IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

Enhancing Cloud Storage Security with Public Auditing

A. Lakshmipathi Rao[1], Paka Chandu Yadav[2], MD Sohail[3], Rohan Lambe[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2-4]

ABSTRACT: We propose a credible alliance-chain-based public auditing scheme (CACPA) to properly address the trust problem of third-party auditor (TPA) in the traditional audit scheme for cloud storage. Based on the non-tamperability and traceability of blockchain, we design a novel incentive mechanism to enforce honest and reliable behaviors of TPA. The basic idea is to organize TPA as a group of blockchain nodes conducting mutual surveillance. Other nodes to maintain good reputation of the group will inspect any behavior of a TPA node, and malicious behaviors will bring severe punishments. Accordingly, we develop system model of the proposed CACPA, as well as smart contracts to deal with transactions-related issues, such as dispute resolution. Finally, performance evaluation validates that our scheme enjoys acceptable efficiency and suits for real-world applications.

KEY WORDS: CACPA Third-Party Auditor (TPA) Trust Problem Blockchain Traceability Non-Tamper ability Incentive Mechanism Mutual Surveillance Reputation Management Malicious Behaviour Punishment System Model Smart Contracts Transaction Dispute Resolution Performance Evaluation

I. INTRODUCTION

After years of development, cloud storage has been widely used in our lives as a new storage model. Under this model, users outsource their data to cloud servers via the Internet, which removes the burden of consuming large local storage costs on user side. Nevertheless, this data outsourcing model also brings some security issues that the most important one is data integrity. After user's data is uploaded to cloud server, it will be deleted in order to save their local storage. In this situation, users will lose control of their own data, and it is hard to check whether their data is intactly stored by the cloud server. Furthermore, data damage and data loss may occur under various circumstances, such as fire accidents, damage to hard disks, hacker attacks, and so on. Besides, cloud service providers may delete some data in order to reduce storage costs, or hide data corruption incidents to maintain a good reputation. Therefore, it is necessary to verify data integrity regularly, but this inevitably increases computation and communication burden of users, contradicting the original intention of saving resources on user side. As a result, **third-party auditors** (**TPA**s) have been introduced that can regularly complete data integrity audits. In the literature, many related research works have been proposed, such as: public verification, support of dynamic operations multiple-replica integrity auditing multi-user setting and privacy preservation.

II. LITERATURE SURVEY

Title: Blockchain-based public integrity verification for cloud storage against procrastinating auditor
Year: 2021
Author: Y. Zhang, C. Xu, X. Lin and X. Shen
Description: The deployment of cloud storage services has significant benefits in managing data for users. However, it also causes many security concerns, and one of them is data integrity. Public verification techniques can enable a user to employ a third-party auditor to verify the data integrity on behalf of her/him, whereas existing public verification schemes are vulnerable to procrastinating auditors who may not perform verifications on time. Furthermore, most of public verification schemes are constructed on the public key infrastructure (PKI), and thereby suffer from certificate management problem. In this paper, we propose a certificate less public verification scheme against procrastinating auditors (CPVPA) by using blockchain technology. The key idea is to require auditors to record each verification result into a transaction on a blockchain. Because transactions on the blockchain are time-sensitive, the verification can be time-stamped after the transaction is recorded into the blockchain, which enables users to check whether auditors perform the verifications at the prescribed time. Moreover, CPVPA is built on certificate less cryptography, and is free from the certificate management problem. We present rigorous security proofs to demonstrate the security of CPVPA, and conduct a comprehensive performance evaluation to show that CPVPA is efficient.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

Title: Multiple-replica integrity auditing schemes for cloud data storage.
Year: 2021
Author: Y. Lin, J. Li, X. Jia and K. Ren
Description:
Cloud computing has been an essential technology for providing on-demand computing resources as a service on the Internet. Not only enterprises but also individuals can outsource their data to the cloud without worrying about purchase and maintenance cost. The cloud storage system, however, is not fully trustable. Cloud data integrity auditing is crucial for defending against the security threats of data in the untrusted multicloud environment. Storing multiple replicas is a commonly used strategy for the availability and reliability of critical data. In this paper, we summarize and analyze the state-of-the-art multiple-replica integrity auditing schemes in cloud data storage. We present the system model and security threats of outsourcing data to the cloud with classification of ongoing developments. We also summarize the existing data integrity auditing schemes for multicloud data storage. The important open issues and potential research directions are addressed.

Title: CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors
Year: 2021
Author: X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang and Y. Zhang
Description:
Wireless body area networks (WBANs) rely on powerful cloud storage services to manage massive medical data. As precise medical diagnosis analysis is heavily based on these medical data, any altered medical data may cause severe consequences, the integrity of outsourced medical data has become the most concerning security issue. Up to date, most existing public auditing mechanisms have been proposed to check the data integrity, but they could not achieve conditional identity privacy, any patient would not like others to know his/her real identity corresponding to certain serious disease, and some malicious patients should be revoked timely due to misbehaviors. Additionally, they are vulnerable to malicious auditors, by colluding with the cloud server to cheat patients. In this paper, we propose a conditional identity privacy-preserving public auditing (CIPPPA) mechanism for cloud-based WBANs. CIPPPA is the first public auditing mechanism achieving conditional identity privacy of patients in WBANs, the real identity of a patient is unknown to anyone in cloud-based WBANs other than the private key generator (PKG). We attempt to integrate Ethereum blockchain into CIPPPA, which gives assistance to patients for validating malicious auditing behaviors. Formal security analysis and performance evaluation demonstrate that CIPPPA is practical for cloud-based WBANs.

Nowadays, wireless body area networks (WBANs) have become increasingly prevalent. WBANs rely on various kinds of medical sensors and wireless communication technologies to collect and transmit medical data, and flexibly realize remote health status monitoring of patients. Due to the sharp increase in the massive medical data of WBANs, these medical data need to be processed promptly, and the feedback messages from doctors also need to be quickly transmitted. However, it is very difficult to achieve these goals only relying on the traditional WBANs, since they have limited calculation and storage capabilities.

Title: A survey on the security of blockchain systems
Year: 2020
Author: X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen
Description:
Since its inception, the blockchain technology has shown promising application prospects. From the initial cryptocurrency to the current smart contract, blockchain has been applied to many fields. Although there are some studies on the security and privacy issues of blockchain, there lacks a systematic examination on the security of blockchain systems. In this paper, we conduct a systematic study on the security threats to blockchain and survey the corresponding real attacks by examining popular blockchain systems. We also review the security enhancement solutions for blockchain, which could be used in the development of various blockchain systems, and suggest some future directions to stir research efforts into this area.
Although there are some recent studies on the security of blockchain, none of them performs a systematic examination on the risks to blockchain systems, the corresponding real attacks, and the security enhancements. The closest research work to ours is that only focuses on Ethereum smart contracts, rather than popular blockchain systems. From security programming perspective, their work analyzes the security vulnerabilities of Ethereum smart contracts, and provides a taxonomy of common programming pitfalls that may lead to vulnerabilities. Although a series of related attacks on

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

smart contracts are listed, there lacks a discussion on security enhancement. This paper focuses on the security of blockchain from more comprehensive perspectives.

Title: Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing
Year: 2020
Author: X. Xu, Y. Chen, Y. Yuan, T. Huang, X. Zhang and L. Qi
Description:
For the issue of users' sensibility to the QoS (Quality of Service) of multimedia applications, cloudlet has emerged as a novel paradigm which provides closer computing resources to users to improve the performance of multimedia applications and meet the QoS demands of users. However, the increasing users' requirements of migrating tasks pose a challenge to preserve the security and integrity of offloaded data which are processed by cloudlets. In view of this challenge, a blockchain-based cloudlet management method for multimedia workflow, named MWSM, is proposed in this paper. Technically, we first model each multimedia application as a multimedia workflow and formulate the multimedia workflow scheduling problem. Then, blockchain is adopted to secure the data integrity during the offloading procedure. Besides, NSGA-III (Non-dominated Sorting Genetic Algorithm III) is employed to realize the QoS enhancement and ELECTRE (Elimination Et Choix Tradulsant la REaltite) is utilized to solve the decision-making problems of the most optimal scheduling strategies. Finally, experimental evaluations are conducted to demonstrate the efficiency and potential of our proposed scheduling method.

Title: A survey on Ethereum systems security: Vulnerabilities attacks and defenses
Year: 2021
Author: H. Chen, M. Pendleton, L. Njilla and S. Xu
Description:
The blockchain technology is believed by many to be a game changer in many application domains, especially financial applications. While the first generation of blockchain technology (i.e., Blockchain 1.0) is almost exclusively used for cryptocurrency purposes, the second generation (i.e., Blockchain 2.0), as represented by Ethereum, is an open and decentralized platform enabling a new paradigm of computing Decentralized Applications (DApps) running on top of blockchains. The rich applications and semantics of DApps inevitably introduce many security vulnerabilities, which have no counterparts in pure cryptocurrency systems like Bitcoin. Since Ethereum is a new, yet complex, system, it is imperative to have a systematic and comprehensive understanding on its security from a holistic perspective, which is unavailable. To the best of our knowledge, the present survey, which can also be used as a tutorial, fills this void. In particular, we systematize three aspects of Ethereum systems security: vulnerabilities, attacks, and defenses. We draw insights into, among other things, vulnerability root causes, attack consequences, and defense capabilities, which shed light on future research directions.

III. EXISTING SYSTEM

Finally, because TPA can generate challenge information by its own choice, it may forge false audit information without detected by the user. Existing solutions are generally based on a trusted third party to defend against malicious TPA. In our CACPA model, we assume the availability of multiple TPAs, which inherently resolve the singe-point failure problem; besides, CACPA transforms the semi-trusted TPAs into a credible TPA collective by organizing TPAs as a group in alliance chain and developing dedicate smart contracts to regulate the behaviors of TPAs, so as to solve the problems mentioned above.

EXISTING SYSTEM DISADVANTAGES

- Less security.
- Less traceability and security of blockchain.

IV. PROPOSED SYSTEM

- KYC helps in identifying and preventing fraudulent activities. By knowing who their customers are, banks can better detect suspicious transactions and patterns that may indicate fraud.
- Many countries have laws and regulations requiring financial institutions to implement KYC procedures. Compliance with these regulations helps banks avoid legal penalties and ensures that they are operating within the law.
- All actions related to KYC data are recorded on the blockchain, enhancing transparency and accountability.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

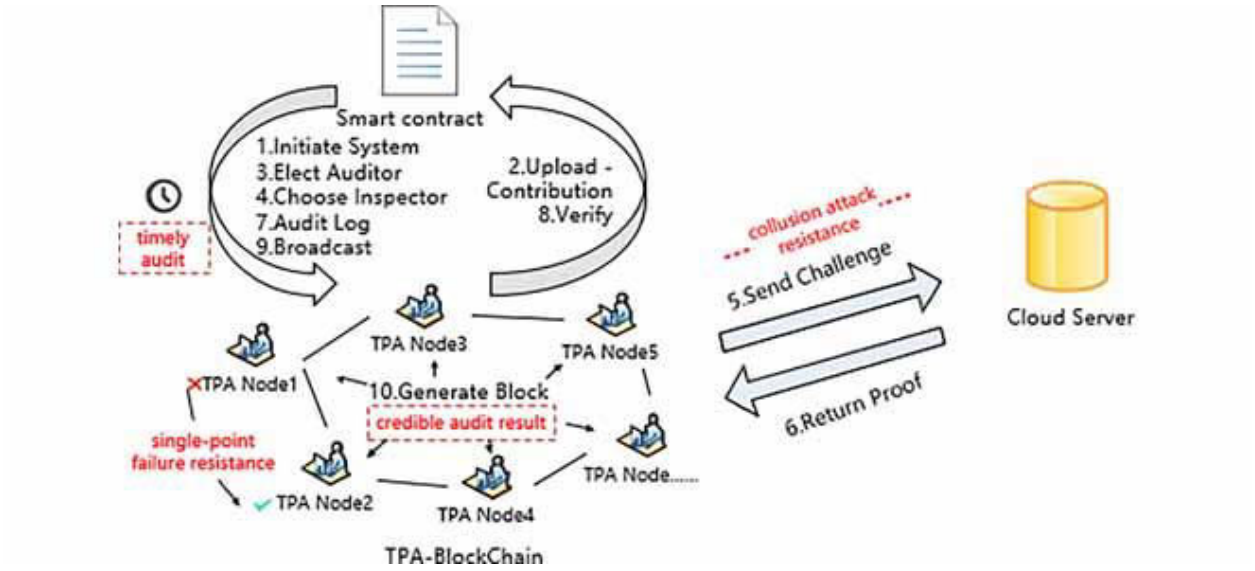
PROPOSED SYSTEM ADVANTAGES

- More Security.
- It more efficiency and authentication service.

We are committed to solving the dishonest behaviour of TPA in the traditional data auditing model through the non-tamperability, traceability and security of blockchain.

V. SYSTEM ARCHITECTURE

Fig:1 System Architecture



The diagram illustrates a blockchain-based cloud data auditing framework that ensures secure, decentralized, and trustworthy verification of data stored in the cloud. The system is initialized through a smart contract that manages tasks such as electing auditors, selecting inspectors, uploading contributions, verifying data, maintaining audit logs, and broadcasting results. Third Party Auditors (TPAs), organized as blockchain nodes, collaboratively handle audit operations. When a challenge is sent to the cloud server, it responds with a cryptographic proof, which TPAs validate to generate credible audit results. This process is resistant to collusion attacks and single-point failures, ensuring reliable and timely audits. Even if a TPA node fails, others maintain the audit process without disruption, highlighting the system's robustness and trustworthiness.

VI. METHODOLOGIES

Modules Name:

1. User Interface Design
2. Data Owner
3. Cloud Server Provider
4. Third Party Auditor
5. User
6. Admin

Modules Explanation :

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. 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.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

2. Data Owner

This is the second module of our project after successful registration is done Data Owner will try to access his account which should be activated by the Cloud Server Provider i.e., after the activation is done by the Cloud Server Provider then only he will be getting a key and his access rights to his registered mail, through which he can login. After entering to the home page Data Owner will have options like File upload, File download, File update basing on his access rights he can chose his actions.

3. Cloud Server Provider

This is the third module of our project which plays a crucial role in the entire project after login in to this module the Cloud Server Provider will have three options like (i) Data Owner's where he can see the no of Data Owner's in the cloud and he can activate them by providing necessary access rights. (ii) Data Owner's Request where he can give them access for the user requests. (iii) Users where he can see the no of users in the cloud and he can activate them by providing necessary access rights.

4. Third Party Auditor

This is the fourth module of our project if a user tries to upload the previous file which he already uploaded in the cloud it will be accepted by the cloud as we are using Duplicatable technique in our project and verify all files. Moreover we are providing strict security constraints to the data uploaded by the Data Owner, the data will be stored in the cloud database in an encrypted format, so that it can prevent from malicious cloud owners.

5. User

This is the fifth module of our project after successful registration is done user will try to access his account which should be activated by the Cloud Server Provider i.e., after the activation is done by the Cloud Server Provider then only he will be getting a key and his access rights to his registered mail, through which he can login. After entering to the home page user will have options like see the all Data Owner files and File download basing on his access rights he can chose his actions.

6. Admin

In this final module of our project after successful admin login attempt admin will be redirected to his page where he will be finding the three options like UPLOADS, DOWNLOADS & UPDATES and All Data Owner Details, All User Details, All Request Details On clicking on each hyperlink he will be able to see what operations cloud users and Data Owners are doing in the cloud.

VII. ALGORITHM USED

EXISTING TECHNIQUE: -

Since a Third-Party Auditor (TPA) has the ability to generate challenge data independently, there is a risk of falsifying audit information without the user noticing. Conventional solutions typically rely on a single trusted entity to mitigate malicious actions by TPAs. However, in the CACPA model, multiple TPAs are incorporated to eliminate single-point failure vulnerabilities. Furthermore, CACPA enhances trustworthiness by converting semi-trusted TPAs into a reliable collective through alliance-chain-based structuring. Dedicated smart contracts are implemented to govern their operations, ensuring accountability and addressing the existing challenges effectively.

PROPOSED TECHNIQUE USED: - KNOW YOUR CUSTOMER:

A Third-Party Auditor (TPA) plays a crucial role in cloud storage, helping to significantly minimize users' computational and communication burdens. Our approach focuses on addressing dishonest practices in traditional data auditing by leveraging the blockchain's non-tamperability, traceability, and security. Specifically, TPAs are integrated into an alliance chain where they monitor each other to uphold their collective reputation, ensuring credibility within the system. We define a detailed structural framework and incentive mechanism for the blockchain while also implementing smart contracts to regulate operations within our proposed scheme..

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

VIII. EXPERIMENTAL RESULTS

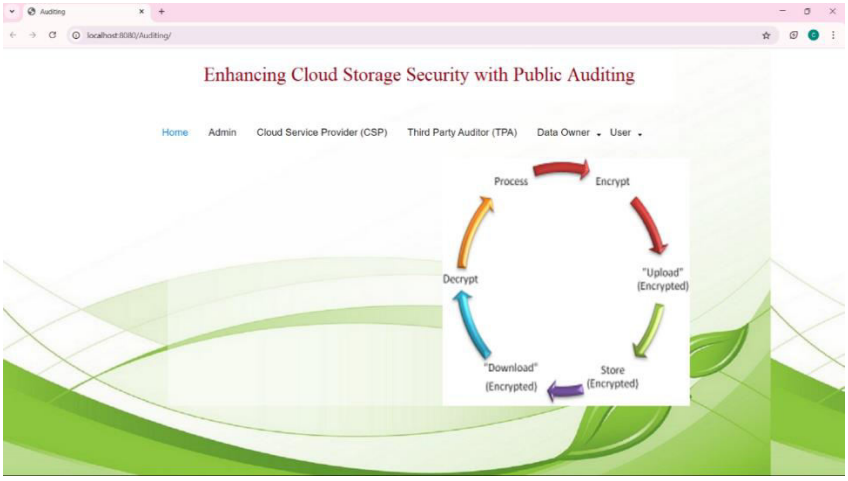


FIGURE2: HOME PAGE

Figure3: USER LOGIN

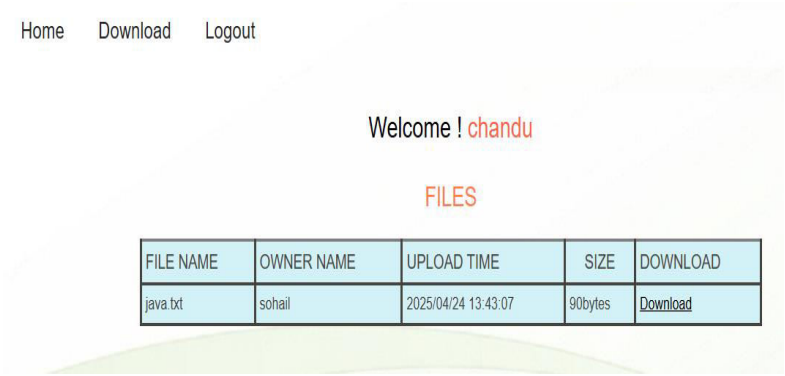


FIGURE 4: USER ACCESS

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

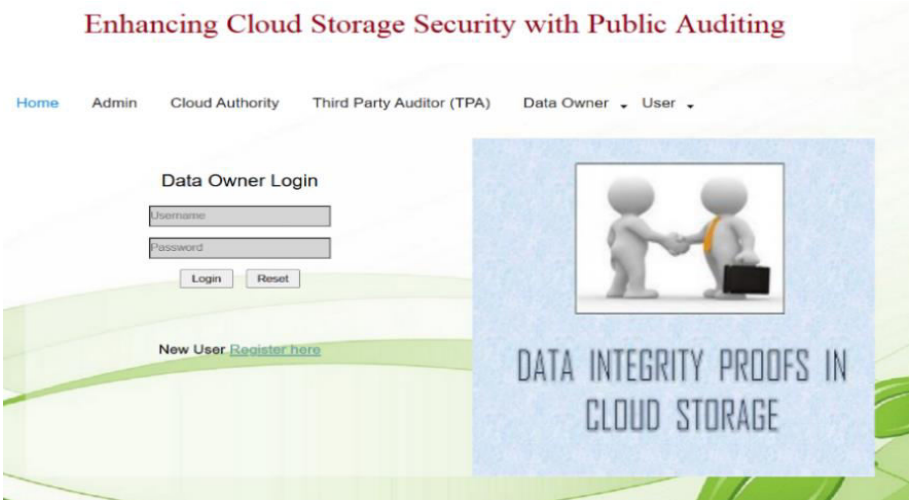


FIGURE 5: DATA OWNER LOGIN

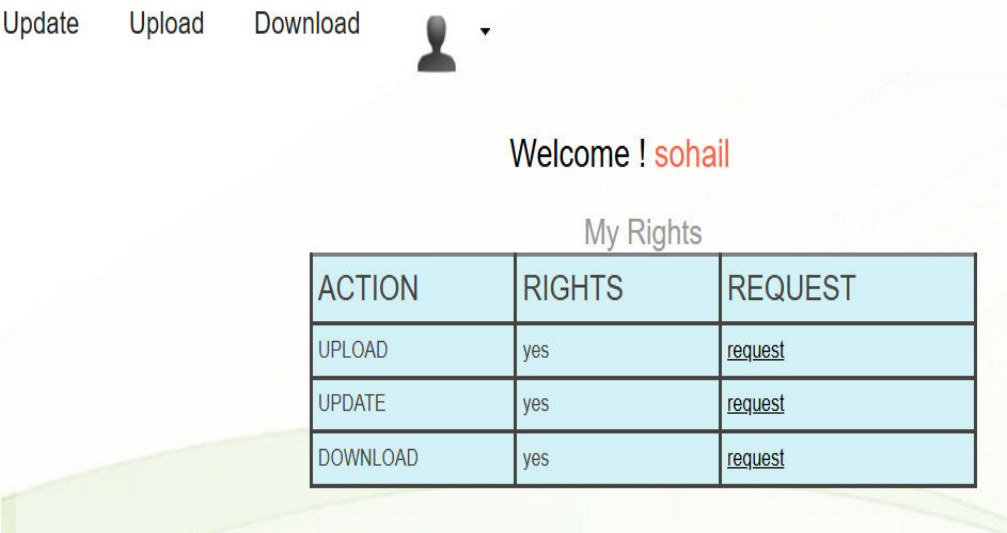


FIGURE **6**: DATA OWNER RIGHTS

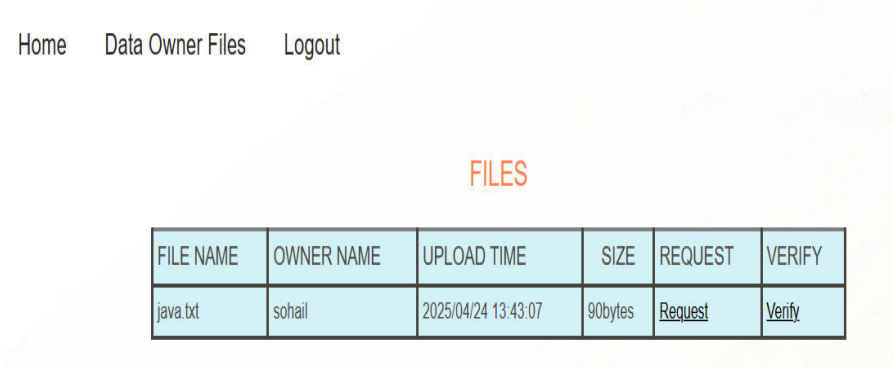


FIGURE 7: TPA ACCESS

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

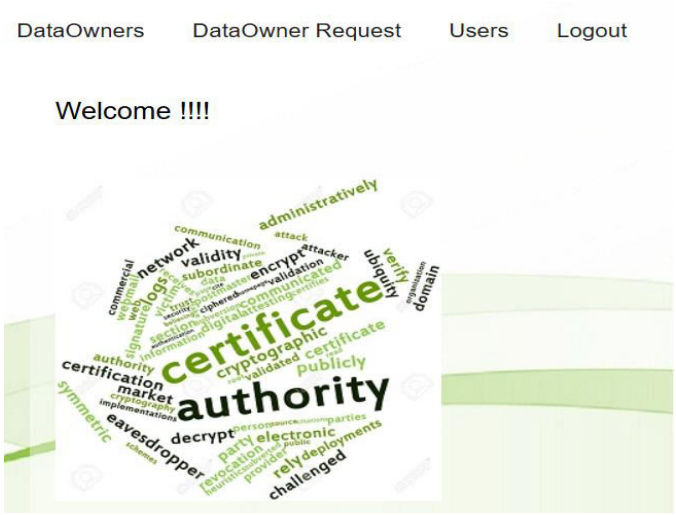


FIGURE 8 : CLOUD SERVICE PROVIDER PAGE

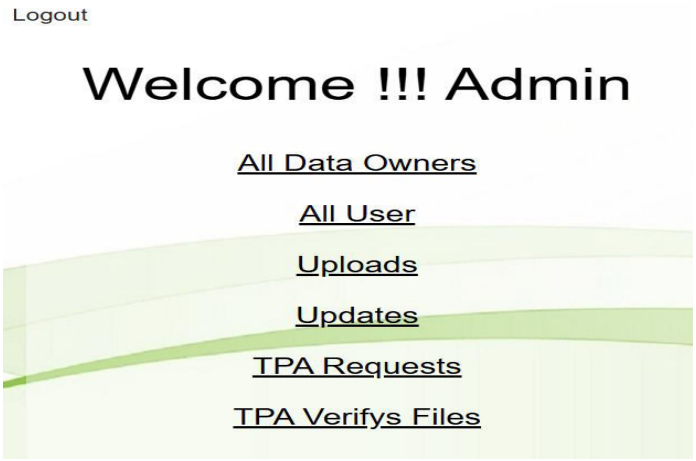


FIGURE 9: ADMIN PAGE

IX. 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.

X. FUTURE ENHANCEMENT

For the future work, we will focus on adjustment and deployment of the underlying framework of our CACPA to other blockchain based application scenarios, such as smart grid.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203107

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.
16. X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, "A survey on the security of blockchain systems", Future Gener. Comput. Syst., vol. 107, pp. 841-853, Jun. 2020.
17. L. M. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms", Proc. 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. (MIPRO), pp. 1545-1550, May 2018.
18. Z. Xiong, Y. Zhang, D. Niyato, P. Wang and Z. Han, "When mobile blockchain meets edge computing", IEEE Commun. Mag., vol. 56, no. 8, pp. 33-39, Aug. 2018.
19. N. Fotiou, V. A. Siris and G. C. Polyzos, "Interacting with the Internet of Things using smart contracts and blockchain technologies" in Security Privacy and Anonymity in Computation Communication and Storage, Melbourne, NSW, Australia:Springer, Dec. 2018.
20. Y. Zhang, R. H. Deng, X. Liu and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing", Inf. Sci., vol. 462, pp. 262-277, Sep. 2018.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com