Efficient Traceable Authorization Search System for Secure Cloud Storage

ABSTRACT

Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may

intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this paper, we propose an escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption (EF-TAMKS-VOD). The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user revocation is enabled after the malicious user is figured out. Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded. Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result. Security analysis indicates that EF-TAMKS-VOD is provably secure. Efficiency analysis and experimental results show

that EF-TAMKS-VOD improves the efficiency and greatly reduces the computation overhead of users’ terminals.

**EXISTING SYSTEM**

Later, Xu et al. [17] presented a general framework to combine PEKS and fuzzy keyword search without concrete construction. Tang [18] proposed a multiparty searchable encryption scheme together with a bilinear pairing based scheme. In 2016, Chen et al. [3] introduced the concept “dual-server” into PEKS to resist off-line keyword guessing attack.

 Yang et al. [19] introduced time-release and proxy reencryption method to PEKS scheme in order to realize timecontrolled authority delegation. Wang et al. [1] proposed a ranked keyword search scheme for searchable symmetric encryption, in which the order-preserving symmetric encryption is utilized [35]. Cao et al. [36] designed a novel system to realize multiple keyword ranked search. Searchable encryption is also further studied in [20], [21], [22].

* **Disadvantages**
* Inflexible authorized keyword search.
* Inefficient decryption and Abuse of attribute secret key.

**PROPOSED SYSTEM**

* **Flexible Authorized Keyword Search**. EF-TAMKSVOD achieves fine-grained data access authorization and supports multiple keyword subset search. In the encryption phase, a keyword set KW is extracted from the file, and both of KW and the file are encrypted. An access policy is also enforced to define the authorized types of users. In the search phase, the data user specifies a keyword set KW0 and generates a trapdoor TKW0 using his secret key. In the test phase, if the attributes linked with user’s secret key satisfy the file’s access policy and KW0 (embedded in the trapdoor) is a subset of KW (embedded in the ciphertext), the corresponding file is deemed as a match file and returned to the data user. The order of keywords in KW0 can be arbitrarily changed, which does not affect the search result.
* **Flexible System Extension**. EF-TAMKS-VOD supports flexible system extension, which accommodates flexible number of attributes. The attributes are not fixed in the system initialization phase and the size of attribute set is not restricted to polynomially bound, so that new attribute can be added to the system at any time. Moreover, the size of public parameter does not grow with the number of attributes. No matter how many attributes are supported in the system, no additional communication nor storage costs is brought to EF-TAMKS-VOD. This feature is desirable for the cloud system for its ever increasing user volume.
* **Efficient Verifiable Decryption**. EF-TAMKS-VOD adopts the outsourced decryption mechanism to realize efficient decryption. Most of the decryption computation are outsourced to the cloud server, and the data user is able to complete the final decryption with an ultra lightweight computation. Moreover, the correctness of the cloud server’s partial decryption computation can be verified by the user.
* **White-box Traceability of Abused Secret Key**. Traitor tracing can be divided into white-box and black-box traceability. If an authorized user leaks or sells his secret key, white-box traceability is capable to identify who leaks the key. Black-box traceability is a stronger conception, in which the leakage of a malicious user is the search and decryption equipment instead of the secret key. EF-TAMKS-VOD achieves white-box traceability. Any subscriber who leaks the secret key to a third party intentionally or unintentionally can be traced. Furthermore, the traceability of EFTAMKS- VOD does not bring additional computation and transmission overhead.
* **Efficient User Revocation**. Once a user is identified as traitor through tracing algorithm, EF-TAMKS-VOD revokes this malicious user from the authorized group. Compared with the existing scheme [7], the revocation mechanism of EF-TAMKS-VOD has much better efficiency.

**Advantages**

* The system Generates Secure File and Keyword Index.
* The system Retrieves Matched Files and fast Outsourced Computing.

**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