Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 2: 2025
ISSN : **1906-9685**

Securing Data with Quad Merkle Tree and Blockchain Technology

#1.K.JAYA KRISHNA, #2. J. DURGA BHAVANI

#1 Assistant Professor

#2 MCA Scholar

DEPARTMENT OF MASTER OF APPLICATIONS

QIS COLLEGE OF ENGINEERING AND TECHNOLOGY

Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract

Increasing numbers of users are outsourcing data to the cloud, but data integrity is an important issue. Due to the decentralization and immutability of blockchain, more and more researchers tend to use blockchain to replace third-party auditors. This paper proposes a data integrity system based on blockchain expansion technology that aims to solve the problem of high cost for blockchain network maintenance and for user creation of new blocks caused by the rapid growth of blocks in the data integrity audit scheme of existing blockchain technology. Users and cloud service providers (CSP) deploy smart contracts on the main chain and sub-chains. Intensive and frequent computing work is transferred to the sub-chain for completion, and the computation results of the sub-chain are submitted to the main chain periodically or when needed to ensure its finality. The concept of non- interactive audit is introduced to avoid affecting user experience due to the communication with the CSP during the audit process. In order to ensure data security, a reward pool mechanism is introduced. Comprehensive analysis from aspects such as storage, batch auditing and data consistency proves the correctness of the scheme. Experiments on the Ethereum blockchain platform demonstrate that this scheme can effectively reduce storage and computational overhead.

Introduction:

Cloud computing is a distributed computing model based on a large shared virtualized computing resource pool, it helps users use powerful computing and storage resources. And it can greatly reduce the burden of data storage on hardware and software for users, which encourages many enterprises and individuals to store their data on cloud servers. Despite the great success of cloud storage, it also faces various challenges and its security, reliability and privacy have always been a serious issue .After the user stores the data on the cloud server, the

server provider may damage or delete the user data due to various factors , verifying the integrity of outsourced data becomes a crucial issue in cloud storage. Remote data integrity audit technology is very convenient and safe to help users check the integrity of data stored in outsourced There fore, the essence of cloud data security is how cloud storage providers (CSP) can establish trust with users. Cloud device failures, illegal attacks, and CSPs may be bribed to view user data, all of which can lead to illegal infringement of user data. Furthermore, even if the user data is damaged, the user may not be able to hold the CSP accountable effectively, since the CSP may evade responsibility and deny it This is due to the lack of trust between the two parties, resulting in the party being questioned being unable to come up with evidence that would convince the other party. In addition, the current law on cyber security is not sound, which makes it difficult for users to obtain due compensation. In traditional cloud auditing schemes, there is an entity called auditors (often referred to as third-party auditors, or TPA) which implement public audits . The TPA accept audit mandates from data owners and perform as instructed. In each of these methods, a trusted Third Party Auditor (TPA) must be found to assist the user in auditing, but in reality it is difficult to find fully trusted third-party auditors. For example, TPA will also partner with CSP for some ulterior purpose to hide data corruption, or with data owners to avoid penalties. The emergence of block chain can solve this problem very well. Block chain has the properties of decentralization, tamper resistance, consistency and traceability. Therefore, information stored on the block chain is open and transparent. In recent years, more and more researchers use block chain to replace third-party auditors . Although the use of block chain as a trusted third-party auditor can well address users' concerns in cloud computing environments, but the rapid growth of blocks will lead to high cost for block chain network maintenance and for user creation of new blocks . To solve the above problems, a data integrity verification scheme based on block chain expansion technology is proposed. By slowing the growth of the block chain, reducing storage and calculation costs. In particular, our contribution can be summarized in three aspects:

 A data integrity audit protocol based on plasma smart contracts is proposed. By introducing plasma sub-chains and deploying smart contracts on the main chain and sub-chains, the storage pressure of the main chain can be reduced and the growth rate can be slowed down through this protocol. TPA audit protocol can be executed with low computational and communication overhead.

 A batch auditing scheme is proposed, the scheme can batch-process multiple audit tasks at the same time. In order to avoid affecting the user experience due to the communication with the CSP during the audit process as much as possible, the concept of non-interactive audit is introduced. For the sake of ensuring the correctness of the audit, the reward pool

mechanism is adopted, and the verification node can obtain reasonable rewards.

 An analysis of the security of the scheme shows that it can achieve the expected security objectives. Numerous experiments on the ether block chain also showed the efficiency and effectiveness of the scheme.

LITETATURE SURVEY

1.Title: A Blockchain-Based Flexible Data Auditing Scheme for the Cloud Service Author: FAN Kefeng, LI Fei, YU Haiyang, YANG Zhen Year: 01 November 2021 Now-a-days, with the continuous development of information technology and network facilities, as well as the intersection of information technology and human life, global data starts to explosively grow. According to statistics, the total amount of global information was 21.6ZB in 2017, and it is expected to reach 44ZB in 2020.The amount of data in various industries and fields such as industry, finance, and retail is increasing every day. The continuous surge in data has driven the vigorous development of the big data industry. cloud storage technology has become a hot topic, and an increasing number of users are concerned with the security of their data in the cloud. Many auditing schemes on the cloud are proposed and the introduction of a third-party auditor to assist users in verifying the integrity of cloud data. As a centralized node, the third party auditor has to communicate with all cloud users and cloud service providers, which becomes the bottleneck of the whole scheme. To solve this problem, we design a blockchain-based flexible cloud data auditing scheme. In our scheme, a decentralized auditing framework is proposed to eliminate the dependency on the third-party auditor, which increases the stability, security and performance of the whole scheme. Since the cloud service provider can automatically generates auditing proofs, our scheme can relieve the communication burdens of the cloud service provider. The proposed scheme also adapts the Merkle Hash tree to improve the verification performance. Security analysis and experiments show that the proposed scheme is secure and has better stability and verification efficiency. This paper designs a flexible cloud auditing scheme based on consortium chain. This paper constructs a decentralized auditing framework, which removes the reliance of the Third-party auditor and ensures the security andstability of the entire scheme. The auditing proof stored on the auditing consortium chain is valid, Page 11 of 90 tamper-proof, authentic and traceable. Merits:- The user or Third-party auditor can perform auditing without challenging the Cloud service provider, which reduces the communication costs during auditing. The security analysis shows the security of this scheme under the random oracle model. Their scheme's performance analysis shows that their work can effectively improve the performance of verification whilst reducing the computational cost of the overall scheme. Demerits:- Due to the large scale of data storage in cloude data can be decentralise and can be difficult to aquire the required information in database.

2.Title:-Blockchain Based Data Integrity Verification for Large-Scale IoT Data

Auther :- Haiyan Wang; Jiawei Zhang Year:- July 2019 A data verification integrity scheme based on blockchain and bilinear mapping is proposed in this paper. Firstly,They combine smart contracts with bilinear mapping and propose a new data integrity verification framework. Slice the data into shards, and calculate metadata of each data shard for smart contract to execute verification. On this basis, the corresponding data integrity verification protocol and algorithm are proposed. They also introduce provable update mechanisms to deal with the dynamic property of IoT data in their scheme. Secondly, proposing a prototype system with an edge computing to process the IoT data. Experimental results finally demonstrate that the proposed BB-BIS outperforms existing blockchain based methods in terms of computational cost and communication overhead for large-scale IoT data. Merits:- A blockchain based data integrity verification framework is proposed for large-scale IoT data. Prototype system is built with an edge computing processor in the vicinity of the IoT devices to preprocess the large-scale IoT data so that communication cost and computation burden can be reduced significant. Page 12 of 90 Demerits:- Traditional distributed database systems cannot satisfy the requirements of data management in the IoT environment, and Cloud Storage Services (CSSs) arise consequently.

3.Title:- Blockchain-Based Data-Driven Smart Customization Authors:- Ang Liu, Yuchen Wang ,Xingzhi Wang Year:- 10 October 2021 The rapid development of cyber-physical systems (CPS) and big data, product customization is evolving from traditional mass customization to data-driven smart customization. Data-driven smart customization is a new paradigm that highly emphasizes the reconfiguration of products in the use phase. This paradigm calls for a new architecture to enhance collaboration to perform customization. This chapter proposes a blockchain-based data- driven smart customization framework, in which blockchain functions to maintain the evolved customization data and decentralized consensus among stakeholders. A case study of smart vehicle customization is conducted to demonstrate its efficacy. Merits:- It can enhance the new architecture to collaboration to perform customization.By using blockchain technology the data stored in cloud can be prevented from data theft ,data de-duplication and data decentralization as well. Demerits:- Eventually the big data can cause some data loss while storing large scale of information.

4.Title:- A Blockchain-Based Document Verification System for Employers Authors:- Kshitij Dhyani, Jahnavi Mishra, Subhra Paladhi ,I. Sumaiya Thaseen Year :- 28 Feb 2022 Academic institutions often maintain records and documents of the students enrolled within the institute. These records are greatly regarded by employers and Page 13 of 90 often verified before giving employment offers. While all the other sectors in academia are moving towards automation, this specific use case is still quite primitive in its functioning. Even when this is a regular activity undergone by academic institutes, methodologies with

vulnerabilities and reasonable overhead are employed. There is a need for a tamper-proof, reliable, and faster mode of document verification for employers which can be used on the go with complete reassurance for the authenticity of the provided documents. This paper puts forward a blockchain-based platform that allows academic institutes to offer a secure, dependable, cost-effective, and scalable verification of documents via a Web interface. The platform is built upon the logic written in solidity and utilizes the ethereum blockchain to enforce immutability of the document, and the backend is linked to the user interface using the web3.js library. Additionally, the platform offers a statistical comparison of these records to other students and assists the employer to assess the performance of the student being recruited. Merits:- One of the useful merit of this project research is tamper-proof, reliable, and faster mode of document verification for employers which can be used on the go with complete reassurance for the authenticity of the provided documents. By using blockchain technology,it allows academic institutes to offer a secure, dependable, cost-effective, and scalable verification of documents via a Web interface. Demerits:- Storing large groups of students or employers data can be difficult to store in place. Due to this huge amount of information the cloud platform can store it in different slots which is difficult to retrieve the data.

5.Title:- Blockchain-based Integrity Verification of Data Migration in Multi-cloud Storage. Author:- Kun Xu, Weiwei Chen and Yanan Zhang Year :- December 2021 In this paper, to address the problem that data integrity is vulnerable to corruption in the process of multi-cloud data migration, a blockchain-based data Page 14 of 90 integrity verification scheme is proposed. In this scheme, a blockchain network is used instead of TPA, and for each migration, a multi-cloud broker will send integrity verification requests to the blockchain at three different times. A smart contract will verify the data integrity according to the RSA- based homomorphic verification tags. Then, the security of the scheme is analyzed. Finally, simulation experiments and tests are conducted on Ethereum, and the results prove the feasibility of the scheme. Merits:- One of useful and required merits of this project is avoiding third party applications. While using TPA the data that stored in the cloud platform can be loss or may theft by unauthorised people. To reduce this data theft they used blockchain technology which is secure for data migration in multiple cloud storages. Demerits:- These are the demerits that comes under this project article. ¬ Increased complexity: The use of blockchain technology and smart contracts may add complexity to the data migration process, potentially leading to increased costs and difficulties in implementation. ¬ Scalability concerns: Blockchain networks can be limited in terms of scalability, which may impact the performance of the data integrity verification scheme, particularly for large-scale data migrations. ¬ Security risks: While blockchain technology is generally considered secure, it is not immune to risks.

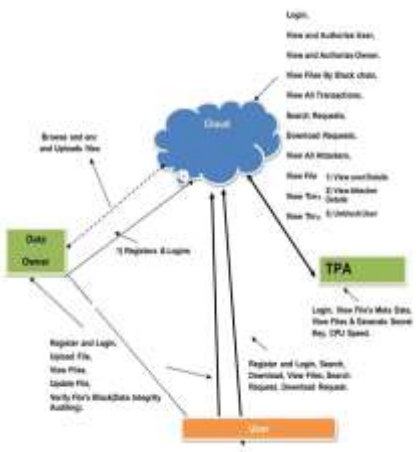
Potential vulnerabilities in the smart contract or blockchain network could compromise the security of the data integrity verification scheme. ¬ Dependence on blockchain network: The scheme's reliance on a blockchain network may introduce dependencies on the network's availability, ¬ performance, and security, which could impact the overall reliability of Page 15 of 90 the data integrity verification process.

6.Title:- Blockchain data-based cloud data integrity protection mechanism Authors :- Peng Cheng Wei , Dahu Wang , Yu Zhao , Sumarga Kumar Sah Tyagi , Neeraj Kumar Year:- January 2020 This paper uses mobile agent technology to deploy distributed virtual machine proxy model in the cloud. Through virtual machine agent, multi- tenant can cooperate with each other to ensure data trust verification, and complete virtual data storage, monitoring and verification through virtual machine proxy mechanism. Waiting for tasks, this is also a necessary condition for building a blockchain integrity protection mechanism. The blockchain-based integrity protection framework is built by. Merits:- Improved data trust verification is one of the merits comes under this project article. The use of virtual machine agents enables multi-tenant cooperation, ensuring data trust verification and secure data storage. Virtual machine proxy mechanism allows for real-time monitoring and verification of data, ensuring data integrity and security. Demerits:- Complexity is one of the demerits of this article .The integration of mobile agent technology and blockchain may add complexity to the system, potentially leading to increased costs and difficulties in implementation.

7.Title:- Decentralized big data auditing for smart city environments leveraging blockchain technology Authors:- Haiyang Yu; Zhen Yang; Richard O. Sinnott Year:- 20 December 2018 Nowadays, smart cities demand big data collection and the ability to analyze big data using intelligent algorithms such as machine learning. These depend greatly on the quality and the reliability of data. In this paper, we investigate big data integrity auditing in cloud environments to meet the challenges of secure smart city Page 16 of 90 infrastructures. A blockchain-based remote data integrity auditing scheme for the cloud has been proposed. We design a decentralized auditing architecture and a novel blockchain instantiation named the Data Auditing Blockchain (DAB) to improve the stability and reliability of the whole scheme. By introducing the DAB, the proposed scheme can trace all of the auditing history and allow all data files to be verified by any data owner or user at any time. The proposed scheme is further extended to support batch verification of multiple auditing proofs and dynamic auditing. The security analysis demonstrates that the proposed scheme is both secure and privacy- preserving. The performance evaluation shows that our scheme is also efficient compared with the state of the art. Merits: - The use of blockchain technology provides a decentralized and reliable auditing

architecture, ensuring data integrity and security. Data Auditing Blockchain (DAB) allows for tracing all auditing history, providing a transparent and tamper-proof record of data transactions. Demerits: - Performance overhead is one of the demerits of this project article. Using of blockchain and auditing mechanisms may introduce performance overhead, potentially impacting system performance and efficiency. Using of blockchain technology may lead to data duplication, potentially increasing storage requirements and impacting system efficiency. This is also the demerit of this project research

System Architecture:



Module Description:

Data Owner: In this module, the data owner uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Upload File, View Files, Update File, Verify File's Block(Data Integrity Auditing).

Cloud:The Cloud manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, View and Authorize User, View and Authorize Owner, View Files By Block chain, View All Transactions, Search Requests, Download Requests, View All Attackers, View File Rank Chart, View Time Delay Results, View Throughput Results.

User: In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, Search, Download, View Files, Search Request, Download Request.

TPA – responsible for Login, View File's Meta Data, View Files & Generate Secret Key, CPU Speed.

SCREENSHOTS:

This page is a Cloud Server Login interface from the project titled “Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management.” The purpose of this page is to authenticate cloud server users by requiring them to enter their name, password, and select the appropriate cloud server from a dropdown menu. A submit button is provided to complete the login process. This login interface is part of a larger system architecture that includes modules for Data Owner, Proxy Server, Cloud Server, and End User, all working together to support a cloud-based solution aimed at efficiently mitigating Distributed Denial of Service (DDoS) attacks through role-based access control and modular resource management

This page is the End User Login interface from the project “Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management.” It allows end users to log in by entering their Name, Password, and selecting a Cloud Server from a dropdown list. The login process ensures that only authorized end users can access services or resources on the cloud platform. This page is part of a multi role system architecture that also includes modules for Data Owners, Proxy Servers, and Cloud Servers.

This screenshot shows a web interface titled "Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management." It features a navigation bar with tabs for Home Page, Data Owner, Proxy Server, Cloud Server, and End User. The active tab is Proxy Server. Below, there's a Server Login form requiring a name and password, along with a "Register" link and a Submit button. The page also has a "Menu" section listing the same navigation options. The design includes a banner with tech-themed images.

This is the Data Owner Registration page for the Secure Data Transfer system, which focuses on minimizing financial costs during DDoS attacks in cloud environments. It allows new data owners to register by filling in required details such as username, password, email, mobile number, address, date of birth, location, cloud server, and profile picture. Once completed, they can click the REGISTER button to create an account and access cloud-based data transfer features.

This image shows a webpage titled "Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management." It appears to be related to cybersecurity, specifically focusing on protecting cloud systems from Distributed Denial of Service (DDoS) attacks. The webpage discusses a method to optimize resource management to defend against DDoS attacks while minimizing financial costs by scaling resources appropriately. It mentions the effectiveness of this approach through analyses and experiments, highlighting significant cost savings compared to existing methods. The page includes navigation links for Home Page, Data Owner, Proxy Server, CloudServer, and EndUser, suggesting a structured site with related content sections.

This page is the End User Login interface from the cloud-based project “Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management.” It prompts end users to log in by entering their Name, Password, and selecting a Cloud Server from a dropdown menu. A "Register" link is also provided for new users. This interface is part of a multi-role access system that enables secure and

role-based interactions within the cloud environment.

This page is the Data Owner Login interface for a system called Secure Data Transfer, which focuses on defending against DDoS attacks in cloud environments. It allows data owners to log in by providing their name, password, and selecting a cloud server where they want to store or manage data securely. The page also includes a register option for new data owners and is part of a larger system with sections for Proxy Server, Cloud Server, and End User management.

CONCLUSION As cloud computing and cloud storage technologies evolve faster and faster, the amount of data in cloud storage grows explosively, how can we ensure that the full information stored by users on cloud servers becomes an important topic for discussion . This article proposes a data integrity scheme based on block chain expansion technology. In our scheme, we use the block chain network to overcome some of the shortcomings of traditional auditing, improving the efficiency and security of the scheme. In addition, we introduce plasma sub-chain and deploy smart contracts on the main chain and sub-chain respectively. Through this protocol, the storage pressure of the main chain can be greatly reduced, the growth rate can be slowed down, the storage and computational overhead can be reduced, and the system performance can be improved. At the same time, the reward pool mechanism and the concept of non-interactive audit are introduced to ensure the correctness of the audit and avoid the interaction between the smart contract platform and the CSP during the contract execution process, and the solution can achieve the expected security goals.

REFERENCE

[1] K. Hao, J. Xin, Z. Wang, and G. Wang, ``Outsourced data integrity veri_cation based on blockchain in untrusted environment," World Wide Web, vol. 23, no. 4, pp. 2215_2238, Jul. 2020.

[2] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, ``One secure data integrity veri_cation scheme for cloud storage," Future Gener. Comput. Syst., vol. 96, pp. 376_385, Jul. 2019.

[3] H. Wang and J. Zhang, ``Blockchain based data integrity veri_cation for large-scale IoT data," IEEE Access, vol. 7, pp. 164996_165006, 2019.

[4] Z. Miao, C. Ye, P. Yang, R. Liu, B. Liu, and Y. Chen, ``A scheme for electronic evidence sharing based on blockchain and proxy re encryption," in Proc. 4th Int. Conf.

Blockchain Technol. Appl., Dec. 2021, pp. 11_16.

[5] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ``A blockchain-based _exible data auditing scheme for the cloud service,'' Chin. J. Electron., vol. 30, no. 6, pp. 1159_1166, Nov. 2021.

[6] K. He, J. Shi, C. Huang, and X. Hu, ``Blockchain based data integrity veri_cation for cloud storage with T-Merkle tree,'' in Proc. Int. Conf. Algo- rithms Archit. Parallel Process. Cham, Switzerland: Springer, Oct. 2020, pp. 65_80.

[7] Y. Lei, Z. Jia, Y. Yang, Y. Cheng, and J. Fu, ``A cloud data access authorization update scheme based on blockchain,'' in Proc. 3rd Int. Conf. Smart BlockChain (SmartBlock), Oct. 2020, pp. 33_38.

[8] Y. Yuan, J. Zhang, W. Xu, and Z. Li, ``Identity-based public data integrity veri_cation scheme in cloud storage system via blockchain,'' J. Supercomput., vol. 78, pp. 8509_8530, Jan. 2022.

[9] S. Wang, D. Zhang, and Y. Zhang, ``Blockchain-based personal health records sharing scheme with data integrity veri_able,'' IEEE Access, vol. 7, pp. 102887_102901, 2019.

[10] A. Liu, Y. Wang, and X. Wang, ``Blockchain-based data-driven smart customization,'' in Data-Driven Engineering Design. Cham, Switzerland: Springer, 2022, pp. 89_107.

[11] K. Dhyani, J. Mishra, S. Paladhi, and I. S. Thaseen, ``A blockchain based document veri_cation system for employers,'' in Proc. Int. Conf. Comput. Intell. Data Eng. Singapore: Springer, 2022, pp. 123_137.

[12] K. Xu, W. Chen, and Y. Zhang, ``Blockchain-based integrity veri_cation of data migration in multi-cloud storage,'' J. Phys., Conf. Ser., vol. 2132, no. 1, Dec. 2021, Art. no. 012031.

[13] G. Xu, S. Han, Y. Bai, X. Feng, and Y. Gan, ``Data tag replacement algorithm for data integrity veri_cation in cloud storage,'' Comput. Secur., vol. 103, Apr. 2021, Art. no. 102205. [14] G. Xie, Y. Liu, G. Xin, and Q. Yang, ``Blockchain-based cloud data integrity veri_cation scheme with high ef_ciency,'' Secur. Commun. Netw., vol. 2021, pp. 1_15, Apr. 2021.

[15] U. Arjun and S. Vinay, ``Outsourced auditing with data integrity veri_cation scheme (OA-DIV) and dynamic operations for cloud data Page 82 of 90 with multi-copies,'' EAI Endorsed Trans. Cloud Syst., vol. 7, no. 20, Jul. 2018, Art. no. 169423.

[16] A. V. Ezhil, G. K. Indra, and K. Kulothungan, ``Auditable attribute based data access control using blockchain in cloud storage,'' J. Supercomput., vol. 78, pp. 10772_10798, Jan. 2022.

[17] R. Mishra, D. Ramesh, D. R. Edla, and M. C. Trivedi, ``Blockchain assisted privacy-preserving public auditable model for cloud environment with ef_cient user revocation,'' Cluster Comput., pp. 1_25, Jan. 2022.

[18] X. Tao, Y. Liu, P. K.-Y. Wong, K. Chen, M. Das, and J. C. P. Cheng, ``Con_dentiality-minded framework for

blockchain-based BIM design collaboration," Autom. Construct., vol. 136, Apr. 2022, Art. no. 104172.

[19] P.Wei, D.Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ``Blockchain data-based cloud data integrity protection mechanism," Future Gener. Comput. Syst., vol. 102, pp. 902_911, Jan. 2020.

[20] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, ``Blockchain empowered arbitrable data auditing scheme for network storage as a service," IEEE Trans. Services Comput., vol. 13, no. 2, pp. 289_300, Mar. 2020.

[21] H. Yu, Z. Yang, and R. O. Sinnott, ``Decentralized big data auditing for smart city environments leveraging blockchain technology," IEEE Access, vol. 7, pp. 6288_6296, 2019. Page 83 of 90

[22] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacy- preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362_375, Feb. 2013. [23] L. Chen, Q. Fu, Y. Mu, L. Zeng, F. Rezaeibagha, and M.-S. Hwang, ``Blockchain-based random auditor committee for integrity veri_cation," Future Gener. Comput. Syst., vol. 131, pp. 183_193, Jun. 2022.

[24] H. Yuan, X. Chen, J. Wang, J. Yuan, H. Yan, and W. Susilo, ``Blockchain- based public auditing and secure deduplication with fair arbitration," Inf. Sci., vol. 541, pp. 409_425, Dec. 2020.

[25] C. Yang, Y. Liu, F. Zhao, and S. Zhang, ``Provable data deletion frome fcient data integrity auditing and insertion in cloud storage," Comput. Standards Interface, vol.

AUTHORS Profile

Mr. K. Jaya Krishna is an Associate Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai, and his M.Tech in Computer Science and Engineering (CSE) from Jawaharlal Nehru Technological University, Kakinada (JNTUK). With a strong research background, he has authored and co-authored over 90 research papers published in reputed peer-reviewed Scopus-indexed journals. He has also actively presented his work at various national and international conferences, with several of his publications appearing in IEEE-indexed proceedings. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mrs. J. DURGA BHAVANI has received his MCA (Masters of Computer Applications) from QIS college of Engineering and Technology Vengamukkapalem (V), Ongole, Prakasam dist., Andhra Pradesh-523272 affiliated to JNTUK in 2023-2025