International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 05
April 2017

A Survey On data using convergent encryption for cloud data storage

RAASHID SHAHAB [1], SYED SAMEER [2], MIRZA SHOEB [3], SHAIK MAHEBOOB [4]
[1]B-Tech, Lords Institute Of Engineering And Technology, Mail Id: ridzshah.339@gmail.com
[2]B-Tech, Lords Institute Of Engineering And Technology, Mail Id: syedsameer1410@gmail.com
[3]B-Tech, Lords Institute Of Engineering And Technology, Mail Id: mirzashoeb518@gmail.com
[4]Assistant Professor, Lords Institute of Engineering and Technology,
Mail Id: skmb7086@gmail.com

Abstract: - In cloud storage accommodations, Deduplication technology is commonly used to reduce the space and bandwidth requisites of accommodations by eliminating redundant data and storing only a single replica of them. Deduplication is most efficacious when multiple users outsource the same data to the cloud storage, but it raises issues relating to security and ownership. Proof of- ownership schemes sanction any owner of the same data to prove to the cloud storage server that he owns the data in a robust way. However, many users are liable to encrypt their data afore outsourcing them to the cloud storage to preserve privacy, but this hampers Deduplication because of the randomization property of encryption. Recently, several Deduplication schemes have been proposed to solve this quandary by sanctioning each owner to apportion the same encryption key for the same data. However, most of the schemes suffer from security imperfections, since they do not consider the dynamic vicissitudes in the ownership of outsourced data that occur frequently in a practical cloud storage accommodation. In this paper, we propose a novel server-side Deduplication scheme for encrypted data. It sanctions the cloud server to control access to outsourced data even when the ownership changes dynamically by exploiting randomized convergent encryption and secure ownership group key distribution. This averts data leakage not only to revoked users albeit they aforetime owned that data, but withal to a veracious-but-curious cloud storage server. In advisement, the proposed

scheme guarantees data integrity against any tag erraticism attack. Thus, security is enhanced in the proposed scheme. The efficiency analysis results demonstrate that the proposed scheme is virtually as efficient as the antecedent schemes, while the supplemental computational overhead is negligible.

Key words: - De-duplication, convergent encryption, cloud storage, cryptographic, Access control, cloud computing, proxy re-encryption.

1. INTRODUCTION

CLOUD computing provides scalable, low-cost, and location-independent online services ranging from simple backup services to cloud storage infrastructures. The fast growth of data volumes stored in the cloud storage has led to an increased demand for techniques for saving disk space and network bandwidth. To reduce resource consumption, many cloud storage services, such as Dropbox Wuala , Mozy and Google Drive employ a Deduplication technique, where the cloud server stores only a single copy of redundant data and provides links to the copy instead of storing other actual copies of that data, regardless of how many clients ask to store the data. The savings are significant and reportedly, business applications can achieve disk and As customers are concerned about their private data, they may encrypt their data before outsourcing in order to protect data privacy from unauthorized outside adversaries, as well as from the cloud service provider .This is justified by current security trends and numerous industry regulations such as PCI DSS . However, conventional encryption makes Deduplication impossible for the following reason. Deduplication techniques take advantage of data similarity to identify the same data and reduce the storage space. In contrast, encryption algorithms randomize the encrypted files in order to make ciphertext indistinguishable from theoretically random data.

2. RELEGATED WORK

Existing System

When a user uploads data that already exist in the cloud storage, the user should be deterred from accessing the data that were stored before he obtained the ownership by uploading it (backward secrecy) 2. These dynamic ownership changes may occur very

frequently in a practical cloud system, and thus, it should be properly managed in order to avoid the security degradation of the cloud service. In the former approach, most of the existing schemes have been proposed in order to perform a PoW process in an efficient and robust manner, since the hash of the file, which is treated as a "proof" for the entire file, is vulnerable to being leaked to outside adversaries because of its relatively small size. a data owner uploads data that do not already exist in the cloud storage, he is called an initial uploader; if the data already exist, called a subsequent uploader since this implies that other owners may have uploaded the same data previously, he is called a subsequent uploader.

Proposed System

Several Deduplication schemes have been proposed to solve this problem by allowing each owner to share the same encryption key for the same data. However, most of the schemes suffer from security flaws, since they do not consider the dynamic changes in the ownership of outsourced data that occur frequently in a practical cloud storage service. In this paper, we propose a novel server-side Deduplication scheme for encrypted data. It allows the cloud server to control access to outsourced data even when the ownership changes dynamically by exploiting randomized convergent encryption and secure ownership group key distribution. a Deduplication scheme over encrypted data. The proposed scheme ensures that only authorized access to the shared data is possible, which is considered to be the most important challenge for efficient and secure cloud storage services in the environment where ownership changes dynamically. It is achieved by exploiting a group key management mechanism in each ownership group. The proposed scheme ensures security in the setting of PoW by introducing a re-encryption mechanism that uses an additional group key for dynamic ownership group. Most of the schemes have been proposed to provide data encryption, while still benefiting from a Deduplication technique, by enabling data owners to share the encryption keys in the presence of the inside and outside adversaries. Since encrypted data are given to a user.

3. IMPLEMENTATION

Dynamic Ownership

DE duplication is most efficacious when multiple users outsource the same data to the cloud storage, but it raises issues relating to security and ownership. Proof of- ownership schemes sanction any owner of the same data to prove to the cloud storage server that he owns the data in a robust way. However, many users are liable to encrypt their data afore outsourcing them to the cloud storage to preserve privacy, but this hampers Deduplication because of the randomization property of encryption. the ownership changes dynamically by exploiting randomised convergent encryption and secure ownership group key distribution. This averts data leakage not only to revoked users albeit they aforetime owned that data but additionally to a veracious-but-curious cloud storage server. In additament, the proposed scheme guarantees data integrity against any tag erraticism attack.

Group Key

Server-side DE duplication scheme for encrypted data. It sanctions the cloud server to control access to outsourced data even when the ownership changes dynamically by exploiting randomised convergent encryption and secure ownership group key distribution, It is achieved by exploiting a group key management mechanism in each ownership group. As compared to the antecedent Deduplication schemes over encrypted data, the proposed scheme has the following advantages in terms of security and efficiency.

Cloud Storage

This obviates data leakage not only to revoked users albeit they antecedently owned that data but withal to a veracious-but-curious cloud storage server. In integration, the proposed scheme guarantees data integrity against any tag erraticism attack. Thus, security is enhanced in the proposed scheme. The efficiency analysis results demonstrate that the proposed scheme is virtually as efficient as the antecedent schemes, while the adscititious computational overhead is negligible. Then, the server is able to deduplicate the identified data by decrypting it with its private key pair. However, this solution sanctions the cloud storage server to obtain the outsourced plain data, which may infringe the privacy of the data if the cloud server cannot be plenarily trusted. This is a client who owns data and wishes to upload it

into the cloud storage to preserve costs. A data owner encrypts the data and outsources it to the cloud storage with its index information, that is, a tag.

Deduplication

Data Deduplication is a specialised data compression technique for eliminating duplicate facsimiles of reiterating data. Cognate and scarcely synonymous terms are perspicacious (data) compression and single-instance (data) storage. This technique is utilised to ameliorate storage utilisation and can additionally be applied to network data transfers to reduce the number of bytes that must be sent. In the Deduplication process, unique chunks of data, or byte patterns, are identified and stored during a process of analysis. Deduplication techniques capitalise on data homogeneous attribute to identify the same data and reduce the storage space. In contrast, encryption algorithms randomise the encrypted files in order to make ciphertext indistinguishable from theoretically desultory data.

4. EXPERIMENTAL RESULTS

Fig:-1 Showing User Registration Page

Fig: 2 Showing Owner Ship Login Page

Fig:-3 Download files from Cloud

Fig:-5 Showing File Encryption

Fig:-6 Showing File Upload Page

Fig:-7 Showing Graph Page

5. CONCLUSION

Dynamic ownership management is a paramount and challenging issue insecure Deduplication over encrypted data in cloud

storage. In this study, we proposed a novel secure data Deduplication scheme to enhance a fine-grained ownership management by exploiting the characteristic of the cloud data management system. The proposed scheme features an encryption technique that enables dynamic updates upon any ownership vicissitudes in the cloud storage. Whenever an ownership change occurs in the ownership group of outsourced data, the data are encrypted with an immediately updated ownership group key, which is securely distributed only to the valid owners. Thus, the proposed scheme enhances data privacy and confidentiality in cloud storage against any users who do not have valid ownership of the data, as well as against a veracious-but-curious cloud server. Tag consistency is withal ensured, while the scheme sanctions full advantage to be taken of efficient data Deduplication over encrypted data. In terms of the communication cost, the proposed scheme is more efficient than the anterior schemes, while in terms of the computation cost, taking adscititious 0:1 □ 0:2 ms compared to the RCE scheme, which is negligible in practice.

6. REFERENCE

[1] Hur, Junbeom, et al. Secure data deduplication with dynamic ownership management in cloud storage. IEEE Transactions on Knowledge and Data Engineering 28.11 (2016): 3113-3125.

[2] Harnik, Danny, Benny Pinkas, and Alexandra Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security & Privacy 8.6 (2010): 40-47.

[3] Halevi, Shai, et al. Proofs of ownership in remote storage systems. Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011.

[4] Juels, Ari, and Burton S. Kaliski Jr. PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.

[5] Ateniese, Giuseppe, et al. Provable data possession at untrusted stores. Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.

[6] Douceur, John R., et al. Reclaiming space from duplicate files in a serverless distributed file system. Distributed Computing Systems, 2002. Proceedings.

22nd International Conference on. IEEE, 2002.

[7] Xu, Jia, Ee-Chien Chang, and Jianying Zhou. Leakage-resilient client-side deduplication of encrypted data in cloud storage. IACR ePrint Archive, 15pages (2011).

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart. Message-locked encryption and secure deduplication. In EUROCRYPT, pages 296– 312, 2013.

[9] 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.

Web Sites Referred:

www.cloudxl.com

www.cloud-computing.com

www.talkincloud.com

www.cloudcomputing.sys-con.com

www.virtualizationreview.com/Home.aspx

www.thecloudtutorial.coms