Computer Networks 133 (2018) 157–165

Contents lists available at ScienceDirect

Computer Networks

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

An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited☆

Hui Cui[a,b,*], Robert H. Deng[b], Junzuo Lai[c], Xun Yi[a], Surya Nepal[d]

[a] School of Science, Royal Melbourne Institute of Technology (RMIT) University, Melbourne, Australia
[b] School of Information Systems, Singapore Management University, Singapore
[c] Department of Computer Science, Jinan University, Guangzhou, China
[d] Data 61, CSIRO, Sydney, Australia

ARTICLE INFO

Article history:
Received 28 July 2017
Revised 13 November 2017
Accepted 18 January 2018

Keywords:
Cloud storage
Data security and privacy
Access control

ABSTRACT

Ciphertext-policy attribute-based encryption (CP-ABE) has been regarded as one of the promising solutions to protect data security and privacy in cloud storage services. In a CP-ABE scheme, an access structure is included in the ciphertext, which, however, may leak sensitive information about the underlying plaintext and the privileged recipients in that anyone who sees the ciphertext is able to learn the attributes of the privileged recipients from the associated access structure. In order to address this issue, CP-ABE with partially hidden access structures was introduced where each attribute is divided into an attribute name and an attribute value and the attribute values of the attributes in an access structure are not given in the ciphertext. Though a number of CP-ABE schemes with partially hidden access structures have been proposed, most of them only enable restricted access structures, whereas several other schemes supporting expressive access structures are computationally inefficient due to the fact that they are built in the composite-order groups. To our knowledge, there has been little attention paid to the design of expressive CP-ABE schemes with partially hidden access structures in the prime-order groups. In this paper, we revisit this problem, and present an expressive CP-ABE scheme supporting partially hidden access structures in the prime-order groups with improved efficiency.

1. Introduction

In recent years, there has been an increasing demand for storing data to the cloud [2–4]. Users may not like to store his/her data containing sensitive information to a public cloud without security and privacy guarantee, but they may need to share their data with others possessing certain attributes (or credentials). Ciphertext-policy attribute-based encryption (CP-ABE) [5] is a mechanism meeting this requirement, where each user is given a private attribute-key in terms of his/her attributes issued by an attribute authority (AA), each message is encrypted under an access structure (or access policy) over a set of attributes, and a user can decrypt a ciphertext with his/her private attribute-key if his/her attributes satisfy the access policy ascribed to this ciphertext.

Though a ciphertext generated by a CP-ABE scheme (e.g., [5–8]) does not reveal the identities of the recipients, anyone accessible to a ciphertext may learn some information about the underlying message and the privileged recipients from the access structure clearly included in the ciphertext [9–11]. For example, in a cloud system storing electrical medical records (EMRs) [12,13] of patients as in Fig. 1, there is a ciphertext on an EMR under an access structure "(Patient: NR005289 AND Hospital: City Hospital) OR (Doctor: Cardiologist AND Hospital: General Hospital)". The access structure defines that a patient numbered as NR005289 at the City Hospital or any Cardiologist at the General Hospital can decrypt the ciphertext to obtain the EMR, from which it is not difficult to conclude that a patient NR005289 in the City Hospital is suffering a heart problem. Definitely, cloud users do not expect such an information leakage, so it is crucial to build CP-ABE schemes with attributes hidden in the access structures.

It has been stated in [9] that a CP-ABE scheme with hidden access structures can be built from an attribute-hiding inner-product predicate encryption (IPE) scheme [14], but it is inefficient to implement a CP-ABE scheme with fully hidden access structures (where the attributes are completely hidden from the ciphertext) built from an attribute-hiding IPE scheme [7]. In order to have a trade off between fully hidden access structures and efficient CP-ABE, many CP-ABE schemes with partially hidden access structures (e.g., [9,15–18]) have been proposed. However, some schemes

☆ This paper is an extension to the original publication in ProvSec 2016 [1].

* Corresponding author at: School of Science, Royal Melbourne Institute of Technology (RMIT) University, Melbourne, Australia.

E-mail address: hui.cui@rmit.edu.au (H. Cui).

https://doi.org/10.1016/j.comnet.2018.01.034
1389-1286/© 2018 Elsevier B.V. All rights reserved.

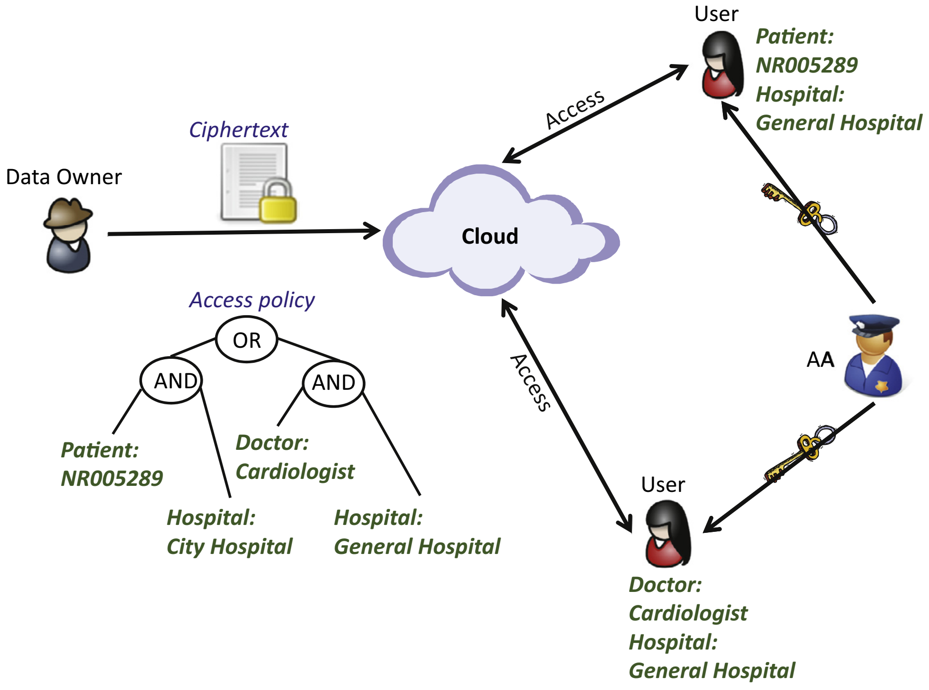

Fig. 1. An architecture of a cloud storage system based on a CP-ABE scheme.

(e.g., [15–18]) only allow restricted access structures (expressed in AND gates), while other schemes (e.g., [9]) supporting expressive access structures are built in the inefficient composite-order groups (note that “a Tate pairing on a 1024-bit composite-order elliptic curve is roughly 50 times slower than the same pairing on a comparable prime-order curve, and this performance gap will only get worse at higher security levels” [19]). There exist techniques (e.g., [19]) to convert schemes in the composite-order groups to that in the prime-order groups, but they cause a significant degradation in the performance [20]. Consequently, it is desirable to construct expressive CP-ABE schemes with partially hidden access structures in the prime-order groups.

1.1. Our contributions

Generally, generic attribute names contain less sensitive information than concrete attribute values. Take the scenario in Fig. 1 as an instance, it is obvious that the attribute values “Cardiologist” and “NR005289” are more sensitive than the attribute names “Doctor” and “Patient”. Motivated by this observation, it has been suggested to use CP-ABE with partially hidden access structures [9,15] which divides each attribute into an attribute name and an attribute value, and the attribute values of an access structure are not included in the ciphertext. Specifically, the full access structure in Fig. 1 is replaced by a partially hidden access structure “(Patient: * AND Hospital: *) OR (Doctor: * AND Hospital: *)” to be included in the ciphertext.

One naive method to build a CP-ABE scheme with partially hidden access structures is to simply remove the attribute names from the access structure of the ciphertext. The resulting scheme, however, suffers off-line dictionary attacks [1], by running which an adversary can determine whether an attribute value is associated with an access structure if the space of the attribute values is not sufficiently large. To overcome this challenge and build an expressive CP-ABE scheme with partially hidden access structures in the prime-order groups, Cui et al. [1] applied the “randomness splitting” [21] technique to the Rouselakis–Waters CP-ABE scheme [20] to hide the sensitive attribute values from the ciphertext. In this way, an access structure with only attribute names (i.e., attribute values are not present) is sent along with the ciphertext. Besides, to convince a user that he/she is a privileged user to the resulting “anonymous” ciphertext, Cui et al. [1] combined a commitment scheme [22] on the message to the corresponding ciphertext such that a user can check the correctness of the decryption result. In this paper, we revisit the expressive CP-ABE scheme with partially hidden access structures in the prime-order groups given in [1], and improve its efficiency by removing the commitment scheme without weakening the security. In the proposed expressive CP-ABE scheme with partially hidden access structures in the prime-order groups, the encryption and decryption algorithms add no exponentiation or pairing calculations to that of the underlying Rouselakis–Waters scheme [20], while the expressive CP-ABE scheme with partially hidden access structures in the prime-order groups in [1] adds several exponentiation operations to that of the underlying Rouselakis–Waters scheme [20].

In summary, the proposed expressive CP-ABE scheme with partially hidden access structures in this paper is similar to the one in [1] except that the former improves the efficiency of the latter by removing the commitment scheme yet allowing a user to check whether he/she is a privileged recipient of a ciphertext without including the associated attribute values.

1.2. Related work

Attribute-based encryption (ABE) was introduced by Sahai and Waters [23], which was then formulated into key-policy ABE (KP-ABE) and CP-ABE [24]. In a KP-ABE scheme, the ciphertext is associated with an attribute set and the private attribute-key is ascribed to an access policy, while the situation is reversed in a CP-ABE scheme. Nevertheless, a CP-ABE scheme is more flexible than a KP-ABE scheme because the access policy in the latter is determined once the user’s private attribute-key is issued. The first CP-ABE scheme was proposed by Bethencourt, Sahai and Waters [5], but it was secure under the generic group model. The first CP-ABE scheme secure in the standard model was presented by Cheung and Newport [6], but it only supported the access structures