Efficient Traceable Authorization Search System for Secure Cloud Storage

[1] C.SARMILA
M.Sc. (Computer Science)
Besant Theosophical College, Madanapalle.

[2]D.Venkata Siva Reddy
Head of the Deapartment
Besant Theosophical College, Madanapalle.

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

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 .

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 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.

IMPLEMENTATION

Module Description

1. Key generation centre
2. Cloud server
3. Data owner
4. Data user

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.

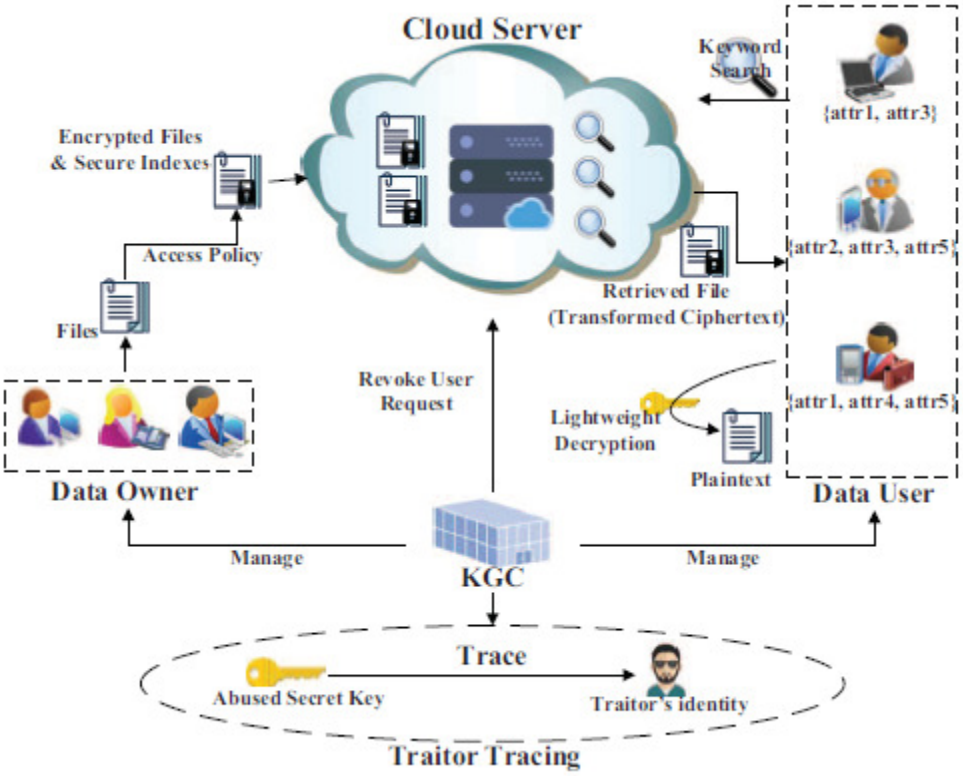
3.Data owner

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'ssecret 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.

ARCHITECTURE



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.

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] J. Crowcroft, "On the duality of resilience and privacy," in Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 471, no. 2175. The Royal Society, 2015, p. 20140862.

[2] A. Bessani, M. Correia, B. Quaresma, F. Andre, and P. Sousa, "Depsky: ´ dependable and secure storage in a cloud-of-clouds," ACM Transactions on Storage (TOS), vol. 9, no. 4, p. 12, 2013.

[3] H. Chen, Y. Hu, P. Lee, and Y. Tang, "Nccloud: A network-coding-based storage system in a cloud-of-clouds," 2013.

[4] T. G. Papaioannou, N. Bonvin, and K. Aberer, "Scalia: an adaptive scheme for efficient multi-cloud storage," in Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis. IEEE Computer Society Press, 2012, p. 20.

[5] Z. Wu, M. Butkiewicz, D. Perkins, E. Katz-Bassett, and H. V. Madhyastha, "Spanstore: Cost-effective geo-replicated storage spanning multiple cloud services," in Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles. ACM, 2013, pp. 292–308.

[6] G. Greenwald and E. MacAskill, "Nsa prism program taps in to user data of apple, google and others," The Guardian, vol. 7, no. 6, pp. 1–43, 2013.

[7] T. Suel and N. Memon, "Algorithms for delta compression and remote file synchronization," 2002.

[8] I. Drago, E. Bocchi, M. Mellia, H. Slatman, and A. Pras, "Benchmarking personal cloud storage," in Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013, pp. 205–212.

[9] I. Drago, M. Mellia, M. M Munafo, A. Sperotto, R. Sadre, and A. Pras, "Inside dropbox: understanding personal cloud storage services," in Proceedings of the 2012 ACM conference on Internet measurement conference. ACM, 2012, pp. 481–494.

[10] U. Manber et al., "Finding similar files in a large file system." in Usenix Winter, vol. 94, 1994, pp. 1–10.

[11] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud storage with minimal trust," ACM Transactions on Computer Systems (TOCS), vol. 29, no. 4, p. 12, 2011.

[12] A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, "Sporc: Group collaboration using untrusted cloud resources." in OSDI, vol. 10, 2010, pp. 337–350.

[13] F. Dabek, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Wide-area cooperative storage with cfs," in ACM SIGOPS Operating Systems Review, vol. 35, no. 5. ACM, 2001, pp. 202–215.

[14] L. P. Cox and B. D. Noble, "Samsara: Honor among thieves in peer-to-peer storage," ACM SIGOPS Operating Systems Review, vol. 37, no. 5, pp. 120–132, 2003. [15] H. Zhuang, R. Rahman, and K. Aberer, "Decentralizing the cloud: How can small data centers cooperate?" in Peer-to-Peer Computing (P2P), 14-th IEEE International Conference on. Ieee, 2014, pp. 1–10.

S