Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
December 2014, 21(6): 45–51
www.sciencedirect.com/science/journal/10058885
The Journal of China Universities of Posts and Telecommunications
http://jcupt.xsw.bupt.cn

Secure personal data sharing in cloud computing using attribute-based broadcast encryption

FU Jing-yi[1,2,3] (✉), HUANG Qin-long[1,2,3], MA Zhao-feng[1,2,3], YANG Yi-xian[1,2]

1. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China
3. Beijing National Security Science and Technology Co., Ltd, Beijing 100086, China

Abstract

The ciphertext-policy (CP) attribute-based encryption (ABE) (CP-ABE) emergings as a promising technology for allowing users to conveniently access data in cloud computing. Unfortunately, it suffers from several drawbacks such as decryption overhead, user revocation and privacy preserving. The authors proposed a new efficient and privacy-preserving attribute-based broadcast encryption (BE) (ABBE) named EP-ABBE, that can reduce the decryption computation overhead by partial decryption, and protect user privacy by obfuscating access policy of ciphertext and user's attributes. Based on EP-ABBE, a secure and flexible personal data sharing scheme in cloud computing was presented, in which the data owner can enjoy the flexibly of encrypting personal data using a specified access policy together with an implicit user index set. With the proposed scheme, efficient user revocation is achieved by dropping revoked user's index from the user index set, which is with very low computation cost. Moreover, the privacy of user can well be protected in the scheme. The security and performance analysis show that the scheme is secure, efficient and privacy-preserving.

Keywords data sharing, ABBE, ABE, user revocation, partial decryption, privacy preserving

1 Introduction

In recent years, cloud computing has emerged as one of the most influential paradigms in information technology area. For benefits of cloud computing, such as reduced costs, capital expenditures, increased operational efficiencies, scalability, flexibility, more and more people tend to outsource their personal data such as personal health records to the cloud. However, security and privacy concerns arise at the same time, since the cloud service provider (CSP) is semi-trusted, which may disclose the personal data to other parties for benefits [1].

A feasible approach to guarantee personal data security in semi-trusted cloud will give encryption for the data processed before outsourcing. For using public key encryption and identity-based encryption, data owners may face a serious obstacle. That is the data owners have to encrypt the same data many times using different user's public key or identity, since the ciphertext encrypted by a particular public key or identity can only be decrypted by users with corresponding private key.

The traditional BE can break through this obstacle. BE actually allows the broadcaster to choose dynamically a subset of privileged users inside the set of all possible recipients and to send a ciphertext, readable only by the privileged users with their private key. Compared with traditional one-to-one encryption technology, BE is a one-to-many encryption technology which is efficient and very applicable to data sharing scenarios [2]. However, Existing BE schemes can only support simple receiver list. It is hard to support flexible, fine-grained access control policies [3].

To achieve the fine-grained access control, a notion of ABE has been introduced in recent years [4]. ABE features a mechanism that enables a fine-grained access control over encrypted data using access policies and ascribed attributes among secret keys and ciphertexts. Especially

Received date: 29-04-2014
Corresponding author: FU Jing-yi, E-mail: fujingyi@bupt.edu.cn
DOI: 10.1016/S1005-8885(14)60344-7

the CP-ABE which is conceptually closer to the role-based access control models, enables the data owner to customize the access policy over a number of attributes that the user possesses in order to decrypt the ciphertext [5]. Nevertheless, applying CP-ABE in the data sharing scheme has a main drawback of efficiency in revocation [1], since each user has amount of attributes and each attribute may be conceivably shared by multiple users, revocation of any user would affect others who share the same attributes. Thus, efficient revocation in existing CP-ABE adopted data sharing scheme is nontrivial to deal with.

Based on CP-ABE and BE, the ABBE has been proposed. Compared to existing BE, ABBE is more flexible because a broadcast data can be encrypted by an expressive access policy, either with or without explicit specifying the receivers. ABBE can significantly address the obstacle of efficient revocation. However, the data decryption algorithm in so far existing ABBE schemes is time-consuming for the receiver, since it entails the computation of a large number of pairing operations. Moreover, in both CP-ABE and ABBE, the access policy of ciphertext is exposed, from which other parties can learn the required attributes of decryption of ciphertext. These required attributes are associated with receiver's attributes, such as receiver's address, faculty, occupation, which reveal the personal information of receiver. Thus, this could be a potential threat to receiver privacy.

Above all, in this article, the authors make the following main contributions:

1) Propose the EP-ABBE, which significantly reduces the decryption computation of user, and protects user privacy by obfuscating the access policy of ciphertext and user's attributes.

2) Propose, based on EP-ABBE, a secure and flexible personal data sharing scheme in cloud computing. The data owner can enjoy the flexibly of encrypting personal data using a specified access policy and a user index set which is a list of selected users' indexes. Thus, only the user whose index is in index set and attributes satisfy the access policy can access the personal data.

3) The proposed data sharing scheme achieves efficient user revocation by dropping user index from the user index set of ciphertext. The data owner does not need to update the secret key of non-revoked user, which has very low computation cost and is more efficient compared with current attribute-based data sharing schemes.

This article is structured as follows: the related work is reviewed in Sect. 2. The preliminaries are introduced in Sect. 3, and present the definition of EP-ABBE in Sect. 4. The system model and the detailed construction are provided tin Sect. 5. The security and performance of our scheme is analyzed in Sect. 6. The conclusion is given in Sect. 7.

2 Related work

2.1 ABE in cloud computing

ABE is widely adopted in current data sharing schemes in cloud for its advantage of achieving fine-grained access control.

Liang et al. adopted ABE to protect data security in mobile social networks [6]. This scheme proposed a user revocable construction based on ABE, which enables a trusted authority to revoke a specific user's data decryption capability in each time slot. On the downside in this scheme, the revoked user is able to access the encrypted data even if it does not hold the attribute any more until the next expiration time. Li et al. proposed a secure sharing of personal health record in cloud computing based on ABE [7], which achieves immediate revocation. However, in the user revocation process of this scheme, the multi-authority needs to work together to re-encrypt ciphertexts and update unrevoked users' attribute secret keys, which is inefficient and incurs extra communication cost. Hur et al. proposed a data outsourcing scheme using CP-ABE [8]. This scheme enables immediate user revocation in each attribute level rather than the system level. But there is an amount of data redundancy since ciphertexts must be re-encrypted many times for different attribute groups. Moreover, all of these above ABE based schemes did not consider that the access policy of ciphertext might reveal the decryption range, which is a potential threat to user privacy. Hur proposed another CP-ABE based data sharing scheme in smart grid with hidden policy solved this problem [9], however, this scheme is not clear how to realize user revocation.

2.2 ABBE

ABBE was first proposed by David et al. [10], in which broadcasters can encrypt data with access policy and a receiver list, only the receiver is in this list and satisfies the access policy that can decrypt ciphertext.