloud.

After the data owner uploads the file to the cloud server the data owner sends the metadata to the cloud administrator. Information about the file details is transferred to the cloud admin so that admin can keep track of the attacker details and file details etc.If the file that is uploaded is of no use then the data owner deletes the file from the cloud and the file deletion confirmation is sent back to the data owner after the successful deletion of a file. The data that is residing in the cloud is not required then that data is deleted and the acquired space for this file is de-allocated so that this space can be better utilized by other user.

B. Cloud Server

Cloud Server can view all the files that the owner has uploaded to the cloud. Cloud Server can view all the blocked users. The cloud server can view the privileged users who can access the data. If an unauthorized user enters the wrong secret keys they are automatically blocked by the cloud server. Allowing only authorized users are to access the data from the cloud.

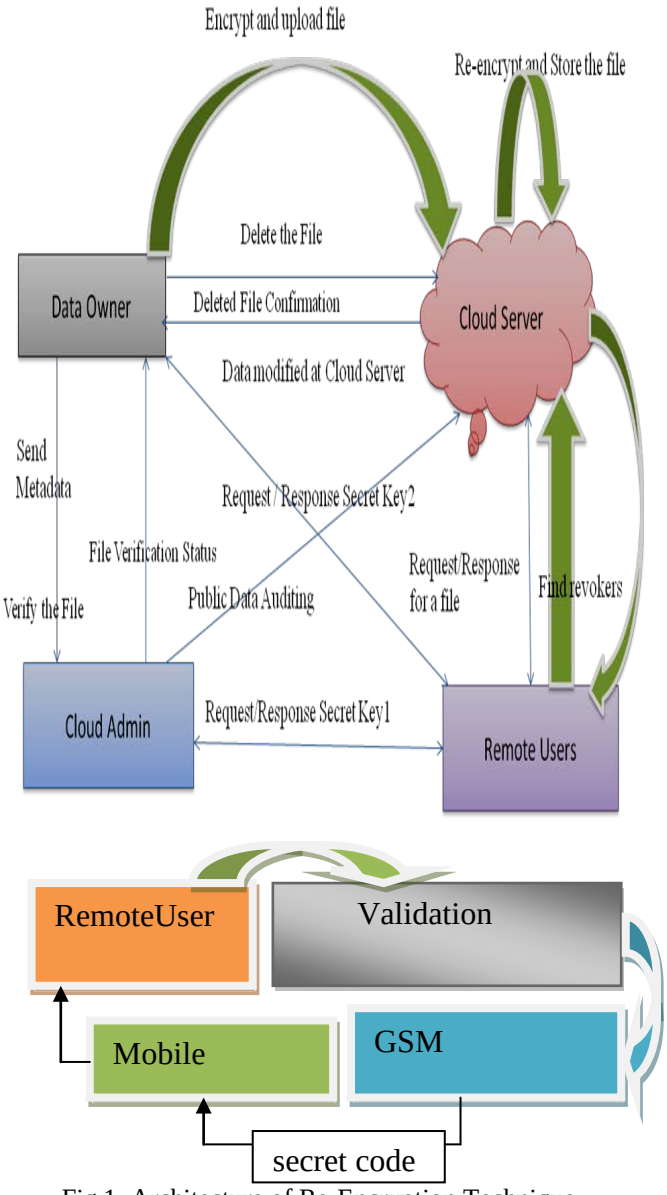

Fig 1. Architecture of Re-Encryption Technique

The data that is uploaded to the cloud server is modified or if the attacker tries to modify the file immediate notification is sent to the data owner. Data owner can verify the file if the data in the cloud is modified or the data is tampered. If the unauthorized user is trying to get

the data from the cloud then the cloud admin automatically blocks the users. The blocked users will not be able to access the data. Cloud Server can unblock the blocked users upon request from the users. If the users are providing the wrong secret keys in order to access the data then they are automatically blocked.

C. *Remote User*

Remote Users before accessing the secret keys from the owner and cloud server. User authentication is checked twice before accessing the secret keys. Once user validation is performed with login authentication and second time the users authenticate is done by sending the secret code to the users mobile.If the user is revoker then the cloud admin automatically blocks the unauthorized users. Second type of validation is checked by using interfacing technology called as gsm.Gsm is used to send the messages to the users as well as to the cloud admin.Remote User should request two secret keys from the cloud owner and one secret key from the cloud server so that the data that is encrypted can be decrypted.

D. *Cloud Administrators*

The details such as attacker-name, file name, date, public key and secret key can be viewed by the cloud admin. If the attacker is providing the invalid secret keys then this remote user is automatically blocked. The details such as file-names that are residing in the cloud space can be viewed or audited.The roles of the remote users and data owners will be created by the Cloud Administrators. The privileges are provided to the data owners by the Cloud Administrators. The maintenance of the information about the data owners and remote users is done by the Cloud Admin. Remote Users Name, Download Permission, Attribute Name all these details will be maintained by the Cloud Administrator. Over all maintenance of the receiver and the data owners details will be done by the cloud administrators.

V. **PROPOSED WORK**

In this paper verification of the file is done at the cloud server if the data is modified then automatic notification messages are sent to the data owner.In this paper the data owner load is reduced by delegating most of the access control duties to the cloud.Re- Encryption is performed so that the data that is uploaded is highly secure. Before uploading the data the data owner encrypts the data and uploads the data by assuring data confidentiality from the cloud server. Data Integrity is achieved by performing Re-Encryption so that the data is not modified at the cloud server side. Only the authorized users are allowed to access the data by providing secret keys to the users. A data owner encrypts the data and the cloud server re-encrypts on the owner encrypted data so that if the revoked users change there is no need for the data owners to download the data and re-encrypt the data and produce new keys. This reduces the Communication costs. Computation costs are reduced since there is no need for the data owners to established private communication channels to re-distribute the new keys to the users.In this two-step verification process the users are validated with user name and password and in anther step a interfacing technology called as global system for mobile communication in this a code is sent to the users mobile so that the users are authenticated twice.

The main objective of this paper is Data Protection, Data Confidentiality ,Data Integrity and Data Availability. Since the users are allowed to provide two secret keys to get the data only the authorized users are allowed to access the data. Unauthorized users are traced and blocked automatically. The load on the data owner is reduced by delegating most of the access control to the cloud.

VI. **CONCLUSIONS**

In this paper Re-Encryption technique is implemented so that the data is higly secure and data confidentiality is achieved.If the data is modified at the cloud server it is verified by the dataowner in order to achieve the task of data integrity.Data availability is achieved so that the users can accesss the data all the time. Communications costs are reduced by implementing the re-encryption technique in cloud computing.In future enhancements alternative way of re-encrypting technique is implemented so that implementation costs are reduced.

REFERENCES

[1] M.Nabeel, E.Bertino," Privacy Preserving Delegated access control in Public clouds", June 2013.

[2] M.Nabeel and E.Bertino, "Attribute based Group Kay Management Scheme", IEEE Transactions on Dependable and Secure Computing.

[3] A.Fait and M.Naor, "Broadcast Encryption". In Proceedings of the

13th Annual International Cryptology Conference.

[4] D.Naor,M.Naor and J.B.Lotspiech "Revocation Tracing Schemes for stateless receievers",in proceedings of the 21st Annual International Cryptology,2001

[5] X.Liu, Y.Zhang ,B.Wang,J.Yan,"Mona:Secure Mutli-owner Data Sharing in the group"

[6] M.Nabeel and E.Bertino,"Towards attribute based key Management" ,"IEEE Tran. On parallel and distributed systems.

[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[9]Websites referred are www.gmail.com and www.google.com