iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** III **Month of publication:** March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3112

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Data-Deduplication with Dynamic Ownership Management in Cloud Storage

Miss. Dive Pratibha[1], Miss. Pinjari Afrin[2], Miss. Kadam Pallavi[3], Miss. Kaygude Shital[4]
[1,2,3,4]*Department of Information Technology, SVPM's College of Engineering*
Malegaon (Bk), Tal-Baramati, Dist-Pune, Savitribai Phule Pune University.

Abstract: ***In cloud storage services, de-duplication technology is commonly used to reduce the space requirements of services by eliminating redundant data and storing single copy of them. When multiple users uploads the same data to the cloud storage, it leads to security issues Multiple users encrypts their data before outsourcing it to the cloud storage. In this paper, we propose a novel server-side de-duplication 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. The proposed scheme guarantees data integrity. Proof-of-ownership scheme allows any owner of the same data to allow to cloud server that he owns the data in robust way***
Keywords: User; Private Server; Cloud Server;

I. INTRODUCTION

To reduce resource consumption, there are many cloud storage services, such as Dropbox, Wuala, Mozy, and Google Drive , employ a de-duplication technique. In these techniques 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. Many owners encrypt their data before outsourcing it to the cloud server to protect data privacy and protect the data from unauthorized access. A convergent encryption algorithm encrypts an input file with the hash value of the input file as an encryption key. The cipher text is given to the server and the user retains the encryption key. In the case of ownership revocation, multiple users have ownership of a cipher text outsourced in cloud storage. After some time, some of these users may request the cloud server to delete or modify their data, and then, the server deletes the owner-ship information of the users from the ownership list for the corresponding data. We propose a de-duplication 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. As compared to the previous de-duplication schemes over encrypted data, the proposed scheme has the following advantages in terms of security and efficiency, and forward secrecy of de-duplication data upon any ownership change.

A. Problem Statement

Secure Data De-duplication with Dynamic Ownership Management in Cloud Storage

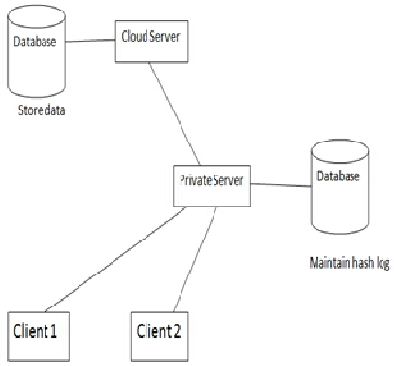
B. Aim of Projects

The aim is to verify the duplicate data by comparing data and eliminate duplicate data and store only single copy of data.

II. PROPOSED SYSTEM

Secure data de-duplication technology is used to reduce the space and bandwidth requirements by storing only single copy of data. User upload his file by dividing the file into chunks and by creating the hash code for each chunk. Private server maintains the log. Private servers database stores the data related to file that is file id, chunk id, hash. Cloud server stores deduplicated data.

A. System Architecture



III. MODULES

A. *Client*

Client owns the data and wish to upload it into cloud storage. This client encrypts the data and then upload it to the cloud storage. Client first selects the file for upload and divide that file into chunk. Hash of each chunk is created and send it to the private server.

B. *Private Server*

Private server receives the hash from client. Database of private server maintains the hash log. It sends this hash code to cloud server for comparison.

C. *Cloud Server*

Cloud server takes the hash code from private server, compare this code. If the hash is already present then it sends signal to private server otherwise encrypt the file with hash as a key and store it.

Algorithms

We are using two algorithms one is for generating the hash code of file and second is for encrypting the file.

SHA-3

AES

SHA-3

Algorithm Framework

Step 1: Append padding bits Message is padded with a 1 and as many 0's as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append length

64 bits are appended to the end of the padded message.

Step 3: Prepare processing functions

It requires 80 processing functions.

Step 4: Prepare processing constants

It requires 80 processing constant words.

Step 5: Initialize Buffer

It requires 160 bits or 5 buffer of words(32 bits)

Step 6: Processing message in 512-bit blocks(L blocks in total message).It loops padded and appended message in 512-bit blocks.

IV. CONCLUSION

This system will help to reduce storage space which is used by saving multiple copies of same file. Dynamic ownership management is an important and challenging issue in secure de-duplication over encrypted data in cloud storage. A novel secure data de-duplication scheme enhances a fine-grained ownership management by exploiting the characteristic of the cloud data management system. Thus, the proposed scheme enhances data privacy and confidentiality in cloud storage against any users who

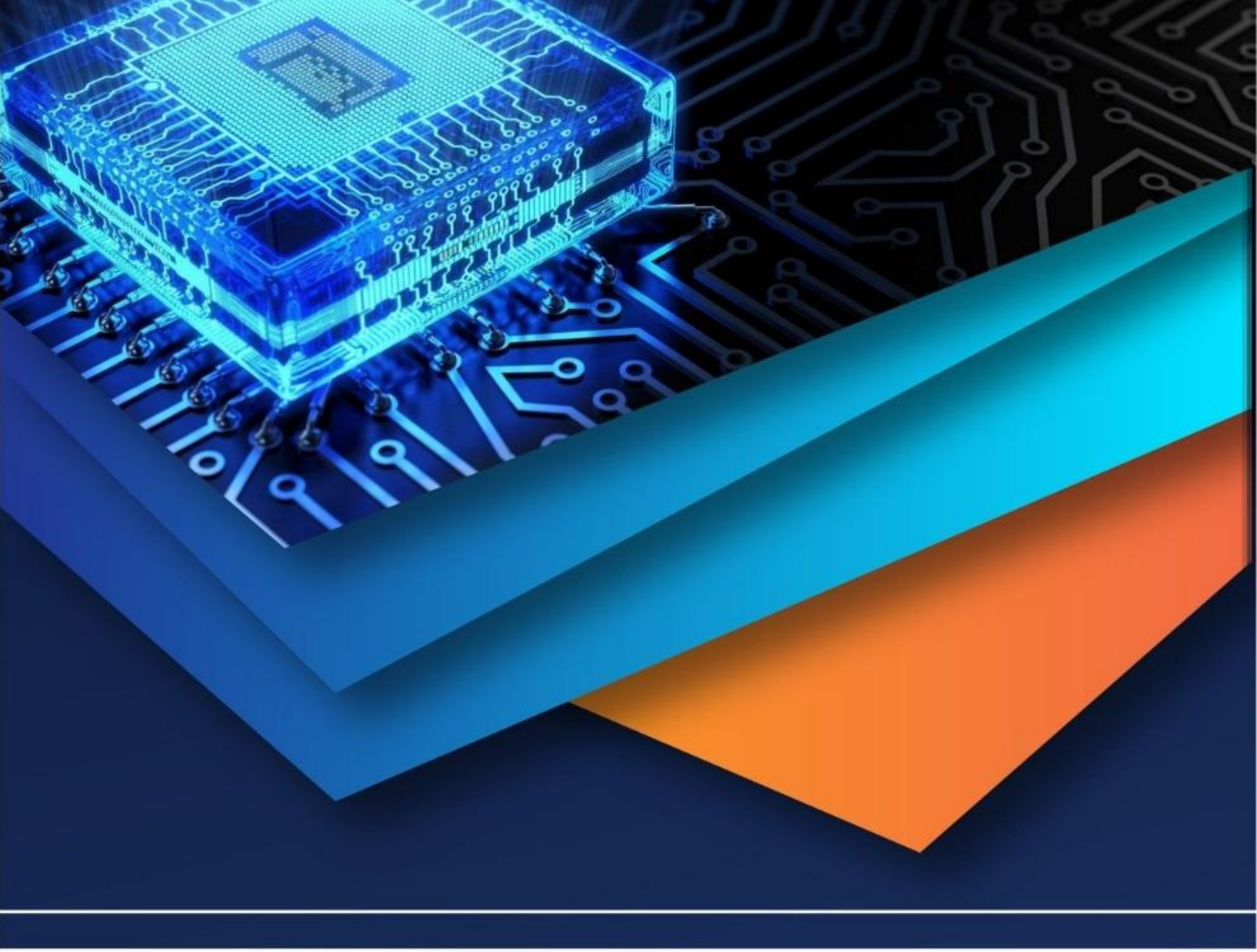
do not have valid ownership of the data.

V. ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. Gawade J.S. and other guidance teacher and Head of the Department Prof. Mali J. N and Principal Dr. Yadav D. M for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of SVPM's College of Engineering, Malegaon (Bk) for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books

REFERENCES

[1] M. Dutch, "Understanding data deduplication ratios," SNIA Data Management Forum, 2008.
[2] W. K. Ng, W. Wen, and H. Zhu, "Private data deduplication protocols in cloud storage," Proc. ACM SAC'12, 2012.
[3] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller, "Secure data deduplication," Proc. StorageSS'08, 2008.
[4] N. Baracaldo, E. Androulaki, J. Glider, A. Sorniotti, "Reconciling end-to-end confidentiality and data reduction in cloud storage," Proc. ACM Workshop on Cloud Computing Security, pp. 21–32,2014.
[5] P. S. S. Council, "PCI SSC data security standards overview,"2013.
[6] Security & Privacy, vol. 8, no. 6, pp. 40–47, 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY