IJCSN International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015
ISSN (Online): 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Data Security Using Reliable Re-Encryption in Unreliable Cloud

[1] **Ajinkya Adhau,** [2] **Payal Bobade,** [3] **Priyanka Zilpe,** [4] **Yashodhara Fulmali**

[1, 2, 3, 4] Student, Department of Computer Technology, RGCER, Nagpur-441110, Maharashtra, India

Abstract - Cloud computing is the innovative research area as it is the solution for next generation. One of the issue in cloud computing is data security. The Data owner stores encrypted data on cloud and issues decryption keys to authorized users.. Re-encryption prevents the left user to decrypting the data by using the old decryption key and to generate new decryption key to valid or authorized user only. So only authorized user can continue to access the data. By considering cloud architecture, such command may not be received properly due to unsecured network communications. In this paper, we have include the time base re-encryption scheme, attribute based encryption scheme (ABE) which able the cloud servers to automatically re-encrypt the data based on their internal clocks , users can access data within given time period.

Keywords - *Cloud Computing, Proxy Re-Encryption (PRE), Unsecured Network, Time Based Re- Encryption, and Attribute Based Encryption.*

1. Introduction

The Cloud Computing is model for delivering information technology services in which resources are retrieved from Internet through the web based tools and applications, then direct connections to the server and resources are provided as long as connected to the web. It has become a viable business and technological proposition because of the significant reduction in both infrastructure and operational costs that it offers when compared to traditional IT services.

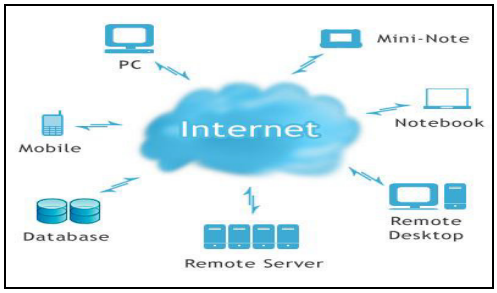

Fig. 1 Cloud

The use of cloud computing is increasingly popular due to the potential cost savings from outsourcing data to the cloud service provider (CSP) [2]. One technique to protect the data from a possible un-trusted CSP is for the data owner to encrypt the outsourced data. The data Security most critical aspects in a cloud computing environment due to the importance of information stored in the cloud. In this paper is related to data security and privacy.

ABE is a new cryptographic technique [1] [4]. It allows data to be encrypted using an access structure comprised attributes are different. Then specific decryption keys for specific files, data users are issued attribute keys. Data users must have the necessary attributes that satisfy the access structure in order to decrypt a file. For example, file encrypted using access structure {(a1 and a2) or a3)} means that either a user with attribute a1 and a2, or user with attribute a3,can decrypt the file. An alternative solution is applied to the proxy re-encryption technique [1]. This is also called as command driven re-encryption scheme as the re-encryption is performed by the servers in the cloud computing environment while receiving commands from the owner of the data.

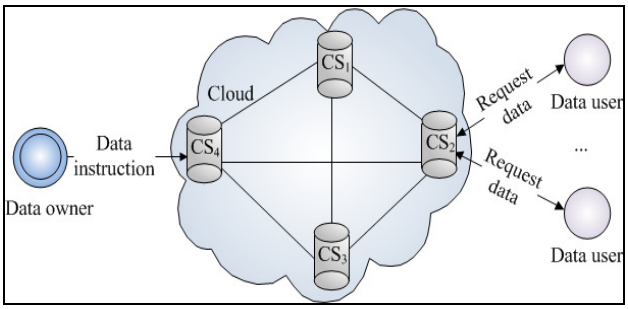

Fig .2 Cloud Environments

As shown in fig. Where Data owner are upload encrypted data on cloud servers CS1,CS2,CS3 and CS4.A cloud is essentially a large scale distributed system where a data owner's data is replicated multiple

servers for high availability. Assume the data owner issues to CS2 a re-encryption command, which should be propagated to CS1, CS3 and CS4.due to the network outstage, CS4 did not receive command and data is not encrypted. At this time, if left users query CS4, they can obtain the old cipher text, and decrypt it using their old key. A best solution is to allow each cloud servers to independently re-encrypt data without receiving any command from the data owner.

2. Literature Survey

Table.1 Literature Review

Sr No	Paper Name	Advantages	Disadvantages
1	Cryptographic Cloud Storage	It is easy to implement and provides security.	Hacking of keys while decryption of data
2	Proxy Re-Encryption system for Identity based Encryption	Data security	There is problem in architecture of cloud ,command not reaches to each server when there is network outage or server crashes
3	Attribute based encryption for fine gained access control encrypted data	It uses ABE which allow to encrypt the data using access structure using different set of attribute	There is problem in this paper which is bottleneck when there is frequent user revocation
4	Reliable Re-Encryption in unreliable cloud	Using time based re-encryption it re-encrypt the data automatically in given time	In this there is space complexity problem

3. Proposed System

We used a reliable re-encryption scheme in un-trusted cloud (R3 scheme for short). [1] R3 is a Time-based re-encryption technique, which allows each and every cloud server to automatically re-encrypt data based on its internal clock. Data user will only get access to that data in a particular time slot. Then time slot gets over so cloud server will automatically re-encrypt the data. Cloud server will check whether requesting user is allowed to access the data on this time slot or not. If the time slot doesn't match, cloud server will not allow data user to access that particular data.

The proposed system is work on the process of Re-encryption for provide data security. We are work on cloud data is encrypted and decrypted on time based automatically. This is a automatic time based re-encryption scheme [1], in which each cloud server to automatically re-encrypted data based on their internal clock. This scheme is to associate data with an access control and an access time. Each valid user is issued key associated with attribute and attribute effective times. The valid user using the key data is decrypted with attributes satisfying the access control and attribute effective times satisfying the access time. The command driven re-encryption scheme, the data owner and this share a secret key, with each cloud servers can re-encrypt data by uploading the access time according to their own internal clock. It does not require perfect clock synchronization among cloud servers.

4. System Architecture

A system architecture or systems model is the conceptual model that defines the structures, behaviors, and different views of a system.

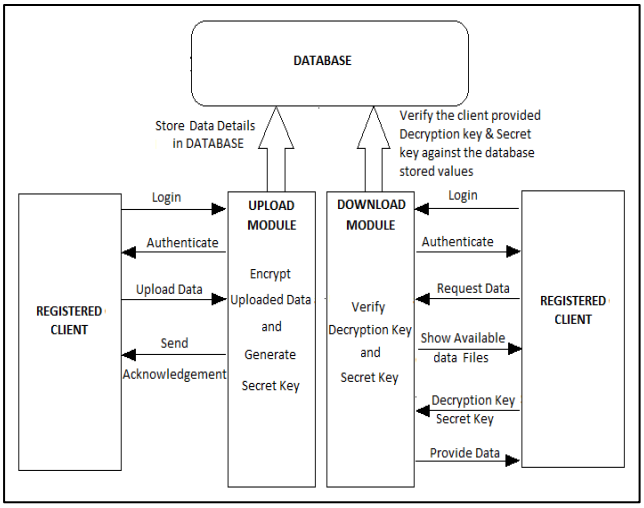

Fig.3 Data Upload and Download module

An architecture description is a formal description and representation of a system, organized in a ways that supports reasoning about the structures and behaviors of the system. As show in fig.2 The software is consist three subsystems:

***Data Owner*:** Data owner is the interface for file up loaders. It generates ABE keys for encrypting the data files, and then encrypted file upload and store in cloud storage.

***Data User*:** Data user is the interface for file downloader. It generates the ABE keys for decrypting the data files, decrypts the file got from the cloud servers.

***Cloud Storage Server*:** Encrypted content along with keys are stored in the cloud servers. Every time read access arrives based on the time, it re-encrypted the file and store in the cloud storage servers.

5. Algorithm

System based on Reliable Re-encryption (R3) algorithm and DES .R3 algorithm has two phases, initial encryption Phase-I and Re-encryption Phase-II.

A. Initial Encryption (Phase-I)

1. Data owner should register on the website.
2. System will send a verification link on data owner email id.
3. After verification the Data owner uploads data on cloud.
4. Generate key using current timestamp and encrypt data using DES algorithm.
5. Store the encrypted data with current timestamp.
6. Authorised user access the data using valid key.

B. Re-Encryption (Phase-II)

1. When Admin changes the user status from active to inactive, then re-encryption module is activated.
2. The data is decrypted using the valid decryption key.
3. A new key is generated using new timestamp and data encrypt using R3 algorithm.
4. The re-encrypted data is stored with new time stamp.
5. Authorized user access the data using valid key.

While receive a request R (File TSi)
Do
If current time is later than ti+1 or change in user management
Then
Re-encryption the file window with TSi
Else
Hold on the read command until ti+1.End.

6. Design Model

The main goal of design is to achieve scalable users evocation while protecting data security in cloud computing. So, we categorize our goal into the following:

Fine Gained Access Control**:** The data owner can specify expressive access structure for each and every data.

Data Consistency: This requires that all authorized data users who request for file F, should obtain the same content in the same time slice.

Data Confidentiality: The Cloud Service Provider (CSP) and malicious user cannot recover data without the data owner's permission.

Cost Efficiency: The re-encryption cost on the CSP (cloud service provider) is relatively low.

The modules are as follows:

Cloud Storage Server:

In the cloud, initially data owner is owner of files and data. The Cloud Service Provider which provide services to the clients. CSP cloud servers are register to the cloud and obtain its ID. After the server login it shows the encrypted data files are uploaded by the data owner.

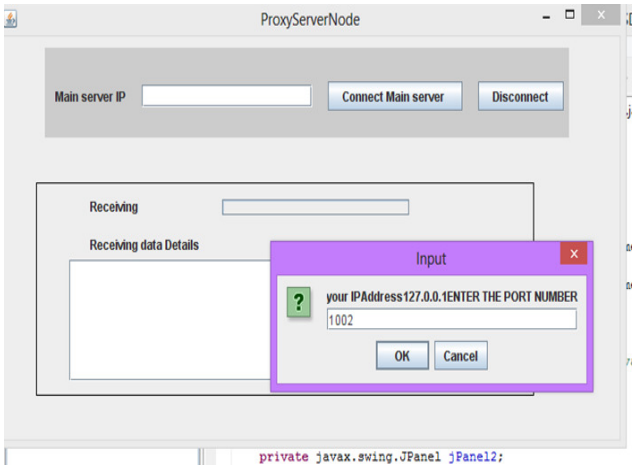

Fig.4 Cloud Server Page

Data Owner Process:
The data owner will be register and login to the cloud and upload encrypted data file into the cloud.

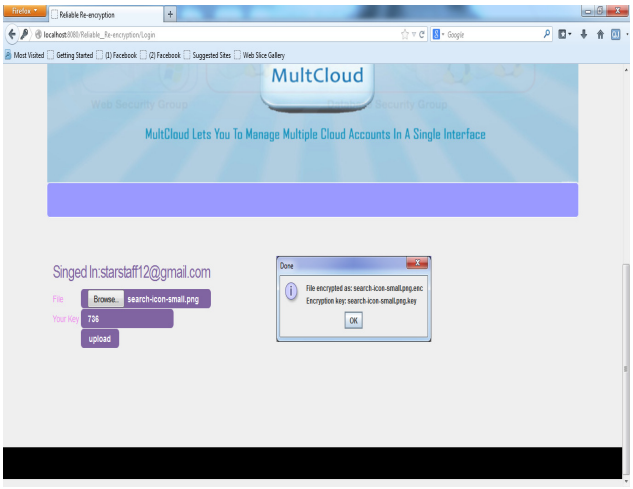

Fig.5 Upload Data Using Encryption Key

The steps are included in this process:

1. Data owner register and login
2. Encrypting data files
3. Upload data files

Data User Process:

The data user are register and login to the cloud, the steps are included in this process:

1. Data user register and login
2. Request Server for key
3. Verify and access server
4. Download the requested data files

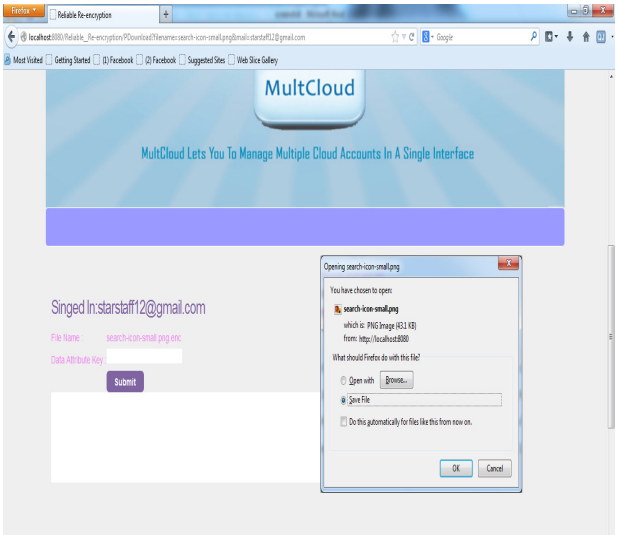

Fig. 6 Download Data Using Attribute Key

7. Conclusion and Future Scope

In this paper, we have worked on the R3 (reliable Re-encryption) scheme, is a new method for managing access control based on the cloud server's internal clock. We have proposed a way for secure cloud computing and used the concept of ABE(Attribute Based Encryption) and PRE (Proxy Re-encryption), proposed one method of time based encryption. Our solution remains secure in many attacks because of instant re-encryption. So that, each and every time attacker will face new combination of cipher-text. Our future work is to allow different effective time periods for different attributes associated with a user.

Acknowledgments

We express our gratitude to Prof. Piyush Dhule for his guidance never ending support and motivation during the project work.

References

[1] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, "Reliable Re- Encryption in Unreliable Clouds"IEEE,2011.

[2] Armbrust m.., A. Fox, A. Joseph, R. Katz, A. Konwinsi, , D. Patterson, A. Rabkin,Lee and Stoica I., "A view of Cloud Computing," communications of the ACM, 2010.

[3] V. Goyal, Pandey O., A. Sahai, and B. Waters, "Attribute-Based Encryption for fine-grained access control of encrypted data," Proc. of ACM, 2006.

[4] J. Bethencourt, Sahai A, and B. Waters, "Ciphertextpolicy attribute based encryption," inProc. of IEEE Symposium on S and P, 2007.

[5] Blaze M.., Bleumer, and M. Strauss, "Divertible protocols and Atomic-Proxy Cryptography," Advances in Cryptology Euro crypt, 1998.

[6] S. Kamara and Lauter K., "Cryptographic cloud storage," security of Data and Financial Cryptography, 2010.

Author's notes

Ajinkya Vijay Adhau Research scholar in the Computer Department, Rajiv Gandhi college of Engineering and Research, RTMNU University. He is pursuing Bachelors Degree in Computer Technology 2015 from RGCER, Nagpur, MH, and India.

Payal Prabhakar Bobade ,Research scholar in the Computer Department, Rajiv Gandhi college of Engineering and Research, RTMNU University. She is pursuing Bachelors Degree in Computer Technology 2015 from RGCER, Nagpur, MH, and India.

Priyanka Sheshrao Zilpe, Research scholar in the Computer Department, Rajiv Gandhi college of Engineering and Research, RTMNU University. She is pursuing Bachelors Degree in Computer Technology 2015 from RGCER, Nagpur, MH, and India.

Yashodhara Girijashankar Fulmali, Research scholar in the Computer Department, Rajiv Gandhi college of Engineering and Research, RTMNU University. She is pursuing Bachelors Degree in Computer Technology 2015 from RGCER, Nagpur, MH, and India