Secure Keyword Search and Data Sharing Mechanism for Cloud Computing.

ABSTRACT

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it’s outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this paper, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison..

**EXISTING SYSTEM**

In an ABE, the users’ identities are described by a list of attributes [1]. After ABE’s pioneering work [1], several scholars extended the notion of ABE. For example, key policy attribute-based encryption (KP-ABE) [2], where the private key of a user is related to an access policy and the cipher text corresponds to an attribute set. In contrast, there is another example called cipher text-policy attribute-based encryption

(CP-ABE) [3], where the private key is generated with an attribute set and the cipher text is related to an access policy. In both KP-ABE and CP-ABE, the cipher text length is linear with the size of the access policy. To reduce the cipher text length, Emura et al. [8] proposed a cipher text-policy attribute-based encryption scheme with constant cipher text length. Although it supports the AND-gates on multi attributes, it doesn’t support the monotonic express on attributes. After that, a number of constructions have come out to enhance the efficiency, security and expressiveness [4], [9], [10]. To illustrate the ABE’s application, Li et al. [11] adopted the notion of attribute-based encryption in the PHR system to achieve fine grained access control on personal health records.

A cipher text policy attribute-based encryption with hidden policy [12] was proposed to hide the access policy which may leak the user’s privacy in the PHR system. The concept of outsourcing decryption attribute-based encryption was introduced to enable a computation-constrained mobile device to outsource most of the decryption work to a service provider [13]. However, there is no guarantee that the service provider could return the correct partial decryption cipher text. To overcome this issue, Lai [14] and Li [15] proposed attribute-based encryption with verifiable outsourced decryption schemes respectively.

Proxy re-encryption was designed to delegate the decryption [16]. Prior work has focused on the scheme’s functionality, efficiency, and security model [17] [18] [19], [20]. Later, Liang et al. [21] presented an attribute-based proxy re-encryption (AB-PRE) scheme by using proxy re-encryption to a attribute based setting. Meanwhile, another AB-PRE scheme was proposed to support “AND” gates on positive and negative attributes [22]. Following their work, Liang et al. [23] proposed a cipher text-policy attribute-based proxy re-encryption (CPABPRE) scheme supporting a monotonic access formula in the selective model. Later, the security has been improved in an adaptive model [24]. Ge et al. [25], [26] presented two KPABE schemes that are secure in the selective and adaptive model respectively. Liang et al. [27] proposed a deterministicfinite automata (DFA) based PRE scheme, where the access policy is viewed as a DFA. Unfortunately, the privacy could not be preserved in keyword search in all of these schemes.

Disadvantages

* + In the existing work, the system does not provide **Data integrity proof**.
  + This system is less performance due to lack of strong encryption techniques.

**PROPOSED SYSTEM**

The proposed system first introduces a ciphertext-policy attribute-based mechanism

with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The searching and sharing functionality are enabled in the ciphertext-policy setting. Furthermore, our scheme supports the keyword to be updated during the sharing phase. After presenting the construction of our mechanism, we proof its chosen ciphertext attack (CCA) and chosen keyword attack (CKA) security in the random oracle model. The proposed construction is demonstrated practical and efficient in the performance and property comparison.

**Advantages**

1) allows the data owner to search and share the encrypted health report without the unnecessary decryption process.

2) supports keyword updating during the data sharing phase. 3) more importantly, does not need the exist of the PKG, either in the phase of data sharing or keyword updating.

4) the data owner can fully decide who could access the data he encrypted.

**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