ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

Secure Paper Distribution on Cloud Using Re-encryption

Prof.A.G.Nadaph[1], Amol Dashwant[2], Dipali Bhivare[3], Shrikrishn Badade[4], Pratik Jadhav[5]

Assistant Professor, Dept. Of Computer Engineering, TCOER, Pune, India[1]
Research Scholar, Dept. Of Computer Engineering, TCOER, Pune, India[2]
Research Scholar Dept. Of Computer Engineering, TCOER, Pune, India[3]
Research Scholar, Dept. Of Computer Engineering, TCOER, Pune, India[4]
Research Scholar, Dept. Of Computer Engineering, TCOER, Pune, India[5]

ABSTRACT: Today we are familiar with the concept of cloud. Use of cloud is increased in past decade. As use of cloud is increased, the importance of secure cloud computing is the main issue. Now we can see most of the exams that are held online. University puts the paper on cloud at the time of the exam. College issues that paper and distributes it among all the students. Nowadays there are cases of fraud in university exam section. So the university prefers security majors while putting the data on cloud. In traditional method data owner used to store the data on cloud in encrypted format to get security from un-trusted CSP (Cloud service provider). Data owner then sends the decryption keys to the data user. If data owner wants to revoke some users then he simply just sends the re-encryption commands to cloud server and data owner will again issue the decryption keys to the data user. In traditional methods if the re-encryption command is not getting received by the any server due to any problem revoked user will get access to the data on server. To solve this problem we are using time based re-encryption. We are also using *Attribute based encryption* to encrypt the data on cloud [1].

Keywords: Attribute Based Encryption, Time based re-encryption, cloud computing, proxy re-encryption.

I. INTRODUCTION

Use of cloud computing is very important in today's condition, because cloud concept enhance the view of distributed structure of data, also cloud computing is widely get used because its time and cost saving application. In university for paper distribution we can see the use of cloud. Here Data owner means University put their exam paper on cloud and at the time of the exam. Particular college downloads that paper from the cloud. In this method we get benefit in transportation cost and this is time saving method. Along with this the fraud in the exam section has got increased in the past few years. To avoid this fraud we can use encryption concept for the data or paper on the cloud. There is one technique to protect the data from unauthorized user i.e. to use *attribute based encryption* (ABE).[4]

ABE allow data owner to put their data on cloud in encrypted format. The ABE encryption technique is fully based on *attributes*. In this instead of decryption keys data owner issues attribute key to data user. To access the particular data on a cloud data user must have necessary attribute to satisfy that structure. For example, let there is one access structure that is defined by the data owner like $\{(\alpha1 \wedge \alpha2) \vee \alpha3\}$. According to this access structure the users that are having the attribute structure of either $\alpha1$ and $\alpha2$ or $\alpha3$ can only get access to the particular data on cloud. This method has one drawback, when data owner want to revoke the data user, data owner has to send re-encryption commands to the each server. Sending the re-encryption command to each server to prevent access of data from revoked user called *proxy re-encryption (PRE)*. But this method is not feasible where number of data user get frequently changes. We can call *proxy re-encryption* as a command driven encryption.[1]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

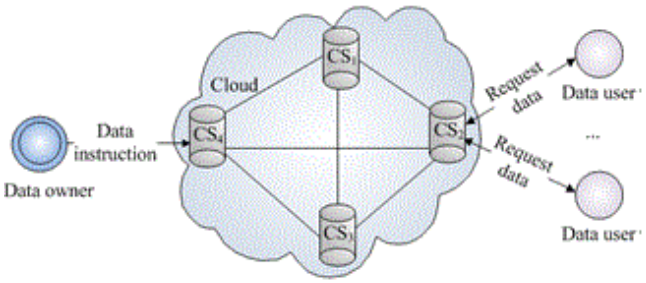

Fig. 1 Network Failure

In command driven encryption data owner sends re-encryption commands to each server. Take an example of above diagram; here we can see there are four cloud servers CS1, CS2, CS3, and CS4. Suppose data owner want to revoke the data user that is previously allowed to access data, data owner sends re-encryption commands to each server. Due to some problems like network congestion or failure does not get the re-encryption command, because of this revoked user get access to the cloud and data owner will get suffered with this loss[1].

Better solution for this problem is that allow each server on cloud to get automatically re-encrypted independently on server clock. In this solution we are using *time based re-encryption*. In this method data owner do not have to send re-encryption command at the time of revoking the data user. Server will automatically get re-encrypted in time based re-encryption.

II. RELATED WORK

In [1] authors proposed the R3 scheme for cloud re-encryption technique. In traditional system command driven encryption technique was used. Command driven technique is not that much useful where number of user that changing rapidly. So, Authors proposed a system which is a combination of ABE and Proxy re-encryption technique. In this paper, wesolve this problem by proposing a time-based re-encryption scheme, which enablesthe cloud servers to automatically re-encrypt data based on their internal clocks. In [1] authors have proposed that data user also can upload the data on cloud. So, we can extend this.In [2] authors proposed an attribute based encryption technique which allows the fine grain access control. We are using the attributes to generate the keys. User having the correct attribute will have access to that file. In [4] authors proposed an encryption technique, Advanced encryption standard. We are using AES to generate the random keys for every attack. When unauthorized user try to access the file on cloud, the cloud server will use the AES algorithm to generate the new key so for each time attacker will face new key. So we can propose that it will increase the level of security for data on cloud.

III. PROPOSED SYSTEM

In proposed system we are using the combination of ABE and PRE which is time based and we can call this system as *Secure University Paper Distribution on Cloud using re-encryption.* In this system first data owner will upload the data on cloud in encrypted form using one primary key. After that data owner will decide which user should have that access in a particular time slot according to that he will again generate new encryption key. The secondary encryption key is a combination of data owner id, the date on which that particular data user is allowed to access that data, and time. After the encryption, data owner will send that primary and secondary key to the data user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

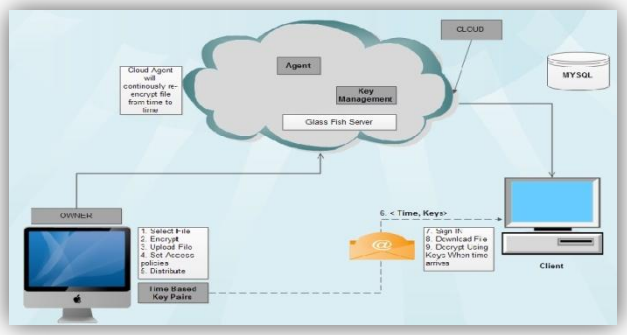

Fig.1 System Architecture

On the other side data user will receive those two keys and he/she get access to that particular data on cloud on an allotted date and time. After getting the access, based on the internal timer, data user will only get access to that data in a particular time slot. When that time slot gets over cloud server will automatically re-encrypt the data.

For example, in the following diagram suppose data user have access to the data on the cloud in the time slot from t2 to t3.

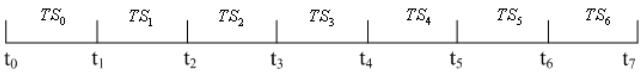

Fig. 3 Timer

Suppose user wants to access that data on a time slot from t1 to t2, here 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.

When that user accesses the data on time slot t2 to t3, user will get access to the data on cloud. Now, when that particular slot gets over cloud server will revoke that user from accessing the data and cloud server will get automatically re-encrypt so that, revoked user will not get access to that data by using previous key after the time slot t2 to t3.

IV. MATHEMATICAL MODEL

Before going through this schema, consider one ideal condition that in this schema all the cloud server shares same synchronized clock because this schema is totally depend on time factor and we are using time based re-encryption which gives enormous power to the data owner to secure his data.

1) *Data owner initialization:* - Data owner first register himself on the system (*DO*). After that, he will upload the file (*F*) on the cloud with the primary key (*PK*). He will assign some users (DU_0-DU_n) to that file such that those '*n*' users are only allowed to access that file from cloud.

2) *Allowing time slots to each user:* - After uploading the file (*F*) and allowing some users (DU_0-DU_n) data owner has to allocate time slots (*TS*) for each user. For user from DU_0 toDU_n time slots will be $TS_0$to TS_n. As per the slots each user will get the secondary key (*SK*). Secondary key is the encryption attribute which is formed by the combination of data user id, primary key (*PK*), allowed date and allowed time. Here we are using double encryption schema at the time of uploading the file.

3) *Download the file from cloud:* - Each data user will receive the key (*K*) through the mail. After that, data user (*DU*) will try to download the file from cloud. As we are using double encryption at the time of uploading the data, data user should have to first decrypt the file using secondary key (*SK*). After that he has to enter the primary key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

(*PK*) for downloading the final key.If the user is trying to access the file before allotted time slot or after allotted time slot, data user will not get the access to the file.

For example, suppose data user (*DU*) is allowed to access the file on 24th January at 9 am and data user (*DU*) is trying to access that file on 23th January at 4 pm. First cloud server will generate the secondary key using the current time that is 23th January at 4 pm which is not matching to the allotted time. So that, cloud server will not allow data user (*DU*) to access that file. And for security purpose cloud server will get re-encrypted by using the next combination which is comprised of current time. So that we can say at each new attack cloud server will get re-encrypted so this will give the best security majors for the data on cloud.

(DO, id, password):- For data owner (DO) initialization
Upload (F):- Upload the file on cloud.
Gen (PK):- Generate primary key.
Gen (SK, DU):- Generate secondary key for each user.
Decrypt (SK, F):- Decrypt file (F) using SK.
Download (PK, F):- Download the file from cloud.

Equation on data user side:-

IF Current time (TS_c) = Allowed time (TS_a) then
Allow user to download the file
Else
Do not allow user to download the file

Equation on data user side after the time slot:-

If Current time (TS_c) > End of Allowed time slot (TS_a) then
Re-encrypt the data to revoke user

Equation on data user side when user tries to access data before or after allowed time slot:-

If Current time (TS_c) != Allowed time (TS_a) then
Re-encrypt the clod data using current time
Else
Allow data user (DU) to access that file

V. ALGORITHMS

Attribute Based Encryption (ABE) Algorithm:-

ABE allow data owner to put their data on cloud in encrypted format. The ABE encryption technique is fully based on *attributes*. In this instead of decryption keys data owner issues attribute key for data user. To access particular data on a cloud data user must have necessary attribute to satisfy that structure.

For example, let there is one access structure that is defined by the data owner like $\{(\beta1 \wedge \beta2) \vee \beta3\}$. According to this access structure the users that are having the attribute structure of either β1 and β2 or β3 can only get access to the particular data on cloud.

In Encryption there are two main things that we use ciphertexts and private keys. In attribute based encryption ciphertexts are used with the help of attributes and access structure is used as a private keys.

Proxy re-encryption (PRE) Algorithm:-

We can call proxy re-encryption algorithm as command driven algorithm. In this algorithm we manually send command to the each cloud server and that command contains the encryption pattern. When data owner want to revoke the data user, data owner has to send re-encryption commands to the each server. Sending the re-encryption command to each server to prevent access of data from revoked user called *proxy re-encryption (PRE)*. But this method is not feasible where number of data user get frequently changes. We can call *proxy re-encryption* as a command driven encryption.

This encryption is very efficient when the number of users is less. So that data owner will not face any overhead while sending the re-encryption commands.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

In proxy re-encryption we have assumed some ideal conditions like there should be no network outage so that each cloud server will receive the re-encryption command from data owner. To overcome this disadvantage of proxy re-encryption we are proposing the proxy re-encryption with time based pattern.

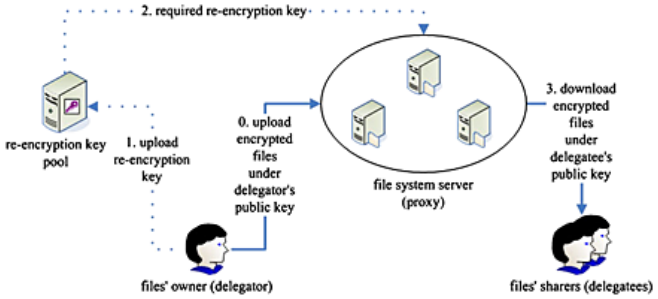

Fig. 4 Proxy Re-encryption

Time based re-encryption:-

In time based re-encryption data owner allow particular slot for each data user. Then each data user get access to the data on cloud on that particular slot but when that slots gets over cloud server should get re-encrypt the data to revoke the previous user. For this data owner can send manual re-encryption command to each cloud server but this is very hectic job and if one of the cloud server does not get the re-encryption command due to the network congestion that server will remain open for revoked user. For this problem we are using time based re-encryption technique. In this technique, cloud server will get automatically re-encrypted. So that, it will reduces the hectic job of data owner and we do not need to worry about network problem.

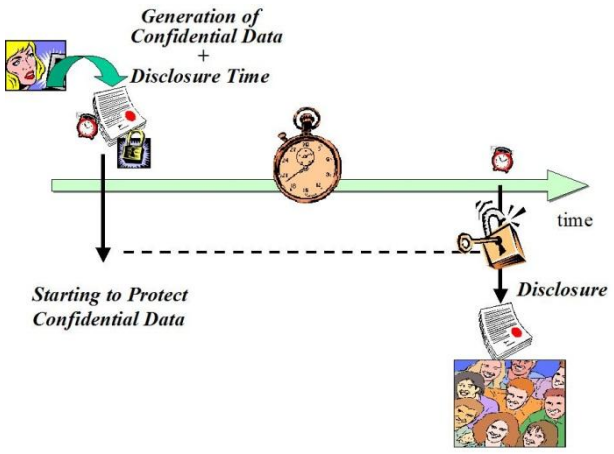

Fig. 5 Time Based Encryption

Advanced Encryption Standard (AES) Algorithm:-

We are using AES algorithm for encryption and re-encryption. It is symmetric key algorithm it can use the same keys or related keys for encryption and decryption of data. We are using two keys primary key and secondary key, primary key is given by owner and secondary key is generated using different attributes. Data owner sends keys to the data user via mail. Using primary key and secondary key data user decrypts the file. At a time 16 bit data is given as input and we get the 16 bit data as a output. If we used larger key size it becomes more difficult to get the encrypted data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

AES is the Advanced Encryption Standard algorithm for encrypting and decrypting data. AES is a advancement over DES. In AES there is a cipher which is of 128 bits. In AES key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds.

The main loop of AES9 performs the following functions:
• SubBytes()
• ShiftRows()
• MixColumns()
• AddRoundKey()

VI. CONCLUSION

In this paper we have proposed a way for secure cloud computing. We have used the concept of ABE and PRE and proposed one method of time based encryption. This method is very helpful in many applications like university paper distribution, deployment of product on time basis. We showed that our solution remains secure in many attack because of instant re-encryption. So that, each time attacker will face new combination of cipher-text.

REFERENCES

1. Qin Liu , Chiu C. Tan, Jie Wu and Guojun Wang, "*Reliable Re-Encryption in Unreliable Clouds*", IEEE transactions School of Information Science and Engineering, Central South University, Changsha, Hunan Province, P. R. China,2011
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-based encryption for fine-grained access control of encrypted data*," in Proc. of ACM CCS, 2006
3. G. Wang, Q. Liu, and J. Wu, "*Hierarchical attribute-based encryption for fine-grained access control in cloud storage services*, "in Proc. of ACM CCS (Poster), 2010.
4. J. Nechvatal, et. al., "*Report on the Development of the Advanced Encryption Standard (AES),"* National Institute of Standards and Technology, October 2, 2000
5. Silicon Laboratories Inc. "*Advances Standard Encryption*"400 West Cesar Chavez Austin,2006
6. For Attribute based Encryption http://link.springer.com/chapter/10.1007%2F978-3-642-36362-7,2011
7. Alexandra Boldyreva,VipulGoyalyVirendraKumarz*"Identity-based Encryption with E_client Revocation"* 14th ACM Conference on Com-puter and Communications Security, CCS 2008, ACM Press, 2008.

BIOGRAPHY

Amol Babanrao Dashwant is a Research scholar in the Computer Department, Trinity college of Engineering and Research, Pune University. He is pursuing Bachelors Degree in Computer Engineering 2014 from TCOER, Pune, MH, and India.

Dipali Kantilal Bhivare is a Research scholar in the Computer Department, Trinity college of Engineering and Research, Pune University. She is pursuing Bachelors Degree in Computer Engineering 2014 from TCOER, Pune, MH, and India.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

Shrikrishn Baliram Badade is a Research scholar in the Computer Department, Trinity college of Engineering and Research, Pune University. He is pursuing Bachelors Degree in Computer Engineering 2014 from TCOER, Pune, MH, and India.

Pratik Kiran Jadhav is a Research scholar in the Computer Department, Trinity college of Engineering and Research, Pune University. He is pursuing Bachelors Degree in Computer Engineering 2014 from TCOER, Pune, MH, and India.