International Journal of Research in Engineering, Science and Management
Volume-2, Issue-1, January-2019
www.ijresm.com | ISSN (Online): 2581-5792

Secure Cloud Computing: Data Sharing using Revocable-Storage Identity-based Encryption

K. Bharathi[1], G. K. Roopa[2]
[1,2]*Assistant Professor, Department of CSE, Vivekananda College of Engineering & Technology, Puttur, India*

***Abstract*: Cloud computing provides a simplest way of data sharing; it provides various benefits to the users. But directly outsourcing the shared data to the cloud 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 remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. Thus, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which introducing the functionalities of user revocation and cipher text update simultaneously.**

***Keywords*: Revocation, Encryption, Key Exchange, Private Key generator, cipher text.**

1. Introduction

A. Cloud computing

Cloud computing facilitates good computation capacity and large memory space at a low cost. It is reliable and consistent, due to the organization that does not need to build or maintain their own in-house computer infrastructure. 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 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.

B. Identity based encryption

Identity Based Encryption is a type of the public key in which the public key of the user is some unique information about the identity of the user's (e.g email address). This means sender who has an access to the public parameters of the system can encrypt a message using identity, as a key. The receiver obtains its decryption key from a central authority, which has needs to be trusted as it generates secret keys for every user. The main advantage of the identity based encryption is that if there are only finite number of users, after all users have been issued with keys the third party's secret key can be destroyed.

C. Revocable storage

The Revocation means that Capable of Cancellation. The non-revocable data sharing system provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. To avoid this problem, the revocation storage makes use of cloud server.

2. Literature survey

- *K.Chard K.Bubendorfer S.Caton O.F.Rana* introduced Social cloud computing: Vision for socially motivated resource sharing. It demonstrates the approach using a social storage cloud implementation in Facebook application. The main advantage of this technique is that, it provides infrastructure and enables sharing of heterogeneous resources. Sharing resources within social cloud is not feasible and exchanged resources should be symmetric.
- *C. Wang S.S Chow Q. Wang Ren W.* Lou proposed Privacypreserving public auditing for secure cloud storage Propose a privacy preserving public auditing system for data storage security in cloud computing. This method eliminates the burden of cloud user from expensive auditing task and reduces the outsourced data leakage. The main problem of this method is cannot robustly cope with large amount of data.
- *K. Yang X. Jia* proposed an efficient and secure dynamic auditing protocol for data storage in cloud computing. It helps in an efficient and inherently

secure dynamic auditing protocol which protects the data privacy against the auditor. This method has lots of advantages such as Dynamic operations that can be done efficiently, securely and at a low computation cost. But it fails to decrypt the data without masking technique.

- *X. Huang J. Liu S. Tang Y. Xiang K. Liang L. Xu* proposed Cost effective authentic and anonymous data sharing with forward security It helps in a a forward secure ID based ring signature essential for building cost effective authentic and anonymous data sharing system. The main advantage of this method is Forward secure ID based system ring signature provides forward security But Relies on random Oracle assumption to prove its security
- *Certificate-based encryption:* A certificate, namely a signature acts not only as a certificate but also as a decryption key. A key holder needs both its secret key and an up-to-date certificate from its CA to decrypt a message. Certificate-based encryption combines the best aspects of identity based encryption and public key encryption. Certificates include at least the name of a user and its public key. Often, the certificate authority includes a serial number as well as the certificate issue date and expiration date.
- *Identity based encryption:* Identity-Based Encryption (IBE) takes a effective approach to the problem of encryption key management. IBE can use any string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the generation of private decryption keys. By separating authentication and authorization from private key generation through the key server, permissions to generate keys can be controlled dynamically on a granular policy driven basis, facilitating granular control
- over access to information in real time.

3. Existing system

- Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority.
- Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users.
- Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant ofWater's IBE scheme.
- Chen et al. constructed a RIBE scheme from lattices.

A. Disadvantages of existing system

Unfortunately, existing solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. However, existing scheme only achieves selective security. This kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users. Furthermore, to update the cipher-text, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

B. Proposed system

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.

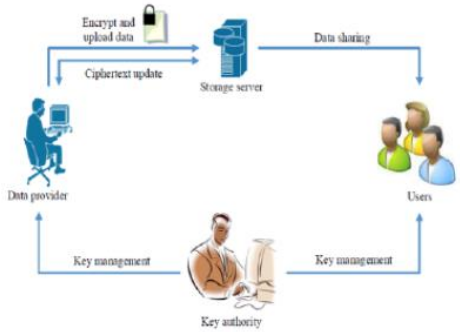

Fig. 1. A natural RIBE-based data sharing system

A RIBE-based data sharing system works as follows:

- *Step 1:* The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher-text of the shared data to the cloud server.
- *Step 2:* When either Alice or Bob 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.
- *Step 3:* In some cases, e.g., Alice's authorization gets expired, David can download the cipher-text of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

C. Advantages of proposed system

We provide formal definitions for RS-IBE and its corresponding security model;

- We present a concrete construction of RS-IBE.
- The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure
- The procedure of cipher text update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by $O(\log(T)^2)$, where T is the total number of time periods.

In the proposed system, we used a concept called revocable-storage identity-based encryption (RSIBE) for building a cost-effective data sharing system that fulfils the three security goals. The security goals are:

- *Data confidentiality:* 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.
- *Backward secrecy:* Backward secrecy says that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.
- *Forward secrecy:* Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

The proposed system attains the following characteristics:

- We can provide formal definitions for RS-IBE and its corresponding security model; and backward/forward secrecy simultaneously.
- We prove that the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption.
- In addition to security, this system will reduce the time complexity and provide a better performance.

4. Conclusion

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and cipher-text update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

References

[1] J. Wei, W. Liu and X. Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," in *IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 1136-1148, 1 Oct.-Dec. 2018.

[2] K. Chard, K. Bubendorfer, S. Caton and O. F. Rana, "Social Cloud Computing: A Vision for Socially Motivated Resource Sharing," in *IEEE Transactions on Services Computing*, vol. 5, no. 4, pp. 551-563, Fourth Quarter 2012.

[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," in *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[4] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1717-1726, Sept. 2013.

[5] X. Huang *et al*., "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," in *IEEE Transactions on Computers*, vol. 64, no. 4, pp. 971-983, 1 April 2015.

[6] Create Your Own Hosted Cloud Storage Server in Minutes-wnCloud https://www.youtube.com/watch?v=BeAMq6TgGus&t=33s

[7] Idea on Create a user account in owncloud https://www.youtube.com/watch?v=esN1VL etSxI