Journal of Engineering Sciences

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

Efficient Traceable Authorization Search System for Secure Cloud Storage

SWAPNA MANDALA[1], HUMA QAMAR KHAN[2]

[1] Assistant Professor, Dept of CSE, Mahaveer Institute of Science and Technology, Hyderabad, TS, India , E-MAIL: **swapnamandala@gmail.com**

[2] PG Scholar, Dept of CSE, Mahaveer Institute of Science and Technology, Hyderabad, TS, India , E-MAIL: humaqk@gmail.com

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 **e**scrow **f**ree **t**raceable **a**ttribute based **m**ultiple **k**eywords **s**ubset **s**earch system with **v**erifiable **o**utsourced **d**ecryption (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.

Keywords: Cloud computing, key generation centre (KGC), data privacy, and Multi-user system.

I.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 3 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 plain text becomes difficult for encrypted data due to the un readability of cipher text. Searchable encryption provides mechanism to enable keyword search over encrypted data. For the file sharing system, such as multi-owner multiuser scenario, fine-grained search 4 authorizations are 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 out sourced 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 some day suddenly find sout 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 2 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 shared by a set of users who own the same set of attributes, it is hard to trace the original key owner. 4 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. 2 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.

II.EXISTING SYSTEM:

Secure search over encrypted remote data is crucial in cloud computing to guarantee the data 1 privacy and usability. To prevent unauthorized data usage, fine-grained access control is 3 necessary in multi-user system. However, authorized user may intentionally leak the secret key 2 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.

Dis advantages

1. Leakage of the secret key.
2. Loss of data.

III.PROPOSED SYSTEM:

The key escrow free mechanism could effectively prevent the key generation centre (KGC) from 2 unscrupulously searching and decrypting all encrypted files of users. Also, the decryption 1 2 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.

SYSTEM ARCHITECTURE

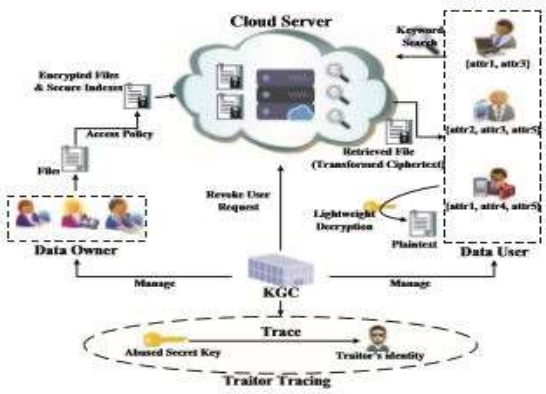

Fig. 1: System Model

CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

IV.RESULTS

Home screen

user register page

User login page

User home page

User profile page

Keyword serach page

Illegal request send to kgc page

View response page

Download key verification page

Request key to another user page

Data owner register page

View key from the user

Data owner home page

User's file download history

Data owner profile page

Data owner login page

Upload file page

View all uploaded page

Find traitor

Kgc login screen

Traitor result page

Kgc home page

Csp login screen

View request page

Cloud welcome screen

User details

Owner details

All files

Kgc request

Download history

CONCLUSION

The enforcement of access control and the support of keyword search are important issues in secure cloud storage system. In this work, we defined a new paradigm of searchable encryption system, and proposed a concrete construction. It supports flexible multiple keywords subset search, and solves the key escrow problem during the key generation procedure. Malicious user who sells secret key for benefit can be traced. The decryption operation is partly outsourced to cloud server and the correctness of half-decrypted result can be verified by data user. The performance analysis and simulation show its efficiency in computation and storage overhead. Experimental results indicate that the computation overhead at user's terminal is significantly reduced, which greatly saves the energy for resource-constrained devices of users.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, W. Lou. "Secure ranked keyword search over encrypted cloud data"[C]//IEEE 30th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2010: 253-262.

[2] Q.Zhang,L.T.Yang,Z.Chen,P.Li,M.J.Deen."Privacy-preserving Double-Projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning," IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.

[3] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server PublicKey Encryption with Keyword Search for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 789-798.

[4] X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. "An efficient

privacypreservingoutsourcedcalculationtoolkitwithmultiplekeys."IEEE Transactions on Information Forensics and Security 11.11 (2016): 2401-2414.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in NDSS, 2004.

[6] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language". IEEE Transactions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.

[7] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Finegrained Owner-enforced Search Authorization in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

[8] K. Liang, W. Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage ,"IEEE Transactions onInformationForensicsandSecurity,2015,vol.10,no.9 ,pp.19811992.

[9] M.Green,S.Hohenberger,andB.Waters,"Outsourcingthedecryption of ABE ciphertexts," in USENIX Security Symposium, ACM, 2011, pp. 34-34.

[10] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 134313

AUTHORS PROFILES

Mrs. Swapna Mandala

GUIDE DETAILS:

Mrs. Swapna Mandala is working as Assistant Professor in Mahaveer Institute of Science and Technology affiliated to JNTUH as vast experience of 14 yrs in the teaching. Completed her Master in Computer Science and Engineering in JNTUH affiliated College.

Her area of interest subjects are Information Retrieval System, Object Oriented Analysis and Design, Software Process and Project Management.

swapnamandala@gmail.com

Author 2:

HUMA QAMAR KHAN (Student)