ISSN 2395-1621

Attribute-Based Storage Supporting Secure Deduplication Of Encrypted Data in Cloud

[#1]Suraj Lodhi, [#2]Tushar Konde, [#3]Akanksha Arya

[1]surajj.wnp@gmail.com
[2]kondetushar9@gmail.com
[3]akanlshaarya247@gmail.com

[#123]Department of Computer Engineering,

Flora Institute of Technology.

ABSTRACT

DE duplication is most important issue for any organisation, so we analysis this issue an avoid the reparative files on cloud storage. Avoidance of the file is advantages the cloud size issue. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing. To better protect data security, on cloud storage. In this system we check the duplicate file on cloud storage also security apply using encryption. We use the encryption algorithm for encrypt the file simultaneously we check the duplicate file using the hashing algorithm. Also enhanced this system using recover option, cloud provide the deleted file backup on requesting. This paper makes the first attempt to formally address the problem of authorized data deduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. We also present several new deduplication constructions supporting authorized duplicate check in local cloud architecture.

Keywords:- Deduplication, Authorized Duplicate Check, Confidentiality, Cloud computing.

ARTICLE INFO

Article History

Received: 28th May 2018

Received in revised form :

28th May 2018

Accepted: 31st May 2018

Published online :

3rd June 2018

I. INTRODUCTION

Cloud computing is a model for delivering information technology services in which resources are retrieved from the internet through web-based interface and application, instead of direct connection to a server. Cloud storage provides a service for the evergreen management of vast amount of data in order to reduce the space and bandwidth. To make reliable and scalable management of data in the cloud computing, deduplication plays a vital role as a conventional technique. Deduplication is a data compression technique which is most commonly used for eliminating repeated copies of data/files in cloud storage to reduce space and bandwidth. This technique is used for reliable storage utilization and to provide scalable network data transfers to reduce number of bytes that must be sent. Data deduplication may occur as file level as well as block level data deduplication. Keeping multiple duplicate copies of file/data with similar content deduplication detects and eliminates the redundant data by keeping original physical copy.

Differential Authorization:
To perform duplicate check based on privilege of user is able to get his/her individual token. Without aid from the private cloud server and for the duplicate check outs token cannot generate by the user.

Authorized duplicate check:
Authorized user is able to use his/her individual private keys to generate query for certain file and the privileges he/she owned with the help of private cloud, while the public cloud performs duplicate check directly and tells the user if there is any duplicate. The security requirements considered in this paper lie in two folds, including the security of file token and security of data files. For the security of file token, two aspects are

defined as un-forge ability and in-distinguish ability of file token. The details are given below.

Data Confidentiality:

Unauthorized users without appropriate privileges or files, including the cloud server, should be prevented from access to the underlying plaintext store. In another word, the goal of the adversary is to retrieve and recover the files that do not belong to them. In our system, compared to the previous definition of data confidentiality based on convergent encryption, a higher level confidentiality is defined and achieved.

The remainder of this work is organized as follows. First section II describes the security analysis and related work in secure deduplication concepts. Then, section III introduces the proposed system finally, concluding in section IV.

II. LITERATURE SURVEY

J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. "Reclaiming space from duplicate files in a serverless distributed file System".in this paper studied the problem of deduplication in multi-tenant environment. The authors proposed the use of the convergent encryption, i.e., deriving keys from the hash of plaintext. [1]

M. W. Storer, K. Greenan, D. D. Long and E. L. Miller. "Secure data deduplication" in this paper author explain Pointed out some security problems, and presented a security model for secure data deduplication. However, these two protocols focus on server-side deduplication and do not consider data leakage settings, against malicious users.[2]

M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature scheme". in this paper Provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. [3]

J. Xu, E.-C.Chang, and J. Zhou, "Weak leakage-resilient client side deduplication of encrypted data in cloud storage", in this solution is based on a cryptographic usage of symmetric encryption used for enciphering the data file and asymmetric encryption for Meta data files, due to the highest sensibility of this information towards several intrusions. [4]

M. Bellare, S. Keelveedhi, and T. Ristenpart. "Dupless: Server aided encryption for deduplicated storage, proposed a solution here the data which is common between users to increase the speed of backup and reduce the storage requirement namely backup algorithm. Supports client-end per user encryption is necessary for confidential personal data. [5]

III. PROPOSED SYSTEM

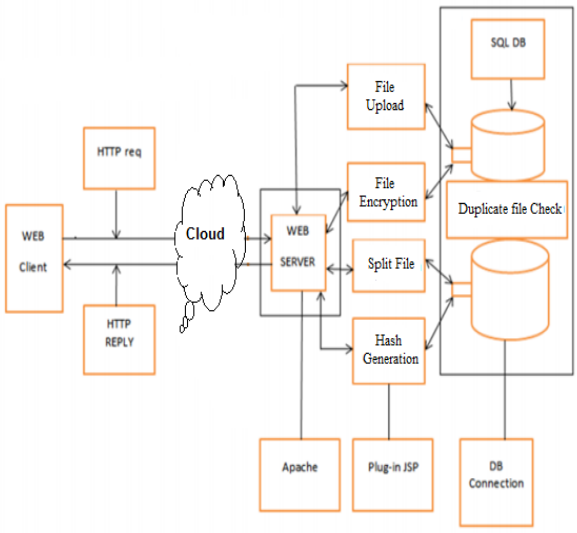

Fig 1. System Architecture

Data DE duplication by providing the proof of data by the data owner. This proof is used at the time of uploading of the file. users is allowed to perform the duplicate check and access the files. Before submitting his duplicate check request for some file, the user needs to take this file and own privileges as inputs. The user is able to find a duplicate for this file if and only if there is a copy of this file and a matched privilege stored in cloud.

Module:

1) File Uploading Protocol: This protocol aims at allowing clients to upload files via the auditor. Specifically, the file uploading protocol includes three phases:

I) Phase 1 (cloud client → cloud server): Client takes the duplicate check with the cloud server to confirm if such a file is stored in cloud storage or not before uploading a file. If there is a duplicate, another protocol called Proof of Ownership will be run between the client and the cloud storage server. Otherwise, the following protocols (including phase 2 and phase 3) are run between these two entities.

II) Phase 2 (cloud client → authority): Client uploads files to the auditor, and receives a receipt from authority.

III) Phase 3 (authority → cloud server): Authority helps generate a set of tags for the uploading file, and send them along with this file to cloud server.

V. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

IV. CONCLUSION

In this paper we implement the DE duplication techniques for better confidentiality and security in cloud computing. The detection of redundant data and removal of this redundant data is an important task for keeping the cloud storage clean and scalable. This duplicate data elimination has a great advantage for cloud storage. We have surveyed various techniques for DE duplication.

REFERENCES

[1] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. "Reclaiming space from duplicate files in a serverless distributed file System". In Proceedings of 22nd International Conference on Distributed Computing Systems (ICDCS, 2002).

[2] M. W. Storer, K. Greenan, D. D. Long and E. L. Miller. "Secure data deduplication". In Proceedings of the 4th ACM International Workshop on Storage Security and Survivability, StorageSS 08, pages 1–10, 2008.

[3] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature scheme". 2009

[4] J. Xu, E.-C.Chang, and J. Zhou, "Weak leakage-resilient client side deduplication of encrypted data in cloud storage", 2013

[5] M. Bellare, S. Keelveedhi, and T. Ristenpart. "Dupless: Server aided encryption for deduplicated storage". In USENIX Security Symposium, 2013.

[6] Z. Li, X. Zhang, and Q. He, Analysis of the key technology on cloud storage, in International Conference on Future Information Technology and Management Engineering, 2010, pp. 427428.

[7] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491500. ACM, 2011.

[8] D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security & Privacy, 8(6), 2010.

[9] Q. He, Z. Li, and X. Zhang, Data deduplication techniques, in International Conference on Future Information Technology and Management Engineering,pp.431-432,2010.

[10] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless:Server aided encryption for deduplicated storage. In USENIX Security Symposium, 2013.

[10] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

[11]S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011),2011.

[12]W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S Ossowski and P. 2012.

