Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

Cloud Storage Auditing with Deduplication with Strong Privacy Protection

Apoorvaditya Singh
Department of Electronics and Communication Engineering, RV College of Engineering Bengaluru, Karnataka

Mrs. Anusha L. S
Assistant Professor,
Department of Electronics and communication Engineering, R V college of Engineering Bengaluru, Karnataka

Dhanyashree R Prasad
Department of Electronics and Communication Engineering, RV College of Engineering Bengaluru, Karnataka

Dilip Kumar B. C
Department of Electronics and Communication Engineering, RV College of Engineering Bengaluru, Karnataka

Samiksha Rana Singh
Department of Electronics and Communication Engineering,
RV College of Engineering Bengaluru,
Karnataka

***Abstract*—The cloud storage auditing with deduplication is in a position to verify the integrity of knowledge stored within the cloud while the cloud must keep only one copy of a duplicated file. To the simplest of our knowledge, all of the prevailing cloud storage auditing schemes with deduplication are susceptible to brute-force dictionary attacks, which incurs the leakage of user privacy. In this paper, we focus on a new aspect of being against brute-force dictionary attacks on cloud storage auditing. We propose a cloud storage auditing scheme with deduplication supporting strong privacy protection, in which the privacy of the user's file would not be disclosed to the cloud and other parties when this user's file is predictable or from a small space. In the proposed scheme, we design a completely unique method to get the file index for duplicate check, and use a replacement strategy to get the key for file encryption.**

***Keywords*—Cloud,deduplication,auditing,storage**

I. INTRODUCTION

Nowadays, cloud computing has been widely used and is witnessing rapid development. Cloud storage is in demand for its advantages like low cost, universal access and services. Cloud users can safely store their data in the cloud and are free from local storage burden. Users' privacy is well protected from the outside world. There are chances of loss of data due to some operational errors or any technical failures in the cloud. It is important to ensure that data stored is free from security threats.

II. ARCHITECTURE

The system architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue.The architecture of the proposed design is shown in figure 1 .

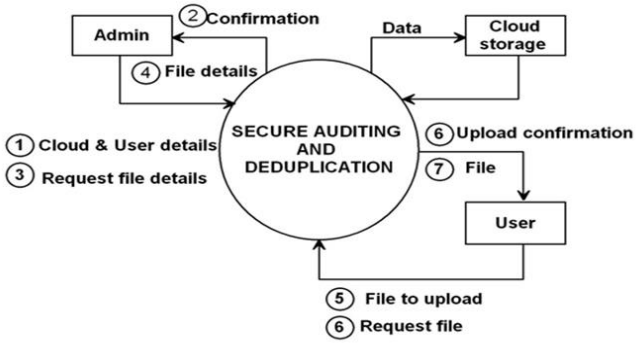

fig. 1

III. ADMIN MODULE

Admin should provide admin id and password for login. Admin can see their profile details and they can edit profile details and password.Admin can see all user details. They can add new users, edit existing user details, and be able to delete any user account and can see all cloud account details. They are allowed to see the hash tag generated for all blocks which is uploaded by users and can check transaction details of any user by selecting the desired user account. After finishing the task Admin should click on the sign out option to come out from the existing session.

. USER MODULE

Users should sign in into their account providing user ID and password, then they are directed to their profile. User has to upload the file and the file is broken into blocks of data and assigned a hashtag for each block. After every file upload generated hash tag is compared with existing hash tag from database if hash tag matched in that case file will

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

not uploaded into cloud, the number of instance of that block in database table will be increased, If hash tag did not match then that block hash details will be added in database and block will be uploaded in cloud. Logical Block Addressing(LBA) technique is used to identify what are the blocks present in a file. To download a file , the user has to select the file and using LBA ,the server has to find the block numbers of the selected file, download blocks and merge them to give the user a complete file. User can see all their transactions and has to logout finishing all the tasks to sign off the session

V. CLOUD SECURITY

One of the main objectives of the proposed design is the protection of user's privacy. Files uploaded are only accessible to the owners. The system runs an algorithm to check the authentication of the user and provides access to the file.

When the initial user uploads a file, the authenticator generation algorithm generates the private key ,authenticators and hash tag and uploads them to the cloud and the user will be provided with the link to the uploaded file. symmetric key encryption algorithm is used to encrypt the plain text. User is provided with the private key which is used to decrypt the ciphertext. If there is any change in the uploaded file, then the integrity check fails and a message is delivered to the user regarding the change of content.

If the user wants to access the file, the user has to send a request to the cloud by providing a keyword, the system verifies the identity of the user and provides the ciphertext, authenticators and hash value. If the user doesn't pass the verification, the cloud rejects the user's request. Once receiving the information from the cloud ,using the private key, the user can retrieve the file from the cloud and symmetric encryption key is used to decrypt the ciphertext and access the file. This process is explained in figure 2.

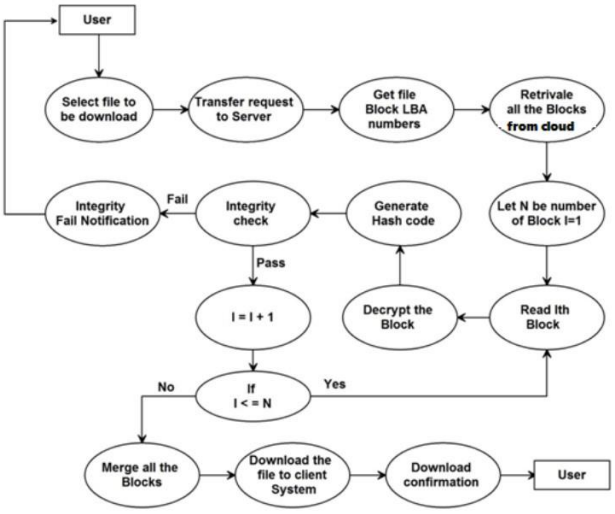

fig 2.

VI. CLOUD DEDUPLICATION

Data deduplication is a specialized data compression approach for removing replica copies of repeating data .Often known as Intelligent (data) compression Single-instance (data) garage .Used to enhance garage usage and also can be carried out to community information transfers to lessen the range of bytes that should be sent. In this process, unique chunks of knowledge , or byte patterns, are identified and stored during a process of study Chunks are compared to the stored copy and whenever a match occurs, the redundant chunk is replaced with a reference that points to the stored chunk. Figure 3 explains the deduplication process

Data deduplication compares objects (usually files or blocks) and removes objects (copies) that already exist in the data set.
Process consists of four steps:

1. Divide the data into "chunks" or blocks. In this project, each chunk is 500 bytes.
2. For each block of data, compute a hash value.
3. Use these values to see if the same data has already been placed in another block..
4. Replace the duplicate data with a reference to an existing database object.

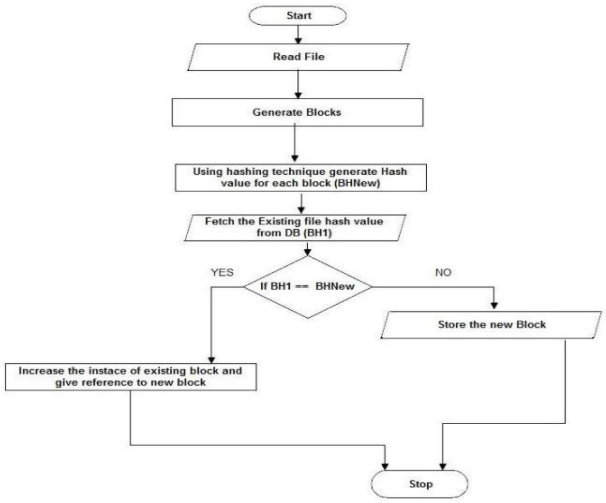

fig 3.

VI. CONCLUSION

In this paper, we have discussed how to protect the user's privacy and save the storage space in the cloud using the deduplication process. This paper discusses the detailed methodology of deduplication. The results obtained show that the proposed system has higher efficiency in saving storage space and also has better integrity protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 06, June-2021

ACKNOWLEDGMENT

We are indebted to our guide, Mrs. Anusha LS, Assistant Professor, RV College of Engineering . for the wholehearted support, suggestions and invaluable advice throughout our project work and also helped in the preparation of this thesis.

We also express our gratitude to our panel members Dr. Rajani Katiyar, Assistant Professor and Dr. Veena Devi, Associate Professor, Department of Electronics and Communication Engineering for their valuable comments and suggestions during the phase evaluations.

Our sincere thanks to the project coordinators Prof. Subrahmanya K N, Dr. Nithin M and Dr. Veena Devi for their timely instructions and support in coordinating the project.. Our sincere thanks to Dr. K S Geetha, Professor and Head, Department of Electronics and Communication Engineering, RVCE for the support and encouragement. We express sincere gratitude to our beloved Principal, Dr. K. N. Subrahmanya for the appreciation towards this project work. We thank all the teaching staff and technical staff of the Electronics and Communication Engineering department, RVCE for their help. Lastly, we take this opportunity to thank our family members and friends who provided all the backup support throughout the project work.

REFERENCES

[1] The Gnu Multiple Precision Arithmetic Library (GMP) , Oct. 2019.
[2] H. Cui, R. H. Deng, Y. Li, and G. Wu, ``Attribute-based storage supporting secure deduplication of encrypted data in cloud," IEEE Trans. Big Data, vol. 5, no. 3, pp. 330_342, Sep. 2019.
[3] M. Bellare, S. Keelveedhi, and T.Ristenpart, ``Message-locked encryption and secure deduplication," in Proc.Annu. Int. Conf. Theory Appl. Crypto- graph. Techn. Berlin Germany: Springer, 2013, pp. 296_312.
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ``Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2017, pp. 598_609
[5] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, ``Lightweight privacy- preserving identity-based veri_able IoT-based health storage system," IEEE Internet Things J., vol. 6, no. 5, pp. 8393_8405, Oct. 2015.
[6] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ``One secure data integrity veri_cation scheme for cloud storage," Future Gener. Comput. Syst., vol. 96, pp. 376_385, Jul. 2019.
[7] J. Gantz and D. Reinsel , '' Encrypted Data In Cloud ", IEEE Trans. Big Data, vol. 5, no. 3, pp. 330_342, Sep. 2019.
[8] W. Guo, H. Zhang, S. Qin, F. Gao, Z. Jin, W. Li, and Q. Wen, ``Out- . . sourced dynamic provable data possession with batch update for secure . . cloud storage," Future Gener. Comput. Syst., vol. 95, pp. 309_322, Jun. . . 2019.
[9] Wenting Shen , Ye Su and Rong Hao, Lightweight Cloud Storage . . Auditing With Deduplication Supporting Strong Privacy Protection , . . . March 2020
[10] Shunrong Jiang, Tao Jiang, Liangmin Wang, "Secure and Efficient Cloud Data Deduplication with Ownership Management", IEEE Transactions on Services Computing, vol. 13, Issue 6,2020