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 **e**scrow **f**ree **t**raceable **a**ttribute based **m**ultiple **k**eywords **s**ubset search system with **v**erifiable **o**utsourced **d**ecryption (EF-TAMKS-VOD).

CONTINUE

- 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.

EXISTING SYSTEM

- Wcloud computing becomes the most notable one, ITH the development of new computing paradigm, 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.

PROPOSED SYSTEM

- In this paper, we propose a novel primitive: **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-TAMKSVOD).
- **(1) Flexible Authorized Keyword Search**. 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.
- **(2) Flexible System Extension**. EF-TAMKS-VOD supports flexible system extension, which accommodates flexible number of attributes.

CONTINUE

- The attributes are not fixed in thesystem 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.
- ***(3) Efficient Verifiable Decryption***. EF-TAMKS-VOD 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.

HARDWARE REQUIREMENTS

- Processor - Pentium –III
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

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.

REFERENCE

[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.

CONTINUE

[4] X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. ”An efficient privacypreserving outsourced calculation toolkit with multiple keys.” 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.