

Revocable-Storage Identity-Based Encryption in Cloud Computing

Chinthaguntla Aparna

B.Tech Student,
Department of CSE,
Mahatma Gandhi Institute of
Technology.

G Mounika Reddy

B.Tech Student,
Department of CSE,
Mahatma Gandhi Institute of
Technology.

G.Naga Sujini

Assistant Professor,
Department of CSE,
Mahatma Gandhi Institute of
Technology.

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 cryptographic 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. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present 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. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

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.

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographic tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data.

EXISTING SYSTEM

- Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, 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 of Water's IBE scheme.

- Chen et al. constructed a RIBE scheme from lattices.

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 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.

PROPOSED SYSTEM

- 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., 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

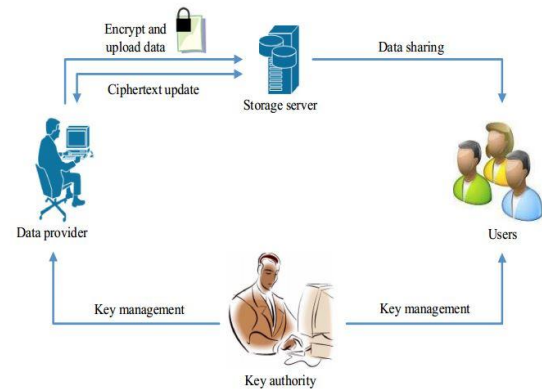
uploads the ciphertext of the shared data to the cloud server.

- Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding 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., Alice's authorization gets expired, David can download the ciphertext 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.

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 ciphertext 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.

SYSTEM ARCHITECTURE:



IMPLEMENTATION MODULES:

- System Construction Module
- Data Provider
- Cloud User
- Key Authority (Auditor)

MODULES DESCRIPTION:

System Construction Module

In the first module, we develop the proposed system with the required entities for the evaluation of the proposed model. 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 ciphertext of the shared data to the cloud server.

When either Alice or Bob 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.

Data Provider

In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data

Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and Ciphertext update the file. Once after completion of the process, the Data Provider logs out the session.

Cloud User

In this module, we develop the Cloud User module. The Cloud user module is developed such that the new users will Signup initially and then Login for authentication. The Cloud user is provided with the option of file search. Then cloud user feature is added up for send the Request to Auditor for the File access.

After getting decrypt key from the Auditor, he/she can access to the File. The cloud user is also enabled to download the File. After completion of the process, the user logout the session.

Key Authority (Auditor)

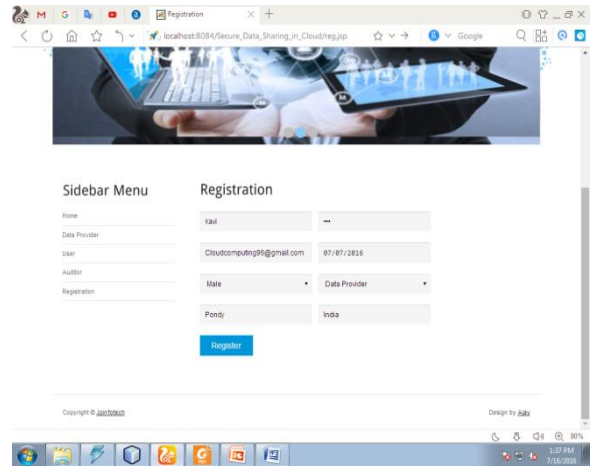
Auditor Will Login on the Auditor's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After the complete process, the Auditor logout the session.

SCREEN SHOTS:

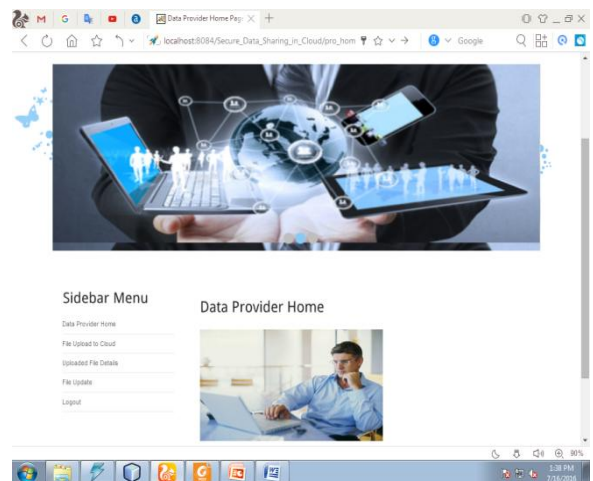
Home:



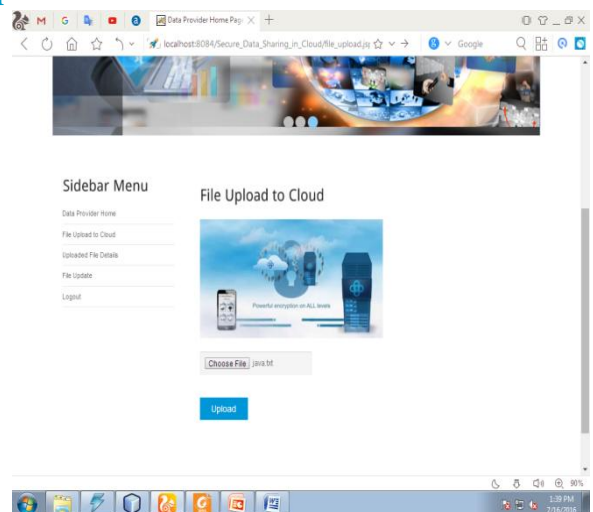
Registration:



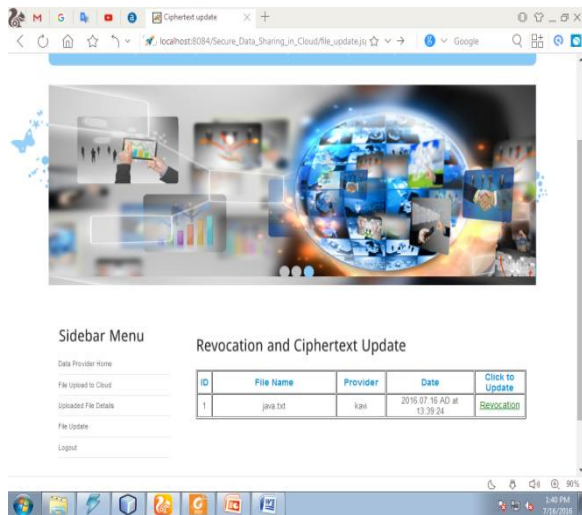
Data Provider Home:



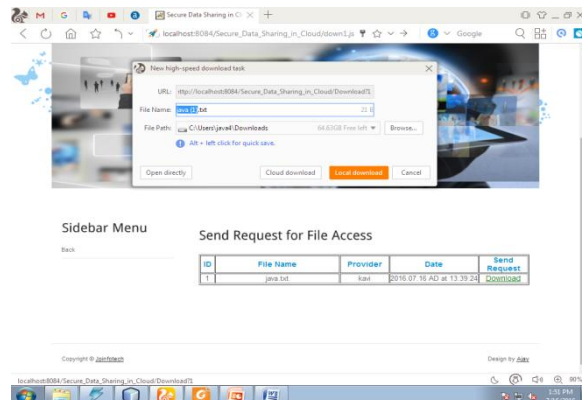
Upload File:



Revocation:



File Download:



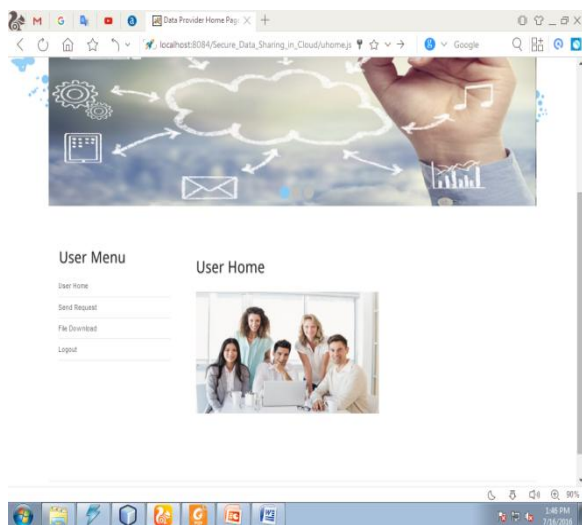
CONCLUSION

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 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 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.

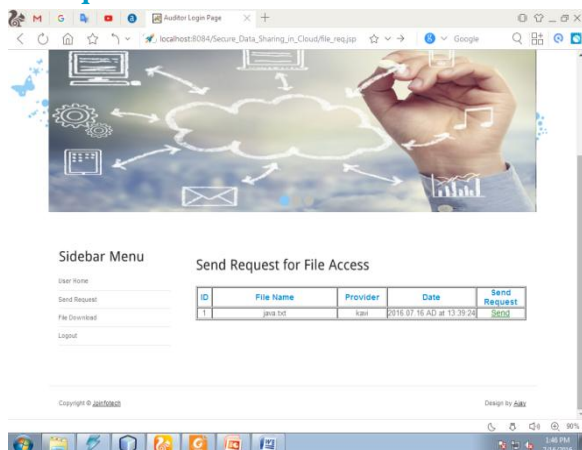
REFERENCES

- [1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.
- [2] iCloud. (2014) Apple storage service. [Online]. Available: <https://www.icloud.com/>
- [3] Azure. (2014) Azure storage service. [Online]. Available: <http://www.windowsazure.com/>

User Home:



Send Request for File Access:



- [4] Amazon. (2014) Amazon simple storage service (amazon s3).[Online]. Available: <http://aws.amazon.com/s3/>
- [5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.
- [6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.
- [7] G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.
- [8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.
- [9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2904–2912.
- [10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 384–394, 2014.
- [11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *Computers, IEEE Transactions on*, 2014, doi: 10.1109/TC.2014.2315619.
- [12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 468–477, 2014.
- [13] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.
- [14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.