Pervasive and Mobile Computing 28 (2016) 135–149

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Efficient attribute-based data sharing in mobile clouds☆

Yinghui Zhang [a,b,*], Dong Zheng [a,**], Xiaofeng Chen [c], Jin Li [d], Hui Li [c]

[a] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, PR China

[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, PR China

[c] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, PR China

[d] School of Computer Science and Educational Software, Guangzhou University, Guangzhou, PR China

ARTICLE INFO

Article history:
Available online 14 June 2015

Keywords:
Attribute-based encryption
Data sharing
Constant cost
Mobile clouds

ABSTRACT

Ciphertext-policy attribute-based encryption (CP-ABE) is extremely suitable for cloud computing environment in that it enables data owners to make and enforce access policies themselves. However, most of existing CP-ABE schemes suffer severe efficiency drawbacks due to large ciphertext size and computation cost, and hence are not suitable for mobile clouds, where users are usually resource-limited. In this paper, we first present a generic attribute-based data sharing system based on a hybrid mechanism of CP-ABE and a symmetric encryption scheme. Then, we propose a CP-ABE scheme which features constant computation cost and constant-size ciphertexts. The proposed CP-ABE scheme is proven selective-secure in the random oracle model under the decision n-BDHE assumption, where n represents the total number of attributes in universe. It can efficiently support AND-gate access policies with multiple attribute values and wildcards. Theoretical analysis and experimental results indicate that the proposed scheme is extremely suitable for data sharing in mobile clouds.

1. Introduction

Mobile cloud computing is an increasingly important computing paradigm. It leverages the development of cloud computing, wireless communication and networking technologies. Cloud computing significantly improves people's life quality by providing flexible, inexpensive, and quality services. It realizes the pay as you go environment in which various resources are made available to users as they pay for what they use. Although the advantages of the new technology are desirable, data privacy and security issues have become major concerns for individuals and organizations using such services, especially in the case of mobile clouds. In order to prevent potential threats to their data such as improper use by the cloud storage server and unauthorized access by outside users, people would like to make their private data only accessible to users authorized by them. However, in traditional mechanisms based on access control lists, it is required that the storage server should be in the same security domain as data owners and enforce access policies himself. Therefore, those

☆ A preliminary version of this paper appears in ProvSec 2014.

* Corresponding author at: National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an, 710121, PR China.

** Corresponding author.

E-mail addresses: yhzhaang@163.com (Y. Zhang), zhengdong@xupt.edu.cn (D. Zheng), xfchen@xidian.edu.cn (X. Chen), jinli71@gmail.com (J. Li), lihui@mail.xidian.edu.cn (H. Li).

http://dx.doi.org/10.1016/j.pmcj.2015.06.009
1574-1192/

Table 1
An example of $\mathbf{AND}^*_m$.

Attributes	ω_1	ω_2	ω_3	ω_4
Description	Institution	Department	Duty	Gender
Values	Univ. A Univ. B Univ. C Univ. D	IS CS CE /	Administrator Teacher Student /	Male Female / /
CP1	Univ. A	IS	Student	$*$

traditional methods are no longer suitable for cloud-based data sharing, where the server is not fully trusted by users. In particular, fine-grained data access control is necessary for cloud-based data sharing and different levels of access privileges should be granted to different users according to their attributes and roles. With the rapid development of cloud computing technology, the above security issues are thrown into sharp focus. This motivates researchers to consider a paradigm shift, where instead of trusting and being dependent on service providers, data owners can make and enforce fine-grained access policies themselves.

As a one-to-many public-key primitive, attribute-based encryption (ABE) is very promising in implementing fine-grained data sharing systems in cloud computing. In ABE systems, descriptive attributes and access policies, which are associated with attribute secret keys and ciphertexts, are used to enable fine-grained access control over encrypted data. A particular attribute secret key can decrypt a ciphertext if and only if associated attributes and the access policy match each other. ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the access policy is enforced in secret keys and ciphertexts are labeled with a set of attributes. In CP-ABE, the roles of the attribute set and the access policy are swapped from what we described for KP-ABE: every ciphertext is associated with an access policy, and every secret key is associated with a set of attributes. Compared with KP-ABE, CP-ABE is more suitable for cloud-based data sharing in that it enables data owners to make and enforce access policies themselves.

Nevertheless, there remain several challenges to the application of CP-ABE in data sharing in mobile cloud computing, where users are usually resource-constrained to some extent. On the one hand, in most of existing CP-ABE schemes, the computation cost incurred by bilinear pairing (**pair**) and exponentiation (**exp**) operations linearly grows with the complexity of the access policy. On the other hand, most of existing CP-ABE constructions have large-size ciphertexts, which leads to a large communication cost in data sharing. Therefore, before wide deployments on mobile cloud computing platforms, it is indispensable to reduce the computation cost and ciphertext length of CP-ABE while keeping its expressiveness.

To the best of authors' knowledge, the AND-gate CP-ABE construction due to Chen et al. [1] is most efficient.[1] It only needs three **exp** in encryption phase and two **pair** in decryption phase, and has constant-size ciphertexts. However, the AND-gate policy in scheme [1] only supports three values of attributes: positive value, negative value, and wildcards,[2] and we denote the policy by $\mathbf{AND}^*_{+,-}$. In this paper, we aim to give a more efficient CP-ABE scheme supporting AND-gate policies with multiple values and wildcards, which is denoted by $\mathbf{AND}^*_m$. It is worth noting that $\mathbf{AND}^*_m$ is indeed more expressive than $\mathbf{AND}^*_{+,-}$. In other words, in the sense of the same expressiveness, $\mathbf{AND}^*_m$ based scheme is more efficient than $\mathbf{AND}^*_{+,-}$ based one. We show this in the following.

Assume there are n attributes in universe and the attribute set is $\mathcal{U} = \{\omega_1, \omega_2, \ldots, \omega_n\}$. Each attribute has multiple values, and suppose $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,n_i}\}$ is the multi-value set for ω_i and $|S_i| = n_i$. In Table 1, we consider an $\mathbf{AND}^*_m$ policy $\mathbf{CP1} = v_{1,1} \wedge v_{2,1} \wedge v_{3,3} \wedge *$, where the attribute ω_4 associated with "Gender" is not cared for. In other words, if someone's attributes match **CP1** in terms of the first three attributes, he/she can decrypt the ciphertexts under **CP1** regardless of the gender. Note that $n = 4$, $n_1 = 4$, $n_2 = 3$, $n_3 = 3$, $n_4 = 2$ in Table 1, and IS, CS and CE represent "Information Security", "Computer Science" and "Communication Engineering", respectively. In order to realize the same expressiveness as **CP1** based on $\mathbf{AND}^*_{+,-}$ policies, the ciphertext policy **CP2** in Table 2 has to be adopted, where $\mathbf{CP2} = \omega_1^+ \wedge \omega_2^{-1} \wedge \omega_3^{-1} \wedge \omega_4^{-1} \wedge \omega_5^+ \wedge \omega_6^{-1} \wedge \omega_7^{-1} \wedge \omega_8^{-1} \wedge \omega_9^{-1} \wedge \omega_{10}^+ \wedge * \wedge *$. Obviously, the total number of attributes associated with $\mathbf{AND}^*_{+,-}$ is significantly larger than that of $\mathbf{AND}^*_m$, and this often leads to more storage overheads at users' side because of attribute secret keys and public system parameters.

In summary, to realize practical fine-grained data sharing systems in resource-constrained mobile clouds, it is of importance to construct CP-ABE schemes, which support $\mathbf{AND}^*_m$ policies and enjoy constant computation cost and constant-size ciphertexts.

Our contribution. We first present a generic attribute-based data sharing system based on a hybrid mechanism of CP-ABE and a symmetric encryption scheme. Then, we propose a CP-ABE scheme and prove its selective security against chosen plaintext attacks (CPA) in the random oracle model under the decision n-Bilinear Diffie–Hellman Exponent (n-BDHE)

[1] Although the CP-ABE scheme in [2] has smaller ciphertexts than [1], it only supports AND-gate policies on positive and negative values without wildcards in essence, which is denoted by $\mathbf{AND}_{+,-}$. It easily follows that the wildcards used in the ciphertext policy of [2] cannot play the role of "don't care".

[2] After a simple analysis, we know that the ciphertext policy of scheme [1] successfully supports wildcards.