RESEARCH ARTICLE OPEN ACCESS

BLOCKCHAIN- BASED DECENTRALIZEDCLOUD STORAGE WITH PRIVACY- PRESERVING ACCESS CONTROLUSING IPFSAND ECC

K. Rajaprabu *, Joel Newton D**, Saran V **, Sivanesan T**,SuryaS**

*Assistant Professor -J.J. College of Engineering and Technology,Tiruchirapalli,Tamil Nadu
**UG Students J.J. College of Engineering and Technology,Tiruchirapalli,Tamil Nadu
India

Abstract

The rapid adoption of cloud storage applications in managing large-scale data has brought significant challenges related to security and privacy, especially in direct user-to-cloud architectures. The problems encountered with existing systems include poor access control, weak delegation of credentials, and the absence of data integrity [12], [13]. Centralized infrastructures further contribute to risks such as single points of failure and heavy dependency on third parties [14]. This paper proposes a decentralized and secure cloud storage architecture based on Blockchain, InterPlanetary File System (IPFS), and Elliptic Curve Cryptography (ECC) to address these issues. ECC ensures highly secure data encryption, while IPFS provides distributed and immutable storage. Blockchain enables decentralized access control through smart contracts, ensuring secure data access and transparent auditing [11], [14]. Additionally, Proxy Re-Encryption (PRE) and Zero-Knowledge Proofs (ZKP) facilitate secure data sharing and authentication without compromising user privacy [11]. The proposed system enhances security, scalability, fault tolerance, and user ownership of data, making it a robust solution for next-generation cloud storage systems.

Keywords: Cloud storage, cloud security, blockchain, interplanetary file system (IPFS), elliptic curve cryptography (ECC), proxy re-encryption (PRE), zero-knowledge proofs (ZKP), access control, data privacy, data integrity, secure data sharing, decentralized systems, distributed storage, smart contracts, cryptographic security, authentication, fault tolerance.

1.Introduction

The fast pace of the development of digital applications and online services has led to the explosive increase in the number of user-generated data, and cloud storage has become one of the essential elements of the contemporary computing system. Clouds are scalable, flexible, and cost-effective, and direct file user-to-cloud upload technologies are now common in the applications to help decrease server load and enhance performance. Nonetheless, there are serious security and privacy threats posed by such architectures. The recent research has found several vulnerabilities such as insecure management of upload credential, ineffective access control, uncontrolled file upload, and data integrity problems, which may result in unauthorized access, data leakage, and abuse of the resources.

Traditional cloud storage systems are designed based on centralized systems where data storage, authentication and access control are operated by one service provider. Even though this model makes management simple it comes with its own limitations, including single points of failure, lack of transparency and high levels of third party trust. Consequently, customers do not have as much control over their information, and the threat of massive data breaches and system failures grows immensely. Decentralized technologies are also potential solutions to these challenges. The blockchain technology allows access control via distributed ledgers with impartiality and transparency, and the Interplanetary File System (IPFS) offers a content-addressable, peer-to-peer content storage system that can increase the availability of data and tamper resistance. Also, modern cryptographic methods like Elliptic Curve Cryptography (ECC), proxy re-encryption and zero-knowledge proofs are used to enable secure data encryption and controlled sharing and privacy-preserving authentication.

The proposed paper is a decentralized cloud storage system based on the combination of Blockchain, IPFS, and ECC, to improve the shortcomings of the traditional cloud systems. The suggested model provides data confidentiality due to encryption, integrity due to distributed storage, and access control security based on blockchain-based measures. In addition, it allows sharing of data with security and flexibility and maintains privacy of users, which makes it a solid and scalable solution in next-generation cloud storage systems.

I. BACKGROUND

The current cloud storage systems are becoming more of a architecture that enables the users to upload files to the cloud storage services eliminating overhead on the server side and enhancing scalability of the system. The model has three primary participants including the user of the web (client), the web server, and the cloud storage service. The communication between these parties is usually in a defined workflow that is made up of three steps; credential generation, file upload and the notification of results. The user requests an upload credential on the web server in the first stage. The user is verified against the server and a temporary uploading credential generated according to a defined set of security policies on file type, size, storage path and expiration time.

The second step involves uploading the file to the cloud storage service by the user using the credential that is provided. The cloud service authenticates the credential and enforces the policies to be used before accepting the file. The last stage is a callback notification to the web server to check the status of the upload and update system records. Notwithstanding, the efficiency and scalability of this architecture, it creates complicated interactions among various entities, expanding the vulnerability to attacks. The cloud storage service will only generally verify the upload credential and not the identity of the user, so the system highly relies on the management of credits. Even minor policy misconfiguration of the credential policies, access control systems, and validation systems may result in severe security weaknesses. Recent studies have revealed that such systems have a number of serious security concerns such as the ability to achieve credentials without restriction, mismanagement of credential validity, file unrestricting, file overwriting, unauthorized access to files and spoofing of call-back notification.

These weaknesses may lead to data breaches, resource abuse, and loss of data integrity, which puts more secure and robust architectures of storage into the spotlight. In order to meet these issues, new technologies like Blockchain and IPFS enable decentralized options that are more secure and transparent. Blockchain can guarantee immutable logging and access control and IPFS can guarantee distributed and tamper resistant storage. These technologies together with cryptographic protocols such as ECC are bases of secure and privacy-based cloud-based storage systems.

II. PROPOSED SYSTEM

This paper will suggest a decentralized, secure and privacy-saving cloud storage system through the combination of Blockchain, Interplanetary File System (IPFS) and Elliptic Curve Cryptography (ECC). The main task is to have the ability to surpass the shortcomings of centralized cloud systems, including single points of failures, no transparency, and poor access control and to have secure data storage and data sharing under controlled circumstances.

A. System Overview

The suggested system is a decentralized and secure cloud storage model that aims at addressing the constraints of the conventional centralized cloud designs. It incorporates Blockchain, Interplanetary File System (IPFS), and Elliptic Curve Cryptography (ECC) to provide high security, openness, and data control to users. Under this architecture the data owner will encrypt and upload files whereas the data user will seek access to the shared data. The cloud server will serve as a communication and coordination interface between the parts, and blockchain network will record the transactions, metadata, and access permissions, which cannot be changed. The system increases trust and reduces single points of failure and the overall system reliability, by eliminating dependence on centralized authorities.

B. Data Prioritization and Data storage.

The proposed system will store files encrypted by Elliptic Curve Cryptography (ECC) to guarantee data privacy. ECC offers high security, less key sizes, lowering the computation rates and making it resource efficient. ECC may be used together with symmetric encryption algorithms like AES (hybrid encryption) to enhance its performance. Once encrypted, the information is stored on IPFS, a peer-to-peer content-addressed storage network which is decentralized.

The files receive unique Content Identifiers (CID) on the basis of their hash value. This makes sure that the slightest change in the file produces an entirely new hash and thus the data integrity and tampering is eliminated. Also, IPFS spreads data to more than one node enhancing availability and fault tolerance.

C. Access Control Mechanism

The proposed system uses the blockchain-based access control system to impose secure and transparent authorization. All the metadatas, accessibility and transaction records are recorded on the blockchain as unalterable records. This makes sure that access policies cannot be altered, deleted or forged by the malicious parties. In the event a data user wishes to gain access, the system validates such a request by reference to the records of the blockchain, which ensures that only legitimate users are permitted to do so.

The blockchain structure is decentralized and eliminates the reliance on centralized authentication nodes and allows verification without trust. Moreover, it is possible to use smart contract-like logic to automate access control decisions and enhance efficiency and decrease human involvement.

D. Secure Data Sharing

The system incorporates proxy re-encryption (PRE) to allow the secure and flexible sharing of encrypted information. Under this method, the data owner will produce a re-encryption key that will enable a semi-trusted proxy (cloud server) to convert encrypted ciphertext intended to be decrypted by one authorized user into encrypted ciphertext that can be decrypted by another authorized user.

This system does not need to share the private keys directly and thus high levels of confidentiality. It is also fine-grained access control, and data owners can dynamically add and remove access. Consequently, the protection of data sharing

is realized without the loss of the security of the initial encryption keys

E. Privacy-Preserving Authentication.

The suggested system applies the methods of zero-knowledge proof (ZKP) to enjoy privacy-respecting authentication. ZKP also allows a user to identify themselves or gain access without the revelation of sensitive data to grant privileges like passwords or personal keys. This will go a long way in minimizing the chances of credential leakage and safeguarding the privacy of users whenever they are going through authentication processes.

Making sure that no sensitive information is revealed in the process of the verification, ZKP improves the overall security of the system and meets the requirements of privacy protection in the distributed systems of the modern era.

III. METHODOLOGY

A. DATA OWNER MODULE

The Data owner module shall be responsible of uploading safe data, encryption as well as access of the proposed decentralized system. First, files are selected and uploaded by the owner of the data and then encrypted with the assistance of the Elliptic Curve Cryptography (ECC) which offers high confidentiality of the data with small computational requirements. The reason why this encryption is done is to protect the sensitive information against an unauthorized usage of the information when storing and transmitting the information.

The encrypted data is subsequently uploaded to the Interplanetary File System (IPFS) it is stored in an intended and resistant to manipulation format. The hash of the file will be stored on blockchain with metadata as an Identifier (CID) of the file. This not only ensures data integrity is ensured but also enables the verification of the data to be done safely because any modification of the file will result in a different hash value.

Determining access control policies is done by the owner of the data i.e. the users who are permitted to read the data and is kept in the blockchain as an unalterable record. This will provide safe and open access control. The data owner is also in position to trace the access of files and give the permission dynamically. To exchange data safely, the proxy re-encryption (PRE) is applied whereby encrypted data may be viewed by authorized parties without disclosure of the secret keys therefore guaranteeing the full ownership and control of data.

B. CLOUD SERVER MODULE

The Cloud Server Module serves as a point of coordination that helps the data owner, data user, IPFS storage, and blockchain network to communicate. The cloud server is decentralized but the system through which the request is handled and the operation of the system is managed is available in the cloud server. When a data owner uploads a file, the cloud server is fed with the encrypted data, which is safely transferred to the IPFS network to store and distribute the information. This strategy will make sure that sensitive data is not stored in one central place hence mitigating any data breach and enhancing reliability of the system.

Along with data manipulation, metadata processing, such as file hashes (CIDs), storage references, and access logs are managed by the cloud server. When a file has been uploaded via IPFS, the hash is computed by the cloud server and stored on the blockchain with access permissions to it. This allows secure data verification, traceability and integrity verification. The cloud server also communicates with the blockchain to authenticate user requests such that only authorized user can access or retrieve specific files according to pre-determined access control policies.

In addition, the cloud server provides availability of data, scalability, and an efficient access of files stored. When a request is sent by a data user to the server, the permissions are checked with the blockchain, and the relevant encrypted file of IPFS is recovered. It then transmits the information to the authorized user to decrypt. The module also has access logs to track the user activity and prevent unauthorized access. The cloud server provides better performance to the systems and retains the decentralized nature, confidentiality, and integrity of the overall storage system since it acts as a secure intermediary.

C. IPFS MODULE

One of the significant components of the suggested system is the IPFS Module which provides a distributed and tamper-resistant encrypted information data storage which is decentralized. Compared to the classical cloud storage systems that are founded on centralized servers, IPFS is a peer-to-peer (P2P) network, which means that data is distributed between multiple nodes. This eliminates single points of failure and increases system reliability, availability and fault tolerance significantly.

When its owner uploads a file to the IPFS network, the file is encrypted before being transmitted to the IPFS network by the cloud server. IPFS divides the file into tiny fragments and publishes the file to multiple nodes and forms a Content Identifier (CID) which is the result of the cryptographic hash of the file. This is a mechanism of addressing which based on content that ensures that any file can be identified and altered.

Any modifications to the file result in a completely new hash, and therefore integrity of the data is maintained

as well as it does not undergo tampering by the unauthorized personnel. The obtained CID is by this time stored on the blockchain with metadata and access control data in such a way that it can be traced and verified safely. The IPFS implementation equally offers good files retrieval and sharing across the network. The system will locate and retrieve the encrypted data using CID in the nearest or most responsive node to reduce the latency and maximise the performance of the system in case of a request by an authorized user of a file. Due to the potential of multiple copies of the data existing in the network, IPFS guarantees high availability even when the nodes fail. In addition, the module integrates well with the cloud server and blockchain whereby authenticated and authorized only requests are processed.

The IPFS component enables a trade off between the scalability, security, and performance of the decentralized storage and cryptographic validation to become one of the critical components of the proposed cloud storage system.

D. DATA USER MODULE

The Data User Module will be developed to offer safe, restricted, and privacy protecting access to files that are shared by the data owners within the decentralized system. It allows users to seek and get information and ensure that the protected contents are still accessed by authorized parties. The module provides interactive interface, where users are able to request access, view shared files and manage their permissions effectively.

Upon a request presented by a data user to access a file, the system conducts authorization verification in the network of the blockchain. Access control information stored on the blockchain is permanent and readable, and only authenticated individuals have the right to advance. The system also uses zero-knowledge proof (ZKP) to increase privacy by enabling users to disclose their authorization without providing information that is sensitive, including private keys or credentials. This guarantees secure authentication and retention of the privacy of users.

After a successful authentication of the user, the system makes use of proxy re-encryption (PRE) in a bid to safely allow access to the encrypted data. The proxy (cloud server) alters the original ciphertext such that it can only be decrypted by the authorized user. The user of the data then requests the file encrypted by the user of the IPFS network through the content identifier (CID) and then decrypts it on the local machine with the help of a personal key. This methodology will make sure that sensitive information will never be revealed in the process of transmission. Moreover, the Data User Module keeps a record of access logs and permission records enabling the user to monitor their access and confirm their access privileges. This increases accountability and transparency in the system. The module requires integrating blockchain-based authorization, ZKP-based authentication, and PRE-based secure sharing to provide a high level of data access security and efficiency with great privacy assurance.

IV. EXPERIMENT

The suggested decentralized cloud storage system was tested and installed in a controlled condition on the regular hardware settings. The system was installed on a machine with an Intel core processor (2.6 gHz) with a 1GB RAM and 160GB hard disk with a windows platform.

User interaction was done through peripherals which included a standard keyboard and 15 inch monitor. This configuration offered a stable and economical platform to prove the viability and workability of the offered framework under conditions of a normal system.

The implementation of the software was done through front-end and back-end technologies. Frontend interface was created with the use of HTML, CSS and JavaScript, which allowed data owners and data users to interact easily. The Python language was used to implement the backend system, which performs the encryption procedures and data management and communicates with decentralized elements, including IPFS and blockchain. The PyCharm Integrated Development Environment (IDE) was used to aid the development process by supporting the creation of the code, debugging process, and integration of the system.

The experimental system is a system that combines Blockchain, IPFS, and advanced cryptographic technology to guarantee efficient and secure functionality. Elliptic Curve Cryptography (ECC) is used to encrypt files and then uploaded to IPFS where information is stored in a distributed and content-addressable format. Metadata and file hashes are stored in the blockchain layer and the access control policies are documented in an immutable format that provides transparency and security. Also, proxy re-encryption (PRE) can be employed to share data safely without the disclosure of any private keys, and zero-knowledge proofs (ZKP) can be employed to perform privacy-protecting authentication.

The system functionality, reliability and security against unauthorized access were tested on several conditions such as uploading files, validation of access request, and retrieving secure data.

V. DISCLOSURE AND RESPONSE

The vulnerability of security disclosure and responding are critical in ensuring robustness, reliability, and trustworthiness of cloud storage systems. Further, within the suggested decentralized system, the possible security threats are also actively discovered and mitigated using a mixture of cryptographic methods, decentralized storage and blockchain-based access control regimes. The method will make sure that the vulnerabilities that are usually prevalent in traditional centralized systems have been greatly minimized.

The major security risks that have been addressed by the proposed system include unauthorized access, data tampering, credential use, and data leakage. Any sensitive information that is stored is encrypted with Elliptic Curve Cryptography (ECC) and this keeps the confidentiality even in the case the storage nodes are compromised. Distributed storage, which is made feasible by the application of the Interplanetary File System (IPFS), can remove single points of failure, as well as avoid exposing their data to centralized locations.

The system has preventive mechanisms, as well as effective response mechanisms that are incorporated to address potential threats. Authentication between users is conducted with the help of the zero-knowledge proof (ZKP) methods where verification does not require disclosure of sensitive credentials thus ensuring additional privacy. The sharing of data is done with the aid of proxy re-encryption (PRE), where the key of encryption is not revealed in the data sharing. System access requests and access activities are all logged and monitored so that abnormal behavior like frequent unauthorized access attempts or suspicious transactions can be detected.

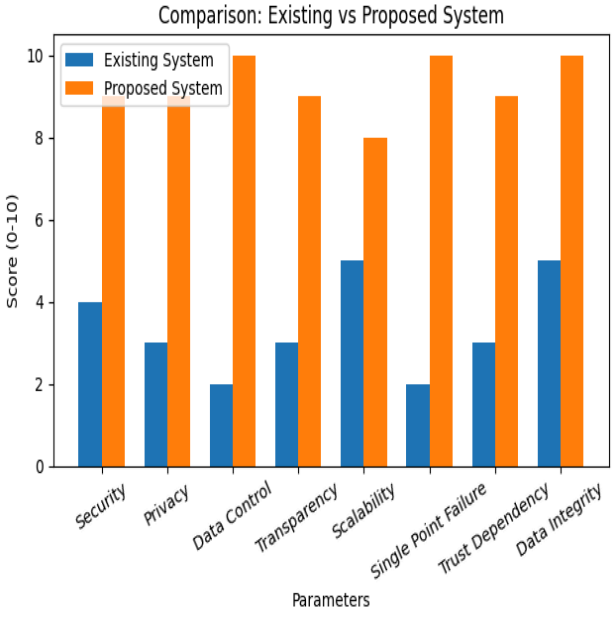
On the whole, the proposed system has a secure-by-design paradigm, in the framework of which prevention and response systems are both embedded in the program structure. With the integration of encryption, decentralized storage, and blockchain-enabled verification, the system also provides high resistance to vulnerabilities as well as data integrity, confidentiality, and privacy of users. This renders the framework very appropriate in secure, scalable and trustworthy cloud storage applications.

Technology	Purpose	Function in Systen
Elliptic Curve Cryptography (ECC)	Data Encryption	Encrypts user data before storing in the system
Interplanetary File System (IPFS)	Decentralized Storage	Stores encrypted data across distributed nodes
Content Identifier (CID)	Data Integrity	Generates unique has for each file to detect changes
Blockchain	Access Control	Maintains metadata, permissions, and transaction logs
Proxy Re-Encryption (PRE)	Secure Data Sharing	Enables sharing of encrypted data without exposing key
Zero-Knowledge Proof (ZKP)	Authentication	Verifies users withou revealing sensitive credentials

VI. RESULT AND DISCUSSION

The decentralized cloud storage suggested was successfully deployed and tested on different situations in addition to file upload, secure storage, validation of access request, and data retrieval. The system has shown the ability to integrate the use of the Blockchain, IPFS, and Elliptic Curve Cryptography (ECC) to provide secure and efficient data management. The experiment findings confirm that encrypted files can be safely stored in the IPFS network and can be retrieved with the help of the corresponding content identifier (CID) without the loss or integrity problems.

ECC encryption tremendously enhanced security and also the computational overhead was a lot lower and thus the system was efficient even in resource-constrained situations. The storage system based on IPFS provided high availability and fault tolerance because it was possible to access files on the distributed nodes. Also, the blockchain layer was effective in imposing access control policies that made sure that only authorized users could access the requested data. Blockchain verification and authentication mechanisms were successfully used to mitigate unauthorized access attempts. Moreover, the zero-knowledge proof (ZKP) systems provided privacy-sensitive authentication, which avoids revelation of sensitive user credentials during authentication. Access logs were also kept by the system that enhanced transparency and ease of monitoring user activities. The proposed model exhibited high data security, integrity and user control as compared to the traditional centralized cloud storage systems. This has improved the reliability of the system by removing a single point of failure, and also, decreased the chances of massive data breaches because of the decentralized storage. In general, the obtained findings suggest that the suggested system offers scalability, high-security, and efficiency to the latest cloud storage problems, which is why it can be directly applied in practice when privacy is the primary concern.



VII. CONCLUSION

In the present paper, the limitations of the traditional centralized cloud system have been addressed by presenting a decentralized and secure cloud storage framework. Secure data storage, efficient access control, and privacy of users are facilitated by the combination of Blockchain, Interplanetary File System (IPFS) and Elliptic Curve Cryptography (ECC). The system guarantees high levels of data confidentiality by encrypting data prior to storage and the use of distributed storage via IPFS to remove single points of failures.

Immutable and transparent management of metadata, access permissions, and transaction records are ensured with the use of blockchain technology, which is why unauthorized changes are prohibited and trust is increased. Moreover, it can support privacy-preserving authentication by implementing proxy re-encryption (PRE) and share data safely and flexibly without exposing key information, and zero-knowledge proofs (ZKP). Through experimental evidence, it has been established that the proposed system is better in terms of security, scalability, and reliability than the traditional cloud storage models. It serves well to eliminate risks of unauthorized access, data tampering and data leakage in addition to offering full control of data to the user. On the whole, the suggested framework is strong and effective in solving the next-generation cloud storage systems, as this model will be applicable to the applications that may need high security and privacy.

ACKNOWLEDGMENT

The authors would wish to offer our heartfelt thanks to our project guide, Mr. Rajaprabu K, Assistant Professor, Department of Information Technology, who has continuously given guidance, meaningful suggestions, as well as his full support to this research project. We also wish to say a huge thank you to the members of the faculty of the Department of Information Technology, who have made the resources and motivation that gave us the strength to implement this project successfully. And, lastly, we would like to express our gratitude to our friends and family members who encouraged and supported us throughout the research and enabled us to finish our research work successfully.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982]

[6] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[7] K. Eves and J. Valasek, “Adaptive control for singularly perturbed systems examples,” Code Ocean, Aug. 2023.Available: https://codeocean.com/capsule/4989235/tree

[8] D. P. Kingma and M. Welling, “Auto-encoding variational Bayes,” 2013, arXiv:1312.6114.Available: https://arxiv.org/abs/1312.6114

[9] S. Liu, “Wi-Fi Energy Detection Testbed (12MTC),” 2023, gitHub repository. [Online]. Available: https://github.com/liustone99/Wi-Fi-Energy-Detection-Testbed-12MTC

[10] “Treatment episode data set: discharges (TEDS-D): concatenated, 2006 to 2009.” U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies, August, 2013, DOI:10.3886/ICPSR30122.v2

[11] Liu, Xiaoguang, Jun Yan, Shuqiang Shan, and Rongjun Wu. "A blockchain-assisted electronic medical records by using proxy reencryption and multisignature." Security and Communication Networks 2022 (2022).

[12] Alabdulatif, Abdullah, NavodNeranjan Thilakarathne, and Kassim Kalinaki. "A novel cloud enabled access control model for preserving the security and privacy of medical big data." Electronics 12.12 (2023): 2646.

[13] Dhinakaran, D., et al. "Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration." arXiv preprint arXiv:2401.00794 (2024).

[14] Wang, Weizheng, et al. "Smart contract token-based privacy-preserving access control system for industrial Internet of Things." Digital Communications and Networks 9.2 (2023): 337-346.