CryptCloud+ Secure and Expressive Data Access Control for Cloud Storage

ABSTRACT

Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights), due to the intrinsic “all-or-nothing” decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi-trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as CryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

**EXISTING SYSTEM**

* Li et al. introduce the notion of accountable CP-ABE [23] to prevent unauthorized key distribution among colluded users. In a later work [22], a user accountable multi-authority CP-ABE system is proposed. Liu et al. also proposed white-box [27] and black-box [26] traceability 1 CP-ABE systems supporting policy expressiveness in any monotone access structures.
* Ning et al. [30], [32], [34], [36] propose several practical CP-ABE systems with white-box traceability and black-box traceability. Deng et al. [11] provide a tracing mechanism of CP-ABE to find the leaked access credentials in cloud storage system.
* Sahai et al. [40] define the problem of revocable storage and provide a fully secure construction for ABE based on ciphertext delegation. Yang et al. [49] propose a revocable multi-authority CP-ABE system that achieves both forward and backward security. More recently, Yang et al. [50] propose an attribute updating method to achieve the dynamic change on attribute (such as revoking previous attribute and re-granting previously revoked attribute).
* **Disadvantages**
* There is less security on outsourced data due to lack of Verification Based on Hash code.
* There is no more security in the data access.

**PROPOSED SYSTEM**

* The proposed system presents a formal framework model of the proposed system, designed for practical cloud storage system deployment.
* The system addresses a weakness in the auditing procedure of the conference version. Specifically, a malicious user may change tid of his secret key in the conference version, and the auditing procedure will fail in this case. As a mitigation, we revise the key generation algorithm and add an audit list to detect if the tid is changed.
* The system enhances the functionality of the construction (w.r.t. AAT-CP-ABE) proposed in the conference version and further present two enhanced constructions, namely ATER-CP-ABE and ATIR-CP-ABE. These constructions allow us to effectively revoke the malicious users explicitly or implicitly. We also present the new definitions, technique and related materials of ATER-CP-ABE and ATIR-CP-ABE.
* Based on the new ATER-CP-ABE and ATIR-CPABE, we present CryptCloud+ which is an effective and practical solution for secure cloud storage.
* The system provides general extensions (of our system) on the large universe, the multi-use, and the prime-order setting cases, so that the solution introduced in this paper is more scalable in real-world applications.
* The system comprehensively evaluates the efficiency of the proposed ATER-CP-ABE and ATIR-CP-ABE via experiments.

**Advantages**

* Traceability of malicious cloud users. Users who leak their access credentials can be traced and identified.
* Accountable authority. A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract).
* Auditing. An auditor can determine if a (suspected) Cloud.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL