International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

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

R. Manimekalai[1], M. Chandra Kumar Peter[2]
[1]Final Year-M.Sc, [2]M.Sc, M.Phil, M.Tech, Assistant Professor
Periyar Maniammai Institute of Science & Technology,
Thanjavur, Tamil Nadu, India

ABSTRACT

Cloud computing offers a new way of service provision by re-arranging various resources over the Internet. The most important and popular cloud service is data storage. In order to preserve the privacy of data holders, data are often stored in cloud in an encrypted form. However, encrypted data introduce new challenges for cloud data deduplication, which becomes crucial for big data storage and processing in cloud. Traditional deduplication schemes cannot work on encrypted data. Existing solutions of encrypted data deduplication suffer from security weakness. They cannot flexibly support data access control and revocation. Therefore, few of them can be readily deployed in practice. In this paper, we propose a scheme to deduplicate encrypted data stored in cloud based on ownership challenge and proxy re-encryption. It integrates cloud data deduplication with access control. We evaluate its performance based on extensive analysis and computer simulations. The results show the superior efficiency and effectiveness of the scheme for potential practical deployment, especially for big data deduplication in cloud storage.

Keywords: *deduplication, re-encryption, potential practical deployment*

INTRODUCTION

The most important and popular cloud service is data storage service. Cloud users upload personal or confidential data to the data center of a Cloud Service Provider (CSP) and allow it to maintain these data. Cloud computing schemes presented focus on warehoused data, where the outsourced data is kept unchanged over remote servers In cloud data storage system, users store their data in the cloud and No longer possess the data locally. Thus, the correctness and availability of the multiple data files being stored on the distributed cloud servers must be guaranteed. In existing system, brute-force attack used to avoid multiple copies of dynamic data stored in cloud. When verifying multiple data copies, the overall system integrity check fails if there are one or more corrupted copies. This project propose History Aware Rewriting (HAR) algorithm to avoid de-duplicate encrypted data stored in cloud based on ownership challenge and proxy re-encryption. It integrates cloud data deduplication with access control. Propose a scheme based on data owner-ship challenge and Proxy Re-Encryption (PRE) to manage encrypted data storage with deduplication.aim to solve the issue of deduplication in the situation where the data holder is not available or difficult to get involved. In this method using double encryption key for encrypted data stored in cloud. First the data owner provide the secret key to data user then authorized party (AP) send the secret key to data owner. Both AP key and private key generate the encrypted key that key using for encryption. AES algorithm using the encrypt content stored in cloud.

DESIGN

User Registration and Cloud access

Access users only to have authentication process before registration, Authentication process is always occurred prior to mobility management process included location registrations and service delivery, and it also ensures network resources are accessed by authorized clients and prevents resources from any illegal client or damage. Before the registration of cloud services to ensure whether the client is an authenticated or not to access cloud server. Can ensure the information stored in the cloud is used judiciously by the responsible stakeholders as per the service level agreements.

UPLOAD THE FILE

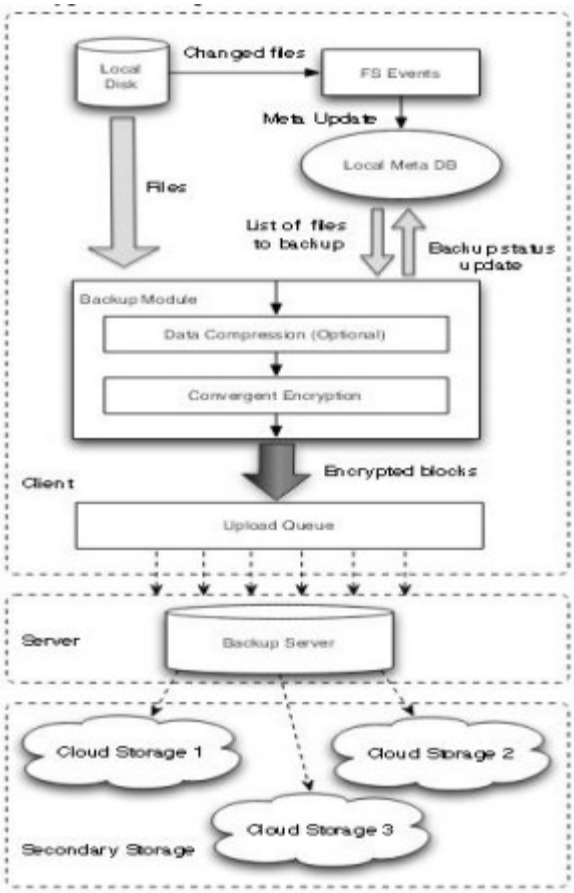
The user needs to upload the file into cloud. An authorized user login for the cloud with decryption key and upload the file into the cloud.

ATTRIBUTE BASED STORAGE SYSTEM

An attribute-based storage system supporting secure deduplication. Our storage system is built under a hybrid cloud architecture, where a private cloud manipulates the computation and a public cloud manages the storage. Attribute based storage system supporting secure deduplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under different access policies.

ATTRIBUTE AUTHORITY CHANGES THE OWNERSHIP PERMISSION

The Attribute Authority issues every user a decryption key associated with the set of attributes. The attribute based storage system check the duplication of the file. The duplication is not occur, the file is stored. If the duplication is occurring, the attribute authority changes the ownership permission.



We are utilizing client accreditations to check the confirmation of the client. In that cases cloud is available two sort of cloud such private cloud and open cloud. In private cloud store the client accreditation and in the open cloud client information present out. In the figure 2. cloud take focal points of both open cloud and private cloud. Open cloud and private cloud are available in the half and half cloud structural engineering. When any client forward solicitation to people in general cloud to get to the data he have to present his data to the private cloud then private cloud will give a record token and client can get the notifications to the document lives on the general population cloud. We have utilized a half and half cloud construction modeling as a part of proposed. We have to need to mind the file name in record information duplication and information DE duplication is checked at the square level. On the other hand, client needs to recover his information or download the information record he have to download both of the document from the cloud server this will prompts perform the operation on the same record this abuses the security of the distributed storage.

RELATED WORK

DupLESS: Server-Aided Encryption for Deduplicated Storage. By looking the example Dropbox, Mozy, and others perform deduplication to spare space by just

putting away one duplicate of every document or file transferred. Should customers routinely scramble their documents, be that as it may, funds are lost. Messagebolted encryption (the most unmistakable appearance of which is concurrent encryption) certify this strain. In any case it is intrinsically subject to savage power assaults that can recoup records falling into a known set. We propose a building design that accedes secure deduplicated stockpiling opposing savage power assaults, and acknowledge it in a framework called DupLESS. In DupLESS, customers encode under message-based keys acquired from a key-server by means of an absent PRF convention. It secures customers to store scrambled information with a current administration, have the administration perform deduplication for their advantage, but then accomplishes solid privacy ensures. We demonstrate that encryption for deduplicated stockpiling can accomplish execution and space reserve funds near that of consuming the stockpiling administration with plaintext information

Secure Deduplication with Efficient and Reliable Convergent Key Management. Deduplication is a system for taking out copy duplicates of information, and has been broadly utilized as a part of distributed storage to decrease storage space and transfer data transfer capacity. Promising as it perhaps, an emerging test is to perform secure deduplication in distributed storage. Albeit joined encryption has been widely received for secure deduplication, a basic problem of making focalized encryption down to earth is to productively and dependably deal with an immense number of united keys. This system makes the first endeavor to formally notify the issue of accomplishing effective and dependable key administration in secure deduplication. Firstly we introduce a pattern approach in which every client holds an autonomous expert key for scrambling the aim keys and outsourcing them to the cloud. On the second way, such a standard key administration plan produces a tremendous number of keys with the expanding number of obliges clients and clients to dedicatedly secure the expert keys. To this end, we propose Dekey , another development in which clients don't have to deal with any keys all alone however rather safely circulate or transfer the united key shares over different servers. Security examination exhibits that Dekey is secure as far as the definitions determined in proposed security model. As a proof of idea, we actualize Dekey utilizing the Ramp mystery sharing plan and show that Dekey brings about restricted overhead in reasonable situations

CONCLUSION

Here we provided reason that our proposed framework information DE duplication of record is done approves way and safely. In this we have additionally proposed new duplication check system which produce the token for the private document. The information client needs to present the benefit alongside the united key as a proof of possession. We have settled more basic piece of the cloud information stockpiling which is just endured by diverse systems. A proposed routine guarantees the information duplication safely.

FUTURE ENHANCEMENT

Future work includes efficient data ownership verification, scheme optimization with hardware acceleration at IoT devices for practical deployment, and development of a flexible solution to support deduplication and data access controlled by either the data owner or its representative agent.

REFERENCES

1) M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Server aided encryption for deduplicated storage. In USENIX Security Symposium, 2013.
2) P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted deduplication. In Proc. of USENIX LISA, 2010.
3) 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.
4) 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 491–500. ACM, 2011.
5) C. Ng and P. Lee. Revdedup: A reverse deduplication storage system optimized for reads to latest backups. In Proc. of APSYS, Apr 2013.
6) W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing, pages 441–446. ACM, 2012.