Future Generation Computer Systems 72 (2017) 239–249

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing

Qinlong Huang [a,b,*], Yixian Yang [a,b], Mansuo Shen [c]

[a] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[b] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[c] *School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*

HIGHLIGHTS

- We present a secure and efficient data collaboration scheme in cloud computing.
- We employ a delegation mechanism based on hierarchical attribute-based encryption.
- We provide partial decryption construction when the user decrypts ciphertext.
- We propose partial signing construction by outsourcing signing computation to cloud.

ARTICLE INFO

Article history:
Received 14 November 2015
Received in revised form
21 September 2016
Accepted 29 September 2016
Available online 2 October 2016

Keywords:
Data collaboration
Hierarchical attribute-based encryptions
Attribute-based signature
Cloud computing

ABSTRACT

With the increasing trend of outsourcing data to the cloud for efficient data storage, secure data collaboration service including data read and write in cloud computing is urgently required. However, it introduces many new challenges toward data security. The key issue is how to afford secure write operation on ciphertext collaboratively, and the other issues include difficulty in key management and heavy computation overhead on user since cooperative users may read and write data using any device. In this paper, we propose a secure and efficient data collaboration scheme, in which fine-grained access control of ciphertext and secure data writing operation can be afforded based on attribute-based encryption (ABE) and attribute-based signature (ABS) respectively. In order to relieve the attribute authority from heavy key management burden, our scheme employs a full delegation mechanism based on hierarchical attribute-based encryption (HABE). Further, we also propose a partial decryption and signing construction by delegating most of the computation overhead on user to cloud service provider. The security and performance analysis show that our scheme is secure and efficient.

1. Introduction

With the widespread applications of network technology and the global rise of cloud technology, cloud computing is rapidly evolving to revolutionize the way how service is offered. Cloud computing benefits the users in that it allows convenient access, use of storage resources, increased operational efficiencies based on the techniques of service-oriented architectures, virtualization, distributed computing and so on. Therefore, in order to achieve cost savings and the flexibility in investments on-demand, more and more enterprises use cloud based services to manage projects, contacts and so on.

Although the great benefits brought by cloud computing paradigm are exciting for enterprises and potential cloud users, security problems including data confidentiality and access control in cloud computing become serious obstacles, since the cloud service provider (CSP) is semi-trusted, the data stored in the cloud may be disclosed by the unauthorized users or malicious employees in the CSP [1]. Thus, if these security problems are not appropriately addressed, they will prevent cloud computing's extensive applications in the future. The promising approach would be to encrypt data before outsourcing. Attribute-based encryption (ABE) is a one-to-many cryptographic primitive which provides fine-grained access control over the outsourced ciphertexts [2].

* Corresponding author at: Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China.

E-mail address: longsec@bupt.edu.cn (Q. Huang).

http://dx.doi.org/10.1016/j.future.2016.09.021
0167-739X/

It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy attribute-based encryption (CP-ABE) enables data owner to define the access policy over a universe of attributes that the user needs to possess in order to decrypt the ciphertext, by which the confidentiality and access control of data can be guaranteed [3]. However, existing solutions mainly focus on how to afford secure data read for users, none of these works considers that multiple users may also write the encrypted data collaboratively in cloud computing.

The data collaboration service as an emerging promising service offered by the CSP, is to support the availability and consistency of the shared data among users [4]. Especially, one of the typical application scenarios of data collaboration service is mobile office which means collaborative data sharing among lightweight mobile devices. Let us consider the following application scenario: the project leader Alice outsources the data related to the project to cloud, and the colleagues Bob and Carol will work collaboratively on Alice's project. Alice first encrypts the data and sends the ciphertext to the cloud. Bob and Carol are authorized users when they join in so that they can access and modify the data with their own mobile devices. After modifying the data, Bob or Carol re-encrypts the data and sends it with their proofs back to the CSP. If they are authorized, the CSP will re-new the ciphertext. In total, three project members share data in a collaborative way. Thus the access policy of the above scenario is: authorized users can access and modify the encrypted data while CSP and other unauthorized users know nothing about the data in data collaboration services.

To realize secure data collaboration services in cloud computing, authorized users have the privilege to modify the cloud data, so the CSP should verify the user's proof. A novel cryptographic technique known as attribute-based signature (ABS) is able to help CSP to verify whether the user is valid when he requests to perform write operations on the data stored in the cloud [5–7]. In an ABS system, user can sign messages with his attributes. Then, from the signature, the CSP can check whether the signer's attributes satisfy the access policy while remaining completely ignorant of the identity of signer. Therefore, adopting ABE and ABS in data collaboration can achieve data confidentiality, fine-grained access control and user verification, but it also brings some drawbacks at the same time. Firstly, some current CP-ABE schemes support for hierarchical user grant, which enables a user to generate attribute secret keys containing a subset of his own attribute secret keys for other users, in order to reduce the workload on the attribute authority [8,9]. However, we hope to provide an appropriate delegation mechanism between attribute authorities, which independently make decisions on the structure and semantics of their attributes, to not only reduce the workload on the attribute authority, but also achieve lightweight key management. Secondly, users may access data using any device in cloud computing [10], however, both ABE and ABS bring high computation cost of decryption and signing to users. The decryption and signing operations require a large number of module exponentiations, which commonly grow linearly with the size of access policies. This presents a significant challenge for users who access and write data on resource-constrained mobile devices. Moreover, most of existing ABE and ABS based schemes focus on how to afford secure data access permission for users and the identity authentication respectively, but to the best of our knowledge, few works consider that multiple users who can be regarded as in a same domain perform write operation on encrypted data collaboratively, in which situation the CSP should be able to verify the write permissions of these users before accepting the re-encrypted data.

In this paper, we present a secure data collaboration scheme with multiple users in cloud computing. Specifically, the main contributions of this paper can be summarized as following:

(1) We propose a secure and efficient data collaboration scheme, in which valid users can share data in a collaborative way. In our scheme, data owner encrypts data with access policy based on CP-ABE, while the cooperative user re-encrypts the modified data and signs the collaboration request with his attributes based on ABS, and then sends the re-encrypted data and signature to CSP which accepts re-encrypted data after verifying the signature. Thus, only the users whose attributes satisfy the access policy can perform read and write operations on the encrypted data stored in cloud.
(2) We employ a full delegation mechanism based hierarchical ABE (HABE), which contains a central authority and a number of independent domains. Each domain has a domain authority that requests a secret parameter from the higher level authority and generates attribute secret keys for its domain user, and the secret parameter of top level domain authority is from central authority. It reduces the workload on attribute authority and achieves lightweight key management in large-scale users.
(3) We propose a partial decryption and signing construction. The users are able to outsource most of the decryption and signing computation overhead to the CSP, which is suitable for resource-constrained mobile devices.

This paper is structured as follows: we review related work in Section 2. We introduce the preliminaries in Section 3, and provide the system model, security model and design goals in Section 4. The detailed construction is given in Section 5. Then, we analyze the security and performance of our scheme in Sections 6 and 7 respectively. Finally, we conclude this paper in Section 8.

2. Related work

In order to enjoy the benefits of cloud computing, enterprises have to entrust their valuable data to CSP, there have been increasing security and privacy concerns on outsourced data. ABE is a promising cryptographic technique to realize scalable, flexible, and fine-grained access control solutions for sharing data in cloud. The notion of ABE was first introduced by Sahai and Waters as a new method for fuzzy identity-based encryption [11]. Bethencourt et al. presented the first CP-ABE construction supporting tree-based structure in generic group model [12]. Hur et al. proposed an access control scheme based on CP-ABE in data outsourcing systems such as cloud computing [13]. Wan et al. proposed a fine-grained access control scheme in cloud storage services [8]. However, these schemes only focus on data sharing and cannot support write operation on the stored data. Li et al. proposed a novel patient-centric framework and a suite of mechanism for data access control to personal health records (PHR) stored in semi-trusted servers [14]. This scheme encrypted data with access policy based on CP-ABE or with a set of attributes based on key-policy ABE (KP-ABE). Although this scheme supports the write operation, the cloud cannot verify the write permission of user after receiving the re-encrypted modified data.

Dong et al. proposed a secure and efficient data collaboration scheme called SECO using multi-level hierarchical identity-based encryption (HIBE), in which users in the same domain can cooperate to complete work [15]. In this scheme, a user encrypts data with multiple recipients' public key, and only these intended recipients can decrypt and modify the data. After performing write operation, the user sends re-encrypted data and ID-based signature (IBS) to cloud. However, the cloud is able to know the identity of user, and it cannot verify whether the user really has the write permission unless it maintains a list of user-permissions values of each data, which will also introduce extra storage cost.

From the other side, the key management of ABE is difficult if there are a large number of users. To solve this problem,