Genlang CHEN, Zhiqian XU, Hai JIANG, Kuan-ching LI, 2018. Generic user revocation systems for attribute-based encryption in cloud storages. *Frontiers of Information Technology & Electronic Engineering*, 19(11):1362-1384.
https://doi.org/10.1631/FITEE.1800405

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

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

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

Motivations

1. Cloud storage is a form of distributed storage that provides massive storage resources and services to meet the demand of data center growth for corporations and remote storage for small businesses and individuals. Although the benefits of cloud storage are compelling, cloud storage does have its potential downsides and risks.

2. Although attribute-based encryption (ABE) is one of the ideal choices for data-centric protection in a cloud environment, dynamic user revocation is the practical limitation.

3. Most current user revocation systems work only with some particular ABE schemes, and are not flexible enough to be adapted to work with general ABE schemes.

Main ideas

1. A practical user revocation system for ABE schemes in an untrusted cloud storage environment should be capable of anonymously identifying a revoked user without including a data owner or a trusted party in the data retrieval process.

2. To achieve generic and anonymous user revocations, we aim at controlling the user access to ABE ciphertexts. We build an extra layer on the top of an ABE scheme to control access to ABE ciphertexts.

3. To achieve better efficiency and scalability, the actual implementations can delegate the management of accumulators, especially witness updates and distribution, to a data-owner trusted third party.

1. User revocation via ciphertext re-encryption (UR-CRE)

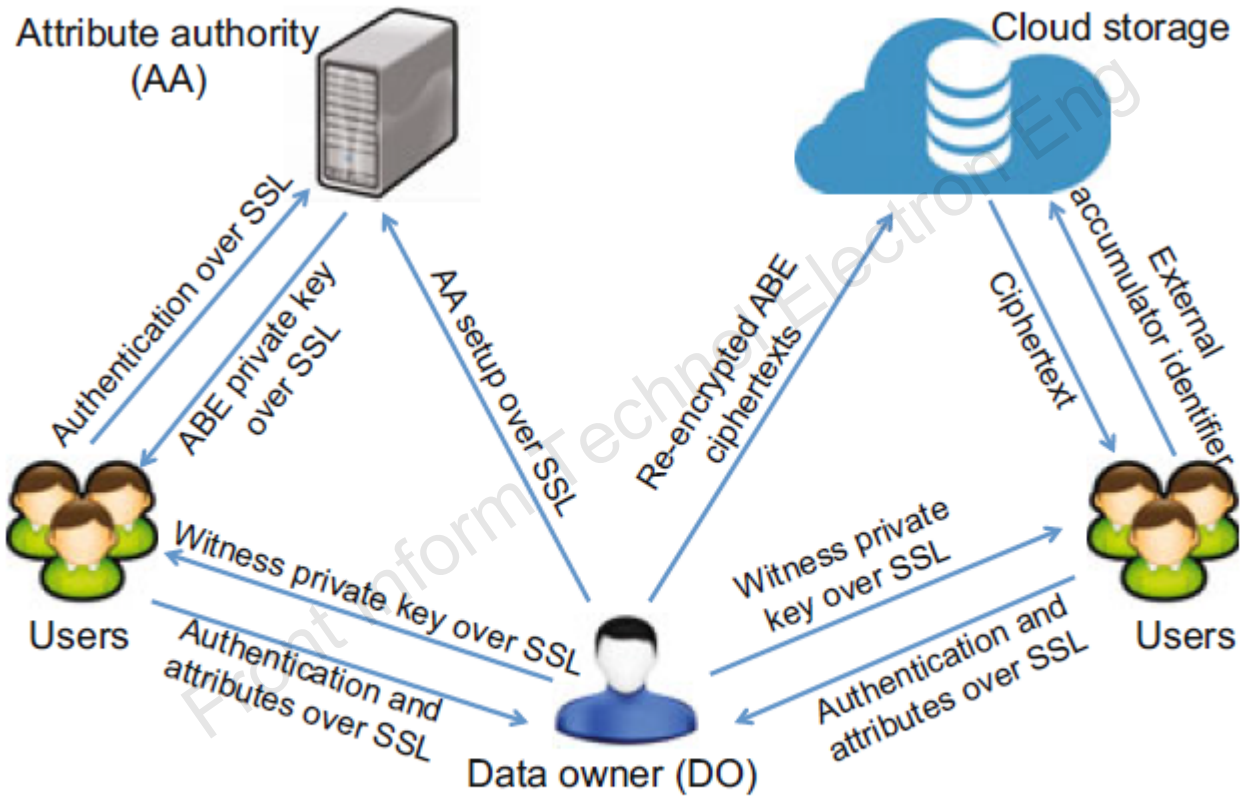

Fig. 1 Trust model of user revocation via ciphertext re-encryption for attribute-based encryption (ABE) in cloud storage

2. User revocation via cloud storage providers (UR-CSP)

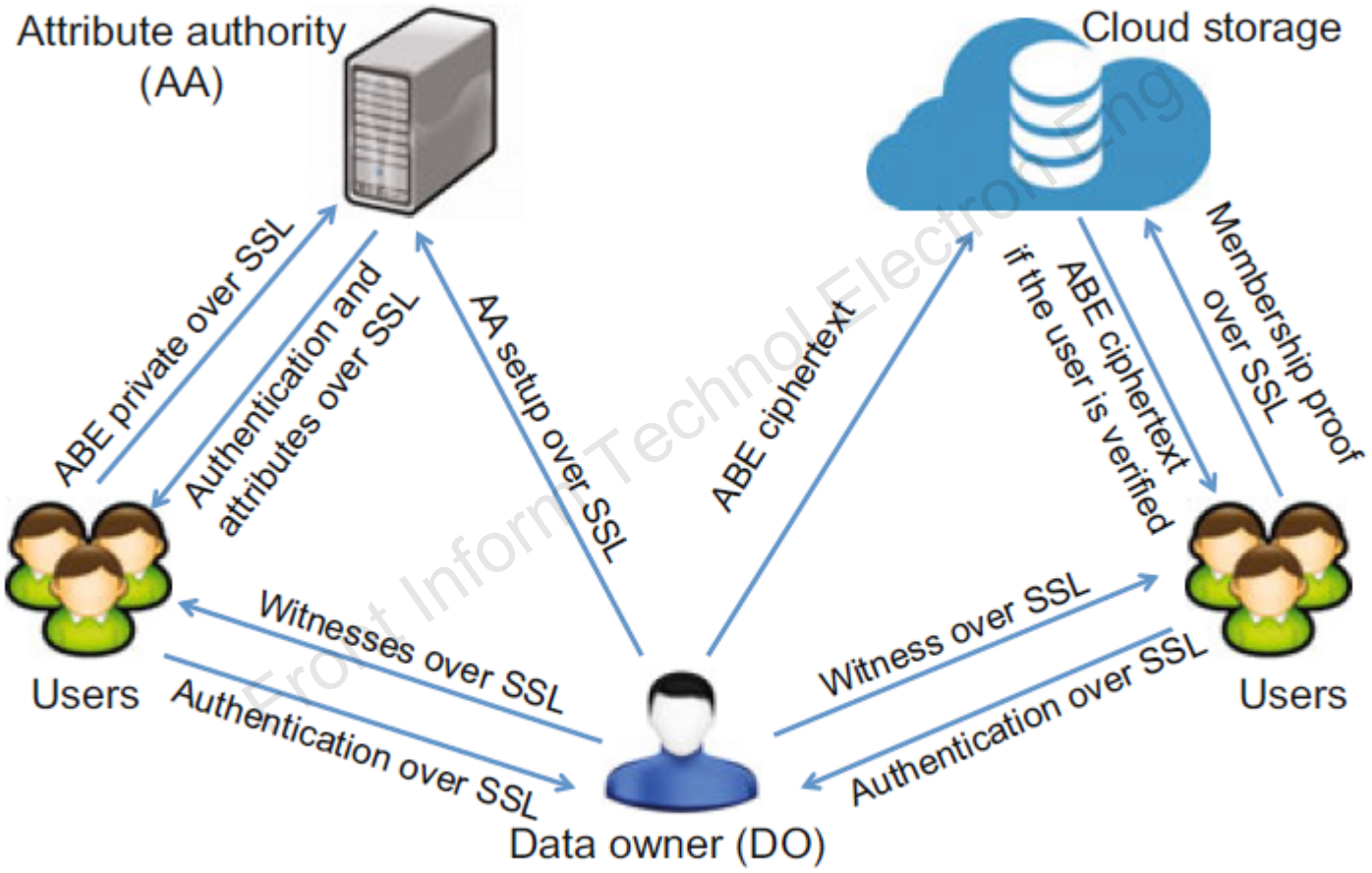

Fig. 3 Trust model of user revocation via cloud service providers for attribute-based encryption (ABE)

3. User revocation overhead analysis

User revocation system	Data owner management	Storage required at a CSP	User witness or key refreshing	Data retrieval
UR-CRE	1. Accumulator management 2. User witness key management 3. ABE ciphertext re-encryptions and updates to CSPs	Multiple copies of ABE ciphertext	The witness keys and key updates provided by the data owner	The re-encrypted ciphertext sent to the user
UR-CSP	1. Accumulator management 2. User witness management 3. Accumulator value updates to CSPs	One copy of ABE ciphertext	The witnesses and witness updates provided by the data owner	1. User verification CSPs 2. ABE ciphertext sent to a verified user

Fig. 5 Overhead comparison of user revocation systems

Major results

1. Dynamic user revocation: Revoked users who have valid ABE private keys are immediately prevented from accessing ABE ciphertext.

2. Ciphertext indistinguishability: The re-encrypted ABE ciphertext should remain indistinguishable against eavesdropping attacks.

3. Unforgeability: Users should not be able to forge their witness private keys to decrypt the re-encrypted ABE ciphertexts.

4. Anonymity: Users remain anonymous to CSPs. CSPs are not required for any user management or administration to fulfill data retrieval requests.

Major results

5. Dynamic user revocation is realized by preventing revoked users from accessing ABE ciphertexts.

6. The system resists eavesdropping adversaries.

7. The system prevents a revoked user from forging the new ciphertext re-encryption key based on the witness private key that the user acquired before the revocation.

Conclusions

1. Two dynamic user revocation systems for ABE schemes have been proposed, which are generic and can be directly applied to any ABE scheme.

2. The user privacy protection have been built into the data retrieval process, making ABE schemes more suitable and practical for deployment in untrusted cloud storage systems.