Chaos, Solitons and Fractals 86 (2016) 107–116

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

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

Security and efficiency data sharing scheme for cloud storage

Ke Han*, Qingbo Li, Zhongliang Deng

Beijing University of Posts and Telecommunications, Haidian District, Beijing, China

ARTICLE INFO

Article history:
Received 20 January 2016
Revised 10 February 2016
Accepted 10 February 2016
Available online 2 March 2016

Keywords:
Data sharing
CP-ABE
Access control
Cloud storage

ABSTRACT

With the adoption and diffusion of data sharing paradigm in cloud storage, there have been increasing demands and concerns for shared data security. Ciphertext Policy Attribute-Based Encryption (CP-ABE) is becoming a promising cryptographic solution to the security problem of shared data in cloud storage. However due to key escrow, backward security and inefficiency problems, existing CP-ABE schemes cannot be directly applied to cloud storage system. In this paper, an effective and secure access control scheme for shared data is proposed to solve those problems. The proposed scheme refines the security of existing CP-ABE based schemes. Specifically, key escrow and conclusion problem are addressed by dividing key generation center into several distributed semi-trusted parts. Moreover, secrecy revocation algorithm is proposed to address not only back secrecy but efficient problem in existing CP-ABE based scheme. Furthermore, security and performance analyses indicate that the proposed scheme is both secure and efficient for cloud storage.

1. Introduction

Cloud storage is an important service of cloud computing [1]. It enables people to easily share their data with friends by uploading their private data into the cloud storage, and rely on the cloud servers to provide data access control. Although people enjoy the advantages of this new technologies and services, their concerns about data security arises as well. One of the prominent security concerns is data security and privacy in cloud storage due to the data outsourcing [2]. People have to give up their data to the cloud server for storage and business operation, while the cloud server is usually a commercial enterprise which cannot be totally trusted. Not only Data confidentiality but flexible and fine-grained access control is strongly desired in the service-oriented model.

To achieve data access control on unauthorized servers, a traditional method is to store only encrypted data on the cloud storage system and make only authorized users hold valid decryption keys [3]. Although these methods can provide secure data access control, the key management is very complicated when more users involved in the system.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a promising cryptographic approach that achieves a fine-grained data access control on cloud storage systems [4,5]. In CP-ABE scheme, shared data is encrypted with a tree access policy chosen by the data owner. Each user will be issued a secret key according to its attributes. A user can decrypt the ciphertext only when its attributes satisfy the access policy. CP-ABE gives the data owner more direct control on access policies and does not require the data owner to manage keys.

Most of the existing CP-ABE schemes are constructed in the architecture where one or more multiple trusted authorities have the power to generate the whole privates keys of users with their master secret information [6]. Thus, the key escrow problem is inherent such that the trusted authority can decrypt every ciphertext addressed to users. Moreover, decryption key is defined with associate attributes shared by multi-users. If a user joins or leaves a sharing group, the associate attributes and

* Corresponding author. Tel.: +861532217430.
E-mail address: hanke@bupt.edu.cn, hanke1543@sina.com (K. Han).

http://dx.doi.org/10.1016/j.chaos.2016.02.010
0960-0779/

Ciphertext should be changed to all the other numbers in the sharing group for backward secrecy [7].

In this paper, we propose an attribute-based access control scheme for data sharing in cloud storage system. The proposed scheme features the following achievements. Distributed multi-parts key generation algorithm is adopted by the proposed scheme to solve the key escrow problem. And the conclusion attack from multi-parts is conquered as well. We enhance backward secrecy with efficiency attributes revocation algorithm.

The rest of the paper is organized as follow. Section 2 provides an overview on related work. Then we present our system model and definitions in Senction3. In Section 4, we describe the construction of our scheme in detail and show how it is used in access control of outsourced data in cloud computing. In Section 5, we prove the security of the proposed scheme. Then in Section 6, we analyze computation complexity of our scheme and evaluate its performance. Lastly, we conclude the paper in Section 7.

2. Related work

Access control is a classic security topic which date back to 1960s or early 1970s [8], and various access control models [9–10] have been proposed since then. Unfortunately, these schemes are only appreciate to systems in which data owner and the sever is within the same trusted domain. Since data owner and the server are usually not in the same trusted domain in cloud storage system, new access control schemes employing attributed-based encryption(ABE) [11] encryption are proposed. ABE comes in two flavors called key-policy ABE(KP-ABE) [12] and Ciphertext Police ABE (CP-ABE) [4]. In KP-ABE, attributes are used to describe the encryption data and policies are built into user's key; while in CP-ABE, the attributes are used to describe user's credentials, and the one who encrypts the data determines a policy on who can decrypt the data. Putting the access policy decisions in the hands of the data owners make CP-ABE more appreciate to the cloud based data sharing system.

Some CP-ABE based data sharing schemes have been proposed to solve the key-escrow and revocation problems.

Taeho proposed an anonymous attribute-based privilege control scheme [13]. It replaced trusted key generation center with multiple semi-trusted authorities to manage attribute keys. Secret sharing technique [14] was used by the authorities to address key-escrow problem but result in conclusion attacks. Wan and Liu proposed multiple authorities scheme HASBE [15] by combining hierarchical identity-based encryption(HABE) [7] and CP-ABE. In [13] and [15], shared data was encrypted by symmetric cryptograph and CP-ABE was used to encrypt the decryption key. Access structure and decryption key were updated during attribute revocation algorithm and it achieved efficient encryption and decryption on shared data. However, the authorized revoked users got the decryption key during their authorized time. They can decrypt the shared data even after their revocation. The revocation schemes were useless to provide backward secrecy.

Dong [16] proposed a secure data sharing scheme in cloud computing by exploiting CP-ABE and combining it with technique of IBE [17]. Their scheme ensured fine-grained data access control, backward secrecy. But there is a trusted key generation center in the scheme.

Junboem proposed an escrow-free key issuing protocol [18]. The key issuing protocol generated and issued user secret keys by performing a secure two-party computation protocol between the key generation center and the cloud storage. Thus, users were not required to fully trust the key generation or the cloud server. As the revocation management was controlled by the cloud server, it cannot prevent the conclusion attacks form cloud server and revoke users.

Yang and Jia [19] proposed DAC-MACS, an effective and secure data access control scheme for multi-authority cloud storage systems. They designed an efficient immediate attribute revocation method for multi-authorized CP-ABE schemes. CP-ABE encryption was carried out by user and cloud server independently. DAC-MACS only required the cloud server to update a few components which were associated with the revoked attributes. But there was a global trusted key generation center in the scheme.

In this paper, the proposed efficiency data access control scheme for cloud storage solves the key-escrow and revocation problems. A distributed multiple parts key generation scheme is proposed to solving key escrow problem. We design an efficient user revocation method for data access control that achieves in backward secrecy at the same time.

3. System and security model

3.1. Sharing and security model

3.1.1. Sharing model

As shown in Fig. 1, the architecture of data sharing system consists of five entities: a cloud server, data owner, users, a key generation center and several key authority centers.

Cloud Server(CS). It is a data storing center and the cloud server has to always be online for shared data accessing. CS is passive attacker [20], it executes the assigned task appropriately in the system most of time. However, it is curious about the data content to gain illegal profits. But we assume it will not collude with neither key generation center nor key authority centers

Key Generate Center(KGC): It is an entity that provides a key management service. It generates public and master global parameters for CP-ABE and stays online all the time for attribute revocation. We assume KGC is passive attackers as well. Thus, unauthorized access from the KGC to the plaintext of the encrypted data should be prevented.

Key Authority Centers(KACs): They generate secret parameters for users to calculate their secret attribute keys. They are in charge of issuing, revoking, and updating parameters for users attribute keys. But they may conclude to get unauthorized data content.

Data Owner: It is a client who owns data and wishes to upload it to the cloud for ease data sharing. It is responsible for defining access policy and encrypting the data under CP-ABE encryption algorithm. Data owner is fully