ISSN (Online): 2456-5717
International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.4 Issue.3 March 2018

Securing File Access using Revocable Storage Identity based Encryption in Big Data

[1]K.Mahesh Kumar, [2]B.Benita
[1]PG Scholar, Dept. of CSE, Francis Xavier Engineering College, Vannarpettai, Tirunelveli.
[2]Asst. Prof., Dept. of CSE, Francis Xavier Engineering College, Vannarpettai, Tirunelveli.

Abstract- **Big Data provides a simplest way of data processing, which provides various benefits to the users. But directly outsourcing the shared data to the server will bring security issues as the data may contain valuable information. Hence, it is necessary to place cryptographically enhanced access control on the shared data, named Identity based encryption to build a practical data sharing system. When some user's authorization is expired, there should be a mechanism that can be removed from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data. The various techniques are available to support user privacy and secure data sharing. In this paper focus on various schemes to deal with secure data sharing such as data sharing with forward security, secure data sharing for dynamic groups, attribute based data sharing, encrypted data sharing and Shared authority based Privacy-Preserving authentication protocol for access control of outsourced data. In this proposed notion called as Revocable Identity Based Encryption (RIBE), which has introducing the functionalities of a user revocation and the cipher text update simultaneously.**

Keywords- Data Sharing, Privacy-Preserving, Forward Security, Identity Based, Revocation

I. INTRODUCTION

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud, Microsoft's Azure and Amazon's S3, can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society. However, it also suffers from several security threats, which are the primary concerns of cloud users. Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's

authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. A natural solution to conquer the aforementioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals.

II. RELATED WORK

In this earlier work the data provider first decides the users who can access the data then the data provider encrypts the data under the identities of users whom are decided by the data provider and uploads the cipher text of the shared data to the cloud server.

When the user wants to get the shared data, she or he can download and decrypt the corresponding cipher text.

However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available. However in some situations authorization gets expired then the data provider can download the cipher text of the shared data and decrypt-then-re-encrypt the shared data

Modules:

1. Data Provider
2. Cloud Server
3. Key Revocation
4. Storage Server

III. DEVELOPMENT OF SYSTEM

The proposed system provides effective solution as Compared to most of the existing systems. It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfils the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the cipher text such that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period.

1. Data Provider

In this module, the data provider first decides the users who can share the data. Then, data owner encrypts the data under the identities shared users, and uploads the cipher-text of the shared data to the cloud server.

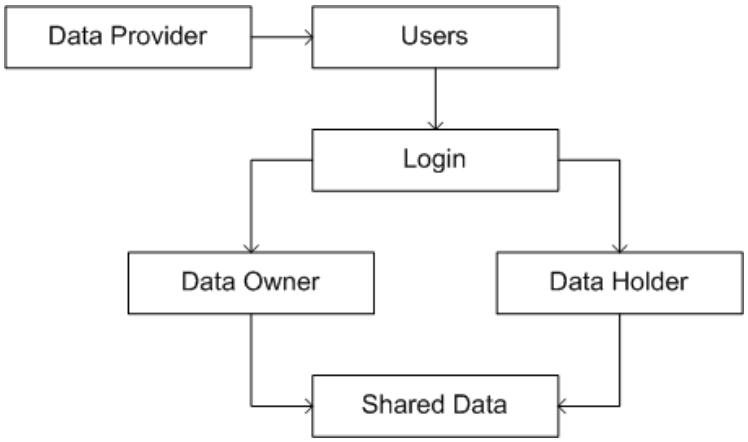

Fig. 1. Data Provider

2. Cloud User

In this module, cloud users get the shared data, can download and decrypt the corresponding cipher-text. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available. In some cases, users authorization gets expired, shared can download the cipher-text of the shared data, and then decrypt-then-re-encrypt the shared data such that data owner is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

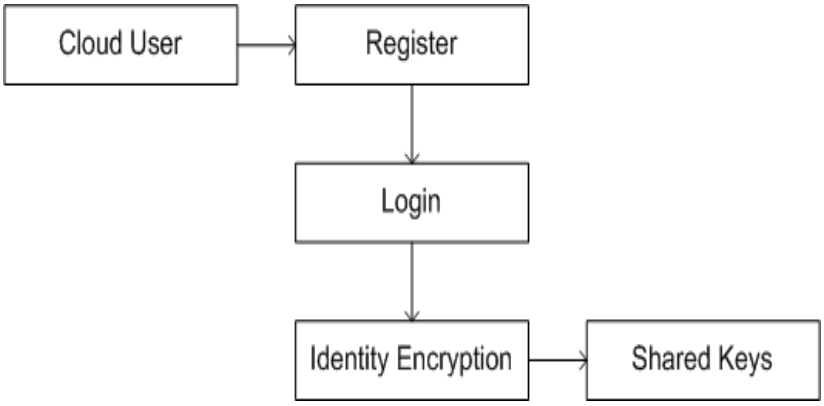

Fig. 2. Cloud User

3. Key Revocation

In this module, delegating the generation of re-encryption key to the key authority, the cipher-text size of their scheme also achieves constant. However, to this end, the key authority has to maintain a data table for each user to store the user's secret key for all time period, which brings storage cost for key authority.

ISSN (Online): 2456-5717
International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.4 Issue.3 March 2018

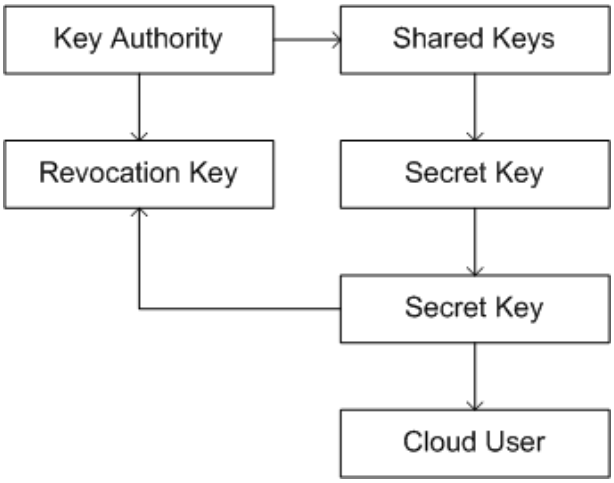

Fig.3. Key Revocation

4. Storage Server

A cloud service provider has huge storage space, computation resource and shared service to provide the clients. It is responsible for controlling the data storage in outside users' access, and provides the corresponding contents.

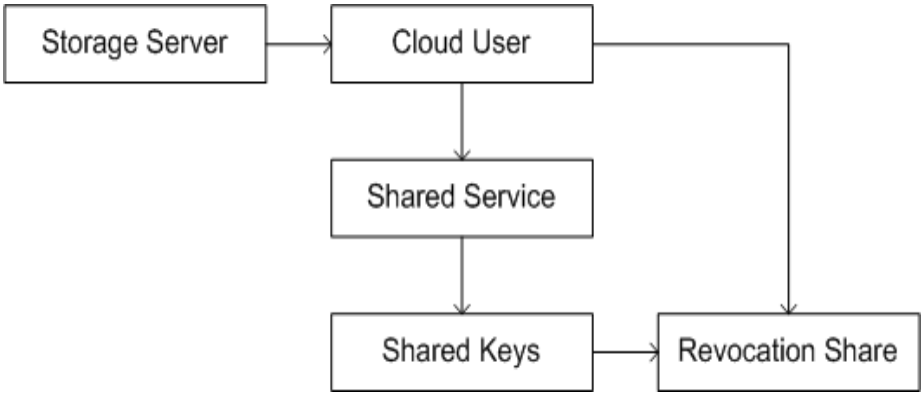

Fig. 4. Storage Server

IV. IMPLEMENTATION

1. $X,Y \leftarrow -\ \emptyset$
2. *for all* $(\eta i , ti) \in RL$ *do*
3. *if* $ti \leq t$ *then*
4. *Add Path*(ηi) *to X*
5. *end if*

6. *end for*
7. *for all θ ∈ X do*
8. *if θl ∈/ X then*
9. *Add θl to Y 10: end if*
10. *if θr ∈/ X then*
11. *Add θr to Y*
12. *end if*
13. *end for*
14. *if Y = Ø then*
15. *Add the root node ε to Y*
16. *end if*
17. *return Y*

V. CONCLUSION

The proposed work can be focused on the critical issue of identity revocation, has been introduced outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme will achieves constant efficiency for both computation at PKG and private key size at user. User needs not to contact with PKG during key update. In other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. No secure channel or user authentication is required during key update between user and KU-CSP. Furthermore, it will consider realizing revocable IBE under a stronger adversary model.

In this Proposed System has an advanced construction and show it is secure under RDoC model, in which at least one of the KU-CSP is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSP collude, it is unable to help such user re-obtain decryptability. Finally, the system should provide extensive experimental results to demonstrate an efficiency of the proposed construction.

In this work leads to analysis the revocation method for multi-authority cloud storage will support more secure and efficient revocation scheme with less CPU process. Also implementation of Forward and Backward Security feature will enable the user to verify the data modification from the storage service with higher accuracy level.

REFERENCES

[1] Agalya, R. V., and K. Karthika Lekshmi, "A Verifiable Cloud Storage Using Attribute Based Encryption and Outsourced Decryption with Recoverability", International Journal of Engineering and Innovative Technology, Volume 3, Issue 10, April 2014.

[2] Wei, Jianghong, Wenfen Liu, and Xuexian Hu ," Secure Data Sharing In Cloud Computing Using Revocable-Storage Identity based Encryption**"**, vol.57,no.2,pp. 137-154, 2016.

[3] Huang, Jyun-Yao, I-En Liao, and Chen-Kang Chiang," Efficient Identity-Based Key Management For Configurable Hierarchical Cloud Computing Environment", IEEE 17th International Conference on parallel and Distributed Systems,2012.

[4] Qiu,Shuo," Identity-Based Private Matching Over Outsourced Encrypted Datasets", IEEE Transactions on Cloud Computing, 2015.

[5] Tseng, Yuh-Min," Identity-Based Encryption with Cloud Revocation Authority and its Applications", IEEE Transactions on Cloud Computing, 2016.