International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 23rd Nov 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-11

Title **EFFICIENT TRACEABLE AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE USING KEY GENERATION CENTRE**

Volume 08, Issue 11, Pages: 202–206.

Paper Authors

E.SAMBASIVA RAO, MIRIYALA SRINIVASA RAO

SRI CHUNDI RANGANAYAKULU ENGINEERING COLLEGE

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

EFFICIENT TRACEABLE AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE USING KEY GENERATION CENTRE

[1]E.SAMBASIVA RAO, [2]MIRIYALA SRINIVASA RAO
[1]ASSOCIATE PROFISSER & HOD OF CSE DEPARTMENT, SRI CHUNDI RANGANAYAKULU ENGINEERING COLLEGE
[2]STUDENT, SRI CHUNDI RANGANAYAKULU ENGINEERING COLLEGE
sambusoft@gmail.com, miriyalasrinivasarao125@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 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.

1. INTRODUCTION

The development of new computing paradigm, cloud computing [1] becomes the most notable one, which provides convenient, on-demand services from as hared 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, un-predictable security and privacy concerns [2], [3] become the most prominent problem that hinders the wide spread adoption of data storage in public cloud infrastructure. Encryption is a fundamental method to protect data privacy in remote storage [4]. However, how to effectively execute key word search for plaintext becomes difficult for encrypted data due to the un readability of ciphertext. Searchable encryption provides mechanism to enable keyword search over encrypted data [5], [6].For the file sharing system, such as multi-owner multi-user 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 [7], [8] require the user to perform a large amount of complex bilinear pairing operations. These over-whelmed computations become a heavy burden for user's terminal, which is especially serious for energy constrained devices. The outsourced decryption method [9] allows user to recover the message with ultra lightweight decryption[10], [11]. However, the cloud server might return wrong half-decrypted information as a result of malicious attacker system malfunction. Thus, it is an important issue to guarantee the correctness of outsourced decryption in publickey encryption with keyword search (PEKS) system [12].The authorized entities may illegally leak their secret key to a third party for profits [13]. 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 orthe 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 [14], [15]. Providing traceability [37] to a fine-grained search authorization system is critical and not considered in previous searchable encryption systems [7], [8], [12].

2. EXISTING SYSTEM

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 .

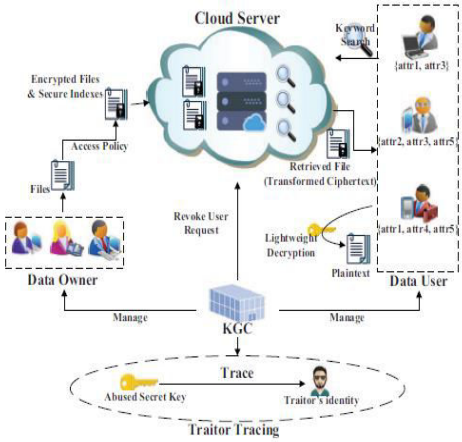
3. PROPOSED SYSTEM

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

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

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. 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.

4. ARCHITECTURE



5. IMPLEMENTATION

1.Key generation centre

KGC is responsible to generate the public parameter for the system and the public/secret key pairs for the users. Once the user's secret key is leaked for profits or other purposes, KGC runs trace algorithm to find the malicious user. After the traitor is traced, KGC sends user revocation request to cloud server to revoke the user's search privilege.

2. Cloud server

Cloud server has tremendous storage space and powerful computing capability, which provides on-demand service to the system. Cloud server is responsible to store the data owner's encrypted files and respond on data user's search query.

3.Data owner

Data owner utilizes the cloud storage service to store the files. Before the data outsourcing, the data owner extracts keyword set from the file and encrypts it into secure index. The document is also encrypted to ciphertext. During the encryption process, the access policy is specified and embedded into the ciphertext to realize finegrained access control.

4.Data user

Each data user has attribute set to describe his characteristics, such as professor, computer science college, dean, etc. The attribute set is embedded into user's secret key. Using the secret key, data user is able to search on the encrypted files stored in the cloud, i.e., chooses a keyword set that he wants to search. Then, the keyword is encrypted to a trapdoor using user's secret key. If the user's attribute set satisfies the access policy defined in the encrypted files, the cloud server responds on user's search query and finds the match files. Otherwise, the search query is rejected. After the match files are returned, the user runs decryption algorithm to recover the plaintext.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

6. ALGORITHM IMPLEMENTATION

Fully homomorphic encryption

A fully homomorphic encryption system enables computations to be performed on encrypted data without needing to first decrypt the data. Such cryptosystems have natural applications in secure, privacy-preserving computation as well as many other areas. Since Gentry's breakthrough work on fully homomorphic encryption (FHE) , there has been much excitement and attention devoted towards developing practical FHE systems. In this project, we provide an implementation of Brakerski's scale-invariant somewhat homomorphic encryption (SWHE) system [Bra12]. In addition, we examine several candidate applications of FHE and SWHE systems, such as performing statistical analysis on encrypted data or evaluating private database queries over an encrypted database.

7. 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 keywordsearch over encrypted cloud data"[C]//IEEE 30th InternationalConference on Distributed Computing Systems (ICDCS), IEEE,2010: 253-262

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

.[3] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server Public-Key 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 privacy-preserving outsourced calculation toolkit with multiple keys." IEEETransactions on Information Forensics and Security 11.11 (2016):2401-2414.

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

[6] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword RankSearch over Encrypted Data in Arbitrary Language". IEEE Transac-tions 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 YourRight: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud," IEEETransactions on Parallel and Distributed Systems, 2016, vol. 27, no.4, pp. 1187-1198.

[8] K. Liang, W. Susilo, "Searchable Attribute-Based Mechanism withEfficient Data Sharing for Secure Cloud Storage," IEEE Transactionson Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981-1992.

[9] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryp-tion 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 encryp-tion with verifiable outsourced decryption," IEEE Transactions onInformation Forensics and Security, 2013, vol. 8, no. 8, pp. 1343-1354.

[11] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-Based Encryptionwith Efficient Verifiable Outsourced Decryption," IEEE Transac-tions on Information Forensics and Security, 2015, vol. 10, no. 7,pp. 1384-1394.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Publickey encryption with keyword search," in: EUROCRYPT, 2004, pp.506-522

.[13] Z. Liu, Z. Cao, D.S. Wong, "White-box traceable ciphertext-policyattribute-based encryption supporting any monotone access struc-tures," IEEE Transactions on Information Forensics and Security,2013, vol. 8, no. 1, pp. 76-88.