Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Secure attribute-based data sharing for resource-limited users in cloud computing

Jin Li [a], *Yinghui Zhang* [b,c,d], *Xiaofeng Chen* [e], *Yang Xiang* [e,f,*]

[a] *School of Computer Science, Guangzhou University, Guangzhou, PR China*
[b] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, PR China*
[c] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, PR China*
[d] *Westone Cryptologic Research Center, Beijing 100070, PR China*
[e] *State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, PR China*
[f] *School of Software and Electrical Engineering, Swinburne University of Technology, Australia*

ARTICLE INFO

Article history:
Received 9 January 2017
Received in revised form 25 July 2017
Accepted 14 August 2017
Available online

Keywords:
Cloud computing
Access control
Attribute-based encryption
Online/offline encryption
Chosen ciphertext security

ABSTRACT

Data sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. As a potential technique for realizing fine-grained data sharing, attribute-based encryption (ABE) has drawn wide attentions. However, most of the existing ABE solutions suffer from the disadvantages of high computation overhead and weak data security, which has severely impeded resource-constrained mobile devices to customize the service. The problem of simultaneously achieving fine-grainedness, high-efficiency on the data owner's side, and standard data confidentiality of cloud data sharing actually still remains unresolved. This paper addresses this challenging issue by proposing a new attribute-based data sharing scheme suitable for resource-limited mobile users in cloud computing. The proposed scheme eliminates a majority of the computation task by adding system public parameters besides moving partial encryption computation offline. In addition, a public ciphertext test phase is performed before the decryption phase, which eliminates most of computation overhead due to illegitimate ciphertexts. For the sake of data security, a Chameleon hash function is used to generate an immediate ciphertext, which will be blinded by the offline ciphertexts to obtain the final online ciphertexts. The proposed scheme is proven secure against adaptively chosen-ciphertext attacks, which is widely recognized as a standard security notion. Extensive performance analysis indicates that the proposed scheme is secure and efficient.

1. Introduction

With the advent of Cloud Computing, more and more data are outsourced to cloud servers from individual users and enterprise. Usually, the cloud service can be divided into three types, that is, the public cloud, private cloud and hybrid cloud, where the public cloud is usually untrusted while the private cloud is assumed to be semi-trusted or fully trusted, and hybrid cloud is the combination of public cloud and private

* *Corresponding author.*
E-mail addresses: lijin@gzhu.edu.cn (J. Li), yhzhaang@163.com (Y. Zhang), xfchen@xidian.edu.cn (X. Chen), yxiang@swin.edu.au (Y. Xiang).
http://dx.doi.org/10.1016/j.cose.2017.08.007

cloud. Thus, when users want to outsource their sensitive data to public cloud, including their personal files, health records, emails etc., they have to implement access control on the data besides preserving privacy and data deduplication (Huang et al., 2017; Li et al., 2014, 2015, 2017). In traditional access control mechanisms, it is usually assumed that the data owner and the storage servers are in the same trusted domain, where the storage servers are fully trusted and are responsible for defining and enforcing access control policies. This assumption however no longer holds in cloud computing in that the data owner and cloud servers are very likely to be in different domains. Some users may encrypt their data and upload corresponding ciphertexts for sharing to protect their privacy. However, the encryption form of the data makes the data sharing difficult, especially for the case of fine-grained data sharing.

Attribute-based encryption (ABE) is one of useful cryptographic primitives to realize fine-grained access control, which has been widely adopted in cloud computing. In ABE, each user obtains a private key related to his attribute set or access policy. More specifically, two kinds of ABE have been defined for access control system, that is, key-policy ABE and ciphertext-policy ABE. In key-policy ABE, the policy for users are bounded in the private keys during the key issuing phase. In ciphertext-policy ABE, such policy is inserted and bounded in the ciphertext instead. Both kinds of ABE have found important application scenarios.

However, the security and efficiency challenges have arisen when typical ABE schemes are directly utilized to design access control systems. For one thing, most of the existing ABE schemes are secure against chosen-plaintext attacks (CPA) which is a notion less desirable than security against adaptive chosen-ciphertext attacks (CCA2). For another, both the encryption and decryption algorithms are bounded with the number of attributes or the size of access formula. The computation overhead is very high especially for the ABE schemes with CCA2 security. Such a drawback becomes more serious for resource-constrained users such as mobile devices and sensors. As a result, these computations cannot be independently completed by such users. For the purpose of reducing the computational overhead, the technique of outsourcing computation was introduced, in which the computation tasks can be outsourced to public cloud servers. In this way, the computational overhead at user side can be reduced greatly. There are many research works for secure outsourcing ABE, such as (Green et al., 2011; Zhou and Huang, 2012). However, all these works require that the users need to blind and upload the computational tasks to the cloud server. After the cloud server returns the results, the users unblind and get its final results. There are three main drawbacks when utilizing such a technique in the computation for resource-constrained users. First, the blind and unblind algorithms require some computational cost, which also has impact on the response time. Second, the users have to interact with the cloud server for computation outsourcing. Finally, the result returned from the cloud servers cannot be fully trusted. As far as the authors' knowledge, the problem of simultaneously achieving fine-grainedness, high-efficiency on the data owner's side, and standard data confidentiality of cloud data sharing still remains unresolved.

1.1. *Our contribution*

Research contributions of this paper can be summarized as follows:

- In order to realize secure attribute-based data sharing (ABDS) suitable for resource-constrained mobile users, we introduce a new online/offline ABE scheme that eliminates a majority of the computation task by adding system public parameters besides moving the encryption computation overhead on the data owner's side to the offline phase.
- A public ciphertext test phase is performed before the decryption phase, which eliminates most of the computational cost resulted from illegitimate ciphertexts. In other words, the public ciphertext test allows a user to check at a low cost whether a potential equation holds for components of a given ciphertext before performing the expensive decryption phase.
- The technique of Chameleon hash function is used to generate an immediate ciphertext, which will be blinded by the offline ciphertexts to obtain the final online ciphertexts. In this way, the proposed scheme is proven CCA2 secure, which is widely recognized as a standard security notion. Theoretical analysis and experimental results indicate that the proposed ABDS system is extremely suitable for resource-limited mobile users in cloud computing.

1.2. *Related work*

In this section, we summarize the related works on ABE, online/offline cryptography and outsourcing computation.

1.2.1. *Attribute-based encryption*

The notion of ABE, known as fuzzy identity-based encryption in Sahai and Waters (2005), was proposed and applied in biometrics encryption by Goyal et al. (2006). In biometrics encryption application, the key extracted from the biometrics such as fingerprint will always be different each time because of the biometric measurement noise during the extraction algorithm. With the technology of fuzzy identity-based encryption, such problem can be solved by introducing error-tolerance in fuzzy identity-based encryption. It allows the private key with slight difference from the original one to decrypt the ciphertext for the original biometric identity. The notion is extended into ABE by defining the identity as a set of attributes. In Goyal et al. (2006), it introduced two different and complementary notions of ABE called KP-ABE and CP-ABE, to deal with the error tolerance in key generation phase or ciphertext generation phase. A secure construction of KP-ABE was given in Goyal et al. (2006) by dividing the private key according to the access policy. A provably secure CP-APE construction supporting tree-based access structure in generic group model was presented by Bethencourt et al. (2007), where a random number for generation of ciphertext is divided according to the access policy specified in the ciphertext.

In the last decade, there are a lot of works on ABE constructions and applications proposed. They range from constructing stronger security schemes to proposing more efficient schemes. For example, to reduce the trust of attribute