Genlang CHEN, Zhiqian XU, Jia-jian ZHANG, Guo-jun WANG, Hai JIANG, Miao-qing HUANG, 2019. Generic attribute revocation systems for attribute-based encryption in cloud storages. *Frontiers of Information Technology & Electronic Engineering*, 20(6):773-786. https://doi.org/10.1631/FITEE.1800512

Generic attribute revocation systems for attribute-based encryption in cloud storage

Key words: Attribute-based encryption; Generic attribute revocation; User privacy; Cloud storage; Access control

Corresponding author: Genlang CHEN
E-mail: cgl@zju.edu.cn

Motivations

1. As a type of cloud service model, cloud storage inherits the benefits of cloud computing and offers a range of advantages over traditional owned storage systems. However, the security challenges arising from the trust in cloud storage providers (CSPs) and shared storage environments have special requirements for data- and user-centric access control.

2. Attribute revocation should allow any number of attributes to be revoked from one user or multiple users without impact on other users, who share or use the same attributes for data decryption.

3. The revocation systems should allow any number of attributes to be revoked rather than all attributes of one person.

Main ideas

1. To be generic and instantaneous to all ABE schemes, the revocation should not require ABE private keys to be re-issued or data to be re-encrypted.

2. The revocation system uses ciphertext re-encryption to control the access to ABE ciphertexts. An AR-ABE system is designed to prevent users from pooling their attribute witnesses to construct any ciphertext re-encryption key.

3. To make an attribute revocation system dynamic, granular, and generic to all types of ABE schemes, we separate revocation control from the underlying ABE schemes.

1. A trust model of an attribute revocation system for ABE in cloud storage

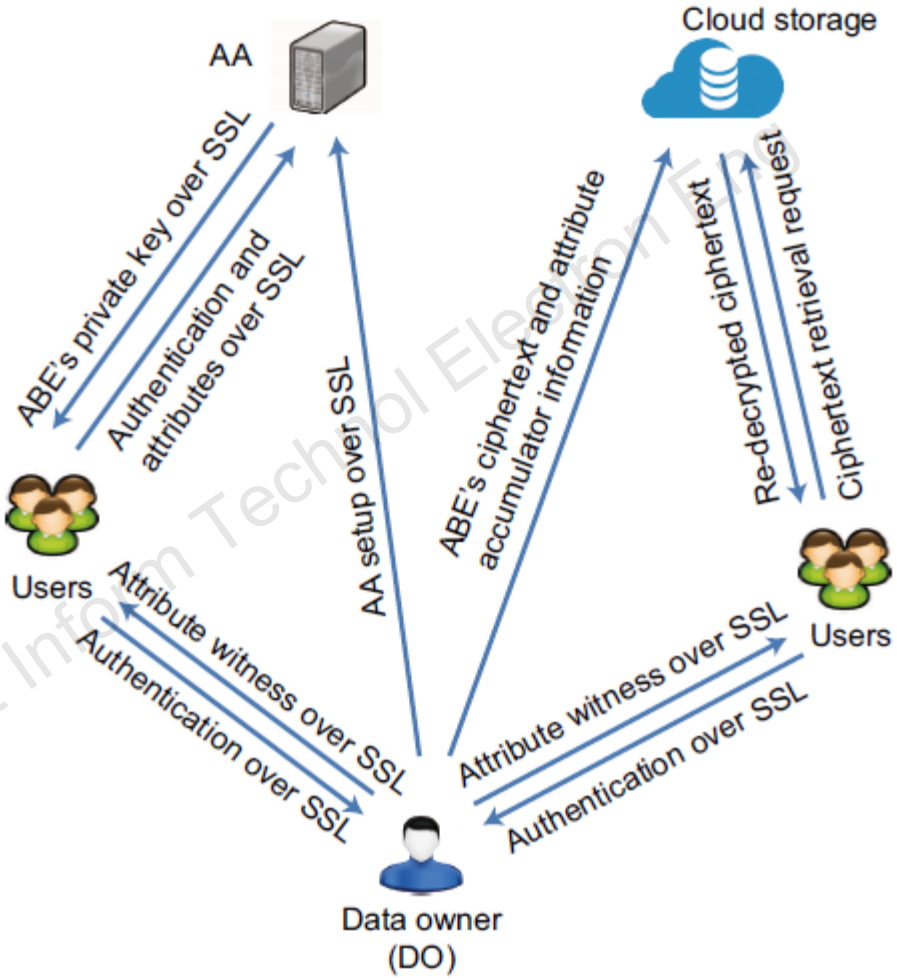

Fig. 1 Trust model of an attribute revocation system for ABE in cloud storage

2. An AATree data structure used for managing user's access to ABE ciphertexts

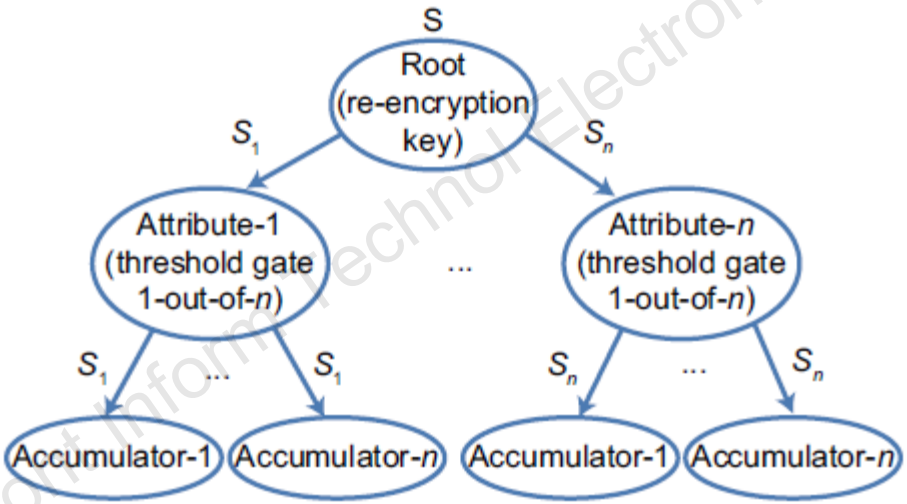

Fig. 2 Attribute accumulator tree

3. Attribute revocation overhead analysis

Adding the attribute revocation system to an ABE scheme introduces the following overhead:

(1) Accumulator management;
(2) Attribute witness updates and management;
(3) One-time encryption key generation and ciphertext re-encryption.

Data owner management	CSP storage requirement	CSP data retrieval management	User witness refreshing
1. Accumulator management; 2. Attribute witness management; 3. AATree management and updates	1. Storage for one copy of ABE ciphertext; 2. Storage for the AATree provided by the data owner	1. One-time re-encryption key generation; 2. Ciphertext re-encryption; 3. One-time re-encryption key embedded to the AATree	Attribute witness and witness updates provided by the data owner

Fig. 4 Overhead of the attribute revocation system (AR-ABE)

Major results

1. Any number of attributes revoked from one user or multiple users does not impact other users using the same attribute or attributes. The users can still use their non-revoked attributes despite their other attributes being revoked. ABE private key is not required to be re-generated after a revocation.

2. Users can anonymously request re-encrypted ABE ciphertexts from CSPs.

3. The system meets the following security requirements: dynamic attribute revocation, witness unforgeability, collusion prevention, anonymity, and ciphertext indistinguishability.

Conclusions

1. An AR-ABE system for ABE schemes has been proposed, which is generic and can be directly applied to any ABE scheme without modifying the underlying ABE scheme.

2. The revocation is dynamic. It does not require the ABE scheme re-issue user private keys or re-encrypt the message for any revoked attribute.

3. There is no limitation on the number of attributes to be revoked from a user or multiple users. It is practical for deployment in untrusted cloud storage environments.