**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:**

* Most of the available systems require the user to perform a large amount of complex bilinear pairing operations. These overwhelmed computations become a heavy burden for user’s terminal, which is especially serious for energy constrained devices. The outsourced decryption method allows user

to recover the message with ultra lightweight decryption. However, the cloud server might return wrong half-decrypted information as a result of malicious attack or system malfunction.

* The authorized entities may illegally leak their secret key to a third party for profits. As a result, the data privacy will be at risk. so, it is extremely urgent to identify the malicious user or even prove it in a court of justice. However which is not possible to identify illegal leakage of secret keys.

**DISADAVANTAGES**

* **Inflexible system extension**: Many existing authorization schemes are inflexible for the system extension. The attribute set needs to be predefined during the system establishment phase, and a maximum number of the attribute set should be determined. If a new attribute is to be added to the system, the entire system has to be re-constructed and all encrypted files have to be re-encrypted. It would be a disaster to the cloud storage system. Security problem
* **Inefficient decryption**: A main drawback of many ABE based fine-grained access control schemes is that the computation cost required for decryption grows linearly with the complexity of access structure.
* **Inefficient user revocation**: User revocation function is important for a multi-user cloud storage system. Most of the available searchable encryption schemes do not support this function.

**PROPOSED SYSTEM:**

* **Flexible System Extension**: We propose an efficient system which 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 the system. This feature is desirable for the cloud system for its ever increasing user volume.
* **Efficient Verifiable Decryption**. We propose a system which adopts the outsouced 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.
* **Efficient User Revocation**. Once a user is identified as traitor through tracing algorithm, system revokes this malicious user from the authorized group. Compared with the existing scheme this revocation mechanism

has much better efficiency.

**ADAVANTAGES**

* Flexible System Extension:
* Efficient Verifiable Decryption.
* Efficient User Revocation.
* Traceability of Abused Secret Key.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 500 GB.
* Input Devices : Keyboard, Mouse
* Ram : 2GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Net beans 7.2.1
* Database : MYSQL