International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

2022 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 27th Sept 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 09

DOI: 10.48047/IJIEMR/V11/ISSUE 09/25

Title **AN EFFICIENT AND SECURE CLOUD STORAGE AUDITING SCHEME FOR SHARED CLOUD DATA**

Volume 11, ISSUE 09, Pages: 219-224

Paper Authors
Dr. J. Suresh Babu, Mr. O. Madhan Mohan, Mr. P. Bhanu teja reddy, Mr. S. Premchand, Mr. M. Naveen

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN EFFICIENT AND SECURE CLOUD STORAGE AUDITING SCHEME FORSHARED CLOUD DATA

[1]Dr. J. Suresh Babu, [2]Mr. O. Madhan Mohan, [3]Mr. P. Bhanu teja reddy, [4]Mr. S. Premchand, [5]Mr. M. Naveen

[1]Professor & HOD, Department of Computer Science and Engineering, Narayana Engineering College, Nellore, Andhra Pradesh, INDIA.

[2,3,4,5]PG Scholar, Department of Master of Computer Applications, Narayana EngineeringCollege, Nellore, Andhra Pradesh, INDIA.

Abstract — Cloud storage is one of the services provided by cloud computing in which data is maintained, managed, backed up remotely, and made available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the data owner's data can be attacked or modified by an outside attacker. Hence, a new concept called "data auditing" is presented, which checks the integrity of data with the help of a module called Third Party Auditor (TPA). The paper aims to develop an auditing scheme that is secure, efficient to use, and possesses the capabilities such as privacy-preserving, public auditing and maintaining data integrity along with confidentiality.

Data sharing is one of the important services provided by Cloud Storage (CS). To share data appropriately and securely, Shen et al. proposed a new cloud storage auditing scheme for shared cloud data, which uses the sanitizable signature to hide sensitive information in cloud. However, it will cause unauthorized access to the data in the cloud, since anyone can access the data stored on the cloud server. This paper implements An Efficient and Secure Cloud Storage Auditing (ES-CSA) scheme for shared data, where authorized users can access the data.

Keywords: Auditing, Data Integrity, Security, Privacy, Storage, Data Sharing, Outsourced Data.

1. INTRODUCTION

Cloud storage services offer a comparatively low cost, scalable, and convenient access for the stored data on cloud. Several clients and organizations outsource their data to the cloud server (CS) for storage. Therefore, cloud storage is widely used [1]-[4]. But it causes the data owner (DO) to lose direct control over its data, which may be corrupted owing to software/hardware failures or human causes [5]-[7]. Hence, various cloud storage auditing schemes have been proposed one after another [8], [9].

Data auditing allows data owners to securely store and process data. Data auditing is a processof verification of data that is stored in the cloud which can be verified either by data owner or by a Third-Party Auditor. It aids in preserving the integrity of cloud-stored data. There are two categories for the verifier's role: The first is private auditability, where only the user or data owner is permitted to verify the integrity of the data stored in the cloud. Nobody else has the right to question the server for handling of the data. However, it tends to increases verification overhead of the consumer. Second, there is public auditability: Anyone can challenge the cloud server, and the use of a third-party auditor allows for data verification in the cloud. The Third-Party Auditor (TPA) is a one of the modules, TPA acts on behalf of the data owner. It has all of the necessary

information, capabilities, expertise and professional capabilities which can be required to address the work of integrity verification and it also reduces the overheadof the data owner. It is important that third-party auditor (TPA) should efficiently audit the cloud data storage without retrieving for the local copy of data in the cloud. Third-Party Auditor (TPA) should have zero knowledge about the data owner's data stored in the cloud server. It should not introduce any additional on-line burden to the data owner [10].

2. LITERATURE SURVEY

1. To verify the integrity of the outsourced information, several cloud storage auditing schemes had been proposed one after other.
2. Ateniese et al. [8] proposed Provable Data Possession (PDP), which uses a random sampling approach and homomorphic authenticator.
3. Juels and Kaliski [9] proposed Proof of Retrievability (PoR), which performs integrity auditing and supports recovery of the outsourced data.
4. Shen et al. [11] proposed a lightweight cloud storage auditing primarily based on a third- party medium, which assists the Data Owner (DO) to generate authenticators while protecting data privacy.
5. Anbuchelian et al. [12] proposed a privacy-preserving cloud storage auditing scheme based on a secure encryption hash algorithm, which uses this hash algorithm to split and encrypt data before storing data in the cloud.

3. PROPOSED WORK

There is a need to develop an efficient and secure auditing scheme which overcomes the limitations of the existing auditing scheme. The proposed system is developed to check the
correctness of outsourced data by Third-Party Auditor (TPA) without retrieving the entire data or without introducing additional online burden to the cloud data owner's and cloud servers as well. It will assure that no cloud data content is leaked to Third-Party Auditor (TPA) during the auditing process. It provides storage, checks the correctness of data, maintains integrity and confidentiality of stored data in cloud.

This paper studies secure cloud storage auditing scheme for shared cloud data and the following is the summary of the contributions:

- We proposed an ES-CSA scheme for shared cloud data, where authorized users can access the data.
- We used Diffie–Hellman protocol when data owner sends auditing authenticators to the Third-Party Auditor (TPA) for checking the correctness of the data.

The three network entities viz. the data owner, cloud server and Third-Party Auditor (TPA) are present in the cloud environment. The data owner is the one who stores data on the cloud. TPA keeps a check on data owner's data by verifying integrity of data on-demand and notifies data owner if any variation or fault is found in data owner's data.

Data owner is a vital part in our proposed system. It plays most of the responsibility related to the cloud data. In the proposed auditing scheme, the data owner first registered and login with cloud server. The new data owner has to firstly register itself by filling the registration form and be the active member of the system. After registered, a message is provided that he

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

successfully registered. If a data owner is already the member of the system, then he or she can perform login process. If the username and password exist in the database, then they will be login successfully for being valid data owner's or else they will receive an error message.

After giving valid credentials the data owner login to the system then he will select the file he wants to store on the cloud server. The file selected by him will be split into four blocks. In order to splitting of the file into individual blocks a FileSplitter algorithm is used. Next, we are using a strong encryption algorithm called Advanced Encryption Standard algorithm (AES) to provide confidentiality to the data and it provides security to the cloud data. The blocks which are split those blocks will be encrypted using AES algorithm by the data owner. Each block of file will be encrypted and stored on the cloud for storage purpose. It encrypts data blocks of a file of 128 bits using symmetric key of size 128 bits. After encrypting the blocks, now for each and every block a hash values is generated separately. For this purpose, a hashing algorithm SHA-2 is being used here. After the hashes are generated, the hashes for each block are concatenated and RSA digital signature is performed on it. Digital signatures are used to authenticate the source of messages of a data owner. Later this signature is sent to the Third-Party Auditor (TPA), where it uses this signature to check the integrity of data stored in the cloud server storage is maintained correctly or not. Data owner is the only one who has authority to request for data integrity check to the Third-Party Auditor (TPA).

The data owner makes use of cloud storage to store the encrypted form of data as blocks in cloud. After data is stored in encrypted form, so the cloud server has no knowledge about the stored data. As well as if the cloud server turns into malicious server or is attacked by any outside attacker or hacker, the data will not be retrieved easily because it is in the encrypted form and outside attacker is not aware about the encryption algorithm used by the data owner.

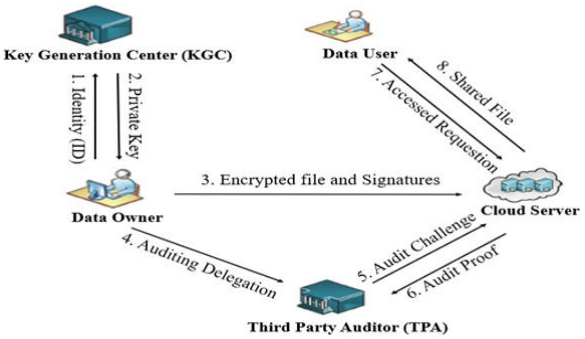

Fig. 1. SYSTEM ARCHITECTURE

In Figure.1 observe the different modules that compose this paper: Data owner, Data user, Third-party auditor (TPA), Key generation center (KGC), Cloud server.

A. Cloud Server

The cloud server offers computational & storage power to perform and store the data. In this module, cloud server admin login to the system and perform various operations like view data owner's details, view data user's details, view file requests, view attacker information, view transactions and view blocks data and authorize the data owner and data user.

The functionalities or activities performed by the cloud server are as follows:

- Authorize Data Owner
- Authorize Data User
- View Data Owner's Details

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

- View Data User's Details
- View Search File Requests and Permit
- View Download File Requests and Permit
- View Attacker Information
- View Transactions
- View Files

B. Data Owner

In this module, data owner register and login to system. After successful login, he performs various operations like upload data blocks, view upload files and update block data. Data owner is the owner of the data and he uploads the data into the cloud.

The functionalities of Data Owner are as follows:

- Upload the File
- Update the File
- View Files

C. Data User

In this module, data user register & login to system. After successful login, he performs various operations like request file to access the data form cloud servers, view file response, decrypt & download file.

The functionalities of Data User are as follows:

- View Files
- Request for access the File
- Search File
- Request for Download the File
- Download File

D. Attacker

In this module, attacker can attack the file blocks in cloud server. Attacker is the unauthorizedaccess to the system.

E. Third Party Auditor (TPA)

It is a public verifier that performs the auditing and returns the auditing results to the dataowner. TPA performs the integrity checking and data auditing.

The functionalities of Third-Party Auditor (TPA) are as follows:

- View File Meta Data
- Verify File's Block (Data Integrity Auditing)

F. Key Generation Center (KGC)

It is a fully trusted authority and responsible for generating a private key for the data ownerfiles.

The functionalities of Key Generation Center (KGC) are as follows:

- View Files and Generate Private Key

4. RESULTS

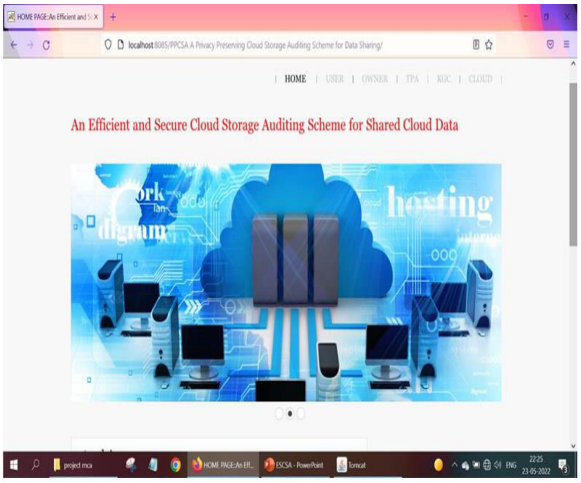

Fig. 2. HOME PAGE

This is the home page of this project. It

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

contains Data Owner, Data User, Key GenerationCenter, Third-Party Auditor, Cloud.

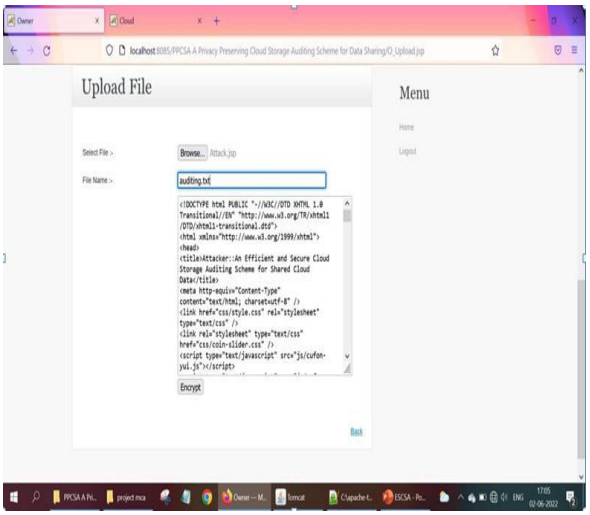

Fig. 3. UPLOAD FILE

In this screen, Data Owner will upload a file to cloud. Data owner will select the required

file to store in the cloud and given a name to the file and encrypt the file for security purposein the cloud.

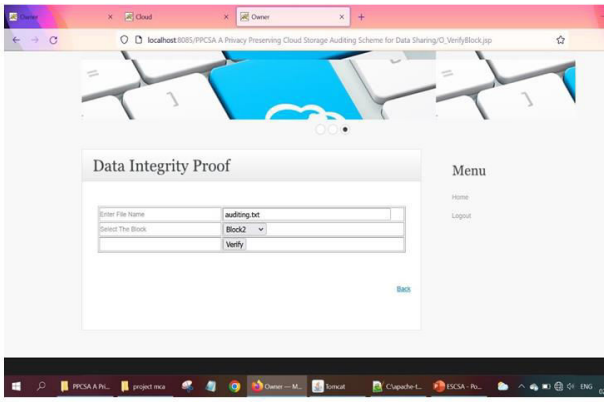

Fig. 4. DATA INTEGRITY PROOF

After successful login of Third-party auditor, the TPA will check the data integrity proof offile blocks in the cloud.

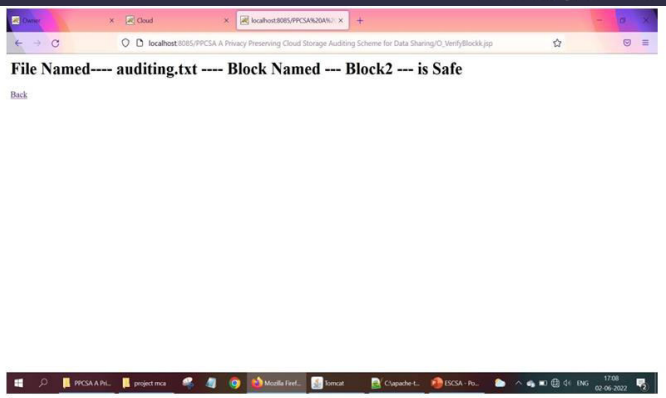

Fig. 5. RESULT PAGE

After verifying the data integrity of a file block, the result page will display. The page shows if the file block either safe or not safe in the cloud.

5. CONCLUSION AND FUTURE SCOPE

An efficient and secure cloud storage auditing scheme for shared cloud data is been proposed. In ES-CSA, only the authorized user can access the file stored in the cloud server to protect the interests of the data owner. It achieves privacy-preserving, public auditing and integrity check for cloud by using a TPA (Third Party Auditor), which does the auditing without retrieving the data copy from cloud, hence privacy is preserved. The data is split into blocks and then stored in the encrypted format in the cloud storage, thus maintaining the confidentiality of data. Experimental results show that the ES-CSA is secure and efficient. Our proposed system achieves better security to auditing of shared data. But still extended this system by adding data dynamic operations as future scope.

6. REFERENCES

[1] C. Sivapragash, S. R. Thilaga, and S. S. Kumar, “Advanced cloud computing in smartpower grid,” in Proc. IET Chennai 3rd Int. Sustain. Energy Intell. Syst., 2014, pp. 356–361.

[2] C. Sivapragash, S. Padmanaban, H. Eklas, J. B. Holmnielsen, and R. Hemalatha, “Location-based optimized

service selection for data management with cloud computing in smart grids," Energies, vol. 12, no. 23, 2019, Art. no. 4517.

[3] S. Kumar and C. Sivapragash, "Time orient traffic estimation approach to improve performance of smart grids," J. Comput. Theor. Nanosci., vol. 13, no. 8, pp. 5037– 5045, 2016.

[4] D. G. Chandra and R. S. Bhadoria, "Role of G-cloud in citizen centric governance," in Proc. IEEE Int. Conf. Parallel Distrib. Grid Comput., 2012, pp. 44– 48.

[5] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[6] K. S. Jadon, R. S. Bhadoria, and G. S. Tomar, "A review on costing issues in big data analytics," in Proc. Int. Conf. Comput. Intell. Commun. Netw., 2015, pp. 727– 730.

[7] R. S. Bhadoria, "Security architecture for cloud computing," Handbook of Research on Securing Cloud-Based Databases With Biometric Applications. Hershey, PA, USA: IGI Global, 2015.

[8] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[9] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[10] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf.

[11] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy- preserving secure cloud auditing scheme for group users via the third party medium," J. Netw. Comput. Appl., vol. 82, pp. 56–64, 2017.

[12] S. Anbuchelian, C. Sowmya, and C. Ramesh, "Efficient and secure auditing scheme for privacy preserving data storage in cloud," Cluster Comput., vol. 22, no. 4, pp. 9767–9775, 2019.