# Data Sharing in Cloud Computing Using (RS-IBE) Revocable Storage Identity-Based Encryption Method

**Suraj Kumar B P[1] , Dr. S Sathish Kumar[2]**
[1]*Final year, MTech, Department of Computer Science, RNS Institute of Technology Bengaluru, India*
[2]*Professor, Department of Computer Science, RNS Institute of Technology, Bengaluru, India*

## ABSTRACT

*Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity based encryption is a promising crypto graphical primitive to build a practical data sharing system. However, access control is not static. That is, 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. A revocable storage identity based encryption (RS-IBE) is used which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, A concrete construction of RS-IBE and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.*

**Key Words:** *RS-IBE, Cloud computing, Cipher text and Cryptographic*

## 1. 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.

•**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 means 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.

## 2. RELATED WORK

**Revocable Identity-Based Encryption**

The concept of identity-based encryption was introduced by Shamir [1], and conveniently instantiated by Boneh and Franklin [2]. IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed. In the traditional PKI setting, the problem of revocation has been well studied [3] and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin [4] 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. Unfortunately, such a 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. To conquer this problem, Boldyreva, Goyal and Kumar [5] 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. However, this scheme only achieves selective security. Recently, Seo and Emura [6] proposed an efficient RIBE scheme resistant to a realistic threat called decryption key exposure, which means that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods. Inspired by the above work, Liang et al. [7] introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and cipher text update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme [8] to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious unrevoked users can share the update key with those revoked users. Furthermore, to update the ciphertext, 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. In 1997, Anderson [9] introduced the notion of forward security in the setting of signature to limit the damage of key exposure. The core idea is dividing the whole lifetime of a private key into discrete time periods, such that the compromise of the private key for current time period cannot enable an adversary to produce valid signatures for previous time periods.In CRYPTO 2012 Sahai, Seyalioglu and Waters [10] proposed a generic construction of so-called revocable storage attribute-based encryption,which supports user revocation and ciphertext update simultaneously.In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of ciphertext update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

## 3. PROPOSED 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 fulfills the aforementioned security requirements for data sharing.RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period.

A RIBE-based data sharing system works as follows:

Step 1: The data provider (e.g.,Rakesh) first decides the users (e.g,Amitha and Babitha) who can share the data. Then, Rakesh encrypts the data under the identities Amitha and Babitha, and uploads the ciphertext of the shared data to the cloud server.

Step 2: When either Amitha or Babitha wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. 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., Amitha's authorization gets expired, Rakesh can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that Amitha is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

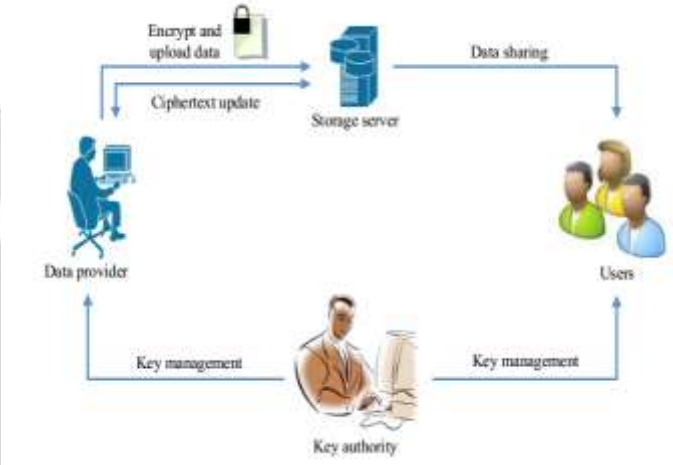


**Fig-1:** System Architecture

In this system architecture 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 ciphertext of the shared data to the cloud server. When the users wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not availableHowever in some situations authorization gets expired then the data provider can download the ciphertext of the shared data and decrypt-then-re-encrypt the shared data such that user whose authorization has been expired is prevented from accessing the plaintext of the shared data and then upload the re-encrypted data to the cloud server again ensuring backward secrecy and forward secrecy.

## 4. IMPLEMENTATION

To show the practical applicability of the proposed RSIBE Scheme, The implementation is taken on a Linux-like system (Win7 + MinGW) with an Intel(R) Core(TM) i5 CPU (650@3.20GHz) and 4.00 GB RAM.In the implementation,we present the running time of the basic algorithms,PKGen (The private key generation Algorithm),KeyUpdate(The Key Update algorithm),DKGen(The decryption key generation algorithm),Encrypt(The encryption algorithm),CTUpdate(The ciphertext update algorithm) and Decrypt(The decryption algorithm),Revoke (The revocation algorithm) for different choice of the total number of time periods.To generate the experimental results, we perform as the following procedure: generate the private key and encrypt a message at the initial time period, then, periodically update the private key and the ciphertext, and decrypt the ciphertext. For a small number of time periods the running time of each algorithm is obtained by computing the average of running the above procedure 100 times. While, for a large number of time periods the running time for each algorithm is obtained by running the above procedure only once, and the running time for update algorithm is the mean of the first 512 time periods.We observe that, the time costs of the algorithms PKGen, KeyUpdate, DKGen and Decrypt are independent of the total number of time periods, and no more than 40 milliseconds.On the other hand, it takes less than 1 second for the user to initially encrypting the message, which would be shared on the cloud. Although the time cost of the algorithm CTUpdate is apparently greater than other algorithms, it is run by a cloud server with powerful capability of computation.Thus, our RS-IBE scheme is feasible for practical applications.

## 5. CONCLUSION

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet to build a cost-effective and secure data sharing system in cloud computing, Hence RS-IBE, which supports identity based revocation and ciphertext 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 RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption.The comparison results demonstrate that scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

## 6. ACKNOWLEDGMENT

I would like to thank my parents for their constant support and motivation and my internal guide Prof. S Sathish Kumar, Department of Computer Science at RNS Institute of Technology for their guidance in successfully undertaking the project. I would also like to thank our beloved Dr. G T Raju, who is the professor, dean and HOD of Department of Computer Science for the encouragement and support. Finally I would also like to thank my teaching and non-teaching staff for providing us wonderful teaching and all the necessary support.

## 7. REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586– 615, 2003.

[3] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 417–426.

[5] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in *Public-Key Cryptography–PKC 2013*. Springer, 2013, pp. 216–234.

[6] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Computer Security-ESORICS 2014*. Springer, 2014, pp. 257–272.

[7] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts," *International journal of information security*, vol. 12,no. 4, pp. 251–265, 2013.

[8] R. Anderson, "Two remarks on public-key cryptology (invited lecture)," 1997.

[9] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advancesin Cryptology–CRYPTO 2012*. Springer, 2012, pp. 199–217.

[10] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advances in Cryptology–CRYPTO 2012*. Springer, 2012, pp. 199–217.