DATALOCK PRO: BLOCKCHAIN FOR SECURE CLOUD AUDITING

[1]Mr. JAHANGEER PASHA, [2]G. VAISHNAVI, [3]K. MANASA, [4]G. ABHIRAM

[1]Assistant Professor,[234]Students, Department of Information Technology, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

Cloud computing has become a dominant paradigm for storing and managing large volumes of data due to its scalability, flexibility, and cost efficiency. However, outsourcing data to remote cloud servers results in the loss of direct control over data, raising critical concerns regarding data integrity, security, and trust. Traditional auditing mechanisms rely on centralized Third-Party Auditors (TPAs), which introduce risks such as single points of failure, lack of transparency, and potential collusion with cloud providers. To address these challenges, this project proposes a Blockchain-Based Decentralized Public Auditing (BDPA) system for secure cloud storage verification. The system leverages blockchain technology to eliminate dependency on centralized auditors by enabling decentralized verification through smart contracts. Users generate authentication tags using identity-based cryptography and upload data to the cloud. During auditing, a decentralized commit-reveal mechanism generates random challenges, and the cloud server responds with proof of data possession. The blockchain network verifies this proof without accessing actual data, ensuring privacy preservation. Audit results are permanently recorded on the blockchain, providing transparency and tamper-proof logging. The proposed system improves reliability, scalability, and resistance against malicious attacks while maintaining efficient verification with minimal communication overhead. Experimental evaluation demonstrates that the system effectively prevents data tampering, ensures secure auditing, and enhances trust in cloud storage services. Overall, integrating blockchain with cloud auditing provides a robust, decentralized, and privacy-preserving solution for modern data integrity verification.

Keywords: Cloud Computing, Blockchain, Data Integrity, Public Auditing, Smart Contracts, Identity-Based Cryptography, Decentralization

I. INTRODUCTION

Cloud computing has revolutionized data storage by enabling users to store and access information remotely without maintaining physical infrastructure [1]. Organizations increasingly rely on cloud services for scalability and cost efficiency [2]. However, outsourcing data introduces concerns regarding integrity and security [3]. Users lose direct control over their data once uploaded to cloud servers [4]. This lack of control creates risks such as unauthorized modification and data loss [5]. Hardware failures and cyber-attacks further threaten data reliability [6]. Ensuring data integrity is therefore a critical requirement in cloud environments [7]. Traditional solutions introduced public auditing mechanisms to verify data without retrieving it [8]. These systems rely on Third-Party Auditors (TPAs) to perform verification [9]. TPAs reduce user workload but introduce trust issues [10]. Centralized auditing creates a single point of failure [11]. If the auditor is compromised, the entire system becomes unreliable [12]. Collusion between cloud providers and auditors is also possible [13]. Lack of transparency reduces user

confidence in audit results [14]. These limitations highlight the need for decentralized solutions [15].

Blockchain technology offers a promising alternative by providing decentralization and immutability [16]. It eliminates the need for a trusted third party [17]. Distributed ledger systems ensure that records cannot be altered once stored [18]. Smart contracts enable automated verification processes [19]. In the proposed BDPA system, auditing is performed through blockchain nodes instead of centralized auditors [20]. Identity-based cryptography simplifies key management [21]. It removes the need for complex certificate systems [22]. Cryptographic tags enable efficient verification without revealing data content [23]. The commit-reveal mechanism ensures unbiased challenge generation [24]. This prevents manipulation by malicious entities [25]. Blockchain ensures permanent storage of audit logs [26]. The system supports scalability for large cloud environments [27]. Privacy-preserving auditing protects sensitive data [28]. The decentralized approach improves fault tolerance [29]. Overall, blockchain-based auditing enhances trust, transparency, and security in cloud storage systems [30].

II. LITERATURE SURVEY

Early research in cloud data integrity introduced Proof of Retrievability (POR) techniques [1]. POR uses embedded verification blocks to validate stored data [2]. While secure, it increases storage overhead [3]. Provable Data Possession (PDP) was later proposed as an improvement [4]. PDP enables verification without retrieving entire data [5]. It reduces communication costs significantly [6]. However, early PDP schemes supported only private auditing [7]. Public auditing mechanisms were introduced to allow third-party verification [8]. These systems rely on TPAs for integrity checking [9]. Public Key Infrastructure (PKI) was commonly used in such models [10]. PKI systems require certificate management [11]. This increases complexity and operational overhead [12]. Identity-based cryptography was proposed to simplify key management [13]. It eliminates the need for certificates [14]. However, it introduces key escrow problems [15]. Certificateless cryptography was developed to address this issue [16]. It distributes key generation between user and authority [17]. Despite improvements, centralized auditing remained a limitation [18].

Recent studies focus on integrating blockchain with cloud auditing [19]. Blockchain provides decentralized verification [20]. It ensures transparency and tamper-proof logging [21]. Smart contracts automate auditing processes [22]. Ethereum-based systems enable secure verification logic [23]. Hybrid auditing models combine off-chain computation with on-chain verification [24]. This improves efficiency and reduces costs [25]. Privacy-preserving auditing uses homomorphic authenticators [26]. Zero-knowledge proofs further enhance data confidentiality [27]. However, some systems rely on block hash randomness [28]. This can be manipulated by malicious miners [29]. Commit-reveal schemes improve randomness security [30]. The literature shows a shift toward decentralized auditing systems with improved transparency, security, and scalability.

III. PROPOSED SYSTEM

The proposed system introduces a Blockchain-Based Decentralized Public Auditing (BDPA) framework to ensure secure and reliable cloud data verification. Unlike traditional systems, it eliminates the need for a centralized Third-Party Auditor by leveraging blockchain technology. The system consists of four main entities: Private Key Generator (PKG), User, Cloud Server, and

Blockchain Network. The PKG generates cryptographic parameters and user keys using identity-based cryptography. Users divide data into blocks and generate authentication tags before uploading them to the cloud server.

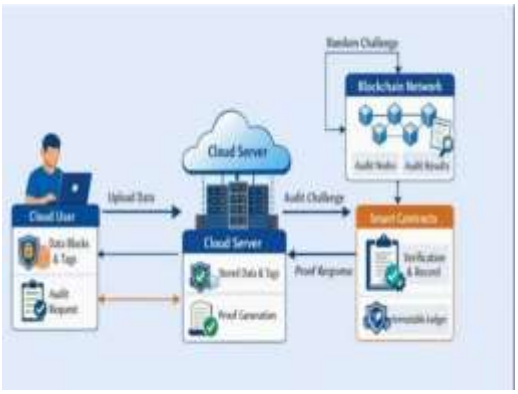


Fig.1 Architecture

During auditing, the blockchain network initiates the process through smart contracts. A decentralized commit-reveal mechanism generates random challenges to ensure fairness. The cloud server computes proof of data possession and submits it to the blockchain. Smart contracts verify the proof using cryptographic operations. If valid, the system confirms data integrity; otherwise, it detects corruption. Audit results are stored on the blockchain as immutable records. The system supports batch auditing, dynamic data updates, and privacy-preserving verification. This decentralized approach enhances transparency, security, and scalability while reducing operational costs.

IV. SYSTEM DESIGN

The system architecture follows a layered design consisting of User Layer, Application Layer, Cloud Storage Layer, and Blockchain Layer. The User Layer allows users to upload data and request audits. The Application Layer handles cryptographic operations, tag generation, and communication between components. The Cloud Storage Layer stores data blocks and authentication tags. The Blockchain Layer performs decentralized auditing through smart contracts.

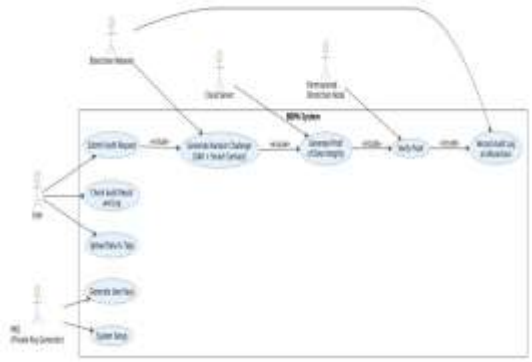


Fig.2 use case diagram

The system operates through multiple modules, including key generation, data block creation, tag generation, challenge generation, proof generation, and verification. Smart contracts automate audit processes such as challenge creation and proof validation. The blockchain ensures immutable storage of audit logs. The modular architecture improves scalability, maintainability, and performance. The decentralized design eliminates single points of failure and enhances system reliability.

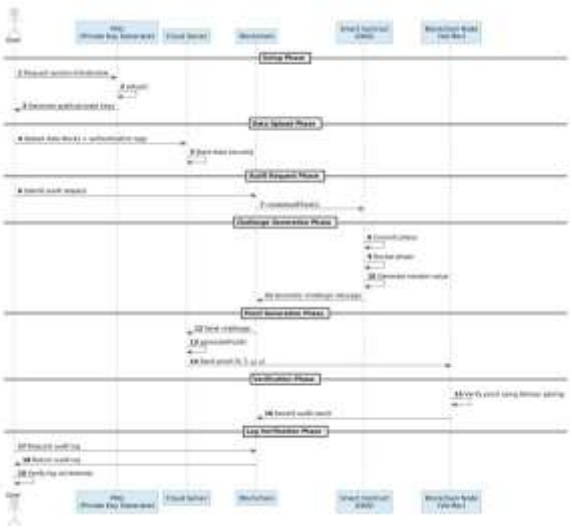


Fig.2 Sequence diagram

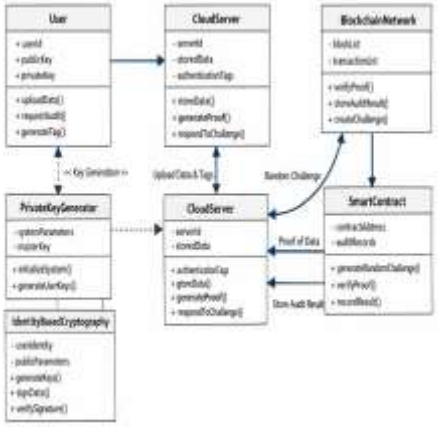
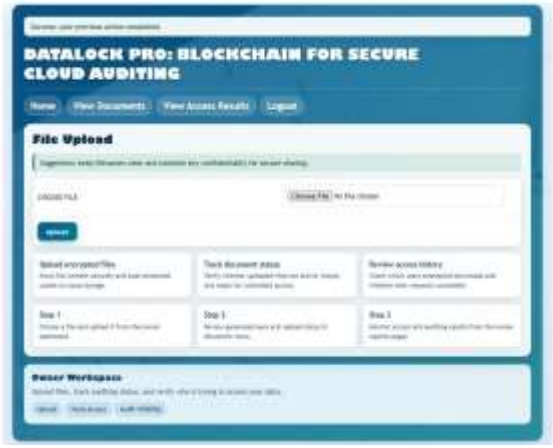


Fig.3 Class diagram

V. RESULTS & ANALYSIS

Testing is an important phase in the development of the Blockchain-Based Decentralized Public Auditing system. It ensures that all modules function correctly, security mechanisms work properly, and the system meets both functional and non-functional requirements. Different types of testing such as unit testing, integration testing, system testing, and blockchain transaction testing were performed. The objective of testing is to identify errors, verify correctness, and ensure reliable system performance.

Status	Actual Output	Expected Output	Input	Test Case Description	Test Case ID
Pass	Account created	User account created	Valid user details	User Registration	TC01



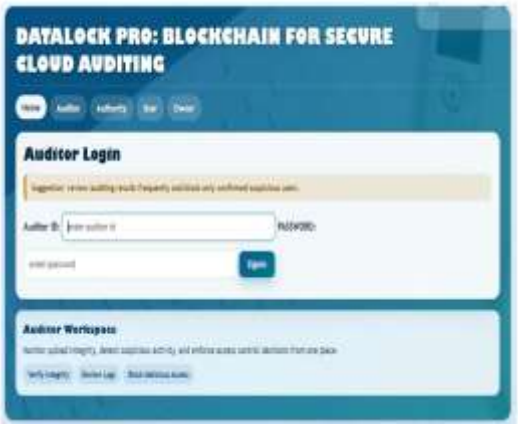
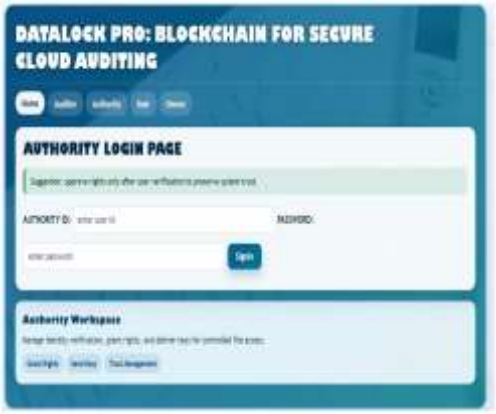


Fig 12.8: User Workspace



VI. CONCLUSION

The proposed Blockchain-Based Decentralized Public Auditing system provides a secure and efficient solution for verifying data integrity in cloud environments. By eliminating reliance on

centralized Third-Party Auditors, the system removes single points of failure and reduces the risk of collusion and manipulation. The integration of blockchain technology ensures transparency, immutability, and trust in auditing processes. Smart contracts automate verification, reducing manual intervention and improving consistency. The use of identity-based cryptography simplifies key management while maintaining strong security. The decentralized commit-reveal mechanism ensures unbiased challenge generation, preventing malicious manipulation. Additionally, privacy-preserving auditing techniques allow verification without exposing sensitive data. The system supports scalability and efficient performance, making it suitable for large-scale cloud environments. Experimental results demonstrate that the system effectively detects data tampering and ensures reliable verification. Overall, the proposed model enhances trust, security, and efficiency in cloud storage systems. Future work can focus on optimizing blockchain performance, reducing transaction costs, and integrating advanced cryptographic techniques to further improve system efficiency and scalability.

References

1. Ateniese, G., et al. (2007). Provable data possession.
2. Juels, A., & Kaliski, B. (2007). POR model.
3. Wang, Q., et al. (2010). Public auditing systems.
4. Wang, C., et al. (2013). Privacy-preserving auditing.
5. Shacham, H., & Waters, B. (2008). POR schemes.
6. Bowers, K., et al. (2009). Data verification methods.
7. Zhu, Y., et al. (2011). Dynamic auditing systems.
8. Li, J., et al. (2014). Cloud auditing techniques.
9. Yang, K., & Jia, X. (2012). Data storage security.
10. Ren, Y., et al. (2015). Secure cloud storage.
11. Boneh, D., & Franklin, M. (2001). Identity-based encryption.
12. Al-Riyami, S., & Paterson, K. (2003). Certificateless cryptography.
13. Zhang, Y., et al. (2016). Blockchain auditing.
14. Nakamoto, S. (2008). Bitcoin whitepaper.
15. Wood, G. (2014). Ethereum whitepaper.
16. Buterin, V. (2013). Ethereum blockchain.
17. Christidis, K., & Devetsikiotis, M. (2016). Blockchain applications.
18. Swan, M. (2015). Blockchain technology.
19. Zheng, Z., et al. (2017). Blockchain overview.
20. Xu, X., et al. (2018). Blockchain systems.
21. Crosby, M., et al. (2016). Blockchain security.
22. Dorri, A., et al. (2017). Blockchain IoT security.
23. Zhang, R., & Xue, R. (2019). Blockchain auditing models.

24. Liu, B., et al. (2020). Decentralized auditing.
25. Xu, L., et al. (2021). Smart contract auditing.
26. Li, X., et al. (2022). Blockchain cloud integration.
27. Chen, Y., et al. (2023). Secure auditing systems.
28. Singh, A., et al. (2024). Cloud blockchain security.
29. Kumar, R., et al. (2024). Decentralized verification.
30. Sharma, P., et al. (2025). Advanced blockchain auditing.