Block Chain Based Secured File Sharing In The Cloud

S. Samsali Fathima[1], R. Subhiksha[2], Dr. P.Balakumar[3], Dr. R.K. Kapilavani[4]
[1, 2] Dept of Computer Science and Engineering
[3, 4] Assistant Professor, Dept of Computer Science and Engineering
[1, 2, 3, 4] Prince Shri Venkateshwara Padmavathy Engineering College

Abstract- *The demand for cloud based services is to be addressed in a time like this where trustworthiness has become the measuring scale for any service. Cloud based services serves just right for this requirement. Cloud Computing moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Also, the integrity of cloud data is subject to skepticism due to the existence of hardware or software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. Public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a threshold proxy re-encryption, on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. While prior works on ensuring remote data integrity often lacks the support of either public audit ability or dynamic data operations, we achieve both.*

Keywords- Block chain technology, file transfer on cloud, data integrity.

I. INTRODUCTION

Block chain technology is a digital innovation that has the potential to significantly impact trusted computing activities and therefore cyber security concerns as a whole. It is a kind of a linked list linked to one another cryptographically. It is distributed across the servers and the consistency is maintained through consensus. It is a tamper resistant and a great platform create and transaction crypto currency. A block chain is a decentralized, distributed and oftentimes public, digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively.

1.1 TYPES OF BLOCK CHAIN

Public Block Chain: Public Block chain is publicly accessible and has no restriction on who can participate or be a validator. In public block chains, no one has complete control on the network.

Private Block Chain:

A private block chain is permission. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

Consortium Block Chain:

In consortium block chain, some nodes control the consensus process, and some other nodes may be allowed to participate in the transactions. Consortium Block chain is like a hybrid of public and private Block chain.

1.2 NEED FOR BLOCK CHAIN TECHNOLOGY IN CLOUD COMPUTING

Block chain can definitely ensure the security of the information. The data stored in block chain is fully centralized, as it is stored in multiple nodes all over the globe instead of just in one place. This solves the issue of protection of data in case there is an error in storing information. The files that are uploaded on the block chain are not controlled by or accessible to any single party. Moreover, every party holding the information has a key that can be used to access the encrypted files. And even if someone is able to access your file, it is a partial file, which is useless to the person accessing it. The possibility technology taking over is highly probable.

II. RELATED WORK

This section discusses about literature survey, existing system, proposed system and architecture framework.

In a block chain supported cloud system, the files are the rock collection. The data gets broken into bits, stored on a bunch of servers and authorized person with the key needed to put the pieces back together.

III. LITERATURE SURVEY

A. Secure log storage using Block Chain and cloud infrastructure

There are thousands of cyber-attacks taking place around the world at any given moment. Attackers are continuously evolving sophisticated and stealthy techniques to target the victim. They take all the precautionary measures to remove attack traces such as system logs and related information on the victim systems so that they cannot be traced back. Attackers intentionally spread their activities over longer period of time to evade detection. To understand and identify such complex attack, it is required to maintain a secure log records over extended time period. However, preserving the log records form longer time is challenging issues. The system should also ensure the integrity of log files and logging process. In order to overcome these issues, this paper proposes a secure log storage using Block Chain on Cloud platform.

B. Security implications of block chain with analysis of block withholding attack

The block chain technology has emerged as an attractive solution to addresses performance and security issues in distributed systems. Block chains public and distributed peer-to-peer ledger capability benefits cloud computing services which require functions such as assured data provenance, auditing, management of digital assets and distributed consensus. Block chain underlying consensus mechanism allows to builds an tamper-proof environment, where transactions on any digital assets are verified by set of authentic participants or miners. With use of strong cryptographic methods, blocks of transactions are chained together to enable immutability are chained together to enable on the records. In this paper, we first discuss block chains capability in providing assured data provenance in cloud and present vulnerabilities in block chain cloud. We model the block withholding (BWH) attack in block chain cloud considering distinct poor rewards mechanisms.

C. A Block chain based decentralized cloud resource scheduling architecture

Application services in cloud computing model have complex scheduling, composition, configuration and deployment conditions, even in the multi-condition requirements; it can also be based on the change of time to schedule virtual services. Therefore, the demand of optimizing cloud computing scheduling strategy to ensure cloud data security and recovery ability is increasingly prominent. This paper prose a trusted distributed audit method for cloud task scheduling information in the cloud cluster. This method is mainly used as an distributed solution that combines block chain technology and traditional cloud server to solve the problem of integrity and security of cloud task scheduling in order tom prevent potential. The hash data cloud task scheduling information is stored on the block chain network and the original data to the cloud data base, which guarantees the cloud task within the cloud cluster.

D. Block chain based decentralized storage scheme

Different front hr current cloud storage solutions, which are mostly centralized storage providers, this paper proposes a decentralized storage system based on block chain technology, which can make full use of the remaining space of personal hard disks of users around the world. Storage provider performs a data integrity that the verification is passed, the user pays the storage fee to the storage provider through the lightning network technology. All proofs and payment information are stores in the block chain, which stored in the block chain, which guarantees the security and credibility of the system. Compared with the current mainstream distributed storage systems, this scheme has been improved in terms of system access and payment methods.

IV. EXISTING SYSTEM

The traditional cloud based services employed threshold proxy re-encryption to verify the integrity of the data on the cloud with a lack of public auditing with a trusted third party. The problem arises when the trustworthiness of the third party is in a questionable state. Confidential information is inevitably released.

Drawbacks:

1) Verification of correct data storage in the cloud cannot be conducted without explicit knowledge of the whole data.
2) The data stored in the cloud may be frequently updated by the users to appoint where it might become ambiguous.

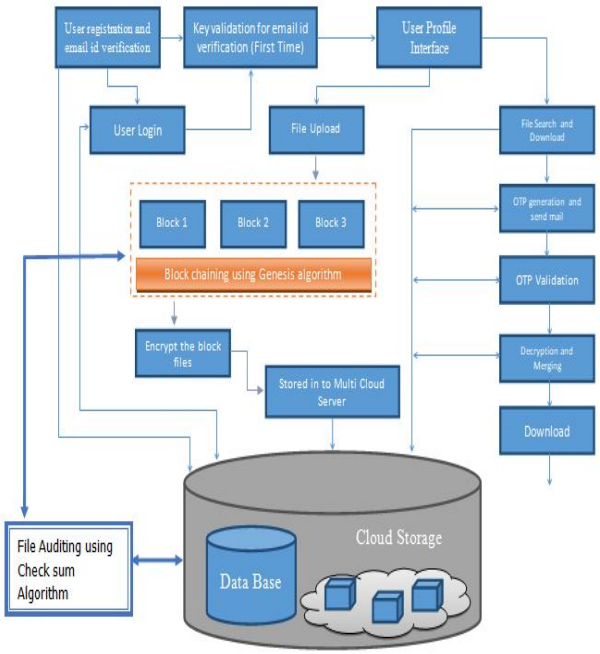
V. PROPOSED SYSTEM

We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user's data in the cloud. We rely on Block Chain Genesis technique in the file distribution preparation to provide redundancies and guarantee the data dependability. By utilizing the homomorphism token with distributed verification of block chained data, our scheme achieves the storage correctness insurance as well as data error localization.

To allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing.

VI. SYSTEM ARCHITECTURE

Our proposed system consists of the following architecture as its backbone. It makes use of the block genesis technique.



VII. MODULES

1) User interface
2) File uploading process
3) File Downloading process
4) Secret key generation
5) Mail alert process

1) USER INTERFACE

Users can use a resource on the cloud from anywhere at any time without being concerned about how computation is done and storage is managed. In this paper, we focus on designing a cloud storage system for robustness, confidentiality, and functionality. A cloud storage system is considered user interface entry level creation in this module.

2) FILE UPLOADING PROCESS

The message of k symbols is encoded into a codeword of n symbols by erasure coding using block chaining technique. To store a message, each of its codeword symbols is stored in a different storage server. A storage server corresponds to an erasure error of the codeword symbol. As long as the number of servers is under the tolerance threshold of the erasure code genesis block, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process.

3) FILE DOWNLOADING PROCESS

A secret key corresponding to a requested file is sent to the user mail id with which the file contents can be decrypted. The blocks of data are combined back to get the whole original data using the SHA1 algorithm.

4) SECRET KEY GENERATION

The data forwarding phase, user forwards his encrypted message with an identifier ID stored in storage servers to user so that they can decrypt the forwarded message by using his secret key. The secret keys of target users, and the shared keys stored in key servers.

Table 1. Testing Report

Test	Requirement or Purpose	Action / Input	Expected Result	Actual Result	Pass / Fail
1	User Register	Enter new and correct details	Registration Success	Same as expected	Pass
2	User Login	Enter username and password	Login Success	Same as expected	Pass
3	File Upload	Keywords not entered	Please enter relevant keywords	Same as expected	Pass
4	File Download	Enter secret key	File download success	Same as expected	Pass
5	File Download	Enter wrong secret key	Please enter the correct secret key	Same as expected	Pass

5) MAIL ALERT PROCESS

The user is forwarded the secret key only after checking their identity through e-mail. The requesting user is not eligible to know the contents of the file and so the secret key will not be forwarded to that kind of access.

VIII. CONCLUSION

Thus the system involved maintaining the integrity of data by employing block chain technology. The data on the cloud were split into blocks and then stored encrypted. This way providing redundancies and data dependability were ensured. The homomorphism token was used with distributed verification of block chained data, achieving storage accuracy insurance as well as data error localization.

IX. FUTURE ENHANCEMENT

In this framework, we utilized just content records. In future we will incorporate the picture, sound, video documents. The OTP is sent to proprietor mail id in our proposed system. In the future, the requestor will get the OTP on a portable authenticator. Ethereum can be used to store the file fragments in the future.

REFERENCES

[1] S. B .Balaji, M. Nikhil Krishnan, Myna Vajha, Vinayak Ramkumar, “Erasure Coding for Distributed Storage: An Overview”, Department of Electrical Communication Engineering, Indian Institute of science, Bangalore June 2018.

[2] Deepak k. Tosh, Sachin Shetty, Xueping Liang, “Security implications of Block chain Cloud with Analysis of block withholding attack” IEEE/ACM International Symposium on Cluster and Grid Computing 2017.

[3] He Zhu, Yichuan Wang, “A Block chain- based Decentralized cloud resource scheduling architecture” International Conference on Network Applications 2018.

[4] Jeffery Austin, Puyallup, John Christopher, “Secure decentralized file sharing systems and methods”, United States Patent Application Publication Feb. 2019.

[5] Le Jiang and Xinglin Zhang , “ BCOSN: A Block chain based decentralized online social networks” in computer and Electrical Engineering 2020.

[6] Taotao Wang, Soung Chang Liew and Shengli Zhang ,”PubChain:A Decentralized open-access publication platform with participants incentivized by Blockchain technology” IEEE Consumer Electronics Magazine, vol.7,oct 2019.

[7] Tara Salman,Maede Zolanvari, Raj Jain ,”Security Services using Block chains: A Sate of the Art Survey” IEEE Communications Surveys and Tutorials 21018.

[8] Songling fu, Ligang he, Cheng chang “Cadros: The Cloud-assisted data replication in decentralized online social networks” IEEE International conference on services computing 2014.

[9] Wenting Shen, Rong Hao, Jing Qin, “Data integrity auditing without private key storage for secure cloud storage” IEEE transactions on cloud computing ,vol.23 2018.

[10] Yuan Zhang, Chunxiang Xu, Xuemin Shen, “ Block chain-based integrity verification for cloud storage against procrastinating auditors”, IEEE Transactions on cloud Computing 2019.