International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

RETRIEVAL OF DATA USING SEARCHABLE SYMMETRIC ENCRYPTION

B. SINDHUJA, Dr.A.SENTHIL KUMAR, M. SURESH
Research Scholar's (M.Phil), Assistant Professor,
Department of Computer Science,
Tamil University,
Thanjavur.

ABSTRACT--*A reasoning storage area program, consisting of a collection of storage area web servers, provides long-term storage area services over the Internet. Storing information in a third person's reasoning program causes serious concern over information comfort. General security schemes protect information comfort, but also limit the functionality of the storage area program because a few functions are reinforced over secured information. Constructing a protected storage area program that facilitates multiple functions is challenging when the storage area program is allocated and has no central authority. It suggests a threshold proxies re-encryption plan and combines it with a decentralized erasure code such that a protected allocated storage area program is formulated. The allocated storage area program not only facilitates protected and robust information storage area and recovery, but also lets a customer forward his information in the storage area web servers to another customer without accessing the information back. The main technical contribution is that the proxies re-encryption plan facilitates development functions over secured information as well as sending functions over secured and secured information. For the first time, formulate the comfort issue from the aspect of likeness importance and plan robustness. It notices that server-side position based on order-preserving security (OPE) inevitably leaks information comfort. To eliminate the leak, it suggests a two-round retrievable security (TRSE) plan that facilitates top-k multi-keyword recovery. In TRSE, it utilizes a vector area design and homomorphism security. The vector area design helps to provide sufficient search accuracy, and the homomorphism security enables users to involve in the position while the majority of computing work is done on the server part by functions only on cipher text.*

Keywords - Cloud, data privacy, ranking, similarity relevance, homomorphism encryption, vector space model

1, INTRODUCTION

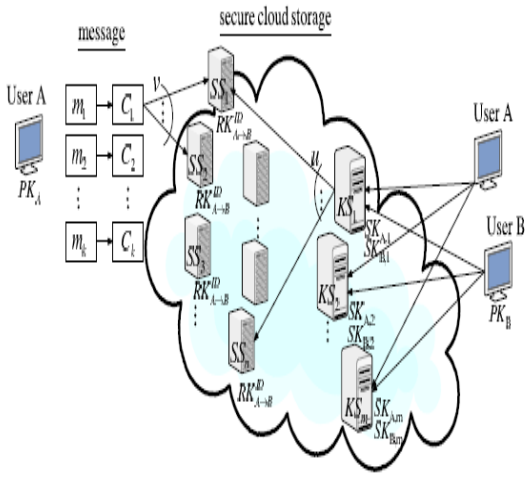
A series of retrievable symmetrical security techniques have been suggested to allow look for on cipher written text. Traditional SSE techniques allow users to safely recover the cipher written text, but these techniques assistance only Boolean keyword and key phrase look for, i.e., whether a keyword and key phrase prevails in a file or not, without considering the difference of importance with the queried keyword and key phrase of these data files in the result. To improve protection without compromising performance, techniques show that they assistance top-k single keyword and key phrase recovery under various circumstances. Writers of made efforts to fix the issue of top-k multi-keyword over secured reasoning information. These techniques, however, suffer from two problems - Boolean reflection and how to attack a balance between protection and performance. In the former, data files are rated only by the number of recovered keywords, which affects look for precision. In the latter, protection is unquestioningly affected to compromise for performance, which is particularly unwanted in security-oriented applications. Avoiding the reasoning from including in position and trusting all the perform to the customer is a natural way to avoid details leak. However, the limited computational power on the customer side and the great computational expense prevents details protection. The issue of secure multi-keyword top-k recovery over secured reasoning information thus is: how to make the reasoning do more perform during the process of recovery without details leak. Present the ideas of likeness importance and plan sturdiness to come up with the privacy issue in retrievable security techniques, and then fix the uncertainty issue by suggesting a two-round retrievable security (TRSE) plan. Novel technological innovation in the cryptography group and details recovery group are employed, including homomorphism security and vector space model. In the suggested plan, the majority of processing perform is done on the reasoning while the customer participates position, which assures top-k multi-keyword recovery over secured reasoning information with great protection and practical performance.

2, DATA RETRIVAL

There are two cases for the data recovery stage. The first situation is that a customer A retrieves his own concept. When customer A wants to restore the concept with the identifier ID, he shows all key web servers with the identification icon. A key server first retrieves unique code word signs from u arbitrarily chosen storage space web servers and then works limited decryption on every recovered unique code word symbol C0. The result of limited decryption is called a partly decrypted code word icon. The key server delivers the partly decrypted code word signs and the coefficients to customer A. After customer a gathers responses from at least t key web servers and at least k of them are initially from unique storage space web servers, he carries out on the t partly decrypted code word signs to restore the prevents. The second situation is that a customer

B retrieves a concept sent to him. User B shows all key web servers directly. The collection and mixing parts are the same as the first situation except that key web servers restore re-encrypted code word signs and perform limited decryption Share- on re-encrypted code word signs.

3, ARCHITECTURE



4, INTEGRITY CHECKING FUNCTIONALITY

Another important functionality about cloud storage space is the function of integrity checking. After user stores information into the storage space system, he no longer possesses the information at hand. The user may want to check whether the information are properly saved kept in storage space servers. The concept of provable information possession and the notion of proof of storage space are proposed. Later, public audit ability of saved information is addressed in. Nevertheless all of them consider the messages in the clear text form.

In the **data sending phase**, customer A delivers his secured concept with an identifier ID stored kept in storage space web servers to customer B such that B can decrypt the submitted concept by his key key. To do so, A uses his key SKA and B's community key PKB to estimate a re-encryption key and then delivers to all storage space web servers. Each storage space server uses the security key to re-encrypt its code word icon for later recovery requests by B. The re-encrypted code word icon is the combination of cipher text messages under B's community key.

In order to distinguish re-encrypted code word signs from unchanged ones, we call them original code word signs and secured code word signs, respectively.

In the **data recovery phase**, customer A requests to retrieve a message from storage space web servers. The message is either stored by him or forwarded to him. User A sends a recovery request to key web servers. Upon receiving the recovery request and executing a proper authentication process with customer A, each key server requests u randomly chosen storage space web servers to get code word signs and does partial decryption on the received code word signs by using the key share. Finally, customer a combines the partially decrypted code word signs to obtain the original message M. System recovering. When a storage space server fails, a new one is added. The new storage space server queries k available storage space web servers linearly combines the received code word signs as a new one and stores it. The system is then recovered.

CONCLUSION

The threshold proxy's security pl an supports development, sending, and limited decryption operations in a distributed way. To decrypt a message of k blocks that are secured and encoded to n code word symbols, each key server only has to partially decrypt two code word symbols in our system. By using the threshold proxies re-encryption plan, present a protected reasoning storage space system that provides protected information storage space and protected information sending functionality in decentralized structure. Moreover, each storage space server individually performs development and re-encryption and each key server individually perform limited decryption. solve the problem of protected multi-keyword top-k recovery over secured reasoning information. We define similarity relevance and plan robustness. Based on order preserving security invisibly leak sensitive information; we devise a server-side ranking SSE plan. We then propose a two-round searchable security (TRSE) plan employing the fully homomorphism security, which fulfills the security requirements of multi-keyword top k recovery over the secured reasoning information.

[6] REFERENCES

[1] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R.Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, "Oceanstore: An Architecture for Global-Scale Persistent Storage," Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190- 201, 2000.
[2] P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent

Peer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.

[3] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer,

"Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proc. Fifth Symp. Operating System Design and Implementation (OSDI), pp. 1-14, 2002.

[4] A. Haeberlen, A. Mislove, and P. Druschel, "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Failures," Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143-158, 2005.

[5] Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The Least-Authority Filesystem," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008.

[6] H.-Y. Lin and W.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

[7] D.R. Brownbridge, L.F. Marshall, and B. Randell, "The Newcastle Connection or Unixes of the World Unite!," Software Practice and Experience, vol. 12, no. 12, pp. 1147-1162, 1982.

[8] R. Sandberg, D. Goldberg, S. Kleiman, D. Walsh, and B. Lyon, "Design and Implementation of the Sun Network Filesystem," Proc. USENIX Assoc. Conf., 1985.

[9] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29- 42, 2003.

[10] S.C. Rhea, P.R. Eaton, D. Geels, H. Weatherspoon, B.Y. Zhao, and J. Kubiatowicz, "Pond: The Oceanstore Prototype," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 1-14, 2003.