Information Sciences 424 (2018) 1–26

Contents lists available at ScienceDirect

Information Sciences

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

Blocked linear secret sharing scheme for scalable attribute based encryption in manageable cloud storage system

Jing Wang [a,b,c], Chuanhe Huang [b,c,*], Neal N. Xiong [d], Jinhai Wang [b,c]

[a] School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China
[b] State Key Lab of Software Engineering, Computer School, Wuhan University, China
[c] Collaborative Innovation Center of Geospatial Technology, China
[d] Colorado Technical University, USA

ARTICLE INFO

Article history:
Received 25 November 2016
Revised 4 September 2017
Accepted 10 September 2017
Available online 23 September 2017

Keywords:
Cloud
Data security
Access control
Attribute-based encryption
Access policy management

ABSTRACT

Cloud provides outsourced storage services in a cost-effective manner. A key challenge of cloud storage is the security and privacy of outsourced data. A security mechanism known as attribute-based encryption (ABE) represents the state-of-the-art in providing fine-grained access control for cloud storage. The managing of access policy is a critical issue of ABE. Policy managing may incur substantial computation and communication overhead in the ABE scheme with unscalable access policy. In this work, we firstly propose a form of scalable access policy named blocked linear secret sharing scheme (BLSSS). The scalability of BLSSS provides efficient policy managing interface for ABE scheme. Then, we propose a scalable ciphertext-policy attribute-based encryption (SCP-ABE) scheme which uses BLSSS as access policy. Significantly, the proposed SCP-ABE is low-cost in computation and communication during policy managing. Furthermore, sufficient simulation experiments demonstrate that SCP-ABE outperforms most existing ABE schemes in terms of policy managing.

1. Introduction

Cloud storage offers a number of advantages over traditional storage in terms of availability, scalability, portability and so on. It develops a unified strategy to collect, preserve and manage data for current and future. Although the advantages of cloud storage are clear, a critical issue of the data outsourcing scenario is the enforcement of strong data security mechanisms [16]. Thus, adequate access control techniques are required to ensure such outsourcing data security. It is important for users to trust the storage service providers. Attribute based encryption (ABE) is a novel cryptographic tool which can provide fine-grained ciphertext access control. The core advantages of such ABE-based access control mechanisms are given as follows: (1) access control of the data is maintained by the customer instead of the service provider; (2) the security properties strictly depend on cryptography technology, as opposed to traditional access control. In brief, it provides great superiority over other access control mechanism based on public cloud infrastructures.

A core concept of ABE is named access policy or access structure, which is provided to describe fine-grained access privilege. Specifically, in a ciphertext-policy attribute-based encryption (CP-ABE) scheme, each ciphertext is assigned with

* Corresponding author.
E-mail addresses: wangj478@mail.sysu.edu.cn (J. Wang), huangch@whu.edu.cn (C. Huang), xiongnaixue@gmail.com (N.N. Xiong), wangjinhai@whu.edu.cn (J. Wang).

https://doi.org/10.1016/j.ins.2017.09.032
0020-0255/

a unique access policy. The data owner manages access privilege of data by maintaining its access policy. In fact, most performances of CP-ABE scheme significantly depend on the access policy properties. For example, the scale of access policy decides the size of ciphertext of ABE scheme, the expression of access policy decides the flexibility of ABE based access control mechanism. Many researchers focus on optimizing CP-ABE by improving the access policy. However, scalability, as an important property of access policy, was usually ignored. The scalability of access policy indicates the ability of dynamic updating. The access policy with strong scalability supports real-time and fine-grained updating while data having been encrypted. It is important that access policy frequently requires to be updated due to various reasons. In most scenarios, the access policy just needs to be partially updated instead of entirely updated. However, the access policy with weak scalability can only be updated by completely re-encrypting data with new policy. It brings heavy computation and communication overhead. Significantly, the strong scalability of access policy is required by the manageable CP-ABE scheme to provide efficient policy updating interface to data owner. It provides three advantages of manageable CP-ABE scheme: (1)supporting real-time policy managing; (2)supporting fine-grained policy managing; (3)low-overhead of policy managing.

The grand challenge of improving policy scalability in a CP-ABE scheme is to jointly guarantee correctness, completeness and security [40]. At the same time, efficiency is further considered as an important requirement in this paper. Recently, policy scalablity only has been discussed in a few ABE schemes [11,27,40]. However, all of these schemes are still hard to meet all requirements in terms of correctness, completeness, security and efficiency. In Goyal and Sahai proposed schemes [11,27], the updated access policy should be more restrictive than the previous one, because the scalability of the access policy is limited. Although Yang's scheme has improved the completeness of policy updating method, the updating process of this scheme is still not efficiency enough [40]. In some cases, the access policy is required to re-construct. Especially, the processing of threshold updating is cumbersome. In general, the policy scalability of these existing schemes is not strong enough.

Focusing on scalability, we propose a new form of access policy called block linear secret sharing scheme (BLSSS), a special linear secret sharing scheme(LSSS). BLSSS provides efficient updating interface which greatly improves the scalability of policy. More specifically, there are four advantages of describing access policy as BLSSS. Firstly, the storage cost of BLSSS is much less than general LSSS. Because BLSSS is generated by a random seed and a tree, data owner only needs to store the seed and tree circuit instead of the whole BLSSS matrix. Secondly, the computation and communication overhead of policy updating are both low. Each block of BLSSS is independent, updating of a block is non-interfering with others. Thus, there is not additional overhead produced for other blocks, the overall updating overhead is minimized. Thirdly, BLSSS is universal for CP-ABE scheme. Not only LSSS, but also other common forms of access policy can be equivalently transformed into BLSSS[1]. Thus, BLSSS can be widely used in most existing CP-ABE scheme. Fourthly, the computational complexity of decryption is reduced for CP-ABE scheme. In the CP-ABE scheme with BLSSS, the decrypting operation can be decomposed and processed in block. Thus, its decrypting computation scale is mitigated[2]. Furthermore, the scalable ciphertext-policy attribute based encryption(SCP-ABE) scheme with strong policy scalability is proposed in this paper. SCP-ABE is provided with efficiency policy managing interface by taking full advantage of BLSSS matrix. A lot of simulation results have demonstrated that the proposed SCP-ABE outperforms the existing main schemes [11,27,40] in terms of policy scalability. The contributions of this paper are summarized as follows.

(1) We proposed a scalable access policy of ABE called BLSSS which is provided with block structure.
(2) We provide efficient scaling functions of BLSSS. These functions are convenient to process arbitrary policy updating.
(3) We provide a SCP-ABE scheme using BLSSS. SCP-ABE outperforms the existing main ABE schemes in terms of policy managing.

The remaining of this paper is organized as follows. Section 2 gives the related work. Then, we propose the scalable access policy(i.e. BLSSS) in Section 3. Thirdly, we propose the SCP-ABE scheme in Section 4. In Section 5, we analyse the performance of our BLSSS and SCP-ABE scheme. Finally, the conclusions and future works are given in Section 6.

2. Related work

Cloud computing is a new architecture can be viewed as the next generation computing paradigm [7,25]. It introduces a major change in data storage and application execution [35]. For instance, the United States Library of Congress moved its digitized content to the cloud [1]. It develops a national strategy to collect, preserve and make available digital content for current and future generations based on cloud storage.

Many researchers focus on the security of cloud storage systems [9,15,29,34,38,39]. ABE provides a smart way to construct a fined-grained access control for cloud [11–13,24,32,36,37]. An important issue of ABE is managing access privilege. Recently, there are two kinds of solution of this issue: key revocation [14,19,20,41] and policy updating [10,11,27,40]. Significantly, policy updating provides more fine-grained management pattern for ABE, it allows data owner to manage the privilege in a more flexible and scalable way.

In fact, in a CP-ABE scheme, access privilege of data is described by expressive access policy which is derived from a secret sharing scheme [30]. A wide range of researches have been proposed to design secret sharing scheme, such as the

[1] The detailed transformation of monotonous Boolean formula and access tree are all given in Section 3.3.1
[2] The detailed explanation, analysis and instance are all given in Section 3.4.1