Research Paper
Impact Factor: 6.304
Peer Reviewed & Indexed Journal
www.ijbarr.com

IJBARR
E- ISSN -2347-856X
ISSN -2348-0653

EFFICIENT DEDUPLICATION USING DYNAMIC ENCRYPTED DATA IN CLOUD STORAGE

S.Vinoth
Gnanamani College of Technology,Namakkal , Tamilnadu .

Abstract
In cloud storage services, deduplication technology is commonly used to reduce the space and bandwidth requirements of services by eliminating redundant data and storing only a single copy of them. Deduplication is most effective when multiple users outsource the same data to the cloud storage, but it raises issues relating to security and ownership.Traditional deduplication schemes cannot work on encrypted data. The static deduplication decision tree is constructed based on the random elements from the client, which does not allow the tree to update. The R-MLE2 scheme is not efficient in the deduplication process because of the comparison of the randomized tag. Propose a novel server-side deduplicat on scheme for encrypted data. It allows the data server to control access to outsourced data even when the ownership changes dynamically by exploiting randomized convergent encryption and secure ownership group key distribution. Thus, security is enhanced in the proposed scheme. The efficiency analysis results demonstrate that the proposed scheme is almost as efficient as the previous schemes, while the additional computational overhead is negligible. The deduplication schema based on data ownership challenge and proxy re-encryption (PRE) to manage the encrypted data backup with deduplication.

Keywords: Traditional deduplication, R-MLE2 scheme, Reduce memory , novel server-side deduplication .

Introduction

Deduplication has received much attention from both academic and industry because it can more improves storage utilization and save storage space, especially for the applications with high deduplication ratio such as accession storage systems. For eliminating duplicate copies of data use data deduplication technique. To reduce storage space and for uploading bandwidth mostly it has been used, in cloud storage. A various deduplication systems has been proposed based on number of policies such as client-side or server-side deduplications, file-level or block-level deduplications. The first attempt to describe the notion of distributed safe deduplication system. The main Aim of our proposed system is to describe the notion of distributed reliable deduplication system with more security. implement new distributed deduplication system, which has more reliability. In that data chunks are distributed across multiple cloud servers. Deduplication technique can save the memory space for the cloud storage service providers; it reduces the reliability of the system. Security analysis indicates that our deduplication systems are secure in terms of the definitions specified in this security model. As a proof of concept, implement the proposed systems that indicate the acquired aerial is very limited in actual environments.De-duplication scheme takes benefit of data similarity to find the same data and scale down the storage space. In contrast, encryption algorithms randomized the encrypted files to make cipher-text same from theoretically random data. Encryption of the same data by dissimilar users with different encryption keys results in different cipher texts, which makes it hard for the cloud server to decide whether the plain data are the same and de-duplicate them. Hence, traditional encryption makes de-duplication impossible for above reasons.

A convergent encryption algorithm works as follows: Firstly, it takes an input file and encrypts them with its hash value as an encryption key. Then, the cipher text is given to the cloud server and user keeps the encryption key. As convergent encryption is deterministic, every time similar files encrypted into similar cipher-text irrespective of who encrypts them. Hence, the cloud server can do de-duplication over the generated cipher text. Then all data owners can download the cipher text and decrypt it later as they have the same encryption key for the file. But convergent encryption has security weakness concern with tag consistency and ownership revocation.

SEARCHABLE SYMMETRIC ENCRYPTION: IMPROVED DEFINITIONS AND EFFICIENT CONSTRUCTIONS

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper, review of existing security definitions, pointing out their shortcomings, and propose two new stronger definitions which we prove equivalent. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees and these are more efficient than all previous constructions.

The client indexes and encrypts its document collection and sends the secure index together with the encrypted data to the server. To search for a keyword w, the client generates and sends a trapdoor for w which the server uses to run the search operation and recover pointers to the appropriate (encrypted) documents. Symmetric searchable encryption can be achieved in its full generality and with optimal security using the work of Ostrovsky and Goldreich on oblivious RAMs.

Using these techniques any type of search query can be achieved e.g., conjunctions or disjunctions of keywords, without leaking any information to the server not even the "access pattern". (i.e., which documents contain the keyword). This strong privacy guarantee however, comes at the cost of a logarithmic (in the number of documents) number of rounds of interaction for each read and write. In the same paper, the authors show a 2-round solution, but with considerably larger square-root overhead.

Conclusion

The secret sharing technique to protect private information. Only the data user who uploads the data first is needed to compute and distribute such secret shares, and subsequent users who have the same copy of data do not have to compute and store those shares. To retrieve copies of data copies, we must access a minimum number of storage servers and retrieve the secret shares to change the data. In different ways, the authorized applications access the copy of the secret release data. Another distinguishing feature of our proposal is that data completeness can be derived in the consistency of the final tags. To further explain if the same value is stored in different cloud stores, deduplication is checked by methods. Our proposed structure supports both traditional deduplication methods. Privacy, credibility and integrity can be achieved in our proposed system. In solution to a type of secret agreement, attacks are considered.

References

1. 1. Batten.C, K. Barr, A. Saraf, and S. Trepetin, "pstore: A secure peer-to- peer backup system," MIT Laboratory for Computer Science, progress report, 2014.
2. Cash.D, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in CRYPTO 2013, ser. Computer Science, R. Canetti and J. A. Garay, Eds. Springer, 2019, vol. 8042 of LNCS, pp. 353–373.
3. Curtmola.R, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of the ACM Conference on Computer and Communications Security, VA, USA, Oct. 2020, pp. 79–88.
4. Dropbox, "Dropbox," https://www.dropbox.com/, your stuff, anywhere.
5. Google, "Google drive," http://drive.google.com, all your files, ready where you are.
6. Jiang.T, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, "Towards efficient fully randomized message-locked encryption," in Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2019, Proceedings, Part I, 2015

Poornima MC (2013) Entrepreneurship development & small Business enterprise (2ndedn), Pearson Education, India.