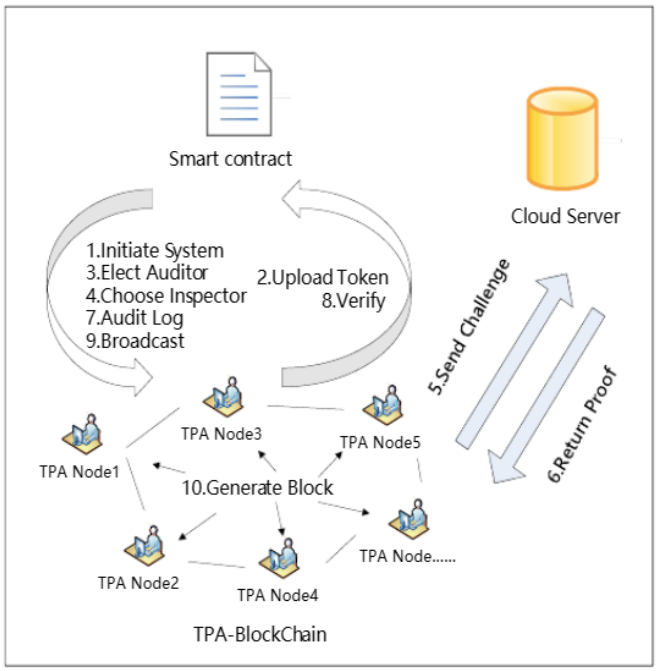
JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CREDIBLE ALLIANCE CHAIN BASED PUBLIC AUDITING SCHEME FOR CLOUD STORAGE

[1]P. Akash, [2]P. Akhil, [3]P. Ananya, [4]Ch. Sushma
[1,2,3]UG Scholars, [4]Asst. Professor
[1,2,3,4]Department of Computer Science and Engineering,
Guru Nanak Institutions Technical Campus (Autonomous), Hyderabad, India.

Abstract : In this study, We provide a thorough investigation of a reliable alliance chain-based public auditing program created especially for cloud storage in this paper. The main goal of the research is to solve the significant problems that come with guaranteeing data security, integrity, and dependability in cloud storage systems. Our research aims to create a new auditing framework that takes advantage of alliance chain technology, a strong and transparent distributed ledger system. This study, "Credible Alliance Chain-Based Public Auditing Scheme for Cloud Storage," aims to improve cloud service providers' credibility and accountability by putting forth a novel method. We place special emphasis on the usage of alliance chains, which provide cryptographic methods and decentralized consensus procedures for ensuring the integrity of data stored in the cloud. Our plan uses this technology to its full potential in order to offer verifiable evidence of data integrity without sacrificing privacy or needing excessive processing capacity. The results of this research should have a significant impact on cloud storage systems' security and dependability, providing a viable path for increasing openness and trust in cloud computing settings. Moreover, our study lays the groundwork for further research into improving alliance chain technology's uptake and usefulness across a range of industries, ultimately advancing the development of trustworthy and safe cloud services. The main objective is to create a cloud environment that is more reliable and trustworthy so that stakeholders can manage and audit their data assets with more assurance and accountability.

Our Shceme :



IndexTerms **- Cloud Storage,Public Auditing,Block chain,Alliance Chain,Data Integrity,Cryptographic Techniques,Trust Model,Decentralization.**

I. INTRODUCTION

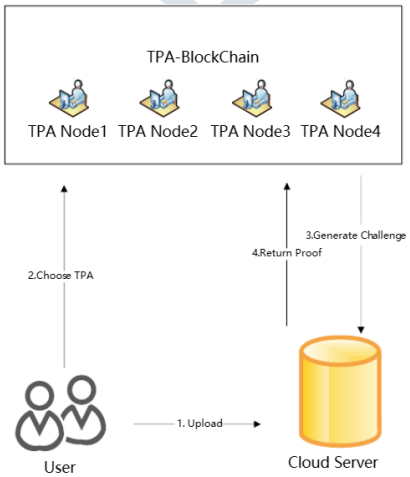
The goal of the project "Credible Alliance Chain Based Public Auditing Scheme for Cloud Storage" project aims to create and execute a novel auditing system that utilizes blockchain technology to guarantee the security and integrity of data kept in cloud environments. Because it is scalable and convenient, cloud storage has become widely used in modern computing. However, issues with data privacy, integrity, and accountability still exist. The goal of this project is to overcome these issues by creating a strong auditing framework that makes use of blockchain's immutable and decentralized characteristics. The project intends to develop a visible and impenetrable process for confirming data integrity and guaranteeing adherence to security standards by merging blockchain with cloud storage auditing. The plan will make use of a trustworthy network of alliances to facilitate effective and dependable public audits, giving interested parties the ability to confirm the legitimacy of data without jeopardizing privacy. Investigating consensus algorithms and cryptographic techniques to enable safe and effective data auditing procedures is the focus of the project. By utilizing blockchain technology, the ultimate goal of this project is to develop reliable cloud storage options. It is anticipated that the proposed plan will improve cloud storage systems' security, accountability, and openness, inspiring more trust from both service providers and customers.

LITERATURE REVIEW

A cloud storage, a reliable alliance-based public auditing program is essential to guaranteeing the security and integrity of remotely stored data. Cloud storage systems must contend with issues with data integrity, privacy, and effective auditing procedures. Numerous academic works emphasize how crucial it is to create reliable auditing systems that use distributed trust models and cryptography to confirm the accuracy of data stored in the cloud. For cloud storage, for example, Wang et al. (2013) suggested an auditing technique based on homomorphic linear authenticators (HLAs) that is both secure and efficient. With the use of this plan, the cloud service provider can demonstrate to outside auditors that the data it has outsourced is authentic without actually disclosing the data. This technique improves cloud storage environments' openness and accountability through the use of a public auditing platform. Similar to this, Liu et al. (2014) investigated the use of a multi-cloud architecture in a cooperative proven data possession (PDP) technique. Their strategy made use of the cooperation of several cloud service providers to guarantee the availability and integrity of data. In cloud storage systems, this collaborative auditing methodology improves fault tolerance and dependability.Furthermore, an alliance-based auditing system using proxy re-encryption and group signatures was presented by Zhu et al. (2015). With the use of this plan, multiple auditors can independently confirm the accuracy of the data without having to reveal the source data. When auditing large-scale cloud storage systems, alliance-based techniques like these increase auditing efficiency and scalability.

II. SYSTEM MODEL DESIGN

Figure 1 shows the architecture of our CACPA. In our model, there are three types of entities: cloud server (CS), data user (U) and and third-party auditor (TPA)-Blockchain, defined as below.

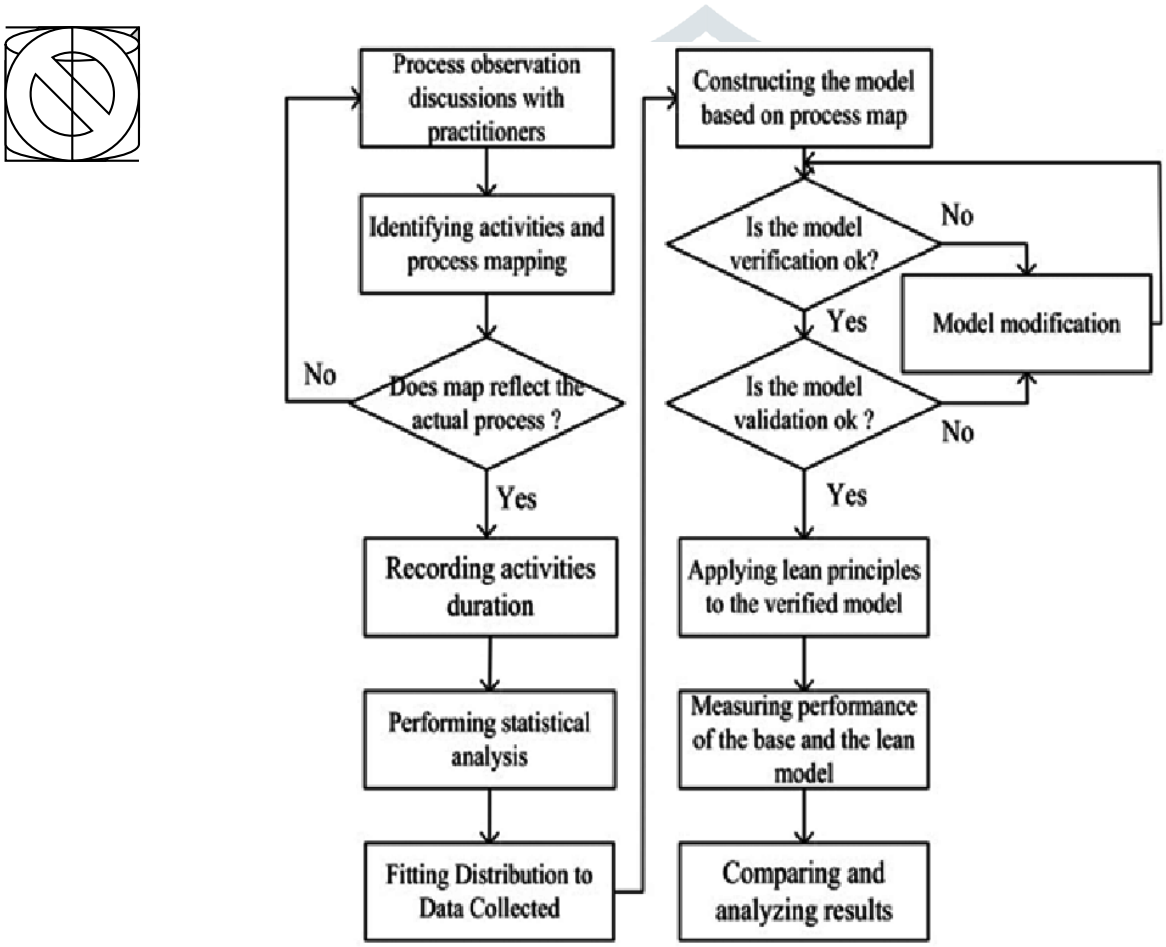


TPA blockchain: The blockchain collective is composed of TPA nodes with a good reputation in the industry to implement credible audit work. TPA node: When the blockchain system receives an audit task, a TPA node may be appointed as an auditor or an inspector. The auditor performs data auditing with CS and the inspector supervises the auditor's work. Inspector carries out inspection work to check the honesty and timeliness of auditor. User: User groups have limited or lightweight computing resources and demand for services of cloud storage and data integrity audit. CS: CS provide cloud storage services, but it may conceal the accidents of data loss or collude with TPA in order to maintain good reputation by cheating users.

Our blockchain-based public auditing scheme works as follows:
1. The user generates tags on his own data and outsources the local data and tags to CS.
2. The user executes the smart contract of the blockchain composed of TPA, Locks currency into the smart contract's address and sets the audit strategy inclusive of parameters like audit times, audit frequency, etc.) At the specified time point, smart contract calls election function, it generates a random seed according to the current blockchain status information. Then it chooses an auditor and some inspectors using the seed.
3. The selected auditor generates a random seed according to the current blockchain status, then uses it to produce a challenge and sends to the CS.
4. CS receiving the challenge and generate a proof by its storage. CS return proof to TPA for verification'

III. RESEARCH METHODOLOGY

This project proposes a secure and efficient public auditing scheme for cloud storage based on credible alliance chains.
The complete architecture diagram is shown as



Our datasets are sourced from the website kaggle, which offers datasets.

III. TECHNIQUE USED OR ALGORITHM USED

3.1 EXISTING TECHNIQUE: -

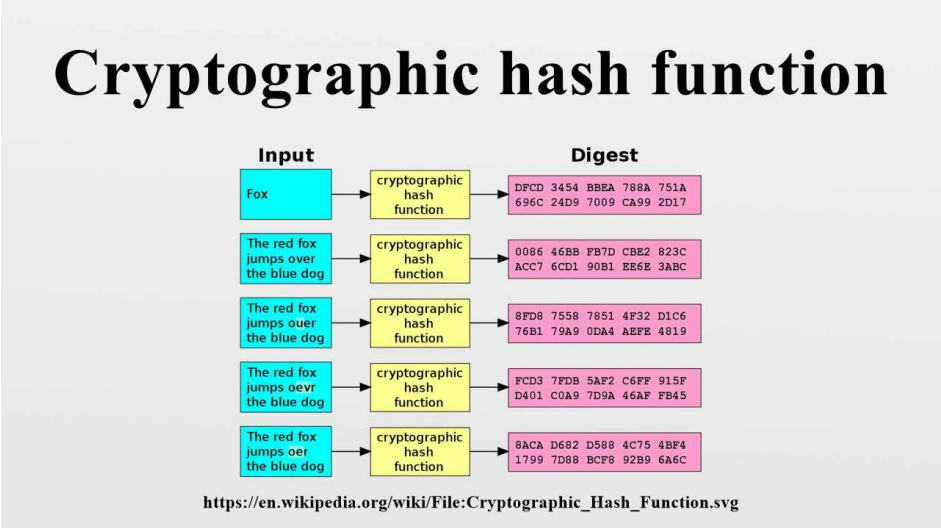
Encryption using Homomorphism
A cryptographic technique called homomorphic encryption makes it possible to do calculations on encrypted material without having to first decrypt it. This maintains privacy while enabling computations on sensitive data to be done securely. The system yields results that match operations on the plaintexts and supports operations such as addition and multiplication on ciphertexts. Different varieties of homomorphic encryption exist based on the kinds of operations that are supported, such as fully homomorphic and partially homomorphic. Despite their strength, homomorphic encryption techniques can be computationally demanding and may need to be optimized before being used in real-world cloud storage auditing situations.

3.2 PROPOSED TECHNIQUE USED OR ALGORITHM USED:

Cryptographic Hash Functions

Secure Hash Algorithm 256 (SHA-256) and other cryptographic hash functions are crucial parts of cloud storage and public auditing projects. These hash algorithms are essential for maintaining the security and integrity of data. Cryptographic hash functions can be used to create distinct hash values, or digests, based on the content of data saved in the cloud. These hash values function as the original data's checksums or fingerprints. A change in the data, no matter how tiny, will cause the hash function's avalanche effect to produce an entirely new hash value. This feature makes it possible to detect unwanted data modifications or tampering with stored data quickly and accurately. When it comes to auditing, the effectiveness of cryptographic hash functions like SHA-256 is especially vital because enormous amounts of data must be processed and validated. These hash functions are quick and easy to use, but they offer robust cryptographic security since they are not susceptible to collisions. This ensures the dependability of integrity checks because it is computationally impossible to identify two distinct inputs that result in the same hash value. Furthermore, the non-reversible nature of cryptographic hash functions makes it nearly hard to recreate the original input data using just the hash result. The confidentiality of the audited data is safeguarded by this attribute.

From the plotting of Cryptographic Hash Functions we get the following figure:



IV. IMPLEMENTATION

The project's goal was to create a solid public auditing program for cloud storage that was built on a reliable alliance network. There were several crucial milestones in the implementation. Initially, the alliance chain was established using a distributed ledger technology framework, which guaranteed security and transparency throughout the auditing procedure. Because Hyperledger Fabric is well-suited for building permissioned blockchain networks, it was used. Second, Solidity was used to create smart contracts that allowed for automatic alliance chain auditing procedures. These agreements made it easier to verify access control and storage integrity. Thirdly, integration of cryptographic techniques like homomorphic encryption ensured privacy and secrecy by safeguarding data during auditing. Furthermore, web technologies like React.js were used to create an intuitive user experience that gave stakeholders easy access to audit logs and verification results. Finally, a thorough testing and assessment process was carried out to confirm that the plan is effective in improving cloud storage security and accountability. This approach promoted trust and dependability among users and service providers alike by utilizing cutting-edge technologies to overcome important difficulties in cloud storage auditing.

V. RESULTS

One major step in guaranteeing data security and integrity in cloud contexts is the creation of a reliable alliance-based public auditing program for cloud storage. This plan uses the combined strength and standing of several impartial auditors, or nodes within an alliance, to confirm the accuracy of data kept on cloud storage. Compared to depending on a single auditor, the plan lowers the danger of collusion or compromise by allocating auditing work among alliance members. Furthermore, by allowing for decentralized verification, this method improves accountability and transparency in cloud storage. Typically, the strategy uses cryptographic methods like Merkle hashing and homomorphic encryption to enable effective and secure auditing without

necessitating direct access to private user data. Auditors are able to confirm the accuracy of data and identify any illegal changes or corruption, giving users confidence and evidence of the accuracy of the data. Because of its scalable nature, this auditing scheme can effectively handle large-scale cloud storage systems.This system addresses issues regarding the integrity and security of cloud-stored data by introducing a layer of confidence and dependability into the auditing process through the establishment of a credible alliance of auditors. In the end, this strategy gives cloud customers more control over their data and encourages them to feel comfortable using cloud storage services for private data .

VI. CONCLUSION

In this paper, we proposed an alliance-chain-based audit scheme CACPA composed of TPA nodes, by introducing blockchain technology into the traditional cloud storage scheme. The key idea is converting semi-trusted TPA nodes into a credible TPA group organized by alliance chain, so as to solve some security issues of TPA, such as: forged audit report, untimely audit, collusion attacks between TPA and cloud service provider, and single point failure problem of TPA. To achieve this goal, we designed a novel incentive mechanism to enforce honest and reliable behaviors of TPA, which gives birth to a new token-based consensus mechanism POTE for improved fairness. We presented our detailed system design and block structure, as well as our audit scheme specification and smart contract program. By comparison to related work, our scheme provides better security without sacrificing its efficiency when it comes to implementation.

VII. FUTURE ENHANCEMENTS

Future developments for reliable alliance chain-based public auditing programs for cloud storage might concentrate on enhancing performance and scalability to effectively manage higher data volumes. In order to ensure wider adoption and dependability in cloud storage environments, it is also possible to improve security, trust, and transparency in the auditing process by incorporating cutting-edge privacy-preserving techniques and investigating novel blockchain consensus algorithms.

VIII. REFERENCES

1. J. Xue, C. Xu, J. Zhao and J. Ma, "Identity-based public auditing for cloud storage systems against malicious auditors via blockchain", Sci. China Inf. Sci., vol. 62, no. 3, pp. 1-16, Mar. 2019.
2. H. Yang, X. Wang, C. Yang, X. Cong and Y. Zhang, "Securing content-centric networks with content-based encryption", J. Netw. Comput. Appl., vol. 128, pp. 21-32, Feb. 2019.
3. Y. Zhang, C. Xu, X. Lin and X. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors", IEEE Trans. Cloud Comput., vol. 9, no. 3, pp. 923-937, Jul. 2021.
4. Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation", IEEE Trans. Inf. Forensics Security, vol. 12, no. 3, pp. 676-688, Mar. 2017.
5. C. C. Erway, "Dynamic provable data possession", ACM Trans. Inf. Syst. Secur. (TISSEC), vol. 17, no. 4, pp. 1-29, 2015.
6. J. Shen, J. Shen, X. Chen, X. Huang and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data", IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402-2415, Oct. 2017.
7. C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang and J. Chen, "MuR-DPA: Top-down levelled multi-replica Merkle hash tree based secure public auditing for dynamic big data storage on cloud", IEEE Trans. Comput., vol. 64, no. 9, pp. 2609-2622, Sep. 2015.
8. Y. Lin, J. Li, X. Jia and K. Ren, "Multiple-replica integrity auditing schemes for cloud data storage", Concurrency Comput. Pract. Exper., vol. 33, no. 7, pp. 1, Apr. 2021.
9. 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, Mar. 2017.
10. J. Yuan and S. Yu, "Public integrity auditing for dynamic data sharing with multiuser modification", IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717-1726, Aug. 2015.
11. C. Po-Jen and H.-C. Chuang, "Effective privacy preservation in third-party cloud storage auditing", J. Inf. Sci. Eng., vol. 35, no. 1, pp. 125-135, 2019.
12. T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes", IEEE Internet Things J., vol. 4, no. 6, pp. 1844-1852, Dec. 2017.
13. Y. Wu, X. Lin, X. Lu, J. Su and P. Chen, "A secure light-weight public auditing scheme in cloud computing with potentially malicious third party auditor", IEICE Trans. Inf. Syst., vol. 99, no. 10, pp. 2638-2642, 2016.
14. K. Qian and H. Huang, "A new identity-based public auditing against malicious auditor in the cloud", Int. J. Embedded Syst., vol. 11, no. 4, pp. 452-460, 2019.
15. X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang and Y. Zhang, "CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors", IEEE Trans. Cloud Comput., vol. 9, no. 4, pp. 1362-1375, Oct. 2021.