**INTRODUCTION**

With the development of new computing paradigm, cloud computing becomes the most notable one, which provides convenient, on-demand services from a

shared pool of configurable computing resources. Therefore, an increasing number of companies and individuals prefer to outsource their data storage to cloud server. Despite the tremendous economic and technical advantages, unpredictable

security and privacy concerns become the most prominent problem that hinders the widespread adoption of data storage in public cloud infrastructure. Encryption is a fundamental method to protect data privacy in remote storage .However, how to effectively execute keyword search for plaintext becomes difficult for encrypted

data due to the unreadability of ciphertext. Searchable en-cryption provides mechanism to enable keyword search over encrypted data For the file sharing system, such as multi-owner multiuser scenario, fine-grained search authorization is a desirable function for the data owners to share their private data with other authorized user. However, 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. Thus, it is an important issue to guarantee the correctness of outsourced decryption in public key encryption with keyword search (PEKS) system. The authorized entities may illegally leak their secret key to a third party for profits . Suppose that a patient someday suddenly finds out that a secret key corresponding his electronic medical data is sold on e-Bay. Such despicable behavior seriously threatens the patient’s data privacy. Even

worse, if the private electronic health data that contain serious health disease is abused by the insurance company or the patient’s employment corporation, the patient would be declined to renew the medical insurance or labor contracts.

The intentional secret key leakage seriously undermines the foundation of authorized access control and data privacy protection. Thus, it is extremely urgent to identify the malicious user or even prove it in a court of justice. In attribute based access control system, the secret key of user is associated with a set of attributes rather than individual’s identity. As the search and decryption authority can be 2168-7161 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications\_standards/publications/rights/index.html for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2018.2820714,

IEEE Transactions on Cloud Computing IEEE TRANSACTIONS ON CLOUD COMPUTING 2 shared by a set of users who own the same set of attributes,

it is hard to trace the original key owner . Providing traceability to a fine-grained search authorization system is critical and not considered in previous searchable

encryption systems . More importantly, in the original definition of PEKS scheme , key generation centre (KGC) generates all the secret keys in the system, which inevitably leads to the key escrow problem. That is, the KGC knows all the secret

keys of the users and thus can unscrupulously search and decrypt on all encrypted files, which is a significant threat to data security and privacy. Beside, the key escrow problem brings another problem when traceability ability is realized

in PEKS. If a secret key is found to be sold and the identity of secret key’s owner (i.e., the traitor) is identified, the traitor may claim that the secret key is leaked by KGC. There is no technical method to distinguish who is the true traitor if the key escrow problem is not solved.

**Searchable Encryption:**

Searchable encryption enables keyword search over encrypted data. The concept of public key encryption with keyword search (PEKS) was proposed by Boneh et al,

which is important in protecting the privacy of outsourced data. Data owners in PEKS schemes store their files in encrypted form in the remote untrusted data server. The data users query to search on the encrypted files by generating a keyword trapdoor, and the data server executes the search operation. Waters et al. showed that PEKS schemes could be utilized to construct searchable audit logs.

Later, Xu et al. presented a general framework to combine PEKS and fuzzy keyword search without concrete construction. Tang proposed a multiparty searchable encryption scheme together with a bilinear pairing based scheme. In 2016, Chen et al. introduced the concept “dual-server” into PEKS to resist off-line keyword guessing attack. Yang et al. introduced time-release and proxy reencryption method to PEKS scheme in order to realize time controlled

authority delegation. Wang et al. proposed a ranked keyword search scheme for searchable symmetric encryption, in which the order-preserving symmetric encryption is utilized . Cao et al. designed a novel system to realize multiple keyword ranked search. Searchable encryption is also further studied

**ABE:**

ABE is an important method to realize fine-grained data sharing. In ABE schemes, descriptive attributes and access policies are associated with attribute secret keys and ciphertexts. A certain secret key can decrypt a cipher text if and only if the associated attributes and the access policy match each other. The notion of ABE was proposed by Sahai et al. in 2005. According to whether the access control policy associates with the ciphertext or the secret key, ABE schemes

can be classified into ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) . Since the Sahai’s seminal work, ABE based access control

becomes a research focus .Considering the challenges in expressing access control policy, ABE scheme with non-monotonic access structure is proposed. ABE systems with constant size ciphertext are constructed to reduce the storage overhead. In order to accelerate the decryption, researchers make effort to speed

up the decryption algorithm . Decentralized ABE is investigated in , in which multiple authorities work independently without collaboration.

**Traitor Tracing:**

Traitor tracing was introduced by Chor et al. to help content distributors identifying pirates. In the digital content distribution system, there is no way to prevent a legitimate user to give (or sell) his decryption key to the others. Traitor tracing mechanism helps the distributor to find out the misbehaved user by running “tracing” algorithm so that he could take legal action against the owner of the leaked secret key. Later, traitor tracing mechanism is introduced to broadcast

encryption, where a sender is able to generate ciphertext and only the users in the designated receiver set can decrypt.The traceability function enables the broadcaster to identify the traitor, and prevents the authorized users from leaking their keys. The approach is to give each user a distinct set of keys, which is deemed as “watermark” for tracing. Traceability is further investigated for broadcast encryption in . In CP-ABE scheme, secret keys are not defined over identities. Instead, they are associated with a set of attributes. Multiple users may share the same set of attributes. This brings convenience to expressive access control. However, given a leaked secret key, it is impossible to figure out the original key owner in traditional ABE system. It means that the malicious user, who sells his secret key, almost has little risk of being identified. The traceability problem in CP-ABE is studied .