DECENTRALIZED AND PRIVACY-PRESERVING ACCESS CONTROL FOR DIGITAL SERVICES

Rasiga Fathima J, Rithikka R, Vanaja S
Department of Computer Science & Engineering
E.G.S Pillay Engineering College, Nagapattinam, Tamil Nadu, India

Abstract -- The system solves the problems of data privacy, user control, and security in digital services. It harnesses the power of blockchain technology to remove centralized powers, creating a trustless security framework free from single points of failure. Custom access control policies can managed by the users themselves, preventing exposure of sensitive data to third parties.

Data access within the system is protected with symmetric encryption and proxy re-encryption. These measures block access to unauthorized entities. Protective measures against data corruption are used to ensure the integrity of data stored within the system. These advancements show the possibilities available from decentralized systems operating in trustless frameworks that bolster user privacy while fortifying the security of the information.

Keywords: Decentralized Access Control, Privacy-Preserving Access Control, Blockchain, Zero-Knowledge Proofs (ZKPs), Access Management, Data Security, Privacy, Security, Cryptographic Techniques.

I.INTRODUCTION

This paper responds to the increasing demand for increased security and privacy in online services by suggesting a decentralized access control system. Centralized systems are usually prone to attacks and provide users with minimal control over their information.

To address these shortcomings, the approach discussed here employs blockchain and distributed ledger technology to create a trustless environment where centralized authorities are removed. This change seeks to give users more control over their access control policies and prevents sensitive data from being exposed unnecessarily. The primary goal of this work is to provide secure data access and preserve data integrity in digital services.The approach is to employ symmetric encryption and proxy re-encryption methods to protect data. By utilizing these methods, the system will only allow legitimate entities to gain access to the data, successfully blocking unauthorized entry.

Additionally, cryptographic methods are used to maintain data integrity and avoid any alteration of data, thus further solidifying the general security of the system. Essentially, the research aims to offer a secure solution to the inherent weaknesses of centralized access control systems. Using blockchain and high-level cryptographic techniques, the new framework seeks to establish a safer, more transparent, and user-oriented way of controlling access to digital service ecosystems.

The approach not only promotes security but also encourages more user trust through assuring that individuals have more ownership over their information and how they are accessed.

II.LITERATURE REVIEW

Blockchain-Based Secure Access Control Model for Cloud Storage (2022): This research discusses the implementation of blockchain technology to ensure decentralized access control within cloud storage while focusing on

stronger data integrity and protection of privacy. It further elaborates how smart contracts can be utilized for avoiding unauthorized access.

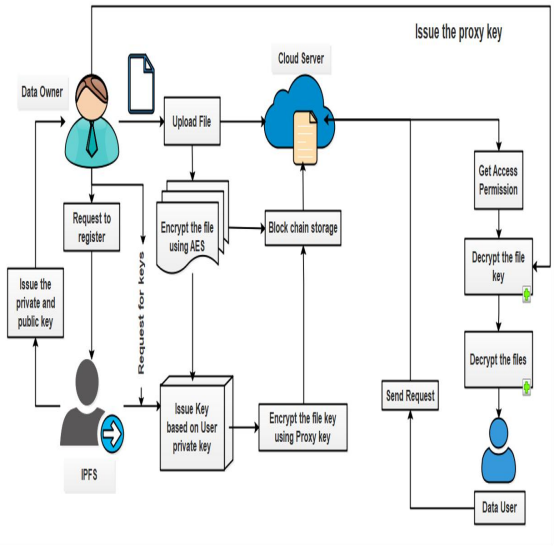
Proxy Re-Encryption for Secure Sharing of Data in Cloud Computing (2021): This study revolves around the deployment of Proxy Re-Encryption (PRE) for facilitating controlled data sharing in cloud computing environments. It maintains confidentiality without revealing decryption keys and diminishes dependence on centralized key management systems.

Decentralized Identity Management with Blockchain (2020): This article goes into self-sovereign identity (SSI) for authentication of users, with the goal of lowering reliance on third-party identity providers. It further considers the application of Zero-Knowledge Proofs (ZKP) in secure authentication processes.

Improving Data Security in Cloud Storage with Hybrid Cryptography (2019): This research hybridizes AES and RSA encryption to provide multi-layer security for cloud storage. It also proposes Homomorphic Encryption for safe data processing and addresses the performance trade-offs between speed and security.

These articles as a whole form the basis of the research by solving different aspects of decentralized access control, such as the application of blockchain, proxy re-encryption, decentralized identity management, and cryptographic methods in order to achieve security and privacy in cloud storage and computing.

III.PROPOSED DESIGN



The suggested system describes a decentralized private authorization system for service providers that emphasizes privacy-preserving and decentralized access control. The core functionality of the system involves the Data Owner and Data User interaction with the Cloud Server and Blockchain as essential building blocks.

Data Owner Workflow:

The Data Owner starts the process by uploading files to the system. They also register themselves, creating and sharing private and public keys required for encryption and decryption. The Data Owner also issues a proxy re-encryption key, which is crucial in secure key management.

Data Handling and Storage:

Uploaded files are encrypted with AES-256 for confidentiality. The encrypted files are subsequently kept on the Cloud Server, and metadata related to the files, such as access records and policies, are logged on the Blockchain. This double storage mechanism utilizes the strengths of both systems: the Cloud Server for data storage and Blockchain for safe, transparent, and immutable record-keeping. In addition, the key of the file itself is also encrypted with the proxy key, providing an additional level of protection.

Data User Access:

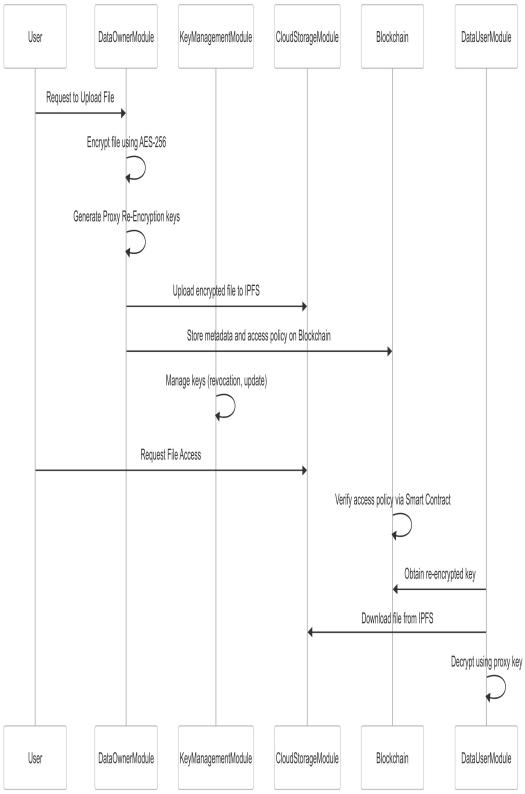
In order to access the stored data, Data Users need to acquire the required keys first. They request the keys, and these are issued according to the private key of the user. Then, the Data User requests access to the system. After successful authentication, the user is able to decrypt the file key and then decrypt the file, accessing the data.

Key Concepts and Technologies:

The framework utilizes various important notions and technologies to reach its aims. Blockchain and Distributed Ledger Technology (DLT) are basic, providing transparency and immutability for data. Smart contracts provide automated access control mechanisms without the need for intermediaries and implement policies in open and auditable fashion. Cryptographic methods, such as AES-256 and Proxy Re-Encryption, are utilized on a broad range of data protection and secure key management purposes.

Generally speaking, the presented system diagram outlines a strong structure for decentralized and privacy-preserving access control. By taking advantage of blockchain technology, encryption, and secure key management procedures, it overcomes the weaknesses of conventional centralized systems and offers a safer and user-focused solution for data access in service provider domains.

ACTIVITY DIAGRAM



IV.REQUIREMENTS

HARDWARE REQUIREMENTS :
Intel Processor
4GB RAM
160GB Hard Disk
SOFTWARE REQUIREMENTS :
Windows OS
PyCharm
MySQL
Hyperledger Fabric

Programming:
Java
Python

ADDITIONAL DEPENDENCIES AND CONSTRAINTS

The operation of the system depends on a number of dependencies critical to its success. To begin with, the InterPlanetary File System (IPFS) is crucial in offering decentralized storage of the data that has been encrypted, complementing the blockchain responsible for metadata processing. The AES-256 encryption

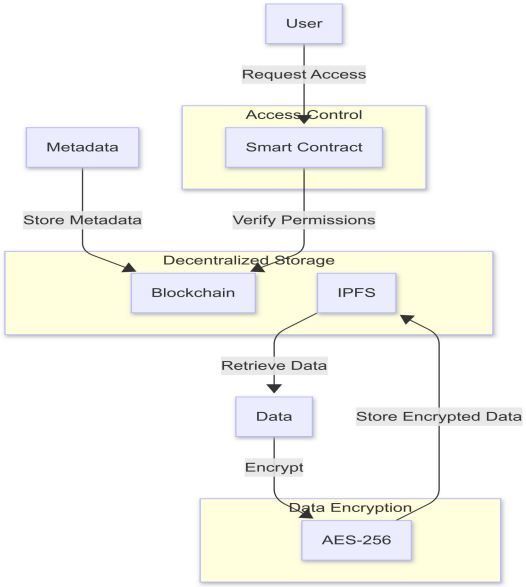
and proxy re-encryption functionalities require strong cryptographic libraries to support data confidentiality and key protection.

In addition, the system relies on a smart contract platform, which has been labeled as Hyperledger Fabric in the PPT, to enforce and automate access control policies. Lastly, an assured network connection is a basic requirement, allowing the Data Owner, Data User, Cloud Server, Blockchain, and IPFS elements to communicate seamlessly. Nevertheless, the system design also has a number of constraints.

Key management complexity raises the challenge of securely distributing and revoking encryption keys without recourse to a central authority. Transaction costs, in the form of high gas charges on public blockchains, have the potential to affect the cost-effectiveness and scalability of the system.

Latency problems because of delays in blockchain verification have the potential to impact the responsiveness of the system for real-time access control. Lastly, the system has to meet strict security and privacy standards, safeguarding user information from unauthorized access and maintaining user privacy.

V.METHODOLOGY



1. System Design:

Decentralized Storage:

The system employs blockchain for metadata and InterPlanetary File System (IPFS) for storing encrypted data. This decentralizes data but also stores it securely and makes it recoverable. Data Encryption:

The AES-256 encryption is employed in the project for protecting data confidentiality before storage or transmission. Any such strong encryption technique is highly necessary in preventing sensitive data from attackers. Blockchain Storage:

Metadata, access records, and policies are stored on the blockchain. This approach is more secure and transparent as all transaction attempts and access are stored immutably, allowing for effortless verification and auditing.

Access Control Smart contracts are utilized to automate and enforce user permissions. This eliminates the intermediaries, thereby making it easier to grant and revoke access to data.

2. Procedure of Proposed Work:

Data Owner Module:

This module is responsible for generating and sending proxy re-encryption keys. The keys grant controlled access to the data in such a way

that only the authorized are able to decrypt the data. Cloud Storage Module

They are kept encrypted in this module, and it also keeps access logs to ensure security. This makes sure that all access attempts are kept on record, leaving a clear trail for accountability. Key Management Module:

This module supports revocation and renewal of the keys in case of a security incident. Proper key management is essential in maintaining the integrity as well as the confidentiality of the information.

Data User Module: The consumers utilize proxy re-encryption keys in order to securely decrypt the data. The module provides assurance that consumers are able to access information they have permission to see without undermining security.

3. Technical Concepts & Details Key :

Concepts: There are several key concepts on which the approach is built, namely.

Blockchain and Distributed Ledger Technology (DLT): Guarantees transparency and immutability of data, which are essential for trust in a decentralized environment.

Smart Contracts: Automate the process of controlling access, which minimizes the need for human intervention and any chance of error by a human.

Cryptographic Techniques: How AES and Proxy Re-Encryption are involved ensures safe protection of data in regards to keeping confidential information confidential, which is critical.

4. Technical Challenges and Solutions:

Key Management Complexity: Securely distributing and revoking encryption keys in the absence of a central authority ends being a key challenge, and this project addresses this challenge through a hierarchical key management system that can handle keys with greater efficiency.

Transaction Costs: Gas fees on public blockchains can have an impact on scalability. This proposal indicates redeploying the chunks to a Layer 2 scaling solution, sidechains or rollups, allowing the solution to continue while combating transaction costs.

Latency: Any delays associated with blockchain verification, which can affect real-time access control, will also be considered in this project. At each step of use in the workflow, this project was built to help blockchain interactions for decreasing latency in user experience.

VI.CONCLUSION

The "Decentralized and Privacy-Preserving Access Control for Digital Services" project is a noteworthy development in the push for improved user privacy and data security in online settings. The project harnesses blockchain technology and removes reliance on centralized authorities, enabling users to control their own data, which is vital at a time when incidents of unauthorized access to data are climbing, raising a number of issues for a user. This decentralization allows users to manage access control policies, while not disclosing sensitive information to third parties.

Advanced cryptographic methods, including AES-256 encryption and proxy re-encryption, amplify the security structure of the system. These methods guarantee the confidentiality of data and protection from unauthorized access, while allowing for data sharing between authorized individuals. Smart contracts facilitate access permission enforcement to automate the process. This allows for an expedited process and reduces the chance for human error. Preliminary testing showed positive results and demonstrated a significant reduction of unauthorized access risks and confirmed the possibility of effectiveness of proposed solutions.

As this project propels forward, many possibilities for future improvements and extensions arise. There are plans to add multiple blockchain networks, and investigate new security mechanisms (for example, hashed biometric data for KYC verification), which increase the utility and adaptability of the system for a variety of industries. In conclusion,

the project creates a secure digital service development capability, while also providing a foundation for subsequent research and developments related to decentralized access control, leading to greater security and privacy in the digital environment.

REFERENCES:

1. **Xu, R., Chen, Y., Blasch, E., & Chen, G.** (2018). *BlendCAC: A Blockchain-Enabled Decentralized Capability-Based Access Control for IoTs*.
2. **Xu, R., Chen, Y., Blasch, E., & Chen, G.** (2018). *A Federated Capability-Based Access Control Mechanism for Internet of Things (IoTs)*.
3. **Xu, R., Chen, Y., Blasch, E., & Chen, G.** (2018). *An Exploration of Blockchain Enabled Decentralized Capability-Based Access Control Strategy for Space Situation Awareness*.
4. **Hashemi, S. H., Faghri, F., & Campbell, R. H.** (2017). *Decentralized User-Centric Access Control Using PubSub over Blockchain*.
5. **Sathyabama, B., SureshKumar, C., Kesau, K., & Karthikeyan, R.** (2019). *Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds*. IJSRST+1ijcert.org+1
6. **Narve, P. N., & Patil, B. M.** (2016). *Secure Data Storage in Cloud by Decentralized Access Control*. IJCA
7. **Ruj, S., Stojmenovic, M., & Nayak, A.** (2014). *Privacy Preserving Access Control with Authentication for Securing Data in Clouds*. IJSRST+1ijcert.org+1
8. **Singh, A., & Hemalatha, M.** (2014). *Decentralized Access Control to Secure Data Storage on Clouds*. ijcert.org
9. **Zhao, X., Zhong, B., & Cui, Z.** (2023). *Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes*. MDPI
10. **Han, J., Susilo, W., Mu, Y., Zhou, J., & Au, M. H. A.** (2015). *Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption*. ACM Digital Library
11. **Kumar, R., & Patel, S.** (2021). *Proxy Re-Encryption for Secure Data Sharing in Cloud Computing*.
12. **Yu, S., Wang, C., Ren, K., & Lou, W.** (2010). *Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing*.
13. **Goyal, V., Pandey, O., Sahai, A., & Waters, B.** (2006). *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*.
14. **Yang, K., Jia, X., & Ren, K.** (2013). *DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems*. IJSRST+1ijcert.org+1
15. **Lewko, A. B., & Waters, B.** (2011). *Decentralizing Attribute-Based Encryption*. ijcert.org
16. **Chase, M., & Chow, S. S. M.** (2009). *Improving Privacy and Security in Multi-Authority Attribute-Based Encryption*. ijcert.org
17. **Nishide, T., Yoneyama, K., & Ohta, K.** (2008). *Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures*. ACM Digital Library
18. **Cui, H., Deng, R. H., Wu, G., & Lai, J.** (2016). *An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures*. ACM Digital Library
19. **Zhao, C., Xu, L., Li, J., Fang, H., & Zhang, Y.** (2022). *Toward Secure and Privacy-Preserving Cloud Data Sharing: Online/Offline Multi-Authority CP-ABE with Hidden Policy*. ACM Digital Library
20. **Han, S., Han, K., & Zhang, S.** (2019). *A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era*. MDPI
21. **Johnson, M., & Wang, L.** (2020). *Decentralized Identity Management Using Blockchain*.
22. **Rouhani, S., Belchior, R., Cruz, R. S., & Deters, R.** (2021). *Distributed Attribute-Based Access Control System Using Permissioned Blockchain*. ACM Digital Library

23. **Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I.** (2021). *Distributed Ledger Technology Review and Decentralized Applications Development Guidelines*. ACM Digital Library
24. **Hu, V. C., Ferraiolo, D., & Kuhn, D. R.** (2006). *Assessment of Access Control Systems*. ACM Digital Library
25. **Benantar, M.** (2005). *Access Control Systems: Security, Identity Management and Trust Models*. ACM Digital Library
26. **Rouhani, S., & Deters, R.** (2019). *Blockchain Based Access Control Systems: State of the Art and Challenges*. ACM Digital Library
27. **Natarajan, H., Krause, S. K., & Gradstein, H. L.** (2019). *Distributed Ledger Technology (DLT) and Blockchain*. ACM Digital Library
28. **Hu, V. C., Ferraiolo, D., Kuhn, D. R., & Schnitzer, A.** (2013). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)*.