A Blockchain-Based Access Control System for Cloud Storage

A.Vijayan
Department of Information Technology, Velammal Engineering College
Email: vijayan@velammal.edu.in
P.S.Priyadharshini
Department of Information Technology, Velammal Engineering College
Email: priya2015dharshini@gmail.com
S.Rasika
Department of Information Technology, Velammal Engineering College
Email: srasika1998@gmail.com

----------ABSTRACT----------

Multi-user system for access control to datasets stored in an untrusted cloud environment. Cloud storage like any other untrusted environment needs the ability to secure share information. Our approach provides an access control over the data stored in the cloud without the provider participation. The main tool of access control mechanism is ciphertext-policy attribute-based encryption scheme with dynamic attributes. Using a blockchain based decentralized ledger, our system provides immutable log of all meaningful security events, such as key generation, access policy assignment, change or revocation, access request. We propose a set of cryptographic protocols ensuring privacy of cryptographic operations requiring secret or private keys. Only ciphertexts of hash codes are transferred through the blockchain ledger. The prototype of our system is implemented using smart contracts and tested on Ethereumblockchain platform.

I. INTRODUCTION

Cloud computing encourages users to outsource their data to cloud storage. Data outsourcing means that users lose physical autonomy on their own data, which makes remote data integrity verification become a critical challenge for potential cloud users. To free user from the burden incurred by frequent integrity verifications, Third Party Auditor (TPA) is introduced to perform verifications on behalf of user for data integrity assurance. However, existing public auditing schemes rely on the assumption that TPA is trusted, thus these schemes cannot be directly extended to support the outsourced auditing model, where TPA might be dishonest and any two of the three involved entities (i.e. user, TPA, and cloud service provider) might be in collusion. In this paper, we propose a dynamic outsourced auditing scheme which cannot only protect against any dishonest entity and collision, but also support verifiable dynamic updates to outsourced data. We present a new approach, based on batch-leaves-authenticated Merkle Hash Tree (MHT), to batch-verify multiple leaf nodes and their own indexes all together, which is more appropriate for the dynamic outsourced auditing system than traditional MHT-based dynamism approaches that can only verify many leaf nodes one by one. Experimental results show that our solution minimizes the costs of initialization for both user and TPA (compared to existing static outsourced auditing scheme), and incurs a lower price of dynamism at user side.

1.1 AES

The Advanced Encryption Standard (AES) is formal encryption method adopted by the National Institute of Standards and Technology of the US Government, and is accepted worldwide.The AES encryption algorithm is a block cipher that uses an encryption key and several rounds of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length.

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryptionkey.With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm. Encryption algorithms that use two different keys, a public and a pivate key, are called asymmetric encryption algorithms.

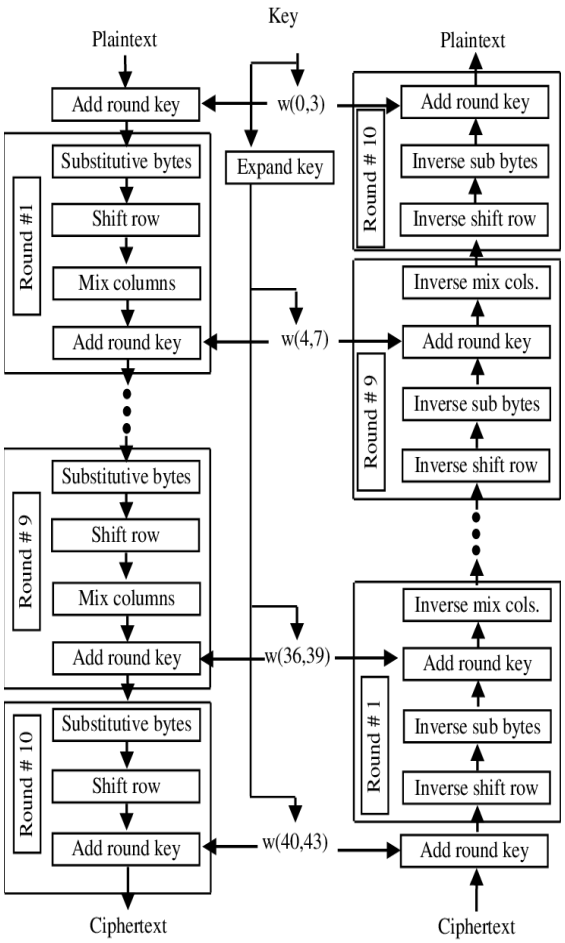


Fig1.1 AES block diagram

1.2 Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data.

1.3 Cloud Storage

Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure.

II. EXISTING SYSTEM

Furthermore, the cost of initialization in existing outsourced auditing scheme Fortress is high. During the Store Protocol (i.e., the data pre-processing step), the whole of user's outsourced data must be downloaded by TPA from cloud. Given that TPA will concurrently provide auditing proxy services for many different cloud users, and the total size of outsourced data of all users will be considerable in cloud. In this case, it must be a very heavy communication cost for TPA, by downloading all outsourced data from CSP, to accomplish above initialization for every user. In practice, to make an outsourced auditing scheme more easily accepted from the perspective of a real TPA, the design of forcing TPA to fetch the whole outsourced data from CSP is a limitation that should be avoided.

III. PROPOSED SYSTEM

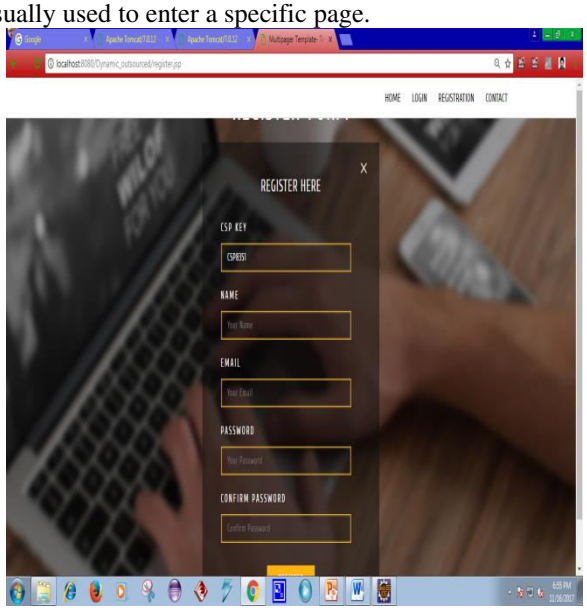
Proposed concept deals with the drawbacks of the private auditing i.e., Third Party Auditor. Third Party Auditor change the corrupted file in the cloud data by generating two types of database in server. As one database data have been corrupted third party auditor change the corrupted data by original data in second database.

IV. MODULES

- USER INTERFACE DESIGN
- FILE OWNER UPLOADING
- FILE REQUESTING
- THIRD PARTY AUDITOR RESPONSE
- FILE RETRIEVAL

4.1 User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



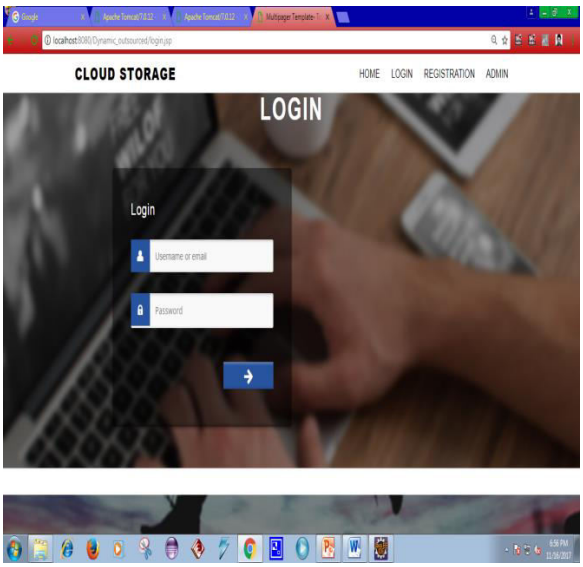


Fig 1 USER INTERFACE DESIGN

4.2File Owner Uploading

This is the module for uploading owner's files or documents into the virtual machines. These constraints serve a dual purpose as they can introduce high-level policies and assist in administration tasks. The user send the file to cloud send the Data so upload the file or Data. Given that we rely on network services for our most security-critical data. A source wants to securely send a message to a set of receivers over cloud network with unit-capacity edges, in the presence of a cloud user

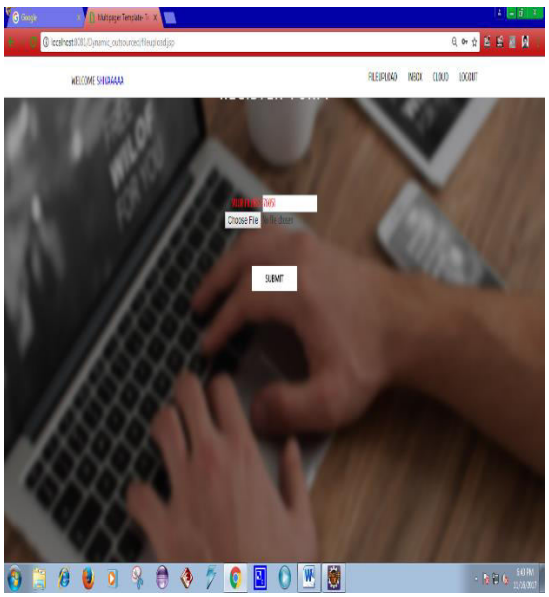


Fig 4.2 FILE OWNER UPLOADING

4.3File Requesting

The file is only view format so the file is share and download purpose in Request send to the data owner, the data owner is check the request and user was authorized person so data owner response and key provide to the user.

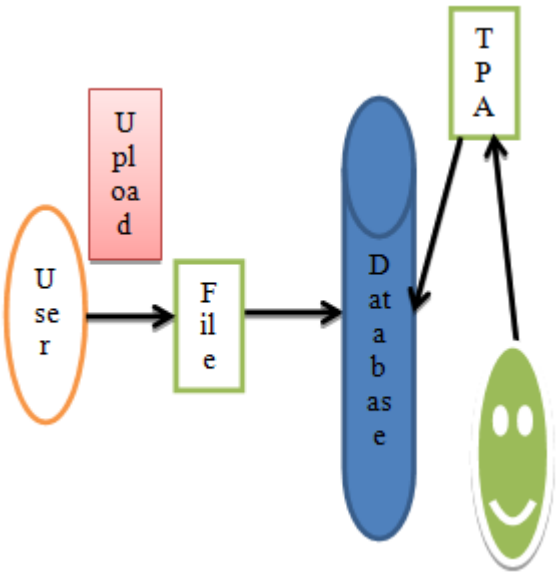


Fig 4.3.FILE REQUESTING

4.4Third Party Auditor Response

The malicious cloud might still forge valid authenticators later than the key-exposure time period if it obtains the current secret key of data owner. In this paper, we innovatively propose a paradigm named strong key exposure resilient auditing for secure cloud storage, in which the security of cloud storage auditing not only earlier than but also later than the key exposure can be preserved.

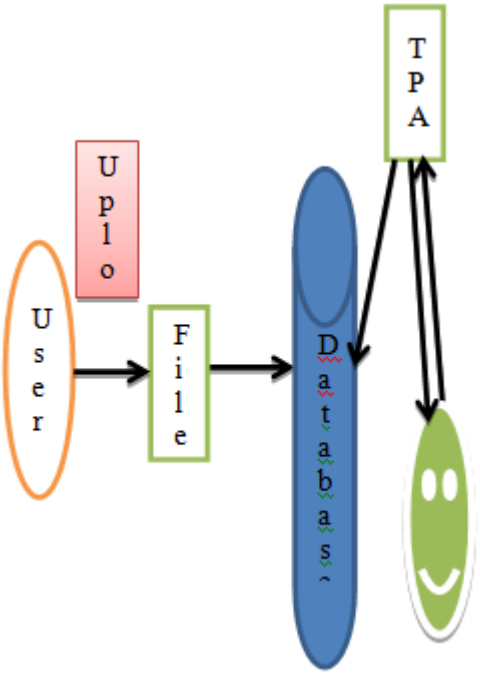


Fig 4.4.THIRD PARTY AUDITOR RESPONSE

4.5File Retrieval

TPA can audit the integrity of the challenged blocks without retrieving these actual blocks from the cloud. But the homomorphic tags can only be computed by user herself to against malicious CSP/TPA. Fortress builds upon the scheme of where the homomorphic tag of data block is constructed by using the corresponding block index.

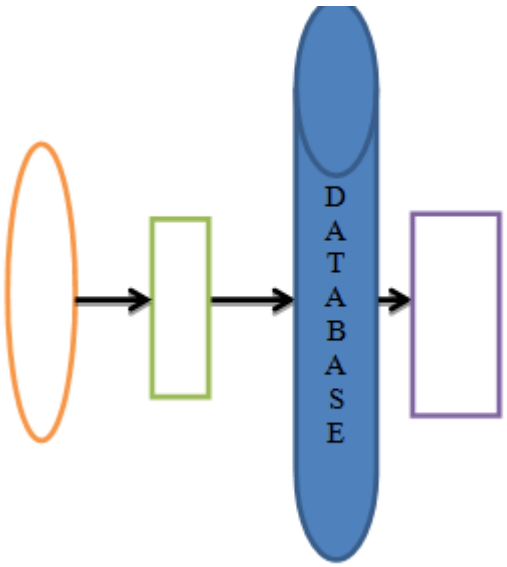


Fig 4.5. FILE RETRIEVAL

V. CONCLUSION

This project helps to secure cloud data through third party auditor. To free user from the burden incurred by frequent integrity verifications, Third Party Auditor (TPA) is introduced to perform verifications on behalf of user for data integrity assurance. However, existing public auditing schemes rely on the assumption that TPA is trusted, thus these schemes cannot be directly extended to support the outsourced auditing model, where TPA might be dishonest and any two of the three involved entities (i.e. user, TPA, and cloud service provider) might be in collusion. In this paper, we propose a dynamic outsourced auditing scheme which cannot only protect against any dishonest entity and collision, but also support verifiable dynamic updates to outsourced data.

REFERENCES

[1] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," Proc. 2009 ACM Workshop on Cloud Computing Security (CCSW '09), pp. 85-90, 2009.

[2] Cloud Security Alliance (CSA), "The Notorious Nine Cloud Computing Top Threats in 2013," https://cloudsecurityalliance. org/download/the-notorious-nine-cloud-computing-top -threats-in-2013, Feb. 2013. [

[3] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[4] Juels and B.S. KaliskiJr, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[7] C.C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[8] D. Cash, A. Küpçü, and D. Wichs, "Dynamic Proofs of Retrievability via Oblivious Ram," Proc. 32nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '13), pp. 279-295, 2013.

[9] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[10] Y. Zhu, G.J. Ahn, H. Hu, S.S. Yau, H.G. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Trans. Services Computing, vol. 6, no. 2, pp. 227-238, April-June 2013