Efficient Retrieval over Documents Encrypted by Attributes in Cloud Computing

ABSTRACT

Secure document storage and retrieval is one of the hottest research directions in cloud computing. Though many searchable encryption schemes have been proposed, few of them support efficient retrieval over the documents which are encrypted based on their attributes. In this paper, a hierarchical attribute-based encryption scheme is first designed for a document collection. A set of documents can be encrypted together if they share an integrated access structure. Compared with the ciphertext-policy attribute-based encryption (CP-ABE) schemes, both the ciphertext storage space and time costs of encryption/decryption are saved. Then, an index structure named attribute-based retrieval features (ARF) tree is constructed for the document collection based on the TF-IDF model and the documents’ attributes. A depth-first search algorithm for the ARF tree is designed to improve the search efficiency which can be further improved by parallel computing. Except for the document collections, our scheme can be also applied to other datasets by modifying the ARF tree slightly. A thorough analysis and a series of experiments are performed to illustrate the security and efficiency of the proposed scheme.

**EXISTING SYSTEM**

* Wang et al. propose a hierarchical attribute-based encryption scheme named FHCP- ABE [28] and have proved its security theoretically. An advantage of the scheme is that the data users can decrypt all the authorized documents by computing the secret key once. Therefore, both the time costs of encryption and decryption are saved.
* Wang et al. design a scheme named HABE [29] with the traits of high performance, fine-grained access control scalability and full delegation. HABE is a combination of hierarchical identity-based encryption and CP-ABE.
* Wan et al. propose hierarchical attribute-set-based encryption scheme (HASBE) [30] by extending cipher text-policy attribute-set based encryption (ASBE) with a hierarchical structure of the data users. The HASBE scheme can be seamlessly incorporated with a hierarchical structure of system users by applying a delegation algorithm to ASBE.
* Deng et al. extend ABE to CP-HABE [31] to support hierarchically distributing and delegating the secret keys which can be used in large organizations. Guo et al. [36] propose a resilient-leakage hierarchical attribute-based encryption scheme to defend against the auxiliary input leakage attack and the security of the scheme is detailed analyzed.
* **Disadvantages**
* There is less security Due to lack of A practical hierarchical attribute-based document collection encryption scheme.
* There is no Data integrity technique to audit outsourced data.

**PROPOSED SYSTEM**

* In the proposed system, the system assumes that the CA center and the cloud server are trustable. Specifically, the CA center can distribute proper attributes to the data users and the cloud server can execute all the instructions honestly. The system further assumes that the data users are greedy and attempt to obtain as many plaintext files as possible.
* The data users try to collude with other users to decrypt the encrypted documents. The system mainly restrict our attention to the process of encryption, document search and decryption

**Advantages**

* The documents can be encrypted and decrypted flexibly based on their attributes. In general, the system hopes that the proposed scheme can get logarithmic encryption and decryption time efficiency..
* For a data user with an attribute set, the system needs to store only one secret key and the key can be used to decrypt all the documents that have legal attributes.
* The proposed scheme aims to achieve logarithmic search efficiency over the encrypted files in general and at least sub linear search efficiency in the worst case.

**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