COMPUTERS & SECURITY 59 (2016) 45–59

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Secure, efficient and revocable multi-authority access control system in cloud storage

Qi Li [a,*], Jianfeng Ma [b], Rui Li [c], Ximeng Liu [b], Jinbo Xiong [d], Danwei Chen [a]

[a] School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[b] School of Computer Science and Technology, Xidian University, Xi'an 710071, China
[c] School of Software and Institute of Software Engineering, Xidian University, Xi'an 710071, China
[d] Faculty of Software, Fujian Normal University, Fuzhou 350108, China

ARTICLE INFO

Article history:
Received 30 April 2015
Received in revised form 15 November 2015
Accepted 4 February 2016
Available online 17 February 2016

Keywords:
Cloud storage
Access control
Multi-authority
Decryption outsourcing
Adaptively secure
Attribute-level revocation

ABSTRACT

Multi-Authority Attribute-Based Encryption (MA-ABE) is an emerging cryptographic primitive for enforcing fine-grained attribute-based access control on the outsourced data in cloud storage. However, most of the previous multi-authority attribute-based systems are either proven to be secure in a weak model or lack of efficiency in user revocation. In this paper, we propose MAACS (Multi-Authority Access Control System), a novel multi-authority attribute-based data access control system for cloud storage. We construct a new multi-authority ciphertext-policy ABE (MA-CP-ABE) scheme with decryption outsourcing. The decryption overhead for users is largely eliminated by outsourcing the undesirable bilinear pairing operations to the cloud servers. The proposed MA-CP-ABE scheme is proven adaptively secure in the standard model and supports any monotone access policy. We also design an efficient attribute-level user revocation approach with less computation cost. The security analysis, numerical comparisons and implementation results indicate that our MAACS is secure, efficient and scalable.

1. Introduction

Cloud storage is a promising application paradigm of cloud computing (Mell and Grance, 2011), which enables data owners to conveniently share their data files via the cloud. Since a large amount of individual data are hosted to the cloud servers, the concern about data confidentiality arises. To alleviate this problem, one common method is to encrypt the data before uploading it to the servers. Such approach also incurs a great challenge to the access control over the encrypted data, since the cloud servers cannot be fully trusted and may attempt to access and analyze the personal data for illegal or financial purposes.

Attribute-based encryption (Sahai and Waters, 2005) is an applicable cryptographic technique for cloud storage, which simultaneously attains data confidentiality and fine-grained access control. In an ABE scheme, the access policy is defined over various attributes. More precisely, ABE schemes can be divided into two types: Key-policy ABE (KP-ABE) and

* *Corresponding author.* Tel.: +86 13851489961.
E-mail address: liqics@njupt.edu.cn (Q. Li).
http://dx.doi.org/10.1016/j.cose.2016.02.002
0167-4048/

Ciphertext-policy ABE (CP-ABE). In a KP-ABE framework, the user's private keys are associated with an access policy, while the ciphertext is associated with some attributes. In a CP-ABE framework, the circumstance is conversed; the ciphertext is labeled with an access policy, while user's private keys are labeled with some descriptive attributes. Especially, CP-ABE is more suitable for the data provider to define the access policy.

Recently, there are several attribute-based access control schemes in the clouds (Hur, 2013; Wang et al., 2011a, 2011b; Yu et al., 2010a). Basing on KP-ABE (Goyal et al., 2006) and proxy re-encryption (Blaze et al., 1998), Yu et al. proposed a fine-grained access control system in clouds (Yu et al., 2010a). By employing CP-ABE (Bethencourt et al., 2007), Hur (2013) proposed an attribute-based data sharing scheme. However, in Bethencourt et al. (2007), Goyal et al. (2006), Hur (2013), Wang et al. (2011a, 2011b), and Yu et al. (2010a), the attribute universe is assumed to be managed by a single authority. This premise may not capture the practical requirements in clouds, where user's attributes may be issued by different authorities. For instance, Alice wants to encrypt a message under access policy ("UNIVERSITY. MIT. GRADUATE" and "IBM. ENGINEER"). In this way, only the recipient who is the graduate of university MIT and now employed as an engineer by IBM can recover the message. University MIT is responsible to issue attributes to students, while IBM is responsible to distribute attributes to its employees.

To track this problem, several multi-authority attribute-based access control schemes (Chase, 2007; Chase and Chow, 2009; Jung et al., 2013; Lewko and Waters, 2011; Liu et al., 2011; Ruj et al., 2011; Yang and Jia, 2012; Yang et al., 2013a) have been proposed. Nevertheless, these schemes are either proven to be secure in the selectively secure model (Canetti et al., 2003) or lack of efficient revocation approach (Lewko and Waters, 2011; Liu et al., 2011). In the selectively secure model, an additional restriction has to be announced in the "Initial phase", which means that the adversary has to claim the challenge attribute (KP-ABE) (Chase, 2007; Chase and Chow, 2009) or access policy (CP-ABE) (Jung et al., 2013; Ruj et al., 2011; Yang and Jia, 2012; Yang et al., 2013a) before seeing the public parameters. Revocation is another notable factor while deploying attribute-based access control schemes in cloud storage. The user's attributes are dynamically changing (graduated, employed or fired, etc.) and his access privilege also could change. The huge amount of users make it difficult to revoke the users' access privilege timely and effectively to guarantee the data security. Besides, in most attribute-based access control schemes, the decryption complexity goes linearly with the number of attributes used in decryption, which will incur heavy computation overhead (especially for the mobile devices). This motivates us to outsource the main undesirable decryption cost to the cloud sever without revealing the private data. Thus, how to construct an efficient and secure multi-authority access control system for cloud storage remains a challenge issue.

In this paper, we present MAACS, a new fine-grained attribute-based access control scheme for multi-authority cloud storage applications. Our MAACS consists of a new adaptively secure MA-CP-ABE scheme with decryption outsourcing and a revocation approach. We lighten the decryption cost for data users by outsourcing the complicated bilinear pairing computation to the clouds. In MAACS, a data provider can define flexible access policies over descriptive attributes and encrypt the sensitive data before uploading it to the cloud severs. A user is authorized only if he possesses proper attributes that satisfy the access policy deployed in the data. To resist collusion attacks from unauthorized users, a unique global identifier (*gid*) is issued to each user in the system. We also provide an efficient attribute-level revocation method for our scheme. That is, when some attributes are revoked from a user, he will not lose all the access privileges. He can still access some other data if his remaining attributes satisfy the access policy. Our revocation approach also achieves two security requirements. On one hand, after some attributes have been revoked from a user, he cannot decrypt the new encrypted data if his remaining attributes do not satisfy the access policy (Forward Secrecy). On the other hand, when a new user joins in the system, he is not able to decrypt the prior encrypted data even if he has the corresponding attributes (Back Secrecy). In summary, this work makes the following contributions:

1. We present a novel adaptively secure MA-CP-ABE scheme. Our scheme is constructed on composite order groups whose order is a product of three different primes. It supports any monotone access policy which is expressed as a linear secret sharing scheme (LSSS). Our scheme is proved to be adaptively secure in the standard model. Compared with the adaptively secure multi-authority scheme (Liu et al., 2011), the single CA in our scheme cannot decrypt any ciphertext. Thus, our scheme does not require multiple CAs and is more efficient and acceptable for real-world applications.
2. We design an outsourcing paradigm to alleviate the undesirable computation cost for users. By extending the decryption outsourcing approach (Green et al., 2011) to the multi-authority settings, we delegate the bilinear pairing operations to the cloud servers without leaking data contents. As a result, each user only needs to calculate exponent operation once. Thus, the decryption overhead for users can be saved significantly.
3. We propose an efficient revocation approach for the proposed multi-authority CP-ABE scheme. Basing on the revocation method (Hur and Noh, 2011), we realize efficiently immediate attribute-level revocation while achieving both backward and forward secrecy. Different from Hur and Noh (2011), we let the AAs be in charge of executing key updating for users, and the cloud server is responsible to re-encrypt the ciphertext. Thus, our revocation paradigm is more appropriate and acceptable in practice.

The remaining of this work is organized as follows. Section 2 introduces the related works on traditional ABE and attribute-based access control systems. We discuss the definitions of composite order bilinear groups, access structure and LSSS in Section 3. In Section 4, we give the overview of the system model, system definition, threat model, security requirements, assumptions and security game. In Section 5, we propose the detailed construction of MAACS. In Sections 6 and 7, we analyze our MAACS in terms of the security and performance, respectively. We conclude in Section 8. The Appendix describes the detailed formal proof of the adaptive security.