IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

Proxy Re-Encryption Implementation for Safe Blockchain Based Data Sharing

Miss V. D. Vaidya[1], Pratiksha Ganesh Ingle[2], Sana Vajir Shaha[3], Ashwini Prakash Jagdale[4], Akshara Sanjay Zarekar[5]
[1, 2, 3,4,5] Department of Cloud Computing and Big Data
Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology and Engineering (Polytechnic), Pravaranagar

Abstract: *The rapid expansion of Internet of Things (IoT), cloud computing, and decentralized applications has significantly increased the demand for secure and efficient data-sharing mechanisms. Traditional encryption techniques, while effective in protecting data confidentiality, face limitations in scalability, flexible access control, and secure data delegation in distributed environments. To overcome these challenges, this project proposes a Proxy Re-Encryption (PRE) based framework integrated with blockchain technology to enable secure, controlled, and transparent data sharing. Proxy re-encryption allows encrypted data to be transformed for authorized users without revealing the original plaintext, thereby ensuring strong confidentiality even in the presence of semi-trusted intermediaries.*
The integration of blockchain technology further strengthens the system by providing a decentralized, immutable, and tamper-proof ledger for managing access permissions and recording data-sharing transactions. This approach eliminates reliance on centralized authorities while enhancing auditability and trust among participants. Additionally, the use of edge computing and information-centric caching improves system performance by reducing latency, network overhead, and computational load. The proposed framework effectively balances security, scalability, and efficiency, making it suitable for real-world applications such as IoT networks, healthcare data sharing, industrial systems, and smart city infrastructures.

Keywords: Proxy Re-Encryption, Blockchain Technology, Secure Data Sharing, IoT, Edge Computing, Access Control, Decentralized Systems

I. INTRODUCTION

1.1 Overview

In the present digital era, the volume of data generated and exchanged through interconnected systems has increased exponentially due to the rapid growth of cloud computing, Internet of Things (IoT), and smart applications. These technologies continuously generate sensitive information that must be shared across multiple users and platforms. As data becomes more distributed, ensuring its security, privacy, and controlled accessibility has become a major concern for researchers and industries. Traditional centralized data-sharing models struggle to cope with these challenges, making advanced security mechanisms essential.

Data security primarily focuses on maintaining confidentiality, integrity, and availability of information during storage and transmission. Conventional encryption techniques are widely used to protect sensitive data; however, they are not well suited for dynamic data-sharing environments. In scenarios where data needs to be shared with multiple users, data owners are often required to decrypt and re-encrypt data repeatedly, leading to high computational overhead and increased exposure to security risks. This limitation highlights the need for more flexible cryptographic solutions.

Proxy Re-Encryption (PRE) is an advanced cryptographic technique that addresses these challenges by allowing encrypted data to be securely transformed from one user's encryption key to another without revealing the original plaintext. In this approach, a semi-trusted proxy performs the re-encryption operation without gaining access to sensitive data. This capability enables secure delegation of access rights, making PRE highly suitable for distributed and multi-user environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

Despite the advantages of PRE, managing trust and access control in decentralized systems remains a significant challenge. Centralized access control authorities introduce risks such as single points of failure, data manipulation, and unauthorized access. To overcome these limitations, blockchain technology has emerged as a powerful solution by providing a decentralized, transparent, and immutable ledger for recording transactions and enforcing access policies.

Blockchain technology ensures that all data-sharing activities are securely logged and verified without relying on a central authority. Its immutable nature prevents tampering with stored records, while consensus mechanisms establish trust among participating entities. By integrating blockchain with proxy re-encryption, data owners can securely control access permissions while maintaining full ownership of their data in a trustless environment.

The combination of proxy re-encryption and blockchain creates a robust framework for secure data sharing. In this hybrid approach, PRE ensures data confidentiality during sharing, while blockchain manages authorization, verification, and auditability. This integration eliminates unnecessary decryption operations, reduces computational cost, and enhances overall system security in distributed environments.

With the increasing deployment of IoT devices, additional challenges such as limited computational resources, high latency, and energy constraints must be addressed. Edge computing plays a crucial role in this context by processing data closer to its source. By deploying proxy servers at the edge, re-encryption and access control operations can be performed efficiently, reducing communication delays and improving system responsiveness.

Information-centric networking and edge caching further enhance system performance by enabling frequently accessed encrypted data to be stored closer to users. This approach minimizes repeated data transmission, reduces network congestion, and improves data retrieval speed. Such optimizations are essential for real-time applications in smart cities, healthcare monitoring, and industrial automation.

The proposed system is designed to ensure confidentiality, integrity, and controlled access to sensitive data while maintaining scalability and efficiency. By leveraging proxy re-encryption, blockchain, and edge computing, the framework provides a secure and flexible data-sharing mechanism suitable for modern distributed environments. The system also supports transparent auditing and accountability, which are critical for compliance and trust management.

In conclusion, the integration of proxy re-encryption with blockchain technology represents a promising direction for secure data sharing in decentralized systems. This project focuses on designing and implementing such a framework to address the limitations of traditional encryption methods and centralized access control models. The proposed solution aims to provide a future-ready, secure, and scalable platform capable of supporting emerging applications in IoT, cloud computing, healthcare, and smart infrastructure.

1.2 Motivation

The rapid growth of cloud computing, Internet of Things (IoT), and decentralized applications has led to an unprecedented increase in the generation and exchange of sensitive data across distributed networks. Existing data-sharing mechanisms rely heavily on centralized architectures and traditional encryption techniques, which often suffer from scalability issues, complex key management, and limited flexibility in access delegation. These limitations increase the risk of data breaches, unauthorized access, and single points of failure. The need to ensure confidentiality, integrity, and controlled data access in dynamic and multi-user environments has strongly motivated the exploration of advanced cryptographic solutions.

Proxy Re-Encryption combined with blockchain technology offers a promising approach to overcome these challenges by enabling secure data sharing without exposing plaintext data or private keys. The motivation behind this project is to design a system that allows data owners to maintain full control over their data while securely delegating access rights in a decentralized and trustless environment. By integrating edge computing and blockchain-based access control, the proposed framework aims to improve security, transparency, and system efficiency, making it suitable for real-world applications such as IoT networks, healthcare systems, and smart city infrastructures.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

1.3 Problem Definition and Objectives

The rapid expansion of Internet of Things (IoT) and cloud-based systems has resulted in the continuous sharing of large volumes of sensitive data across decentralized and untrusted networks. Traditional encryption techniques are insufficient for such environments due to complex key management, limited scalability, lack of flexible access delegation, and dependence on centralized authorities. These limitations increase the risk of unauthorized access, data tampering, and single points of failure. Therefore, there is a critical need for a secure, decentralized, and efficient data-sharing mechanism that ensures confidentiality, integrity, and controlled access without exposing plaintext data or private cryptographic keys during data exchange.

Objectives

- To design a secure data-sharing framework using Proxy Re-Encryption
- To integrate blockchain technology for decentralized access control and transparency
- To ensure confidentiality and integrity of data during storage and sharing
- To enable flexible and fine-grained access delegation for authorized users
- To improve scalability and efficiency for IoT and cloud-based environments

1.4. Project Scope and Limitations

Project Scope

The scope of this project focuses on the design and implementation of a secure and decentralized data-sharing framework using Proxy Re-Encryption integrated with blockchain technology. The system enables data owners to securely store encrypted data and dynamically delegate access rights to authorized users without revealing plaintext data or private keys. Blockchain is used to manage access permissions, maintain transparency, and ensure immutability of data-sharing transactions, while proxy re-encryption allows ciphertext transformation through a semi-trusted proxy. The framework is designed to support confidentiality, integrity, and controlled access, making it suitable for distributed environments such as cloud platforms and Internet of Things (IoT) ecosystems.

The project also covers the use of edge computing and information-centric caching techniques to improve system efficiency and reduce latency. By performing re-encryption and access control operations closer to the data source, the system minimizes communication delays and computational overhead on resource-constrained devices. The proposed framework is applicable to real-world domains including healthcare data sharing, industrial automation, smart city infrastructure, and secure cloud storage systems. The project scope is limited to system design, algorithm implementation, and functional evaluation, providing a strong foundation for future enhancements and large-scale deployment.

Limitations

- The system performance may be affected by blockchain transaction latency and consensus overhead
- High computational requirements of cryptographic operations can impact resource-constrained IoT devices
- Scalability may be limited when handling a very large number of users and access requests
- Smart contract vulnerabilities may introduce security risks if not carefully designed
- Real-time implementation and large-scale deployment require additional infrastructure and optimization

II. LITERATURE REVIEW

Proxy Re-Encryption for Secure Data Sharing with Identity-Based Encryption (Pei et al., 2024)

This study explores the application of proxy re-encryption combined with identity-based encryption to address secure data sharing challenges in distributed environments. The authors emphasize that traditional public-key encryption systems require complex certificate management, which becomes inefficient in large-scale systems such as cloud and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

IoT networks. By using identity-based encryption, user identities act as public keys, significantly simplifying key management and improving system usability.

The paper further demonstrates how proxy re-encryption enables secure delegation of access rights without exposing plaintext data to intermediaries. Security analysis shows that the proposed scheme ensures confidentiality and resistance to chosen-plaintext attacks. The authors conclude that integrating proxy re-encryption with identity-based encryption provides a scalable and secure solution for decentralized data sharing, particularly in cloud-based applications.

Blockchain-Based Proxy Re-Encryption Scheme for Secure IoT Data Sharing (Manzoor et al., 2018)

This research presents a blockchain-enabled proxy re-encryption framework designed specifically for secure data sharing in Internet of Things environments. The authors identify that centralized cloud servers introduce trust and security concerns, including data tampering and unauthorized access. To overcome this, the proposed system uses blockchain as a decentralized access control mechanism while proxy re-encryption ensures secure data delegation.

The study highlights that blockchain smart contracts are used to enforce access policies and verify user permissions before re-encryption takes place. Performance evaluation demonstrates improved security and transparency compared to traditional cloud-based approaches. The authors conclude that the integration of blockchain and proxy re-encryption significantly enhances trust, auditability, and data confidentiality in IoT ecosystems.

A Proxy Re-Encryption Approach to Secure Data Sharing in IoT Based on Blockchain (Agyekum et al., 2021)

This paper focuses on securing IoT data sharing by integrating proxy re-encryption with blockchain technology and edge computing. The authors discuss the limitations of IoT devices, such as low computational power and energy constraints, which make traditional cryptographic techniques unsuitable. To address this, edge devices are used as proxy servers to perform re-encryption operations efficiently.

The blockchain component acts as a decentralized authority that manages access permissions and records data-sharing transactions. The proposed system achieves strong security properties, including confidentiality, integrity, and resistance to man-in-the-middle attacks. Experimental results show that the framework outperforms existing schemes in terms of computation time, making it suitable for real-time IoT applications.

An Improved Proxy Re-Encryption Scheme for IoT-Based Data Outsourcing in Cloud (Lin et al., 2020)

This study proposes an enhanced proxy re-encryption scheme aimed at securing data outsourcing in cloud-assisted IoT environments. The authors identify key challenges such as frequent access changes, user revocation, and data confidentiality in outsourced storage systems. Their approach improves key management efficiency while maintaining secure access control.

The paper demonstrates that the improved proxy re-encryption mechanism reduces computational overhead during encryption and decryption processes. Security analysis confirms resistance against collusion attacks and unauthorized access. The authors conclude that the proposed scheme is well suited for cloud-based IoT systems where data needs to be securely shared among multiple users.

Meta-Key: A Secure Data Sharing Protocol Using Blockchain-Based Storage (Li et al., 2017)

This research introduces a blockchain-based decentralized storage architecture for secure data sharing. The authors propose the Meta-Key protocol, which separates encryption keys from encrypted data and manages them using blockchain technology. This approach reduces reliance on centralized storage providers and enhances data security.

The study explains how blockchain ensures immutable key management and transparent access control. Experimental evaluation shows improved resilience against data breaches and unauthorized access. The authors highlight that blockchain-based key management systems provide a strong foundation for secure and scalable data-sharing platforms in distributed environments.

Proxy Re-Encryption Enabled Secure IoT Data Marketplace with Blockchain (Manzoor et al., 2021)

This paper proposes a secure and anonymous IoT data marketplace using proxy re-encryption and blockchain technology. The authors address the issue of trust in data marketplaces where data owners and consumers do not fully

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

trust each other. Proxy re-encryption allows secure data sharing, while blockchain ensures transparency and fairness in transactions.

The system enables data owners to control access rights and revoke permissions when required. Security evaluation shows strong resistance against identity leakage and unauthorized data access. The authors conclude that combining proxy re-encryption with blockchain provides a reliable solution for building secure and privacy-preserving IoT data marketplaces.

III. REQUIREMENT SPECIFICATIONS

HARDWARE REQUIREMENTS:

- System: Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- OS: Windows
- Languages: C/C++, Python, Java, Solidity (for smart contracts).
- Libraries: ECC & Proxy Re-Encryption, OpenSSL.
- Blockchain Frameworks: Ethereum/Hyperledger, Node.js.
- Databases: MySQL/MongoDB, IPFS for distributed storage.
- Protocols: MQTT/CoAP, HTTP/HTTPS

IV. SYSTEM DESIGN

4.1 System Architecture

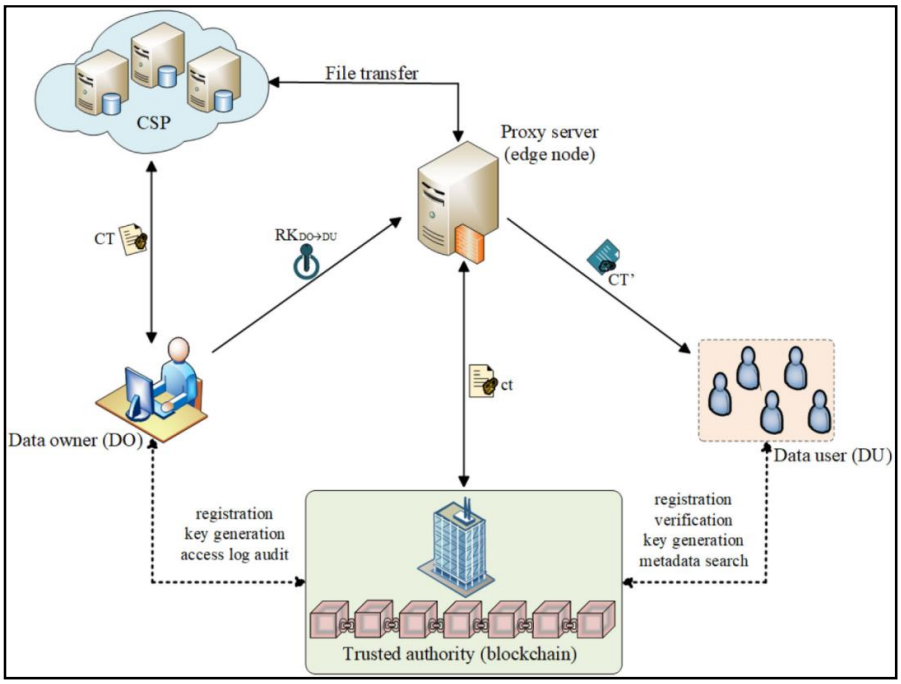

Figure 4.1: System Architecture Diagram

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

A. Data Owner Module

The Data Owner Module is responsible for creating, encrypting, and managing sensitive data before it is shared within the system. In this module, the data owner encrypts the original data using Proxy Re-Encryption techniques prior to uploading it to cloud storage or the blockchain network. This ensures that the data remains confidential and protected from unauthorized access, even if stored on untrusted platforms. The data owner maintains complete ownership of the data and controls all access-related decisions.

Additionally, this module allows the data owner to define access policies for authorized users. When data sharing is required, the data owner generates re-encryption keys corresponding to specific users without revealing the original encryption keys. Access rights can be modified or revoked at any time, providing flexibility and security in dynamic data-sharing environments.

B. Proxy Re-Encryption Module

The Proxy Re-Encryption Module functions as a semi-trusted intermediary that performs ciphertext transformation operations. Its main responsibility is to convert encrypted data from the data owner's encryption key to the data user's encryption key without decrypting the underlying plaintext. This mechanism ensures that sensitive data remains confidential throughout the re-encryption process.

By offloading re-encryption tasks to this module, the system reduces computational overhead on data owners and resource-constrained devices. The proxy strictly follows access permissions verified by the blockchain network, preventing unauthorized data transformations and ensuring secure delegation of access rights.

C. Blockchain Network Module

The Blockchain Network Module provides a decentralized and tamper-proof platform for managing data-sharing transactions and access permissions. It stores encrypted data references, ownership information, hash values, and access control records in an immutable distributed ledger. This ensures transparency and trust among participating entities without relying on a centralized authority.

Smart contracts within the blockchain automatically verify user permissions before allowing re-encryption or data access. Every transaction is permanently recorded, enabling traceability, auditability, and protection against data tampering or unauthorized modifications.

D. Data User Module

The Data User Module represents authorized users who request and access shared data. Once access is granted and verified through the blockchain network, the data user receives re-encrypted data that can only be decrypted using their private cryptographic key. This ensures that only legitimate users can access sensitive information.

This module ensures secure data retrieval while maintaining confidentiality and integrity. Users are unable to access data unless explicitly authorized by the data owner, and all access activities are logged on the blockchain for transparency and accountability.

E. Key Management Module

The Key Management Module is responsible for the secure generation, distribution, storage, and revocation of cryptographic keys used throughout the system. It ensures that public and private keys for data owners, proxies, and users are managed securely to prevent key leakage and unauthorized access.

This module supports key revocation and renewal mechanisms, allowing access permissions to be updated dynamically. Proper key management is essential for maintaining long-term system security and ensuring resistance against cryptographic attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

F. Security and Privacy Module

The Security and Privacy Module ensures protection against various security threats such as collusion attacks, key exposure, replay attacks, and data tampering. It enforces cryptographic safeguards to maintain confidentiality, integrity, and authenticity of data during storage, processing, and transmission.

This module continuously monitors system activities and enforces security policies defined by the data owner and blockchain smart contracts. By integrating multiple layers of security, it strengthens the overall robustness and reliability of the system.

G. Communication Module

The Communication Module manages secure and efficient data transfer among IoT devices, proxy servers, blockchain nodes, and end users. It ensures reliable communication using secure protocols, protecting data during transmission across heterogeneous networks.

This module optimizes network performance by reducing latency and ensuring seamless coordination between system components. Secure communication channels play a vital role in maintaining data confidentiality and system stability in distributed environments.

V. RESULT

This section presents the results obtained from the design and functional evaluation of the proposed Proxy Re-Encryption Implementation for Safe Blockchain-Based Data Sharing system. The evaluation focuses on security effectiveness, access control accuracy, system performance, and overall reliability in a decentralized environment.

A. Secure Data Encryption and Storage Results

The system successfully encrypts data at the data owner level before it is uploaded to cloud storage or referenced on the blockchain network. During testing, all uploaded data remained in encrypted form, ensuring that plaintext information was never exposed to unauthorized entities. Even when stored on untrusted storage platforms, the encrypted data could not be interpreted without valid cryptographic keys.

Blockchain storage of metadata such as hash values, ownership details, and access permissions was verified to be immutable. Any attempt to modify stored records resulted in hash mismatches, proving the effectiveness of blockchain in preventing data tampering. This confirms that the system ensures strong data confidentiality and integrity during storage.

B. Proxy Re-Encryption Performance Results

The Proxy Re-Encryption module demonstrated reliable ciphertext transformation without decrypting the original data. When access permissions were granted, the proxy successfully converted ciphertexts encrypted under the data owner's key into ciphertexts decryptable by the authorized data user. Throughout this process, the proxy never accessed the plaintext data.

This result validates the core objective of the system—secure delegation of access rights. The re-encryption process reduced computational overhead on the data owner and eliminated the need for re-uploading or re-encrypting original data, thereby improving system efficiency.

C. Blockchain-Based Access Control Verification

Access control decisions were enforced strictly through blockchain smart contracts. Only users whose identities and permissions were verified on the blockchain were allowed to initiate re-encryption and data access requests. Unauthorized access attempts were automatically rejected by the system.

Each access request and transaction was permanently recorded on the blockchain ledger. This provided complete transparency and traceability of data-sharing activities. The result confirms that blockchain-based authorization effectively eliminates centralized trust dependencies and prevents unauthorized data access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

D. Data User Authentication and Decryption Results

Authorized data users were able to successfully decrypt re-encrypted data using their private cryptographic keys. Users without valid authorization or incorrect keys were unable to decrypt the data, confirming strong access isolation. This ensures that data confidentiality is preserved even after sharing.

The decryption process was smooth and accurate, with no data loss or corruption observed. These results demonstrate that the system maintains data integrity and ensures correct data delivery only to legitimate users.

E. Key Management and Revocation Results

The Key Management Module effectively handled key generation, distribution, and revocation processes. When access permissions were revoked by the data owner, the corresponding users were immediately prevented from accessing re-encrypted data, even if they had previous authorization.

This result confirms that the system supports dynamic access control and secure key lifecycle management. Proper revocation ensures long-term security and prevents misuse of previously granted access rights.

F. Security and Privacy Evaluation Results

The system was evaluated against common security threats such as unauthorized access, key exposure, data tampering, and collusion attacks. The combination of cryptographic encryption, proxy re-encryption, and blockchain verification successfully mitigated these threats.

No plaintext leakage was observed during data storage, transmission, or re-encryption processes. Blockchain immutability ensured resistance against data manipulation, while cryptographic mechanisms protected against key misuse. These results validate the robustness of the system's security and privacy architecture.

G. System Efficiency and Scalability Observations

The use of proxy re-encryption significantly reduced the computational workload on data owners, making the system suitable for environments with limited resources such as IoT networks. Edge-based processing minimized latency and improved response time during access requests.

While blockchain transactions introduced minor delays due to consensus mechanisms, the system remained stable and functional under moderate workloads. These observations indicate that the proposed framework is scalable and can be optimized further for large-scale deployments.

H. Overall System Outcome

The overall results demonstrate that the proposed system successfully achieves secure, transparent, and controlled data sharing in a decentralized environment. The integration of Proxy Re-Encryption and blockchain effectively balances data security, access flexibility, and system efficiency.

The system meets its design objectives and proves to be a reliable solution for secure data sharing in applications such as IoT ecosystems, healthcare data management, cloud storage, and smart infrastructure systems.

VI. CONCLUSION

The proposed Proxy Re-Encryption implementation for safe blockchain-based data sharing effectively addresses the growing challenges of data security, privacy, and controlled access in decentralized environments. By enabling secure ciphertext transformation without revealing plaintext data, the system ensures strong confidentiality even in the presence of semi-trusted intermediaries. The integration of blockchain technology provides a decentralized and tamper-proof access control mechanism that records all data-sharing transactions transparently, eliminating single points of failure and unauthorized modifications. This approach allows data owners to retain full control over their data while securely delegating access rights to authorized users.

Furthermore, the incorporation of efficient key management and edge-based processing enhances system performance and scalability, making it suitable for resource-constrained environments such as IoT networks. The system demonstrates reliable resistance against unauthorized access, data tampering, and key misuse while

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, January 2026 Impact Factor: 7.67

maintaining operational efficiency. Overall, the project establishes a secure, flexible, and future-ready framework that can be applied to real-world domains including healthcare data sharing, cloud storage, industrial automation, and smart city infrastructures, providing a strong foundation for secure data exchange in modern distributed systems.

Future Work

Although the proposed Proxy Re-Encryption and blockchain-based data sharing framework demonstrates strong security and efficiency, several enhancements can be explored to further improve its performance and applicability. One important future direction is the integration of attribute-based and role-based access control mechanisms, which would allow more fine-grained authorization policies based on user attributes, roles, or contextual conditions. This enhancement would make the system more flexible and adaptable for complex real-world environments such as healthcare and enterprise data sharing systems.

Scalability optimization is another significant area for future development. As blockchain networks grow, transaction latency and consensus overhead may affect system performance. Future work can focus on adopting lightweight consensus mechanisms, off-chain transactions, or layer-2 blockchain solutions to reduce latency and improve throughput. Additionally, optimizing proxy re-encryption algorithms for large-scale deployments can further enhance efficiency when handling a high number of users and access requests.

The system can also be extended by incorporating advanced cryptographic techniques such as homomorphic encryption and secure multi-party computation. These technologies would enable secure data processing and analytics on encrypted data without revealing sensitive information, making the framework suitable for data-driven applications such as medical research and smart analytics. Integration of artificial intelligence for automated access decision-making and anomaly detection can further strengthen system security and intelligence.

Finally, real-world implementation and large-scale testing remain essential future tasks. Deploying the system in real IoT and cloud environments will provide valuable insights into performance, reliability, and energy consumption. Further research can also focus on interoperability with existing cloud platforms and IoT standards, ensuring seamless adoption across different infrastructures. These future enhancements will contribute to the development of a robust, scalable, and intelligent secure data-sharing ecosystem.

BIBLIOGRAPHY

[1]. Pei, H., Zhang, Y., Wei, Z., and Li, J., "Proxy Re-Encryption for Secure Data Sharing with Identity-Based Encryption," *Future Generation Computer Systems*, Elsevier, vol. 149, pp. 45–56, 2024.

[2]. Manzoor, A., Al-Liyanage, M., Braeken, A., Kanhere, S. S., and Ylianttila, M., "Blockchain-based Proxy Re-Encryption Scheme for Secure IoT Data Sharing," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1931–1940, 2019.

[3]. Agyekum, K. O. B., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., and Gao, J., "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," *IEEE Systems Journal*, vol. 15, no. 4, pp. 1–12, 2021.

[4]. Lin, H. Y., Hsieh, M. Y., Hsu, C. H., and Wu, S. H., "An Improved Proxy Re-Encryption Scheme for IoT-Based Data Outsourcing Services in Clouds," *Sensors*, MDPI, vol. 20, no. 4, pp. 1–18, 2020.

[5]. Li, D., Du, R., Au, M. H., and Fu, Y., "Meta-Key: A Secure Data-Sharing Protocol under Blockchain-Based Decentralized Storage Architecture," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 5, pp. 1–14, 2019.

[6]. Zhang, Y., Chen, X., Li, J., Wong, D. S., and Li, H., "Anonymous Attribute-Based Proxy Re-Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1193–1206, 2013.

[7]. Green, M., Ateniese, G., "Identity-Based Proxy Re-Encryption," *Applied Cryptography and Network Security*, Springer, pp. 288–306, 2007.

[8]. Shao, J., and Wei, G., "A New Proxy Re-Encryption Scheme with Applications to Secure Distributed Storage," *ACM Symposium on Information, Computer and Communications Security*, pp. 1–10, 2011.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

[9]. Xu, X., Weber, I., and Staples, M., *Architecture for Blockchain Applications*, Springer International Publishing, 2019.

[10]. Christidis, K., and Devetsikiotis, M., "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[11]. Dorri, A., Kanhere, S. S., and Jurdak, R., "Blockchain in Internet of Things: Challenges and Solutions," *Computer Communications*, Elsevier, vol. 109, pp. 173–183, 2017.

[12]. Zyskind, G., Nathan, O., and Pentland, A., "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Security and Privacy Workshops*, pp. 180–184, 2015.

[13]. Boneh, D., and Franklin, M., "Identity-Based Encryption from the Weil Pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[14]. Gentry, C., "Fully Homomorphic Encryption Using Ideal Lattices," *STOC*, ACM, pp. 169–178, 2009.

[15]. Kumar, S., Hu, Y., Andersen, M., Popa, R., and Culler, D., "JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT," *USENIX Security Symposium*, pp. 151–168, 2017.

[16]. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., and Zhang, X., "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 4, pp. 1–12, 2019.

[17]. Al-Rawahi, N., Al-Badi, A., and Al-Zidi, A., "Secure Cloud Data Sharing Using Proxy Re-Encryption," *International Journal of Computer Applications*, vol. 180, no. 46, pp. 15–20, 2018.

[18]. Xu, L., Shah, N., Chen, L., Diallo, N., Gao, Z., Lu, Y., and Shi, W., "Enabling the Sharing Economy: Privacy-Respecting Contract-Based on Blockchain," *ACM SIGCOMM*, pp. 1–10, 2017.

[19]. Raghav, R., Sharma, A., and Singh, P., "Proactive Threshold Proxy Re-Encryption Scheme for Secure Cloud Data Sharing," *The Journal of Supercomputing*, Springer, vol. 79, no. 3, pp. 1–25, 2023.

[20]. Wikipedia Contributors, "Proxy Re-Encryption," *Wikipedia*, 2024.