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 5, Issue 2, September 2025
Impact Factor: 7.67

A Comprehensive Review of Proxy Encryption Concept and Implementation for Safe Blockchain-based IoT Data Sharing

Miss. Sudhatai Vitthal Harale[1] and Prof. Shubhangi S. Mandwale[2]
Department of Artificial Intelligence and Machine Learning[1,2]
Shreeyash College of Engineering & Technology, Chh. Sambhajinagar

Abstract: *The rapid growth that comprise the Internet of Things (IoT) has made data sharing is among cloud computing's most useful uses. However, despite its potential, data security remains a significant challenge, as unauthorized access can result in severe consequences. This work introduces solution that allows for safe data sharing in cloud environments through proxy re-encryption. Before transferring data to the cloud, owners encrypt it using identity-based encryption. To restrict access to authorised users exclusively, a proxy re-encryption technique is used. Considering the resource limitations of IoT devices, computationally demanding operations are offloaded to an edge device functioning as a proxy server. Additionally, by leveraging information-centric networking, cached content can be efficiently delivered through the proxy, enhancing network bandwidth utilization and improving service quality. The proposed system integrates blockchain technology to provide decentralized data sharing and fine-grained access control, overcoming the drawbacks of traditional centralized approaches. Security examinations and assessments of performance show that the plan effectively preserves data confidentiality, integrity, and overall security.*

Keywords: Internet of Things, Cloud Computing, Data Security, Proxy Re-Encryption, Identity-Based Encryption, Edge Computing

I. INTRODUCTION

1.1 Overview

The Internet of Things (IoT) has evolved into a transformative technology, connecting billions of intelligent devices that continuously sense, transmit, and process data in real time. This interconnected ecosystem produces a massive volume of data, which must be efficiently stored, processed, and shared. Cloud computing has emerged as the most practical solution to meet these requirements, offering scalability, flexibility, and cost-effectiveness. Nevertheless, the explosive growth of IoT introduces serious concerns, particularly related to data privacy and security. Critical information, including healthcare data, industrial process logs, and financial records, must be safeguarded and made available only to authorized entities. Guaranteeing confidentiality, integrity, and availability of data is therefore a fundamental requirement for IoT-based applications.

Conventional data sharing methods often rely on centralized architectures, which are vulnerable to single points of failure, insider threats, and large-scale breaches. To overcome these limitations, researchers have turned to cryptographic techniques such as encryption and access control. Among these, proxy re-encryption (PRE) has emerged as a highly effective method for secure data sharing in cloud environments. PRE enables a semi-trusted proxy to convert ciphertext encrypted under one key into ciphertext under another key—without learning the underlying plaintext—allowing fine- grained access control and reducing the cryptographic burden on IoT devices. This is particularly beneficial given that IoT devices often have limited computational and energy resources.

Despite these advancements, centralized systems continue to face problems such as trust management, limited scalability, and vulnerability to malicious insiders. Blockchain technology offers a powerful solution to these challenges

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 5, Issue 2, September 2025
Impact Factor: 7.67

by providing a decentralized, tamper-resistant ledger. Integrating blockchain with PRE enables transparent, auditable, and secure data sharing. The blockchain network maintains a distributed record of transactions, ensuring that access policies are immutable and verifiable. Additionally, smart contracts can automate key management and enforce access control policies without the need for a centralized authority, thereby enhancing security and trustworthiness.

This work presents a blockchain-assisted proxy re-encryption framework to achieve secure and efficient data sharing in IoT environments. To reduce latency and computational overhead, we employ edge computing, offloading intensive cryptographic operations from resource-limited IoT devices to nearby edge servers. Furthermore, we adopt principles of information-centric networking (ICN) to enable data retrieval based on content rather than location, improving cache efficiency and network bandwidth utilization. Security analysis shows that the proposed model guarantees data confidentiality, integrity, and collusion resistance while maintaining scalability and quality of service (QoS).

With the rise of edge and fog computing, IoT systems are becoming more distributed, enabling computation and storage closer to data sources and minimizing delays for latency-sensitive applications such as smart grids, industrial automation, and autonomous vehicles. However, this distributed nature also increases the number of potential attack points, making secure data exchange between IoT devices, edge nodes, and cloud servers even more crucial. Our proposed architecture ensures that data owners retain control over who can access their encrypted data while still benefiting from distributed computational resources.

Scalability remains another critical issue, as the number of IoT devices continues to grow rapidly. Traditional key management systems struggle under this load, leading to communication delays and security vulnerabilities. Blockchain mitigates these issues by using a decentralized consensus model, removing reliance on a single trusted authority and improving fault tolerance while ensuring that access records remain tamper-proof.

Finally, privacy preservation is essential, especially in domains dealing with sensitive personal or organizational data. Proxy re-encryption allows data to be shared with multiple users without repeated re-encryption, reducing processing overhead and minimizing exposure to attacks. When combined with blockchain's immutable audit trail, this approach provides accountability and regulatory compliance by enabling data owners to track access events. The integration of ICN further enhances performance by allowing cached encrypted data to be delivered from the nearest proxy node, and re-encryption ensures that only authorized users can decrypt and access the content. Together, these features create a secure, scalable, and efficient framework for IoT data sharing that enhances trust and improves overall system performance.

1.2 Problem Definition

One consequence of the exponential expansion of the IoT is the resulted in massive volumes of data that must be securely stored, processed, and shared. While cloud computing provides scalability and cost efficiency, traditional centralized data-sharing methods remain vulnerable to single points of failure, insider attacks, and data breaches. These issues pose serious risks for critical IoT applications such as healthcare, industrial automation, and financial systems, where ensuring data confidentiality, integrity, and availability is essential.

Although cryptographic techniques like proxy re-encryption (PRE) offer a promising approach by enabling secure ciphertext transformation without exposing plaintext, centralized implementations still face trust and scalability challenges . Additionally, resource-constrained IoT devices struggle with the computational load of repeated encryption operations. This creates a need for a decentralized, efficient, and secure data-sharing framework that integrates blockchain for trust and auditability, leverages edge computing to offload heavy computations, and uses information-centric networking (ICN) for optimized content delivery.

II. LITERATURE REVIEW

Recent research highlights the increasing importance of integrating proxy re-encryption (PRE) with blockchain technology and information-centric networking (ICN) to establish secure and efficient data-sharing mechanisms for IoT systems. Multiple studies, such as those by Agyekum et al. and Jhansi Rani et al., propose identity-based PRE models supported by edge computing to shift computationally intensive encryption operations away from IoT devices, thereby preserving confidentiality while enabling fine-grained access control. Blockchain consistently emerges as a key enabler

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 5, Issue 2, September 2025
Impact Factor: 7.67

of decentralized trust, offering transparent key management, verifiable audit trails, and protection against single points of failure. Several works, including those by Farooqui et al. and Chen et al., explore threshold-based PRE techniques, where re-encryption tasks are distributed across multiple nodes, minimizing risks of collusion and assaults that cause a denial of service (DoS). The integration of ICN further strengthens system efficiency by enabling effective caching and rapid content delivery, resulting in reduced latency and improved bandwidth utilization. Collectively, these contributions demonstrate that combining PRE, blockchain, ICN, and edge computing forms a robust and scalable architecture capable of maintaining confidentiality, integrity, and auditability of IoT data.

Key Studies Reviewed

1. "A Proxy Re-Encryption Scheme for Secure Data Sharing in IoT Using Blockchain and ICN" – Agyekum et al. (IEEE Systems Journal)

This work introduces a PRE approach combined together with blockchain, identity-based encryption (IBE), and information-centric networks (ICN) to secure IoT data sharing. Edge devices act as proxies to handle computationally demanding encryption tasks, reducing the load on IoT devices. Blockchain facilitates decentralized and fine-grained access control, while ICN enables faster content delivery through caching. Together, these technologies ensure confidentiality, data integrity, and efficient use of bandwidth.

2. "Secure Data Sharing in Cloud Environment Using Proxy Re-Encryption and Blockchain" – R. Jhansi Rani et al. (International Journal of Current Science, 2023)

The authors propose a PRE-based model integrated with blockchain and ICN within IoT-enabled settings for the safe transfer of data to the cloud. The paper emphasizes the role of edge devices in handling re-encryption tasks and shows how caching improves network efficiency. The model successfully addresses centralization issues while maintaining confidentiality and data integrity.

3. "Blockchain-Based Proxy Re-Encryption Scheme for Secure IoT Data Sharing" – Keshav Kumar Choudhary et al. (INTI Journal, 2024)

This study presents a blockchain-enabled PRE approach with identity-based encryption and edge computing support. ICN integration enhances bandwidth efficiency and overall quality of service. The model is designed to overcome IoT challenges such as interoperability, scalability, and power consumption.

4. "Threshold Proxy Re-Encryption Scheme with Blockchain Consensus for IoT Data Security" – Mohammad Abdul Waheed Farooqui et al. (Volume 08, Issue 01, 2024)

This research focuses on a threshold PRE scheme combined with blockchain consensus mechanisms, removing the dependency on a centralized proxy server. Re-encryption is performed collaboratively by blockchain consensus nodes, improving security, resilience, and transparency. Bilinear pairing and secret sharing techniques protect against collusion and DoS attacks, resulting in a stronger and more fault-tolerant system.

5. "Decentralized Threshold Proxy Re-Encryption for Secure IoT Data Sharing" – Yingwen Chen et al. (Electronics, 2021) Chen et al. propose a decentralized threshold PRE framework that distributes re-encryption keys across multiple proxy nodes, which jointly perform ciphertext transformation. This eliminates single points of failure, strengthens security, and supports granular access control with auditable transaction logs.

III. EXISITING SYSTEM

Existing systems for secure data sharing in IoT environments primarily rely on conventional cryptographic methods for example, ABE and IBE, which stand for identity-based encryption. These approaches provide confidentiality and access control but are often implemented in centralized architectures. Such central systems establish an individual node of failure, making them susceptible to data breaches, insider attacks, and denial-of-service (DoS) incidents. Additionally, the computational load of repeated encryption and decryption operations places a heavy burden on resource-constrained IoT devices, limiting their performance and scalability in real-time applications.

One potential approach to these issues is proxy re-encryption, or PRE. By using PRE, a semi-trusted proxy can securely share data with numerous receivers by converting ciphertext from one encryption key to another without disclosing the plaintext. A lot of current methods offer granular access control by combining PRE with identity-based

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 5, Issue 2, September 2025
Impact Factor: 7.67

encryption. To deal with the computing constraints of Internet of Things devices, several systems employ edge devices or fog nodes as proxies, which offload cryptographic operations and reduce latency, resulting in better efficiency and user experience. Blockchain technology has been integrated into many recent frameworks to overcome the trust issues inherent in centralized systems. Distributed and immutable ledger technology is what blockchain is all about that records access policies and transactions transparently. By using smart contracts, some existing systems automate key distribution and enforce rules for access control that do not rely on a single entity. This ensures auditability, accountability, and resistance to single points of failure, which are critical for sensitive IoT applications such as healthcare, finance, and industrial automation.

In addition, some existing solutions adopt Information-Centric Networking (ICN) principles to improve content delivery performance. ICN allows data to be retrieved based on content rather than location, enabling effective caching and reducing response time. This approach optimizes network bandwidth and ensures faster delivery of frequently accessed content. However, despite these advancements, existing systems still face challenges in terms of scalability, interoperability, and resistance to collusion attacks. There remains a need for more robust frameworks that combine PRE, blockchain, ICN, and edge computing to create a secure, efficient, and fully decentralized data-sharing environment for IoT applications.

IV. SYSTEM DESIGN

4.1 System Architecture

The project's system architecture is detailed in the diagram below.

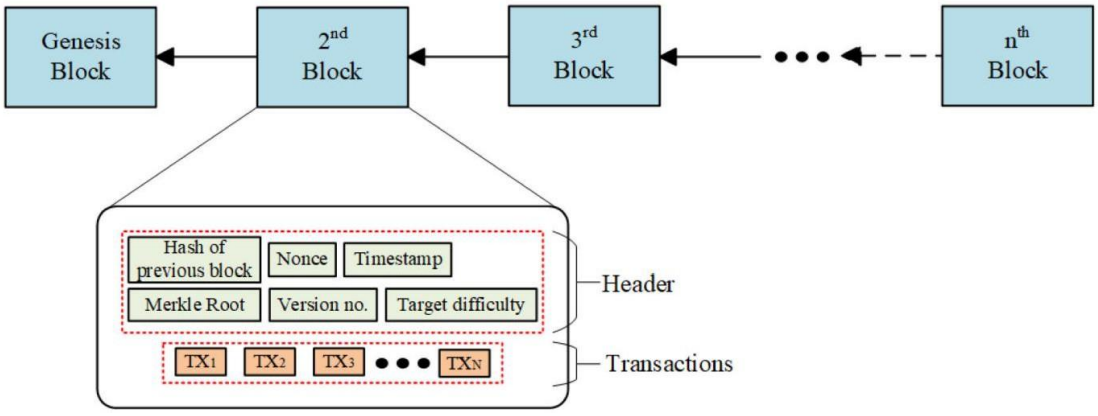

Fig. 1 System Architecture

4.2 Working of the Proposed System

Thanks to the integration of Proxy Re-Encryption (PRE), the suggested system offers a decentralised, secure, and high-performance framework for transferring data between IoT devices. Blockchain, and Information-Centric Networking (ICN). IoT devices, including sensors and smart appliances, generate real-time data and encrypt it using Identity-Based Encryption (IBE) before transmission, ensuring data confidentiality across untrusted communication channels. To address the computational limitations of IoT nodes, an edge computing layer is deployed, functioning as a proxy to perform heavy operations such as re-encryption. This process transforms the ciphertext from the data owner's encryption key to that of an authorized recipient, without exposing the underlying plaintext. Additionally, the edge node maintains a local cache of frequently requested data, reducing response time and improving service quality.

The encrypted data is stored in the cloud, which acts strictly as a storage layer and has no ability to access the decrypted content. Blockchain technology is employed to implement decentralized key management, authorization, and secure logging of transactions. Smart contracts automatically enforce data-sharing policies, eliminating reliance on centralized authorities. Every key request or data-access event is immutably stored on the distributed ledger technology, forming an immutable record of transactions.

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 5, Issue 2, September 2025
Impact Factor: 7.67

When an authorized user requests access to data, the blockchain verifies their identity and permissions. Once validated, the edge proxy forwards the user the re-encrypted ciphertext. After receiving the encrypted data, the recipient can safely retrieve the plaintext by using their private key to decrypt it. All steps of this process are designed to keep sensitive data safe from unauthorised access.

Furthermore, ICN principles enhance network efficiency by enabling data retrieval based on content names rather than physical server locations. This facilitates effective caching and minimizes bandwidth consumption, while re-encryption guarantees that only authorized users can access cached data. Together, these components deliver confidentiality, integrity, fine-grained access control, scalability, and improved Quality of Service (QoS), making the system ideal for security-critical domains such as healthcare, smart city infrastructure, and industrial IoT applications.

Advantages

- Enhanced Security: Proxy Re-Encryption (PRE) ensures that data can may be safely communicated to authorised individuals without disclosing the plaintext, maintaining confidentiality and integrity.
- Decentralization: Blockchain removes autonomy, decreasing reliance on a governing body, and improving trustworthiness.
- Auditability and Transparency: All data-sharing events are recorded on an immutable ledger, providing a verifiable history of access for compliance and accountability.
- Reduced Computational Load: Edge devices handle complex cryptographic operations, minimizing the burden on resource-constrained IoT devices and improving performance.
- Efficient Data Delivery: Information-Centric Networking (ICN) enables content-based retrieval and caching, reducing latency and optimizing bandwidth usage.
- Fine-Grained Access Control: Smart contracts automate and enforce protection measures, guaranteeing that particular information can only be accessed by authorised individuals.
- Scalability: The combination of edge computing and blockchain supports a large number of devices and users without performance degradation.

Disadvantages

- High Initial Setup Cost: Deploying blockchain infrastructure, edge devices, and ICN components may require significant investment.
- Computational Overhead on Proxies: Although edge devices reduce IoT node load, they may still face heavy processing demands under high traffic conditions.
- Latency Due to Blockchain Verification: The time taken for transaction validation and consensus on the blockchain may introduce slight delays in data access.
- Complex System Integration: Combining PRE, blockchain, edge computing, and ICN requires careful system design and implementation, increasing development complexity.

V. CONCLUSION

The proposed system represents a promising step toward secure and efficient information exchange in Internet of Things (IoT) settings that feature cloud computing. Using proxy re-encryption instead with identity-based encryption, the model safeguards data confidentiality while delegating computationally intensive tasks to an edge proxy server, effectively overcoming IoT resource limitations. The inclusion of blockchain technology enhances decentralization and transparency, creating an immutable record of access control operations and reducing reliance on centralized authorities.

Additionally, the use of information-centric networking principles and cryptographic techniques such as AES encryption and SHA-256 hashing strengthens both performance and security. Although the framework shows significant potential for applications in domains like healthcare, smart cities, and industrial IoT, it remains a work in

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 5, Issue 2, September 2025
Impact Factor: 7.67

progress. Further research is being conducted to optimize latency, improve scalability under high traffic, and streamline integration for practical deployment in real-world environments.

BIBLIOGRAPHY

[1]. Chen, Y., Hu, B., Yu, H., Duan, Z., & Huang, J. (2021). A Threshold Proxy Re-Encryption Scheme for Secure IoT Data Sharing Based on Blockchain. Electronics, 10(19).

[2]. Manzoor, A., Liyanage, M., Braeken, A., Kanhere, S. S., & Ylianttila, M. (2018). Blockchain-based Proxy Re- Encryption Scheme for Secure IoT Data Sharing. arXiv preprint arXiv:1811.02276.

[3]. Agyekum, K. O.-B., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Hu, X., & Gao, J. (2021). A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain. IEEE Systems Journal.

[4]. Jabri, A. E., et al. (2025). Leveraging Blockchain and Proxy Re-Encryption to Secure, Traceable, and Privacy-Preserving Data Sharing in IoT Healthcare Systems.

[5]. Wang, S., et al. (2024). Blockchain-based proxy re-encryption access control method for agricultural biological risk traceability. Scientific Reports.

[6]. Proactive threshold-proxy re-encryption with proactive share renewal, cloud-based data sharing applications. (2023). Journal / DOI.

[7]. A Study on Blockchain-Based Data Proxy Re-Encryption Privacy Protection Method. (2024). ACM.

[8]. ―Proxy Re-Encryption Enabled Secure and Anonymous IoT Data Marketplace‖ — A. Manzoor et al. (2021).

[9]. Lattice-based ABE-IBE Proxy Re-Encryption for IoT Systems, Khan M. N., et al. (2021).

[10]. T. Güneysu et al. (2017). Towards Lightweight Identity-Based Encryption for the Post-Quantum Secure Internet of Things.

[11]. Meshram, C., Imoize, A. L., Aljaedi, A., Alharbi, A. R., Jamal, S. S., & Barve, S. K. (2021). A Provably Secure IBE Transformation Model for PKC Using Conformable Chebyshev Chaotic Maps under Human-Centered IoT Environments. Sensors, 21(21):7227.

[12]. Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., & Javaid, N. (2020). Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. Applied Sciences, 10(2):488.

[13]. Dwivedi, A. D., et al. (2019). A Decentralized Privacy-Preserving Healthcare Blockchain System. PMC/NCBI.

[14]. Rai, H. M., et al. (2024). Enhancing Data Security and Privacy in Energy Applications Using Blockchain & Strong Encryption in IoT.

[15]. Protecting IoT Data with Blockchain and Proxy Re-Encryption (2023). IJIRSET.

[16]. IOT Secure Transmission Based on Integration of IBE and PKI (2013). International Journal of Control and Automation.

[17]. Meta-Key: A Secure Data-Sharing Protocol under Blockchain-Based Decentralised Storage Architecture. Li, D., Du, R., Au, M. H., & Fu, Y. (2017).

[18]. Fotiou, N., & Polyzos, G. C. (2017). Securing Content Sharing over ICN. arXiv preprint arXiv:1707.03230.

[19]. Advanced Encryption Standard (AES) – specification and usage details.

[20]. Lattice-Based Cryptography for Internet of Things — Survey of implementations and challenges