International Journal of Information Security and Privacy
Volume 19 • Issue 1 • January-December 2025

FUR-HABE:
A Hierarchical CP-ABE Scheme With Traceable Fine-Grained User Revocation for Cloud Storage

Xiaohui Yang
https://orcid.org/0000-0003-0379-6326
Hebei University, China

Ya'nan Tao
https://orcid.org/0009-0002-3505-0051
Hebei University, China

ABSTRACT

An effective method to protect cloud data is access control. But, the efficiency of key distribution by a single authority is low, and it is difficult to achieve dynamic attribute revocation when system properties are shared by multiple users. Existing attribute revocation mechanisms face challenges in terms of functional complexity and computational efficiency, which hinder their practical application. To address these issues, this paper put forward a Hierarchical CP-ABE scheme with Traceable Fine-grained User Revocation for Cloud Storage (FUR-HABE). In this scheme, most of the decryption calculations are outsourced to cloud servers. It employs a layered key authorization mechanism to provide flexible and scalable key delegation. Additionally, the scheme supports key encapsulation key (KEK) attribute revocation and user revocation to accommodate different revocation needs, enabling flexible revocation.

KEYWORDS

Privacy Protection, Attribute Revocation, KEK, Fine-Grained Access Control, CP-ABE

INTRODUCTION

With the development of cloud computing technology, cloud systems provide users with convenient data services (Mell & Grance, 2011). Simultaneously, it has also facilitated improvements in various systems, from current healthcare and assisted living systems to intelligent city systems (Atzori et al., 2010). Seagate predicts that, by 2025, global data creation will grow to 175ZB, posing a significant challenge of explosive data growth for governments and businesses worldwide ("How Backblaze's Fireball B2 Moves Big Datasets to the Cloud Easily, Safely and Swiftly," 2021). For data storage in the cloud, data anonymization is the process of removing or replacing personally identifiable information through technical means so that data cannot be directly associated with a specific individual can prevent sensitive data from being exposed to unauthorized users, using data encryption to protect the data (Han et al., 2010). Encrypted data is always shared by multiple users, so as more sensitive data is in the cloud, fine-grained access control encryption is needed. Sahai and Waters (2005) proposed attribute-based encryption (ABE), which offers an encryption scheme with fine-grained access control. There are two kinds of ABE: key policy ABE (KP-ABE), which

DOI: 10.4018/IJISP.365602

was proposed by Goyal et al. (2006); and ciphertext-policy ABE (CP-ABE), which was proposed by Bethencourt et al. (2007). In CP-ABE, the ciphertexts are associated with access policies, the decryption key is associated with the attribute, and only users who satisfy this policy can decrypt the data, while, in KP-ABE, the ciphertext is associated with the attribute, data is then encrypted based on the user's attributes, and the decryption key is bound with the access policies. Considering the specificity environment of the cloud, we believe that it is more appropriate to use CP-ABE to protect data security in cloud systems because it allows users to customize access policies.

However, due to various issues, pure CP-ABE is not suitable for direct application in applications. The first of these issues is revocation. Revocation can be divided into user revocation, partial attribute revocation, and system attribute revocation. Partial attribute revocation, known as attribute-level user revocation, is the most finely-grained method of revocation (Han et al., 2020). Revoking any attribute from any user may affect other users in the system because every attribute in the system can be shared by multiple users. Additionally, although attribute revocation is more fine-grained, it is less effective when dealing with users because it requires revoking all attributes of that user. Yu et al. (2010) and Naor et al. (2001) focused on the complexity of attribute revocation. In the direct revocation model, revoking a user's identity to revoke all attributes owned by the user is coarse-grained. The second issue is the burden of authority. Hur et al. (2013), Rouselakis and Waters (2015), and K. Yang, X. Jia, & K. Ren, (2013) found that most existing ABE schemes relying on a single key authorization entity have key escrow issues. Having a single central authority (CA) responsible for all attribute management, key distribution, and revocation operations can lead to overwhelming pressure on the authority, increased latency, lack of efficiency, and potential pitfalls. J. Li et al. (2019) studied a hierarchical access control scheme based on attribute encryption in cloud computing. Their proposed scheme enables users to encrypt multiple files at the same access level. However, this led to performance bottlenecks in distributed cloud systems. In the paper, we solve the above issues by designing a hierarchical ABE scheme with traceable flexible revocation, suitable for practical large-scale cloud storage networks.

Related Work

Sahai and Waters (2005) introduced the first ABE scheme, which has evolved into two forms: CP-ABE and KP-ABE. CP-ABE not only protects the data privacy but also allows data owners to customize flexible access policies. The revocation issue of CP-ABE is one of the main obstacles to its widespread use. Before ABE, the revocation issue was studied in IBE that is a public key encryption mechanism in which a user's public key is directly associated with their identity information, simplifying key management. Boldyreva et al. (2001) proposed a revocable IBE scheme by letting the authority broadcast update materials at each revocation period. Pirretti et al. (2006) solved the property revocation problem by associating an expiration date with each property. Sun et al. 2020) and Huang et al. (2021) proposed a revocation method with periods, conducting revocation updates periodically. However, these schemes cannot achieve real-time attribute revocation. To implement an instant revocation mechanism, Tysowski et al. (2013) and Yu et al. (2010) presented a new approach to perform revocation operations by applying CP-ABE and re-encryption. In this approach, after each revocation, the cloud service provider (CSP) re-encrypts the ciphertext to prevent the revoked user from being able to decrypt. Han et al. (2020) and Zhang et al. (2018) proposed an attribute-based CP-ABE scheme, where the ciphertext consists of two parts: one part is concerning to the access policy for attribute values encryption, and the other is related to revocation information updated during revocation. However, the above schemes only support coarse-grained user revocation. Hur et al. (2010) introduced the concept of attribute groups, providing a foundation for fine-grained attribute revocation. Wang et al. (2018) proposed a revocation method that involves a third party's assistance, and the user's key consists of two parts: user key and group key. Liu et al. (2020) proposed a scheme based on ciphertext policy attributes, utilizing key encapsulation key (KEK) and re-encryption for effective attribute revocation. Wang et al. (2021) studied KEK-based CP-ABE with efficient revocation, where the cloud server implements user logout at the attribute level, which can reduce the burden on

Related Content