INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2017) PAGES 3277 - 3280
RECEIVED : 15.03.2018 PUBLISHED : 18.04.2018
April 18, 2018

SECURE DATA SHARING IN CLOUD COMPUTING USING REVOCABLE-STORAGE IDENTITY-BASED ENCRYPTION

G.Ashok Kumar, M.E(CSE)*, Priyadharshini Engineering College, Vaniyambadi, Vellore.
B.Nagarajan, M.E, Assistant Professor/CSE, Priyadharshini Engineering College.

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. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text 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 2, 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 crypto graphical 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. But the research on these issues is beyond the scope of this paper.

PROPOSED SYSTEM

We introduce a notion called revocable storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. 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. 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.

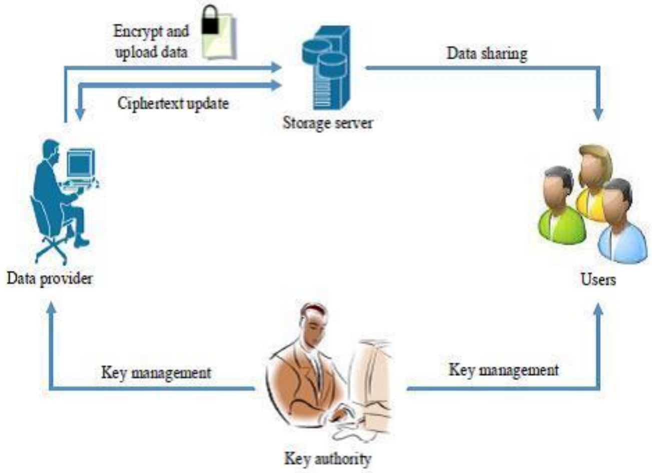
Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. To build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and ciphertext update. A revoked user is prevented from accessing previously shared data, as well as subsequently shared data.

The proposed RS-IBE scheme is proved adaptive-secure. our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

ADVANTAGES

- It fulfills security requirements for data sharing.
- Unauthorized users are prevented from accessing the plaintext of the shared data stored in the cloud server.
- It gives backward and forward data security.
- It’s good for increased need of sharing data over the Internet.

SYSTEM ARCHITECTURE



MODULE DESCRIPTION

- ➢ Data owner
- ➢ Admin
- ➢ Key Authority
- ➢ Data User
- ➢ Revoked user

DATA OWNER

In this module , Data Owner has to register as a new user with unique username and password. After a successful registration, data owner will login to the cloud using unique username. In Data owner page , he will upload files to the cloud server. Uploaded files will store in the cloud server in encrypted format. Data owner can see the upload file list and modify which is in encrypted format.

ADMIN

Cloud server administrator will login to admin page and admin has a access to view uploaded files list. He can also view the data owners, data users and revoked users. Admin can give permission to the revoked users by un-revoke them.

KEY AUTHORITY

Key authority is a responsible person to generate key for a uploaded files. Key authority generates key for a file only when data user requested key for that files and key authority has to verify the key requested file details like data owner name, file name , key requested users which are available in that list. The generated key for that particular file will send to the corresponding data user.

DATA USER

In this module, data user has to register as a new user. After successful register, he will login into the data user page. In this page, data user can download a file which is uploaded by his owner. For downloading a file, first data user should know the file name and owner name. Using the file name and owner name, he need to send a key request to the key authority. After successful verification of requested details by the key authority , key authority will generate a key for download the requested file. Data user search key for that file and using that key , he can download the file by decrypting the encrypted file.

REVOKED USER

If the data user enter the wrong key for the requested file , cloud server consider him as a attacker and hence the cloud server block the user login immediately .Hence the data owner logout automatically. After logout from that page , data user cannot able to login into the server , request key and download files until the cloud admin unrevoke him. Admin can view the attackers details and file key that he tried to download a file. After successful verification of user that he is not an attacker , admin will unrevoke him. Then data user can login into the server page and he has access for all the data user options in that page.

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.