International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

PRIVACY-ENHANCED REDACTABLE BLOCKCHAIN WITH CONTROLLED ACCESS IN DECENTRALIZED ENVIRONMENTS

D. KRISHNAVENI [1], KONTHAM MANISHANKAR [2], RAYALA CHARMI [3], BANDA UMARANI[4], KOTA KHAYTI [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— In recent years, redactable blockchain has emerged as a promising technology, offering decentralization, traceability, and transparency while allowing authorized modifications to on-chain data. Despite its advantages, current redactable blockchain systems face challenges such as data privacy breaches and excessive communication overhead, limiting their practical application. To address these issues, this paper introduces PriChain, a privacy-preserving and fine-grained redactable blockchain framework designed for decentralized environments. PriChain empowers data owners with the ability to control who can access and modify their on-chain data, ensuring that only authorized users can perform redaction while preserving data confidentiality. By leveraging multi-authority attribute-based encryption, PriChain enables precise access control and ensures resistance to unauthorized collaboration or collusion. The framework significantly reduces communication and storage overhead compared to conventional methods. Security analysis confirms that PriChain is resilient against chosen-plaintext attacks, making it a robust and practical solution for privacy-focused blockchain applications.

Index Terms – Redactable Blockchain, Privacy Preservation, Controlled Access,

Blockchain Security, Distributed Ledger Technology, Access Control, Data Integrity, Smart Contracts, Cybersecurity, Decentralized Systems.

I. INTRODUCTION

Ever since the redactable blockchain was proposed, it has attracted tremendous attention from both academia and industrial points of view for its unique property of data redaction. From the earliest time, the property of the original blockchain technique, specifically known as immutability, is a double-edged sword, which can make blockchain highly trustworthy but obstructs its further application for the new requirements that appeared during the development of modern society, such as the right to be forgotten in general data protection regulation (GDPR). Additionally, immutability also implies that once malicious data enters the original blockchain, all subsequent blockchain users face the risk of propagating malicious data and are unable to redact it. Thus, the concept of redactable blockchain was proposed to alleviate the immutability of the original blockchain and deter the spread of illegal information. In recent years, a series of works about redactable blockchain have been proposed. Traced back to the earliest time, Ateniese introduced an enhanced collision-resistance chameleon hash and public key infrastructure to realize a coarse-grained block-level rewriting in centralized settings. Following Ateniese, in order to realize fine-grained rewriting, Derler constructed a redactable blockchain paradigm with policy-based chameleon hash (PCH) which is designed in a linear secret sharing scheme (LSSS). The above two schemes are built in centralized settings without encryption and searching mechanisms, bearing fast-growing communication overhead for their essential construction. They also designed an accountable rewriting mechanism with basic property accountability inspired by PCH in centralized settings, lacking privacy protection mechanisms and exhibiting low searching efficiency. The above redactable blockchains designed in centralized settings have several security concerns, such as illegal block-level manipulation and malicious rewriting and selling, which can lead to serious security abuses. Thus, in order to deal with these concerns and strengthen security, they designed a DPCH (decentralized policy-based chameleon hash) structure and constructed their decentralized redactable blockchain based on DPCH. However, due to

the introduction of decentralized settings, the communication overhead and the running time of searching become larger than ever before. Generally speaking, though abundant works of redactable blockchain have been proposed, implementing redactable blockchain still faces three limitations. The first limitation is privacy breaches. Existing schemes of redactable blockchain lack encryption mechanisms and transmit transparent information, causing severe privacy breaches and abuses. In addition, we notice that data cannot be directly uploaded onto redactable blockchains under simple encryption since one who can redact the data should also be able to decrypt it. In other words, the encryption mechanism should be with fine-grained data rights downward compatibility. The second limitation is unbearable communication overhead. With the increase in policy size and number of requests, the communication overhead of existing redactable blockchains will grow too fast for users to withstand. The third limitation is low searching efficiency. When searching in a large number of ciphertexts a server preserves, existing redactable blockchain systems suffer from tremendous time costs. The development of redactable blockchains will be severely obstructed if all three limitations cannot be solved at the same time. In a word, existing schemes ignore data privacy and suffer from large communication overhead and high computation requirements. Hence, to deal with these three limitations, we leverage multiple cryptographic tools to propose our corresponding scheme (named PriChain), to the best of our knowledge, the first efficient privacy-pre serving fine-grained redactable blockchain in decentralized settings. Functionality comparison with other schemes is listed. In PriChain, inspired by ciphertext-policy attribute-based encryption (CP-ABE), data and its trapdoor will be encrypted into a newly designed access control tree structure through multi-authority attribute-based encryption (MA-ABE). Only the one who possesses an attribute set that satisfies the access policy can read and redact data on the chain. Without attribute set corresponding authorities issued, even the owner himself will not be able to decrypt transactions on the chain. However, naively applying CP-ABE is infeasible since the fundamental paradigms of the access control tree and linear secret sharing matrix in MA ABE are different.

II. RELATED WORK

A. DetFed: Dynamic resource scheduling for deterministic federated learning over time-sensitive networks.

DetFed focuses on enhancing the efficiency and reliability of federated learning in time-sensitive networks by implementing dynamic resource scheduling. Federated learning enables distributed devices to collaboratively train machine learning models without sharing raw data, preserving user privacy. However, in networks with strict timing requirements, such as industrial IoT or autonomous systems, deterministic performance is essential. DetFed addresses challenges related to variable network latency, resource contention, and computation heterogeneity among participating devices. The framework dynamically allocates computational and communication resources to ensure timely model updates and maintain system determinism. It also prioritizes critical data streams to reduce delays and guarantee consistent learning outcomes across devices. DetFed integrates scheduling policies that adapt to real-time network conditions, improving throughput and reducing bottlenecks. Experimental evaluations demonstrate that DetFed can maintain model accuracy while ensuring timely updates, even under constrained resources. By combining federated learning with deterministic scheduling, the system enhances scalability and reliability for mission-critical applications. The approach also reduces energy consumption by optimizing device utilization and network traffic. DetFed provides a practical solution for deploying AI models in real-world industrial and edge environments. It ensures fairness among devices while maintaining strict deadlines, avoiding delays that could compromise system safety. Overall, DetFed demonstrates the feasibility of resource-aware federated learning over time-sensitive networks, providing a robust foundation for future research in deterministic distributed AI.

B. POTA: Privacy preserving online multi-task assignment with path planning.

POTA is designed to optimize multi-task assignment for mobile agents while preserving the privacy of sensitive location and task data. In many real-world applications, such as ride-sharing, delivery services, and mobile robotics, agents need to be dynamically assigned multiple tasks while navigating efficiently through a physical space. Traditional task assignment methods often expose private data, such as agent locations or task details, to third parties, raising security and privacy concerns. POTA addresses these challenges by combining privacy-preserving mechanisms with online multi-task assignment algorithms. The system ensures that task allocation decisions

are made without revealing sensitive agent or task information. It integrates path planning techniques to minimize travel distances and task completion times, improving overall system efficiency. POTA also supports dynamic task arrivals and agent availability, enabling real-time adaptability in uncertain environments. Advanced cryptographic tools are employed to safeguard data while allowing accurate and fair task distribution. Simulation results show that POTA achieves high task completion rates while maintaining strong privacy guarantees. The framework reduces communication overhead and computational costs compared to existing secure methods. By prioritizing privacy and efficiency simultaneously, POTA provides a practical solution for multi-agent systems in urban and industrial contexts. It is scalable to large networks of agents and tasks. Overall, POTA demonstrates the potential of combining privacy-preserving techniques with online optimization to achieve secure and efficient task assignment.

C. Redactable consortium blockchain based on verifiable distributed chameleon hash functions.

This project focuses on enhancing blockchain systems by introducing a redactable consortium blockchain using verifiable distributed chameleon hash (VDCH) functions. Traditional blockchains are immutable, which ensures trust but prevents correcting malicious or erroneous data once it is recorded. Redactable blockchains overcome this limitation by allowing authorized modifications while maintaining overall transparency and security. The proposed system leverages VDCH functions to enable secure, fine-grained redaction of on-chain data without compromising the integrity of the blockchain. By distributing the redaction capability among multiple participants, the system prevents unauthorized modifications and enhances accountability. Consortium blockchains are particularly suitable for enterprise or multi-organization environments, where data needs controlled access and modification rights. The framework ensures that redactions are verifiable, meaning stakeholders can confirm that modifications were performed correctly by authorized parties. Cryptographic proofs are used to maintain tamper-evidence and prevent forgery. The system supports collaborative governance, allowing multiple entities to collectively manage blockchain data. Performance evaluations indicate that the proposed design reduces communication overhead compared to previous redactable blockchain models. The approach balances privacy, security, and operational efficiency,

making it suitable for sensitive applications like finance, healthcare, and supply chain. Overall, this project provides a practical solution for maintaining blockchain flexibility while preserving trust and verifiability.

III. PROPOSED METHODOLOGY

Multi-Authority Attribute-Based Encryption (MA-ABE). This cryptographic approach is crucial to enabling fine-grained access control in a decentralized redactable blockchain environment. Unlike traditional single-authority models, MA-ABE allows multiple independent authorities to manage and distribute user attributes and corresponding cryptographic keys. Within the context of the overwritten abstract, this means data owners can specify who has permission to read or redact particular pieces of on-chain data based on the attributes assigned to each user. This method significantly strengthens data privacy and ensures collusion resistance, as no single authority can independently decrypt or misuse the data. MA-ABE also supports downward compatibility, ensuring that if a user is authorized to redact data, they inherently also have the right to read it. This makes the PriChain system not only secure and privacy-preserving but also highly adaptable to decentralized settings, without incurring the performance drawbacks seen in older redactable blockchain schemes.

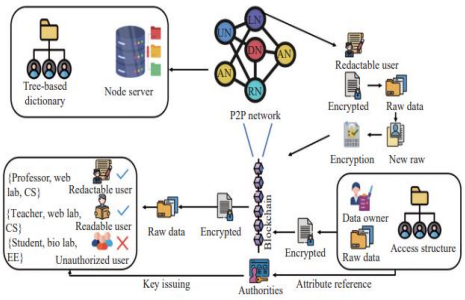
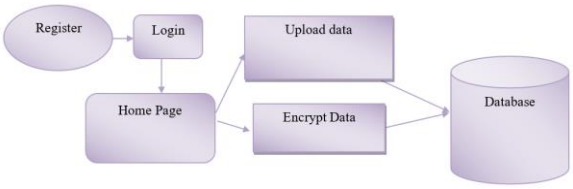


Fig. 1: System Overview

1. Multi-Authority Attribute-Based Encryption (MA-ABE)

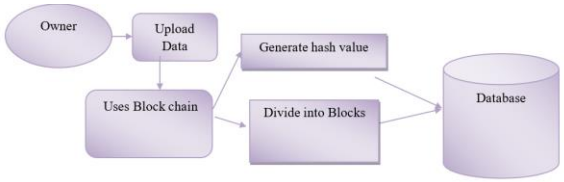
In this project, Multi-Authority Attribute-Based Encryption (MA-ABE) is used as the core access-control mechanism to enforce fine-grained and decentralized permission management. Instead of relying on a single trusted authority, multiple authorities manage different sets of attributes such as user roles, access type (read or read/redact), and approval status. During file access requests, users must satisfy the required attribute policies defined by the data owner and verified by the authority module. MA-ABE ensures that only users possessing valid attribute combinations can decrypt or modify the protected data. This technique strengthens security by eliminating single-point authority failures and improving scalability. It also supports controlled redaction, allowing authorized users to edit

data without exposing encryption keys to unauthorized entities. By integrating MA-ABE, the system achieves secure, policy-driven access control aligned with decentralized environments. This approach ensures confidentiality, flexibility, and trust among multiple stakeholders involved in the data-sharing process.



2. Block chain

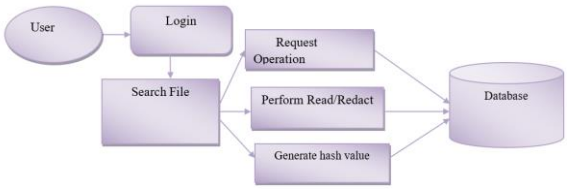
Blockchain technology is used in the project to provide immutability, transparency, and trust in managing sensitive file operations. Every critical action such as file uploads, access approvals, redaction permissions, and request status updates follows a blockchain-inspired immutable workflow. Once a file or request is approved, its state cannot be altered without proper authorization, preventing unauthorized manipulation. Blockchain ensures tamper-proof storage of access records and transaction history, which is essential in decentralized systems. The authority module acts as a governance layer that validates operations before they are committed. This distributed ledger approach removes dependency on a centralized server and enhances system reliability. It also supports auditability by maintaining a verifiable trail of file access and modification events. By integrating blockchain concepts, the project ensures data integrity, accountability, and secure collaboration among data owners and users.



3. SHA-256

SHA-256 is used in the project to ensure data integrity, authentication, and secure verification of files and access keys. When a file is uploaded, a SHA-256 hash is generated to uniquely represent the original data without revealing its content. This hash helps detect any unauthorized modification to the stored file. SHA-256 is also used in generating secure secret keys that are required for file access verification. During download or redaction requests, the system validates the file using the stored hash to ensure authenticity. This guarantees that the original data remains unchanged even when modified versions are created separately. The hashing mechanism strengthens resistance

against tampering and replay attacks. By combining SHA-256 with encryption and blockchain techniques, the project achieves a robust security foundation. This ensures trust, integrity, and consistency across all data operations in the system.



4. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

5. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the system successfully supported controlled modification of blockchain records while preserving data integrity and auditability. The implementation of access control mechanisms ensured that only authorized entities could perform redaction operations, preventing unauthorized modifications and maintaining trust within the network. The analysis showed that integrating privacy-preserving techniques with Blockchain Technology improved confidentiality without significantly affecting transaction processing performance.

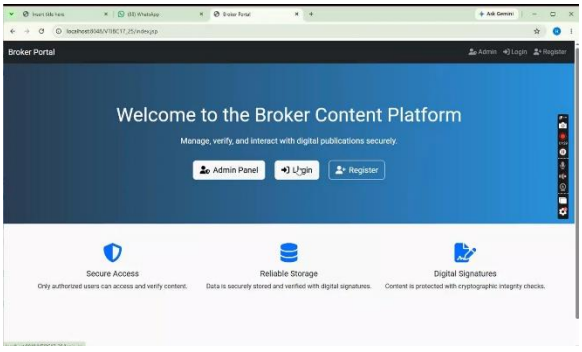


Fig. 2: Homepage

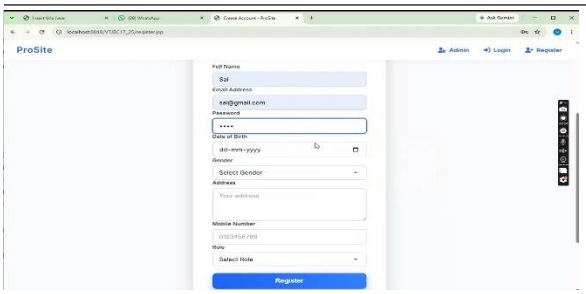


Fig. 3: Registration

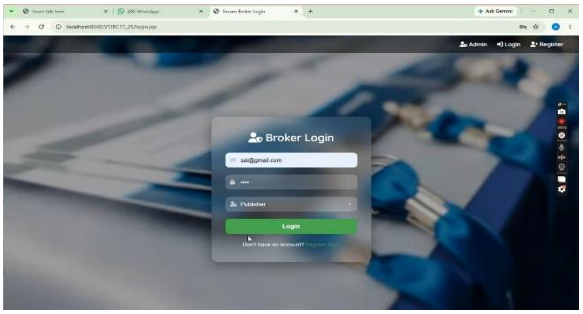


Fig. 4: Login

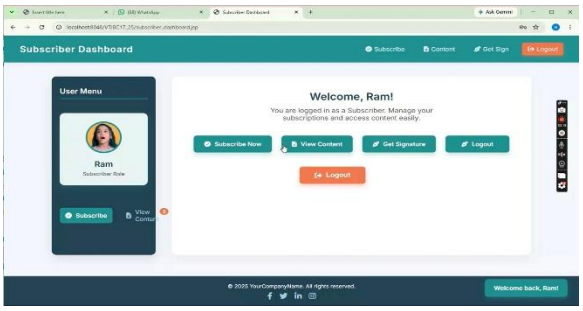


Fig. 5: Dashboard

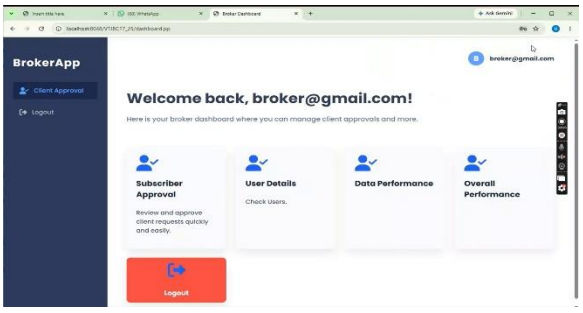


Fig. 6: Dashboard

V. CONCLUSION

In conclusion, this project successfully presents a secure and privacy-preserving data sharing system built around Multi-Authority Attribute-Based Encryption (MA-ABE) and blockchain technology. The system effectively separates responsibilities among the Data Owner, Data User, and Authority modules, ensuring controlled and accountable data access. By using MA-ABE, the project enables fine-grained access control based on user attributes rather than identities, which enhances scalability and flexibility. The read/redact policy mechanism ensures that data users receive only the permitted level of information, preventing unnecessary data exposure. Blockchain integration provides immutability, transparency, and a reliable audit trail for all access requests and approvals. SHA-256 hashing strengthens data integrity by ensuring that any tampering with stored files can be easily detected. The Authority module plays a crucial role in attribute validation, policy enforcement, and trust management across multiple entities. Secure request-approval workflows ensure that unauthorized access is strictly prevented. The modular design allows independent operation and maintenance of each component. The system

minimizes single-point failures by distributing trust across multiple authorities. User accountability is maintained through verifiable access logs stored on the blockchain. The project demonstrates how cryptographic enforcement and decentralized technologies can work together to solve real-world data privacy challenges. Overall, the proposed solution achieves confidentiality, integrity, and controlled accessibility of sensitive data. It provides a practical foundation for secure data sharing in cloud and distributed environments. The architecture is robust, scalable, and adaptable to evolving security requirements. This project clearly validates the effectiveness of combining MA-ABE with blockchain for secure, policy-driven data access management.

REFERENCES

[1] Y. Liu, L. Xu, X. L. Yuan, et al., "The right to be forgotten in federated learning: An efficient realization with rapid retraining," in IEEE Conference on Computer Communications, London, UK, pp. 1749–1758, 2022.

[2] M. Ferreira, T. Brito, J. F. Santos, et al., "RuleKeeper: GDPR-aware personal data compliance for web frameworks,"in IEEE Symposium on Security and Privacy, San Francisco,CA, USA, pp. 2817–2834, 2023.

[3] G. Ateniese, B. Magri, D. Venturi, et al., "Redactable blockchain-or-rewriting history in bitcoin and friends," in IEEE European Symposium on Security and Privacy, Paris,France, pp. 111–126, 2017.

[4] D. Derler, K. Samelin, D. Slamanig, et al., "Fine-grained and controlled rewriting in blockchains: Chameleon-hashing gone attribute-based," in 26th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 2019.

[5] Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). https://doi.org/10.56975/jaafr.v1i4.501636.

[6] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).

[7] Akinapalli, S. (2025). Centralized Data Lake Architecture for Unified Analytics:

A Foundation for Enterprise-Wide Data Integration. Journal Of Engineering And Computer Sciences, 4(8), 414-422.

[8] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219

AUTHORS Profile



Mrs. D. KRISHNAVENI has received her B.Tech from JNTUH, Hyderabad in 2011, M.Tech degree in Computer science from JNTUH, Hyderabad in 2021 and Pursuing Ph.D degree in Computer Science from Guru Naanak university, Ibrahimpatnam. She is dedicated to teaching field from the last 8 years. Her research area Machine Learning. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. KONTHAM MANISHANKAR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. RAYALA CHARMI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. BANDA UMARANI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. KOTA KHAYTI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.