ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.7

Implementation of Convergent Encryption Scheme to Reduce Cloud Storage

Prerana Dakhane[1], Bhageshree Madan[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
Wainganga College of Engineering, Dongargao, Nagpur, India

Abstract:
Data de-duplication is a compression techniques that is used to remove the repetitive which can be used in cloud computing architecture. This paper is to provide both data security and space efficiency for De-duplication in single server storage. The De-duplication feature enables us to reduce storage space usage. The scope of the paper is to perform secure De-duplication in cloud storage using convergent encryption. De-duplication identifies and eliminates redundant data, reducing not only the volume of data stored in database but also the bandwidth required for data transfer. In convergent encryption, encryption keys are generated in a consistent manner from the data content thus, identical file will always encrypt to the same cipher text and in retrieval process they produce same plain text. The integrity of data outsourced into the cloud is managed by the hash calculation of any content that follows the proof -of –ownership module. Proposed system calculate the hash value of the content on source on destination side and request the hash value for the cloud side to predict the tampering of data. The expected analysis shows the flexible improvement in execution time and development cost.

Keywords: Convergent encryption, De-duplication, Cryptographic tuning

I. INTRODUCTION

Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the Internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on a storage server that are built on virtualization techniques. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Data de-duplication is a process that eliminates redundant copies of data and reduces storage overhead. Data de-duplication techniques ensure that only one unique instance of data is retained on storage media, such as disk, flash or tape. Redundant data blocks are replaced with a pointer to the unique data copy. In that way, data de-duplication closely aligns with incremental backup, which copies only the data that has changed since the previous backup. The main objective of the proposed system is to provide a secure cloud computing architecture with storage as a service model. The proposed system understand the problem of outsourcing data to the cloud, is the privacy and security. To make data more secure proposed system to provide convergent encryption scheme. Cryptographic tuning is also applied to make encryption more secure.

II. EXISTING SYSTEM

Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou; A Hybrid Cloud Approach for Secure Authorized De-duplication. IEEE Transaction on Parallel and Distributed System VOL: PP No: 99 Year 2014. Description: Data de-duplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space. To protect the confidentiality of sensitive data while supporting de-duplication, the convergent encryption technique has been used to encrypt the data while outsourcing.[1] To provide better data security, this paper makes the first attempt to formally address the problem of authorized data de-duplication. They also provide several new de-duplication techniques supporting authorized duplicate check in a hybrid cloud architecture. As a proof of concept, they implement a prototype of their proposed authorized duplicate check scheme and conduct test bed experiments using their prototype. They show that there proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

III. PROPOSED SYSTEM

Access to Authorized user:
To develop a system only authorized users should get download access to shared files in his access domain.

Confidentiality:
Cloud service providers are the third party service providers. So, it's not secure to store confidential contents as it is on cloud, to maintain confidentiality the proposed system need to implement encryption/ decryption scheme. But if it stored encrypted files on cloud then, user can't check the new file going to be uploaded on cloud is already present or not. So, in this paper convergence key is generated based on signature/ hash function on original data. So that user can achieve confidentiality as well as de-duplication.

IV. METHODOLOGY

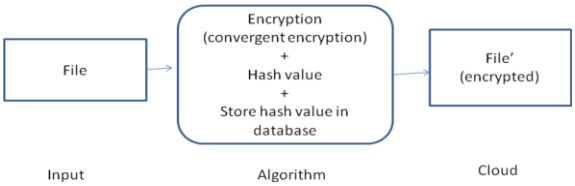


Figure.1. Uploading mechanism

The above figure shows the process of encryption. The convergent encryption is done using hash value while uploading a file. Where hash value is stored in database.

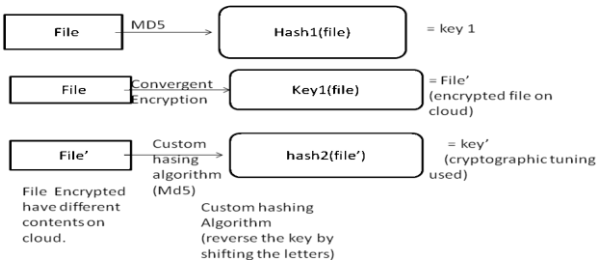


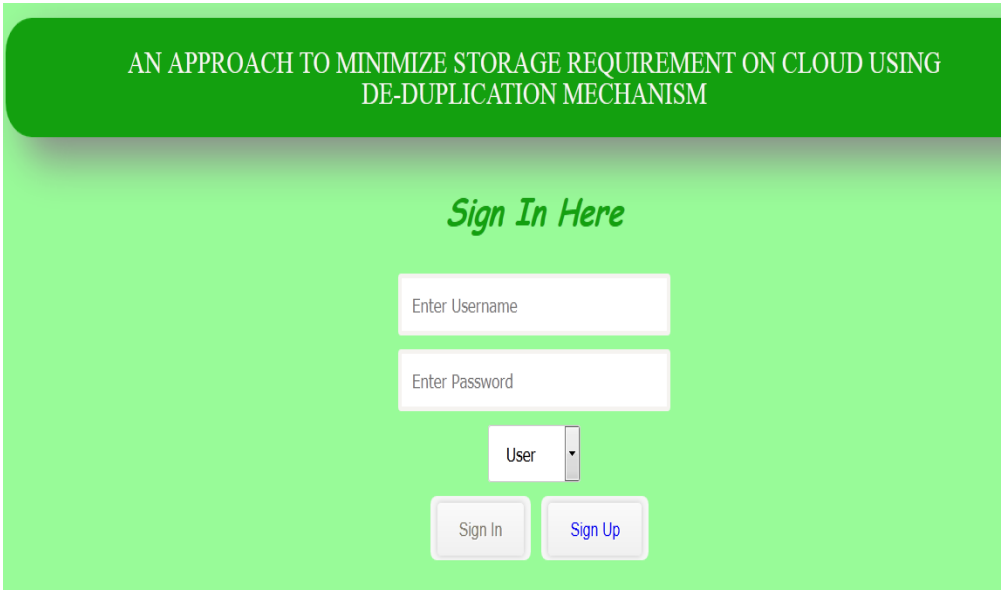
Figure. 2. Encryption Process

Figure 2 shows the process of encryption used while uploading file on cloud. MD 5 is used while uploading a file on cloud and file is encrypted using convergent encryption. Once the file is uploaded on cloud its hash value is stored in database. But when the file is uploaded on cloud it is stored in encrypted format so it is difficult to find same file. Thus we have to apply custom hashing algorithm to the encrypted file (Uploaded file on cloud), as its key will be generated which will again be stored in our database. This will help to find the duplicate file over the cloud. Also cryptographic tuning is applied to key to make it more secure.

V. RESULT

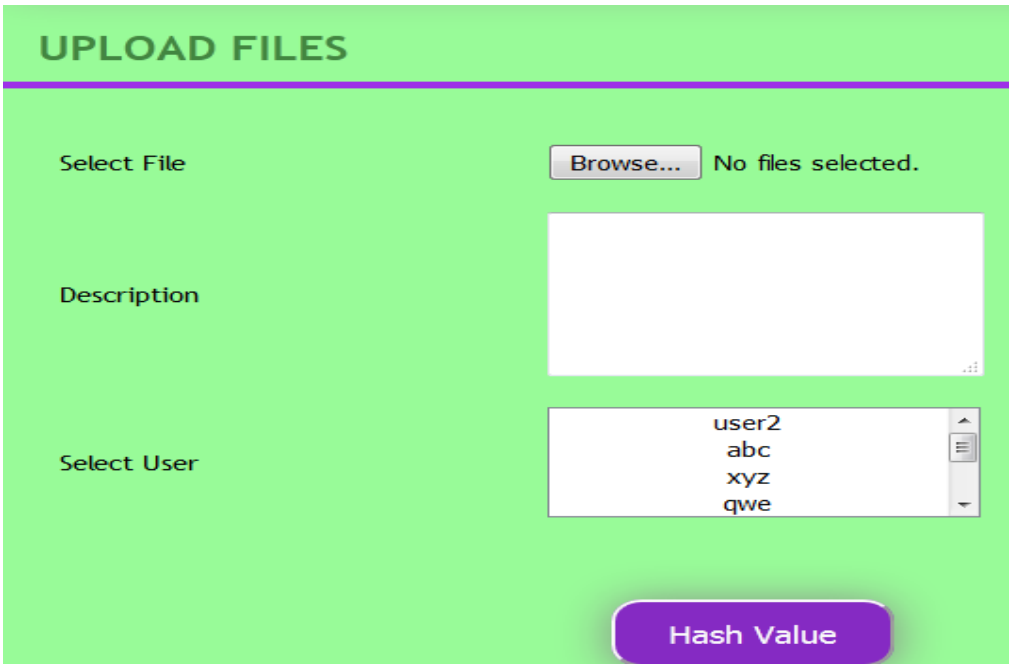
- **Module 1:**

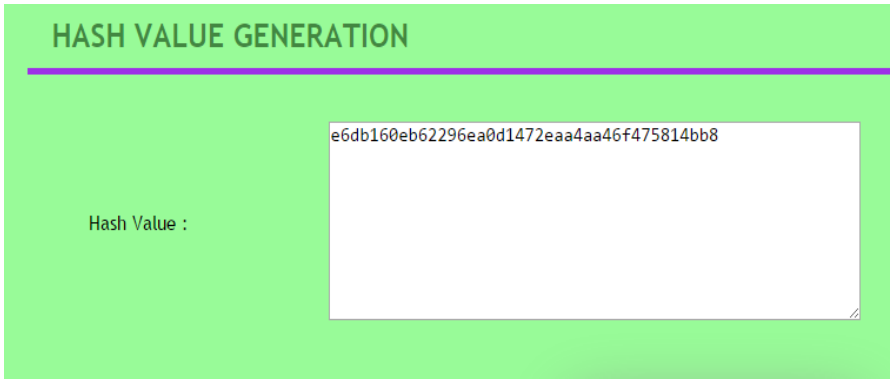
Login Page: This is page helps user to login and access and uploading of files over cloud. Each user will perform action according to their authorization.



- **Module 2:**

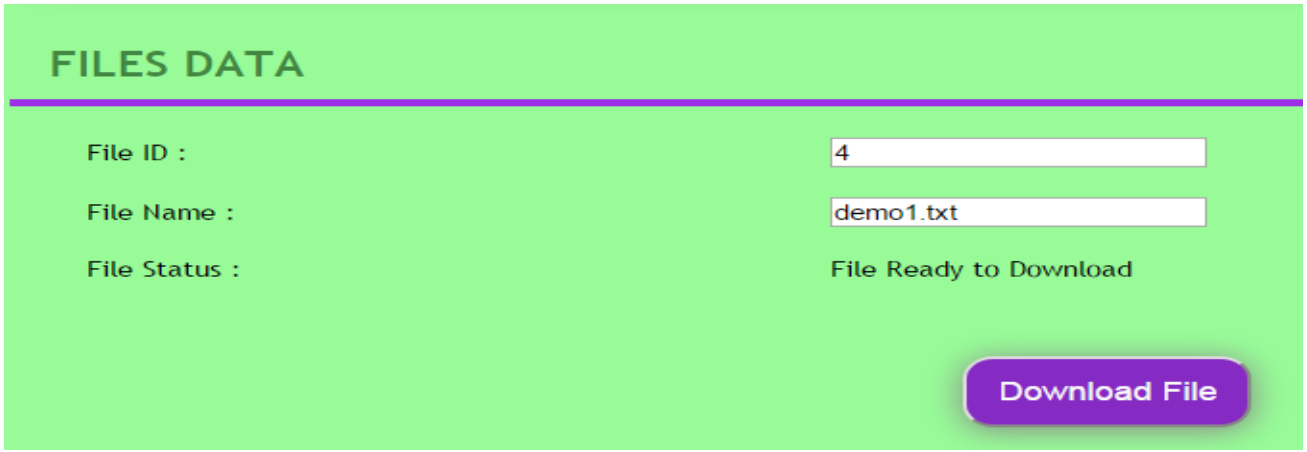
Uploading file: It allows browsing a file from system and uploading o cloud. While uploading it generated a hash value which is stored in data base. User can also select the person with whom he wants to share a file. Also description box is provided to write the description about file. When hash value is generated it is also shared with the person to whom the file is shared.



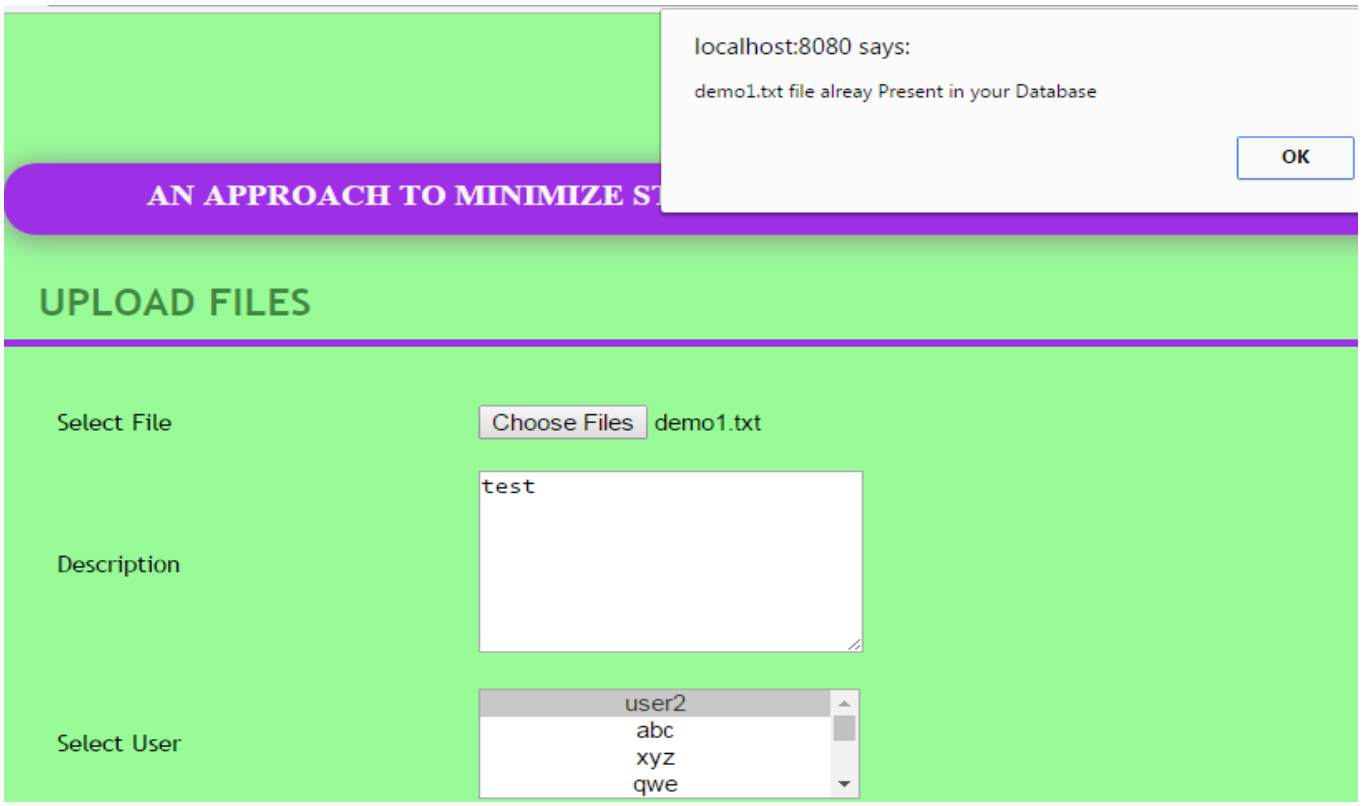


- **Module 3:**

Received File: The user with whom uploaded file is shared can check the shared file in received option. The user have to click on read option . Then there is direct option provided of convergent key. The user have to click on get convergent key which will copy the shared key in the given box. Similarly locator key is also copied in the box. Then click on Decrypt option which will show the details of file. Now the user can download and read the file.



- **Module 4: Checks de-duplication:** It checks de-duplication. If the file is already present over cloud it will show the message that the same file is already uploaded.



VI. CONCLUSION

The notion of authorized data de-duplication was proposed to protect the data security by including differential privileges of users in the duplicate check. [1] We also presented new de-duplication constructions supporting authorized duplicate check in hybrid cloud architecture, in which the duplicate-check tokens of files are generated by the private cloud server with private keys. We used convergent encryption with modification version to deal with brute force attack using Domain Separation and Cryptographic tuning to make better authorized de-duplication technique.

VII. REFERENCES

[1]. "Implementation of Convergent Encryption to minimize cloud storage Requirement" International Journal of Innovative Research and Advanced Studies (IJIRAS) Volume 4 Issue 2, February 2017

[2]. D. Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou. "A Hybrid Cloud Approach for Secure Authorized De-duplication" IEEE transaction VOL:PP NO:99 2014.

[3]. M. Bellare, S. Keelveedhi, and T. "Ristenpart. Message-locked encryption and secure de-duplication". In EUROC RYPT, pages 296–312, 2013.

[4]. P. Anderson and L. Zhang. "Fast and secure laptop backups with encrypted de-duplication." In Proc. of USENIX LISA, 2010.

[5] 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.

[6]. W. K. Ng, Y. Wen, and H. Zhu. "Private data de-duplication 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.

[11]. J. Xu, E.-C. Chang, and J. Zhou. Weak leakage-resilient client-side de-duplication of encrypted data in cloud storage. In ASIACCS, pages 195–206, 2013.

[12]. J. Yuan and S. Yu. Secure and constant cost public cloud storage auditing with de-duplication. IACR Cryptology ePrint Archive, 2013:149, 2013.

[13]. 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.

[14]. 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.