IJRRECS/December 2015/Volume-3/Issue-12/5030-5034 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A CONVERGENT ENCODING TECHNIQUE FOR PROVIDING SECURITY IN CLOUD INFRASTRUCTURE

Akkisetty Sreedhar[1], V.Vijay Kumar[2]

[1]**M.Tech Student, Dept of CSE, Lenora College of Engineering, Irlapally, Rampachodavaram, A.P, India**

[2]**Associate Professor, Dept of CSE, Lenora College of Engineering, Irlapally, Rampachodavaram, A.P, India**

ABSTRACT:

We solve the difficulty concerning de-duplication by means of differential privileges within cloud computing thus we build hybrid cloud architecture that consisting of a public cloud as well as a private cloud. Data de-duplication is a particular data compression practice that is commonly employed for elimination of duplicate copies of repetitive data in storage. It helps in removal of repetitive data by means of maintaining just a single physical copy and referring several repetitive data to that copy. Usual techniques on basis of convergent encryption, even though providing privacy to some amount, do not maintain duplicate check by differential privileges. The new structural design for cloud computing, consist of a twin clouds specifically public cloud as well as private cloud and this hybrid cloud setting has attracted increased attention in recent times. Different from traditional systems, private cloud is concerned as a proxy to permit data owner to perform duplicate check effectively by means of differential privileges and such a construction is realistic and has gained much concentration. In our work we consider just file level de-duplication that is intended for simplicity.

Keywords: Data de-duplication, Twin clouds, Repetitive data, Hybrid cloud, Privileges, Cloud computing.

1. INTRODUCTION:

As cloud computing turn out to be ubiquitous, a growing quantity of data is being stored in cloud and shared by users by means of specific privileges, which describe access rights of stored information [1]. For making data management efficient in cloud computing, de-duplication method has been chosen as an eminent technique that has gained a lot of attention in recent times. Even though data de-duplication offers many benefits, security as well as privacy concerns occur since users' sensitive data are at risk to insider as well as outsider attacks. Convergent encryption was introduced for implementation of data confidentiality while making de-duplication practicable. In the present days, cloud service providers provide a highly accessible storage and extraordinarily parallel computing resources at reasonably low costs. A user obtains a convergent key from every original data copy in addition to encrypting data copy by means of convergent key. This technique encrypts/decrypts a data copy by means of a convergent key, which is attained by computing cryptographic hash value of the content of data copy [2][3]. Contrasting from the existing data de-duplication systems, private cloud is concerned as a proxy to permit data owner to perform duplicate check effectively by means of differential privileges and such a construction is realistic and has gained much attention. Convergent encryption permits cloud to carry out de-duplication on cipher-texts and proof of ownership prevents illegal user to access file. In our work we intend to solve problem of de-duplication by means of differential privileges within cloud computing. Hence we build hybrid cloud architecture that consisting of a public cloud as well as a private cloud.

2. AN OUTLOOK TOWARDS RELATED WORKS:

The practice is used to advance utilization of storage and can moreover be functional in the direction of network data transfers to decrease number of bytes that have to be sent. Earlier techniques of de-duplication cannot maintain differential authorization duplicate check, which is significant in numerous applications. Conventional de-duplication systems on the basis of convergent encryption, even though providing privacy to some amount, do not maintain duplicate check by differential privileges. Data de-duplication is a specific

data compression procedure that is generally employed for elimination of duplicate copies of repetitive data in storage. No differential privileges were considered in de-duplication on basis of convergent encryption method which seems to be opposing if we want to understand de-duplication and differential authorization duplicate check at same occasion. Established encryption, while providing data privacy, is contrary by data de-duplication. Conventional encryption necessitates different users to encrypt their data by means of their own keys. To prevent unofficial access, a protected proof of ownership procedure is also needed to offer the proof that user certainly owns same file when a duplicate is found. Rather than keeping multiple data copies with similar content, de-duplication eliminates outmoded data by means of maintaining just a single physical copy and referring several outmoded data to that copy. A novel de-duplication system that supports differential duplicate check is projected under hybrid cloud structural design where Storage-cloud service provider resides within public cloud. In the projected system user is allowed only to carry out duplicate check for files that are marked with equivalent privileges. In this novel model, private keys intended for privileges will not be provided towards users directly, which will be managed by private cloud server [4]. In this approach, the users cannot allocate these private keys of privileges in this projected construction, which means that it can put off privilege key sharing between users in straightforward structure. To acquire a file token, user requires forwarding a request towards private cloud server. We imagine that all the files are susceptible and essential to be completely protected against public cloud as well as private cloud.

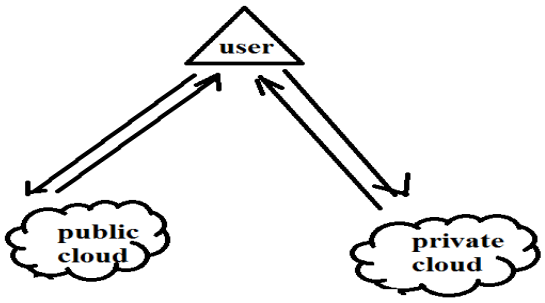

Fig1: Design of Proposed System.

3. AN OVERVIEW OFHHYBRID MODEL:

The view of proof of ownership facilitates users to confirm their ownership concerning data copies towards storage server. In our work we will just consider file level de-duplication intended for simplicity. We have referred a data copy as complete file and file-level de-duplication which removes

storage of any outmoded files. Block-level de-duplication can be simply figured out from file-level de-duplication. Particularly, to load a file, a user performs file-level duplicate check initially. When the file is a duplicate, subsequently the entire its blocks have to be duplicates additionally; if not, a user further performs block-level duplicate check as well as identifies distinctive blocks that are to be uploaded Convergent encryption provides data privacy in de-duplication. A user derives a convergent key from every original data copy in addition to encrypting data copy by means of convergent key.. It is a novel structural design for data de-duplication in cloud computing, which consist of a twin clouds specifically public cloud as well as private cloud. Previous techniques of de-duplication cannot maintain differential authorization duplicate check, which is significant in numerous applications. A new system that supports differential duplicate check is projected under hybrid cloud structural design where Storage-cloud service provider resides within public cloud. In novel representation, private keys intended for privileges will not be provided towards users directly, which will be managed by private cloud server. In our work we assume that all the files are susceptible and essential to be completely protected against public cloud as well as private cloud [5]. Under the supposition, two kinds of adversaries were considered, such as external adversaries which intend to take out secret information to the extent that possible from public cloud as well as private cloud; internal adversaries who intend to get hold of more information on file from public cloud as well as duplicate-check token information from private cloud exterior of their scopes. At a high level, an enterprise system, consist of a group of associated clients who will employ storage cloud service provider and accumulate data with de-duplication method. Such systems are extensive and are regularly more appropriate towards user file backup and synchronization applications than comfortable storage abstractions [6]. In this situation, de-duplication can be commonly used in these settings intended for data backup and failure recovery applications while to a great extent dropping storage space.

4. CONCLUSION:

For building data management competent in cloud computing, de-duplication method has been chosen as an eminent technique that

has gained a lot of attention in recent times. It progresses exploitation of storage and can moreover be functional in the direction of network data transfers to decrease number of bytes that have to be sent. In our work we work out difficulty of de-duplication by means of differential privileges within cloud computing. Hence we build hybrid cloud architecture that consisting of a public cloud as well as a private cloud. Convergent encryption was initiated for carrying out data confidentiality while making de-duplication practicable. Complementary from traditional systems, private cloud is concerned as a proxy to authorize data owner to perform duplicate check effectively by means of differential privileges and such a construction is realistic and has gained a great deal concentration. Usual de-duplication systems on source of convergent encryption, even though providing privacy to some amount, do not maintain duplicate check by differential privileges. Here we will just believe file level de-duplication intended for simplicity and it is a new structural design in cloud computing, which consist of a twin clouds specifically public cloud as well as private cloud. User is authorized only to carry out duplicate check for files that are marked with equivalent privileges in the projected system.

REFERENCES

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

[2] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology, 22(1):1–61, 2009.

[3] 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.

[4] R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.

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

[6] 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.