IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

Enhancing Privacy and Security in Distributed Data Sharing through Re-Encryption

Komal Varpe[1], Shraddha Umbarkar[2], Rohit Kalekar[3], Shashank Singh Rajawat[4], K. S. Mulani[5]
Department of Computer Engineering[1,2,3,4,5]
Sinhgad Institute of Technology, Lonavala, India

Abstract: *Data sharing in cloud computing is a valuable application, but data security remains a concern. To address this, we propose a proxy re-encryption method for secure data transfer in the cloud. Using identity-based encryption, data owners can send encrypted data to the cloud, while authorized users can access it through proxy re-encryption. In IoT environments, an edge device acts as a proxy server, performing complex calculations due to limited device capacity. Leveraging information-centric networking, we enhance service quality and network bandwidth by efficiently utilizing cached data in the proxy. Our system is built on blockchain technology, enabling decentralized data sharing, improving centralized systems' effectiveness, and enabling fine-grained data access management. Through a security study and evaluation, our system offers privacy protection, authenticity, and reliability.*

Keywords: Role-based Access Control (RBAC), Blockchain, Cryptography, Decentralized, Distributed Systems, Cloud Storage

I. INTRODUCTION

In recent years, cloud computing has become an increasingly popular way to store and share data due to its cost effectiveness and accessibility. However, with the rise of cloud-based data sharing, security and privacy concerns have emerged as major challenges. To address these concerns, blockchain technology has been proposed as a promising solution for secure data sharing. Blockchain's distributed and immutable ledger offers a secure and transparent platform for data sharing. However, traditional blockchain systems suffer from scalability and efficiency issues, limiting their applicability in large-scale data sharing scenarios. In this context, this research paper proposes a Data Re-Encryption (DRE) approach to enable secure and efficient data sharing in the cloud using blockchain technology. The proposed approach uses smart contracts to manage access control and re-encryption keys, ensuring that only authorized users can access the shared data. Re-encryption is performed by a trusted third party, i.e., a service provider, which transforms the encrypted data from the owner's key to the recipient's key without revealing the original data. The proposed approach also incorporates a consensus algorithm to ensure the integrity of shared data, and a decentralization mechanism to distribute the blockchain network. The effectiveness of the proposed DRE approach is evaluated through simulation, demonstrating its security, efficiency, and scalability.

II. PROXY RE-ENCRYPTION APPROACH

To address the limitations of ABE and RBAC, we propose a hybrid approach that combines the traditional multi-authority scheme with RAAC. Our approach enables secure and robust data sharing through a proxy re-encryption strategy that allows legitimate users to access data while leveraging the resource limitations of Internet of Things (IoT) devices. The edge device acts as a proxy server to perform complex calculations, and notification-centric networking capabilities serve cached content in proxies to increase quality of service and network bandwidth. We implement our system on blockchain, which allows for decentralized data sharing, reduces inefficiencies in centralized systems, and provides fine-grained data access management. Our security studies and evaluations show that our approach achieves privacy, security, integrity, and reliability. In this paper, we propose a proxy re-encryption strategy to enable secure data sharing in cloud contexts. Our approach combines the traditional multi-authority scheme with RAAC and utilizes blockchain technology for decentralized data sharing. Our security studies and evaluations show that our approach achieves privacy, security, integrity, and reliability while improving quality of service and network bandwidth.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

A. Blockchain

Blockchain is a decentralized, distributed ledger technology that provides a secure approach to data storage for various transaction systems. It has been introduced to achieve the highest level of data security during data transactions and eliminate data attacks from various networks, as well as malicious requests. One of the main advantages of blockchain is that it is based on a consensus algorithm that ensures all nodes on the network agree on the state of the ledger.

B. Decentralization

A decentralized framework is needed to guarantee scalability and resiliency, and to restore many-to-one traffic flows. By using such a decentralized framework, we can remove the same frustration or single-purpose data push. In our model, we use a decentralized coverage system to ensure data is distributed across the network in a secure manner.

C. Authentication of data

A user's system or cloud administration stores sensitive information that should be moved to the blockchain system. During transmission, information can be changed or lost. Protection of such off-base changed information adds weight to the framework and may result in patient harm (death). To guarantee that the information is not modified, we use a light digital signature plot. On the receiver side, the data is verified with the digital signature of the user and when successfully received, it sends an acknowledgment of the data to the patient.

D. Smart contracts

In addition to its use as a distributed ledger, blockchain also allows for the creation and execution of smart contracts. These are self-executing contracts with the terms of the agreement directly written into lines of code. The code and the agreements contained therein exist on the blockchain and are executed automatically when certain conditions are met.

III. LITERATURE SURVEY

The paper provides a brief overview of smart contracts and how they can be used to transfer/control assets or digital flows between parties. The author highlights the advantages of using blockchain technology for storing these contracts due to its security and obscurity. The paper also discusses how smart contracts can enforce policies and contracts, making them a valuable tool for businesses.

This paper proposes an approach to integrate blockchain technology with the internet of things (IoT) by using smarthome technology to understand how IoT can be blocked. The paper introduces blockchain technology into IoT to provide additional security features, but acknowledges that it cannot provide a generic form of blockchain solution for IoT use cases.

The paper presents a multi-user system for access control to datasets stored in an untrusted cloud environment. The approach provides access control to data stored in the cloud without provider investment. The paper proposes a dynamic feature-based encryption scheme as the main tool of the access control mechanism and uses a blockchain-based decentralized ledger to provide an immutable log for all meaningful security events.

The paper proposes a basic IoT blockchain fusion model with four layers that contain different types of IoT devices. The paper discusses how distributed file systems can be used to store large amounts of IoT data. The paper also provides a case study for a blockchain-based IoT application, Machine-to-Machine (M2M) Autonomous Business System, on the Ethereum blockchain. The proposed system uses smart contracts for device registration, data storage, service provision, and fair payments.

The Edgen platform is introduced as a blockchainenabled edge computing platform that uses masternode technology to connect a closed blockchain-based system to the real world. Masternodes, which consist of full nodes of the blockchain and collateral, are deployed on Mobile Edge Computing's Edge Cloud to facilitate the running of Edge Cloud IoT dApps.

The HCloud platform is introduced as a reliable JointCloud platform for IoT systems using a serverless computing model. The platform allows an IoT server to execute multiple server-less functions and schedules these functions to different clouds based on a schedule policy. Blockchain technology is leveraged to ensure that the system cannot fake the cloud state or send target tasks incorrectly.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

A decentralized gasified service exchange platform is introduced where solution providers can dynamically provide and request services in an autonomous peer-to-peer fashion. The platform is based on blockchain technology to provide a tokenized economy where IoT solution providers can implement gasification techniques using smart contracts to maximize profits while offering and requesting services. Costs and decisions to exchange services during operation are set based on gasification strategies as per business objectives.

Vipul Goyalet. Al develops a new cryptosystem to properly share encrypted data, which we call Key-Policy Attribute-Based Encryption (KPABE). In our cryptosystem, the Cephet text is labeled with a set of properties and controls that connect the private key access configuration that the user can decrypt the encryption with. We demonstrate the utility of our product for sharing audit log information and broadcast encryption. Our creation supports private key providers, which subscribe to Hierarchical Identity-Based Encryption (HIBE).

They offer secure electronic health record (EHR) systems based on specialty-based crypto co-occupants and blockchain technology. In our system, we use attributebased encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and identitybased signature (IBS) to apply digital signatures. To achieve the various functions of ABI, IBE and IBS in crypto, we introduce a new cryptographic primitive, called Combined FeatureBased / Identity-Based Encryption and Signature (C-AB / IB-ES). This simplifies system maintenance and eliminates the need to install separate cryptographic systems for various security requirements. In addition, we use blockchain technology to ensure the integrity and verification of medical data. Finally, we offer a demonstration application for medical insurance business.

The seeds required for key generation and a scheme to manage public keys using blockchain. Is a random seed generation scheme necessary for generating the first key? Seeds are created using reverse engineering, out-of-band communication, and hardware variations to avoid the risk of man-in-the-middle attacks. Second is the key management system using blockchain for IoT? The scheme we propose is to distribute public keys on a blockchain network. The public key is used to encrypt the session key that will be used for communication between the devices

Overall, the literature survey provides a good overview of the current state of research in the field of blockchain and IoT. The papers cover different aspects of the integration of these two technologies, including smart contracts, access control, and fusion models

IV. SYSTEM ARCHITECTURE

A. Figures

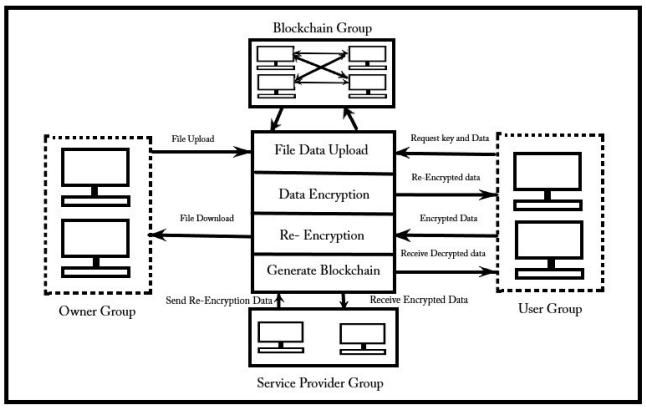


Fig. 1. System Architecture of Proposed System

The system utilizes a blockchain architecture and requires verification of previous blocks before committing new blocks. Users can access data through the internet 24/7. If an unauthorized user or third party attacker changes a block, the system will detect the invalid blockchain during the transaction. To recover from this situation, the system leverages other trusted data nodes to rebuild the blockchain through a majority consensus algorithm. When a user initiates a transaction, the node responsible for recording and transmitting data will authenticate the behavior through a consensus algorithm such as Proof of Work or Proof of Stake. Once the transaction is verified, the data is stored in a new block. All nodes in the network must authenticate the transaction before the data can be added to the blockchain.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

B. Registration and Authentication
Allows data owners, service providers, and users to create their own profiles and authenticate their identity.

C. Data Uploading
Provides the ability for data owners to upload files, which are then encrypted and stored in the database along with their corresponding encryption scheme and keys.

D. Re-Encryption Approach Data Sharing
Enables service providers to perform a re-encryption approach on data, which can then be shared with any user within a cloud group.

E. Access Control
Provides access control for users to view or access files shared with them by other users.

F. File Request and Download
Allows users to request and download files, with key verification being performed before granting access.

G. Distributed Blockchain
Represents the current state of delegated access rights within the system using a distributed ledger (Blockchain). Permissions for interacting with the Blockchain are handled by the Root User Authority and the Authorities.

V. ALGORITHM AND METHODOLOGIES

A. Hash Generation
Input : Genesis block, Previous hash, data d,
Output : Generated hash H according to given data
Step 1 : Input data as d
Step 2 : Apply SHA 256 from SHA family
Step 3 :CurrentHash= SHA256(d)
Step 4 : Return CurrentHash

B. Mining Algorithm for valid hash creation
Input : Hash Validation Policy P[], Current Hash Values hashVal
Output : Valid hash
Step 1 : System generate the hash Val for ith transaction using Algorithm 1
if (hash Val.valid with P[])
Valid hash
Flag =1
Else
Flag=0
Mine again randomly
Step 3 : Return valid hash when flag=1

VI. PROTOCOL FOR PEER VERIFICATION

Input : User Transaction query, Current Node Chain CNode[chain], Other remaining Nodes blockchain NodesChain[Nodeid] [chain]
Output : Recover if any chain is invalid else execute current query
Step 1 : User generate the any transaction DDL, DML or DCL query
Step 2 : Get current server blockchain CchainCnode[Chain]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

Step 3 : For each End for
Step 4 : Foreach (read I into NodeChain) If (!.equals NodeChain[i] with (Cchain)) Flag 1 Else Continue Commit query
Step 5 : if (Flag == 1) Count = SimilaryNodes-
Blockchian()
Step 6 :Cacluate the majority of server Recover invalid blockchin from specific node
Step 7: End if
End for
End for

VII. APPLICATIONS

The Data Re-Encryption Approach to Secure Data Sharing using blockchain has several potential applications, including:

A. Secure Cloud Storage

This project can be used to provide a secure cloud storage solution, where users can upload their data and share it with others using a secure re-encryption approach. This can be especially useful for businesses that need to store sensitive data in the cloud, such as financial records, medical records, or intellectual property.

B. Decentralized Social Networks

This project can be used to create a decentralized social network that provides users with full control over their data and privacy. With the help of blockchain and re-encryption, users can securely share their data with their trusted contacts, without relying on centralized social media platforms.

C. Supply Chain Management

This project can be used to create a secure and transparent supply chain management system, where all stakeholders can securely share data and track the movement of goods. With the help of blockchain, users can verify the authenticity of the data, and re-encryption can be used to ensure that only authorized parties can access sensitive information.

D. Electronic Health Records (EHRs)

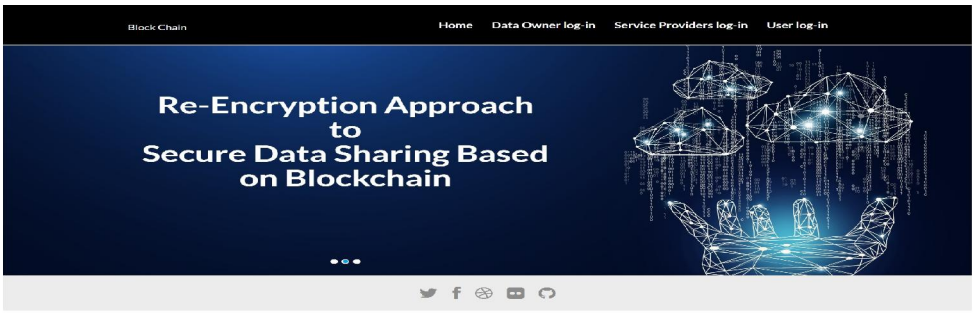
This project can be used to secure the sharing of electronic health records between healthcare providers and patients. By using blockchain and re-encryption, patients can securely share their medical records with their healthcare providers, while maintaining their privacy and control over their data.

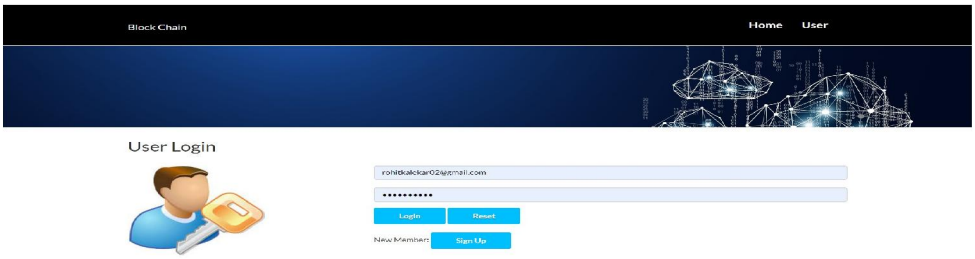
E. Digital Identity Management

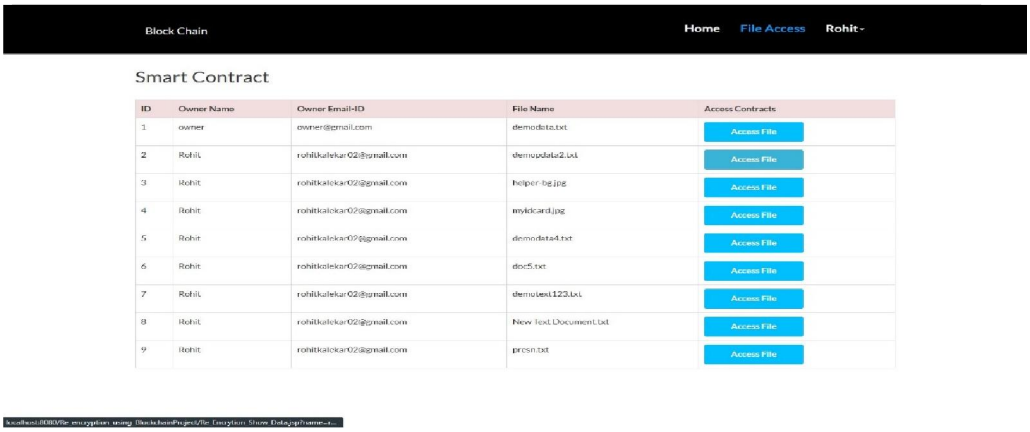
This project can be used to create a decentralized digital identity management system, where users can control their own data and authenticate themselves without relying on centralized identity providers. With the help of blockchain and re-encryption, users can securely share their identity data with third parties, without compromising their privacy.

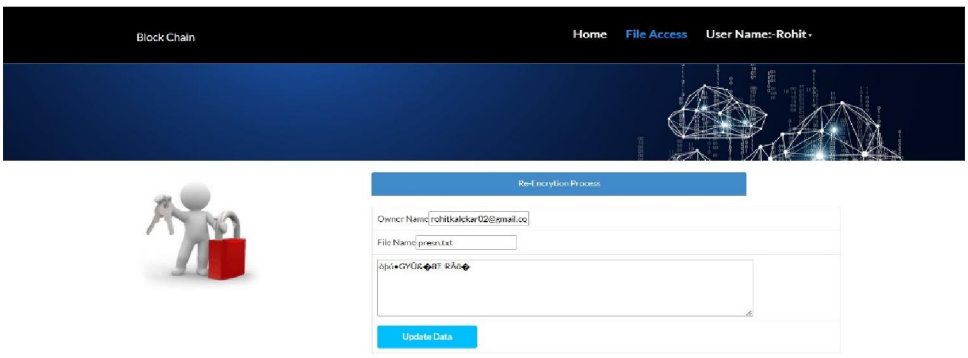
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

VIII. RESULT AND DISCUSSIONS









IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 13, May 2023

IX. CONCLUSION

The major outcome of this project is the creation of a software system prototype that applies the system's access control paradigm to data stored in unsaturated settings.

Acceptable complexity, functionality, and implementation complexity have been chosen to implement the system algorithms. The major outcome of this project is the creation of a software system prototype that applies the system's access control paradigm to data stored in unsaturated settings. Acceptable complexity, functionality, and implementation complexity have been chosen to implement the system algorithms. The ability to customise the access policy for encrypted data without duplicating people to a large number of participants; the ability to define dynamic access policies; access policy change does not require any additional action from other members of a social system, which eliminates the need for regular changes to user keys; the integrity of information about all transactions, including granting and changing access, facts gain a higher level of assurance. A blockchain-based system concept that enables flexible encryption data authorisation.

REFERENCES

[1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, -preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2019.

[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144151, 2019.

[3] J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2019, pp. 187 206.

[4] Xu, Jinliang, et al Edgence: A blockchain-enabled edge-computing platform for intelligent IoTbaseddApps. China Communications 17.4 (2020): 78-87.

[5] Huang, Zheng, Zeyu Mi, and Zhichao Hua. HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain. China Communications 17.9 (2020): 1-10.

[6] Gheitanchi, Shahin. Gamified service exchange platform on blockchain for IoT business agility 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.

[7] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870885, 2019.

[8] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute- keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116 131, 2017.

[9] Choi, Jungyong, et al. quot;Random Seed Generation For IoT Key Generation and Key Management System Using Blockchain.quot; 2020 International Conference on Information Networking (ICOIN). IEEE, 2020.

[10] "Data sharing in cloud computing using blockchain and re-encryption." by S. Chaudhary, P. Kumar, and V. Tyagi. Future Generation Computer Systems 112 (2020): 441-452.