IJRRECS/November 2015/Volume-3/Issue-11/4834-4839 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFICIENT DATA COMPRESSION SCHEME FOR REDUCTION OF CLOUD STORAGE SPACE

Draksharapu Prameela[1], N.Brahma Naidu[2]

[1]PG Scholar , Dept of CSE , Krishnaveni Engineering College for Women, Narasaraopet, AP, India

Email:prameela.draksharapu@gmail.com

[2]Assistant Professor , Dept of CSE , Krishnaveni Engineering College for Women, Narasaraopet, AP, India

Email: nbnaidu1208@gmail.com

ABSTRACT:

Important challenge concerning cloud storage services is data management of rising volume. Convergent encryption will makes sure of secured data in the process of deduplication. Process of convergent encryption was proposed to put into effect data privacy while making of deduplication practicable. For protecting of security in an effective means our work will make an initial attempt to deal with difficulty of authorized data deduplication. Although data deduplication will bring several issues of benefits, security as well as privacy takes place as user sensitive data is vulnerable to attacks. Differential privileges of users are measured in duplicate check in addition to data itself and this is different from the de-duplication methods of earlier ones. In our work we sort out authorization difficulty of deduplication above data within public cloud and also deal with the privacy preserving problem of deduplication within cloud computing. We put forward a novel de-duplication system supporting for Differential Authorization and Authorized Duplicate Check.

Keywords: Convergent encryption, De-duplication, Privacy preserving, Cloud computing, Differential privileges, Data management, Cloud storage.

1. INTRODUCTION:

In the recent times deduplication approach was an eminent method for making data managing more efficient in cloud system. This technique will improve usage of storage and is applicable towards transfers of data network to decrease the sending number of bytes. There is different functioning of convergent implementations of various variants of convergent encryption for secured deduplication. The approach of convergent encryption will provide secured data within the process of deduplication and the user will obtain a convergent key from each of the actual copy of data and encrypts that copy by convergent key. Conventional de-duplication on basis of convergent encryption, though provision of privacy somewhat do not maintain duplicate check by means of differential privileges [1]. For detection of duplicates, user will send tag towards server side for checking whether the matching copy is stored or not. The idea of proof of ownership will permit users to confirm the copies of data ownership to storage server. Particularly proof of ownership is provided as an interactive algorithm that was run by means of prover as well as verifier. There are lots of efficient protocols of identification within literature such as certificate-based, identity-basis identification and so on. While data deduplication will convey numerous issues of benefits, security as well as privacy takes place as user sensitive data is vulnerable to attacks. For protection of security in a better means our work will make an initial attempt to deal with difficulty of authorized data deduplication. Differential privileges of users are considered in the process of duplicate check in addition to the data itself and this is different from the de-duplication methods of earlier ones [2][3]. In our work we deal with the authorization difficulty of deduplication above data within public cloud and also deal with the privacy preserving problem of deduplication within cloud computing. We suggest a novel de-duplication system supporting for Differential Authorization in which each of the approved user is capable to obtain individual file token to carry out duplicate check on privilege basis. Authorized Duplicate Check in which approved user make use of individual keys to produce query for assured file and privileges owned by private cloud, whereas public cloud carry out duplicate check and informs the user regarding any duplicates.

2. METHODOLOGY:

Deduplication will get rid of outmoded information by managing of one copy and referring others to that copy. Traditional encryption procedure, while providing data privacy, is unsuitable to data de-duplication and particularly, traditional encryption process will need users to encrypt their information by their individual keys. In existing deduplication systems, private cloud is concerned as proxy to permit data owner to carry out duplicate check by means of differential privileges and this design is practical. Practice of convergent encryption was projected to put into effect data privacy while making of deduplication practicable. This approach will provide secured data within the process of deduplication and the user will obtain a convergent key from each of the actual copy of data and encrypts that copy by convergent key. Process of convergent encryption will authorize cloud to achieve de-duplication on cipher-texts as well as proof of ownership checks illegal user to have accession to files. While data deduplication will bring several issues of benefits, security as well as privacy takes place as user sensitive data is vulnerable to attacks. Earlier schemes of deduplication will not administer duplicate check of differential authorization, which is significant in lots of applications. In such an approved system of deduplication, each of the users is provided set of privileges throughout the initialization of system. Traditional systems of deduplication on basis of convergent encryption, though provision of privacy somewhat do not maintain duplicate check by means of differential privileges [4]. For security in an improved means our work will make an initial attempt to deal with difficulty of authorized data de-duplication. We deal with the authorization difficulty of deduplication above data within public cloud and also deal with the privacy preserving problem of deduplication within cloud computing. Aiming at solving of deduplication by differential privileges within cloud computing, we consider hybrid architecture including public cloud as well as private cloud.

3. AN OVERVIEW OF PROPOSED SYSTEM:

With cloud computing, data de-duplication in an effective means has attracted attention in recent times. Notion of approved data deduplication was projected to defend data security by means of inclusion of differential

privileges in the process of duplicate check. Deduplication system was proposed by Yuan et al. in cloud storage to decrease storage extent of the tags for checking of integrity. For improving To enhance deduplication security and protect data privacy, Bellare et al has showed protection of data privacy by means of transforming predictable message into un predictable. For protection of sensitive data privacy while supporting of de-duplication, method of convergent encryption was projected to encrypt data earlier than outsourcing. For protection of security in a better means our work will make an initial attempt to deal with difficulty of authorized data deduplication. Aiming at solving of deduplication by differential privileges within cloud computing, we consider hybrid architecture including public cloud as well as private cloud. In the schemes of existing deduplication systems, private cloud is concerned as proxy to permit data owner to carry out duplicate check by means of differential privileges and this design is realistic and has concerned much interest from researchers. In our work we deal with the authorization difficulty of deduplication above data within public cloud and also deal with the privacy preserving problem of deduplication within cloud computing. Differential privileges of users are considered in the process of duplicate check in addition to the data itself and this is different from the de-duplication methods of earlier ones. We propose a novel de-duplication system supporting for Differential Authorization in which each of the approved user is capable to obtain individual file token to carry out duplicate check on privilege basis [5]. Authorized Duplicate Check in which approved user make use of individual keys to produce query for assured file and privileges owned by private cloud, whereas public cloud carry out duplicate check and informs the user regarding any duplicates. Our authorized duplicate check proposal will maintain negligible overhead when compared to convergent encryption as well as network transfer. At high level, enterprise network consists of affiliated clients who will make use of Storage-cloud service provider and store up information by means of de-duplication method. De-duplication is used in these in support of data backup as well as disaster improvement applications although reducing their storage space and such systems are common and more appropriate

to user file backup as well as synchronization applications [6].

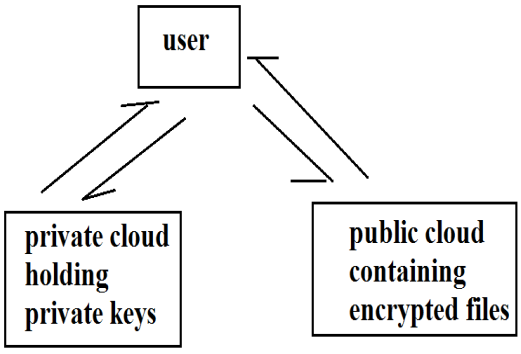

Fig1: an overview of Authorized Deduplication

4. CONCLUSION:

In the popular technology of cloud computing, increasing data is stored in cloud and shared by means of users with particular privileges, which describe access rights of stored information. For improvement of security in a better means our work will make an initial attempt to deal with difficulty of authorized data deduplication. Differential privileges regarding users are considered in the process of duplicate check in addition to the data itself and this is different from the de-duplication methods of earlier ones. In our work we manage authorization complexity of deduplication above data within public cloud and also deal with the privacy preserving problem of deduplication within cloud computing. We put forward a new de-duplication system supporting for Differential Authorization and Authorized Duplicate Check. Aiming at deduplication salvation by differential privileges within cloud computing, we consider hybrid architecture including public cloud as well as private cloud. Our approved duplicate check proposal will preserve negligible overhead when compared to convergent encryption as well as network transfer.

REFERENCES

[1] M. Bellare and A. Palacio. Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In CRYPTO, pages 162–177, 2002.

[2] 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.

[3] 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 ICDCS, pages 617–624, 2002.

[4] S. Quinlan and S. Dorward. Venti: a new approach to archival storage. In Proc. USENIX FAST, Jan 2002.

[5] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui. A secure cloud backup system with assured deletion and version control. In 3rd International Workshop on Security in Cloud Computing, 2011.

[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. IEEE Computer, 29:38–47, Feb 1996.

Draksharapu Prameela received her B.Tech degree in Computer Science and Engineering in the year 2012 and pursuing M.Tech degree in Computer Science and Engineering from Krishnaveni Engineering College for Women.

N.Brahma Naidu received his M.Tech degree in Computer Science and Engineering and B.Tech degree in Computer Science and Information Technology. He is currently working as an Asst Professor in Krishnaveni Engineering College for Women.