Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 9, September 2016, pg.76 – 80

PROVIDING SECURITY BY DATA RE-ENCRYPTION IN CLOUD

Mr. Satheesh[1], Ms. Rohini[2]
[1]M.Tech Student, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India
[2]Assistant Professor, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, India
[1] SathiA62@gmail.com; [2] Rohini.antharmuki@gmail.com

Abstract- *Cloud computing allows the users to share the data among the members of cloud effectively. The use of cloud is increasingly popular as the data maintenance cost is low and also the data will be out-sourced. But the security is not up to the mark. The key approach to secure data in cloud is to encrypt the data. Then authorized users are provided with decryption key to decrypt the encoded data. Here the problem is whenever a user is removed from cloud the data owners will send re-encryption command to cloud in order to re-encrypt the data so that the data is prevented from revoked users. But sometimes such commands may not be executed by all the servers due to unreliable network communication. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud. In this paper we solve this problem by proposing a time based re-encryption scheme. This scheme enables the cloud servers to automatically re-encrypt data based on their internal clocks. Also attribute based encryption scheme is used to provide fine grained access control.*

KEYWORDS: *Attribute based encryption, Proxy-re encryption, Cloud computing*

I. INTRODUCTION

Cloud computing is a technology that delivers many kinds of resources as services, mainly over the internet. The use of cloud computing is increasingly popular due to the potential cost savings from outsourcing data to the cloud service provider (CSP). One technique to protect the data from a possible untrusted CSP is for the data owner to encrypt the outsourced data]. Flexible encryption schemes such as attribute based encryption (ABE) can be adopted to provide fine grained access control. The key problem of storing encrypted data in the cloud lies in revoking access rights from users. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud. A naive solution is to let the data owner immediately re-encrypt the data, so that the revoked users cannot decrypt the data using their old keys, while distributing the new keys to the remaining authorized users.

II. RELATED WORK

2.1 Attribute Based Encryption (ABE)

ABE allows data to be encrypted using an access structure comprised of different attributes. Instead of specific decryption keys for specific files, users are issued attribute keys. Users must have the necessary attributes that satisfy the access structure in order to decrypt a file. For example, a file encrypted using the access structure means that either a user with attributes or a user with attribute.

2.2 Proxy Re-Encryption

Proxy Re-Encryption takes advantage of the abundant resources in a cloud by delegating the cloud to re-encrypt data This approach is also called command- driven re-encryption scheme, where cloud servers execute re encryption while receiving commands from the data owner. command-driven re-encryption schemes do not consider the underlying system architecture of the cloud environment. A cloud is essentially a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. As a distributed system, the cloud will experience failures common to such systems, such as server crashes and network outages. As a result, re-encryption commands sent by the data owner may not propagate to all of the servers in a timely fashion, thus creating security risks.

III. EXISTING SYSTEM

In existing system when a user is revoked they will be using the keys which were issued before to decrypt the data from the cloud. Here unauthorized users access the data of authorized users. To prevent the revoked user from decrypting the data the data owner will issue re-encryption commands to the cloud to re-encrypt the data. Then new decryption keys are generated and given to valid users, so that they can continue to access the data. However, since a cloud computing environment is comprised of many cloud servers, such commands may not be received and executed by all of the cloud servers due to unreliable network communications.

Disadvantages

The disadvantages of the existing system are listed below:-

- Unauthorized users access the data of authorized users.
- Revoked users uses their old keys to decrypt the data once after they are removed from the group.
- Sometimes re-encryption commands may not reach to all of the cloud servers due to unreliable network communication.
- Data security is less.

IV. PROPOSED SYSTEM

In the proposed system we solve above listed problems by proposing a time based re-encryption scheme. This scheme enables the cloud servers to automatically re-encrypt data based on their internal clocks. Also attribute based encryption scheme is used to provide fine grained access control. The objective of the project is to provide security against the revoked users and not allowing them the to access the data of authorized users.

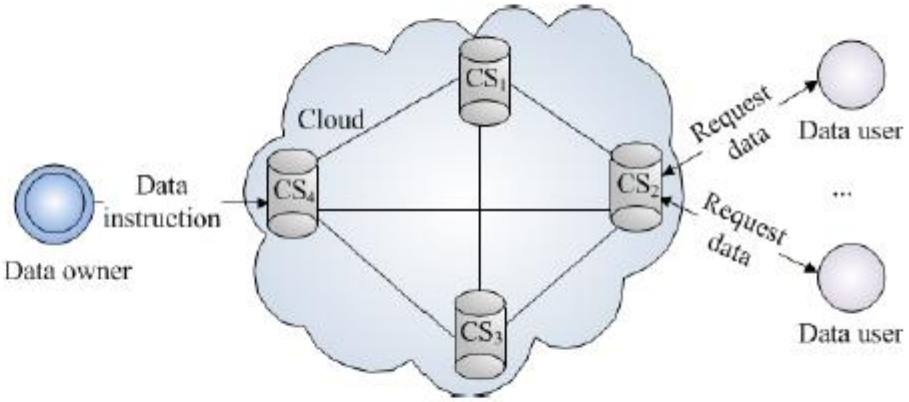
Advantages

The advantages are listed below:-

- Authorized users can only access their data. Unauthorized users are restricted from accessing the sensitive data of authorized users.
- Cloud servers automatically re-encrypt the data whenever a user is revoked. Hence they cannot access the data of authorized users.
- Reliable re-encryption schema provides good security against revoked users.
- In the proposed mechanism, we have proposed ABE algorithm which only allows the users with specific attributes can only access the data.

System Architecture

Proxy Re-Encryption takes advantage of the abundant resources in a cloud by delegating the cloud to re-encrypt data. This approach is also called command- driven re-encryption scheme, where cloud servers execute re encryption while receiving commands from the data owner. A cloud is essentially a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. As a distributed system, the cloud will experience failures common to such systems, such as server crashes and network outages. As a result, re-encryption commands sent by the data owner may not propagate to all of the servers in a timely fashion, thus creating security risks.



To illustrate, let us consider a cloud environment shown in Fig. 1, where the data owner's data is stored on cloud servers *CS*1*;CS*2*;CS*3*;CS*4. Assume that the data owner issues to *CS*4 a re-encryption command, which should be propagated to *CS*1*;CS*2*;CS*3. Due to a network outage, *CS*2 did not receive the command, and did not re-encrypt the data. At this time, if revoked users query *CS*2, they can obtain the old cipher text, and can decrypt it using their old keys. So in this paper we propose a reliable re-encryption scheme in unreliable clouds (R3 scheme for short). R3 is a time-based re-encryption scheme; this allows each cloud server to automatically re-encrypt data based on its internal clock. The basic idea of the R3 scheme is to associate the data with an access control and an access time.

We propose an automatic, instant mailing system suitable for cloud environments. We extend an ABE scheme by advanced mailing password to the valid data user .Our solution does not require perfect clock synchronization among all of the cloud servers to maintain correctness. The advantage of this R3 scheme are When you use internet with the cloud services then your company will have lots more room to store the files and that they need to store. User identified the data losses. Data security and access control when users require data for sharing on cloud server.

V. IMPLEMENTATION

MODULES

Data owner process

In the cloud, data owner is the owner of the data or file. Initially the data owner will register at the cloud and login to the cloud. When the data owner registers himself in to cloud, he will encrypt his file and he uploads it into the cloud.

The steps involved in this process are:

1. Data owner initialization

2. Data user read data

3. Encrypting file

4. Uploading file

Cloud service provider (CSP) Process- server

In the cloud, the CSP are provides services to the client. The CSP server also registers itself to the cloud and obtains its ID. When the server login it views the encrypted file uploaded by the data owner

The steps involved in this process are:

a. CSP registration

b. CSP login

c. Viewing uploaded file

d. Downloading file

Data User Process

There are two types of data user adversary user and malicious user

a. Adversary user: - user who just views the file

b. Malicious user: - user who views and alters the file

The data user must register to login to the cloud, in this main module there are two sub modules a) Server request: It is the sub module by which the data user requests the server to access the required file, here with the help of register

ID obtained from the server the data user will login. After the data user login to the cloud the server ensures that he is a valid user. b) Access server: It is the other sub module where the data user gets the password from his mail inbox. Using that password will login to the server access .Then data user will select the server (i.e. CS0, CS1, CS2….CSn) to view the required file. After he views the requested file he can download that file

The steps involved in this process are:

a. Data user registration
b. Data user login
c. Server request
d. Access server
e. Downloading the requested file

CONCLUSION

In this paper we proposed a scheme called R3 which provides good access control to users based on the internal clock.R3 scheme provides security against un-authorized users. This re-encryption technique does not rely on the cloud to reliably propagate re-encryption commands to all servers to ensure access control correctness. This solution remains secure even without perfect clock synchronization of cloud servers.

REFERENCES

[1] S. Kamara and K. Lauter, “Cryptographic cloud storage,” Financial Cryptography and Data Security, 2010.
[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “A view of cloud computing,” Communications of the ACM, 2010.
[3] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” Advances in Cryptology–EUROCRYPT, 2005.
[4] 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.
[5] J. Bethencourt, A. Sahai, and B. Waters, “Cipher text-policy attribute based encryption,” in Proc. of IEEE Symposium on S&P, 2007.
[6] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” Advances in Cryptology–EUROCRYPT, 1998.
[7] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. of ACM CCS, 2008.
[8] 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.
[9] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. of IEEE INFOCOM, 2010.
[10] Qin Liu, Chiu C. Tan, Jie Wu, and Guojun Wang, “Reliable Re- Encryption In Unreliable Clouds”IEEE,2011.