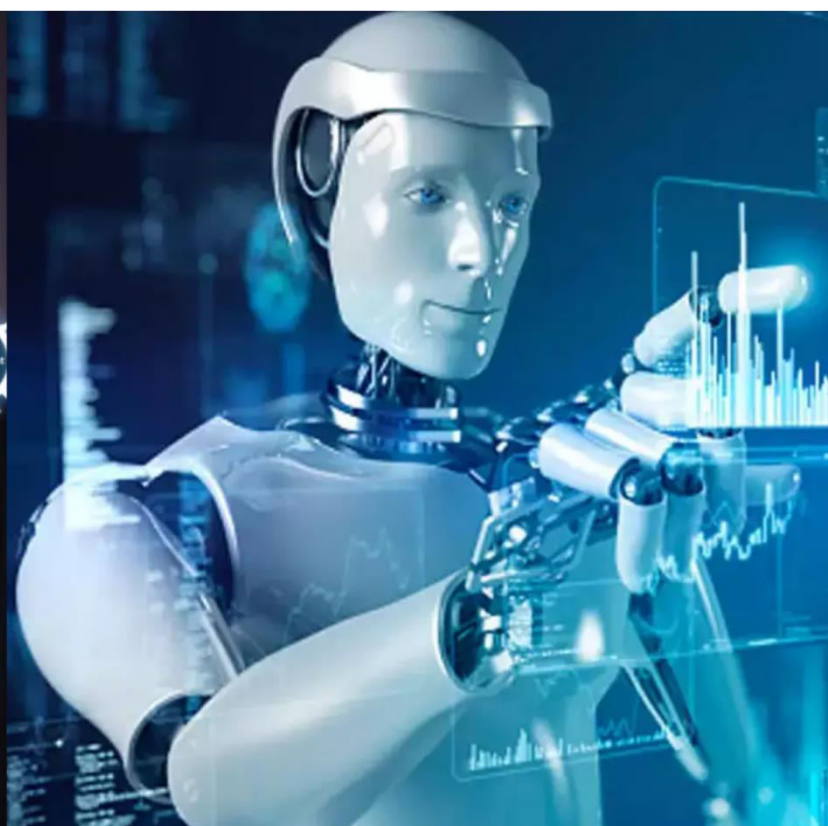




# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 6, June 2025**

# **Blockchain based Proxy Re-encryption for Secure Data Sharing**

**Prof. Ghodake G.K<sup>1</sup>, Gunjal Aditya Ashok<sup>2</sup>, Jadhav Shreyash Ashok<sup>2</sup>, Chikane Mayur Sakharam<sup>2</sup>**

Assistant Professor, Department of Computer Engineering, Samarth College of Engineering and Management,  
Belhe, India<sup>1</sup>

Students, Department of Computer Engineering, Samarth College of Engineering and Management, Belhe, India<sup>2</sup>

**ABSTRACT:** With the rapid increase in decentralized data sharing, ensuring security, privacy, and proper access control has become a significant challenge. Traditional centralized systems often suffer from data breaches, unauthorized access, and a lack of transparency. This paper presents a novel framework that combines blockchain technology with proxy re-encryption (PRE) to provide secure and privacy-preserving data sharing. Blockchain ensures data integrity and decentralized access control through a transparent and tamper-proof ledger. Proxy re-encryption enables encrypted data to be re-encrypted for authorized users without exposing private keys or original content. This approach supports dynamic, trustless collaboration among multiple parties without relying on centralized authorities. The proposed system efficiently handles key management, access delegation, and revocation. It is especially suitable for sensitive domains such as healthcare, finance, and the Internet of Things (IoT). Implementation strategies and performance analysis demonstrate that the framework is both scalable and practical. This work aims to advance secure data sharing in real-world decentralized environments.

**KEYWORDS:** Blockchain, Proxy Re-Encryption, Secure Data Sharing, Decentralized Storage, Data Privacy, Consensus Protocols, Key Management, Data Integrity.

## **I. INTRODUCTION**

The exponential growth of data sharing across diverse sectors has made secure and efficient data management a critical priority. Traditional methods of data sharing, which rely on centralized systems, often suffer from vulnerabilities such as unauthorized access, data breaches, and lack of transparency. These challenges are further compounded by the increasing need for dynamic access control, where data needs to be securely shared among multiple parties without compromising privacy.

Blockchain technology has emerged as a transformative solution for enhancing security and trust in decentralized environments. Its decentralized, immutable, and transparent nature eliminates the need for centralized intermediaries, making it a robust choice for ensuring data integrity and auditability. However, blockchain alone cannot address the complex requirements of secure data sharing, particularly in scenarios requiring dynamic and flexible access control.

To address this limitation, proxy re-encryption (PRE) has gained attention as an effective cryptographic technique. PRE enables secure data sharing by allowing encrypted data to be re-encrypted by a proxy using a re-encryption key, without exposing the original plaintext. This ensures that only authorized parties can decrypt and access the data. By integrating blockchain with proxy re-encryption, a trustless and secure framework for data sharing can be established, overcoming the limitations of traditional methods.

### **Aim**

This paper aims to propose a hybrid framework that leverages blockchain technology and proxy re-encryption to enable secure, privacy-preserving, and efficient data sharing in decentralized environments. The framework seeks to ensure data integrity, dynamic access control, and trustless collaboration among multiple parties.



### Objectives

1. **Enhance Data Security and Privacy:** Utilize proxy re-encryption to enable secure and flexible data sharing while preserving user privacy.
2. **Establish Trustless Data Sharing:** Leverage blockchain to maintain a transparent, immutable ledger of access control and data-sharing transactions.
3. **Eliminate Single Points of Failure:** Employ blockchain's decentralized architecture to mitigate risks associated with centralized systems. **Ensure Scalability and Efficiency:** Design a system capable of handling growing data volumes without significant computational overhead.

### II. LITURATURE SURVEY

Sr. No	Authors	Year	Title
1	Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, K.-K. R. Choo	2015	Cloud Based Data Sharing with Fine-grained Proxy Re-encryption
2	J. Wei, W. Liu, X. Hu	2016	Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption
3	Z. Qin, H. Xiong, S. Wu, J. Batamuliza	2016	A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing
4	M. Sepehri, A. Trombetta, M. Sepehri	2018	Secure Data Sharing in Cloud Using an Efficient Inner-Product Proxy Re-Encryption Scheme
5	K. T. Nguyen, N. Oualha, M. Laurent	2020	Authenticated Key Agreement Mediated by a Proxy Re-encryptor for the Internet of Things
6	A. Rahman, M. J. Islam, R. Islam, D. Kundu, M. R. Karim, Z. Rahman, S. S. Band	2020	Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-based SDN Architecture in IoT Networks
7	W. B. Kim, D. Seo, D. Kim, I. Y. Lee	2021	Group Delegated ID-Based Proxy Reencryption for the Enterprise IoT-Cloud Storage Environment
8	S. Alshehri, O. Bamasaq, D. Alghazzawi, A. Jamjoom	2021	Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment
9	Y. Ould-Yahia, S. Bouzeffrane, H. Boucheneb, S. Banerjee	2022	A data-owner centric privacy model with blockchain and adapted attribute-based encryption for IoT and cloud environment
10	Zia Ullah, Basit Raza, Habib Shah, Shahzad Khan, Abdul Waheed	2022	Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment
11	D. Rani, N. S. Gill, P. Gulia	2022	Design of a Cloud-Blockchain-based Secure Internet of Things Architecture
12	K. O. B. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, J. Gao	2022	A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain

**III. IMPLEMENTATION****Tools and Technologies :**

Category	Tools / Technologies
Front-End Development	HTML, CSS, JavaScript
Back-End Development	JSP (JavaServer Pages), Servlets
IDE	NetBeans
Web Server	Apache Tomcat
Cryptography	AES-256 (Symmetric), ECC (Asymmetric), SHA-256 (Hashing)
Database / Storage	IPFS (Decentralized), Google DriveHQ (Cloud Storage)
Security Protocols	HTTPS, TLS

**Techniques Implemented :**

**End-to-End Encryption:** Sensitive data is encrypted on the client side using AES-256 before upload to ensure confidentiality.

**Key Pair Generation and ReKey Creation:** ECC is used to generate public-private key pairs and derive secure proxy re-encryption (ReKey) values for each authorized user.

**Proxy Re-Encryption for Access Delegation:** A proxy server securely transforms ciphertext using ReKeys without accessing plaintext, enabling authorized sharing.

**Blockchain-Backed Metadata Management:** File hashes and ReKeys are recorded on the blockchain for tamper-proof logging, auditability, and decentralized access control.

**Dynamic Access Control:** Access rights can be granted, modified, or revoked in real time by updating ReKeys, with changes reflected on the blockchain ledger.

**Deployment Steps :****1. User Registration and Key Generation**

Users access the web application and register securely. Upon registration, an ECC-based public-private key pair is generated for each user to facilitate encryption and re-encryption operations.

**2. File Encryption and Upload**

Before upload, the selected file is encrypted on the client side using AES-256 to ensure confidentiality. The encrypted file is then uploaded to cloud storage (e.g., Google Drive), while its hash is computed for integrity verification.

**3. ReKey Generation**

When the file owner decides to share the encrypted file with another user, a ReKey (proxy re-encryption key) is generated using the owner's private key and the recipient's public key. This ReKey enables secure access delegation without revealing the plaintext.

**4. Proxy-Based Re-Encryption**

A trusted proxy server uses the ReKey to transform the encrypted file into a form that is decryptable by the intended recipient. The proxy does not learn or store the plaintext during this process.

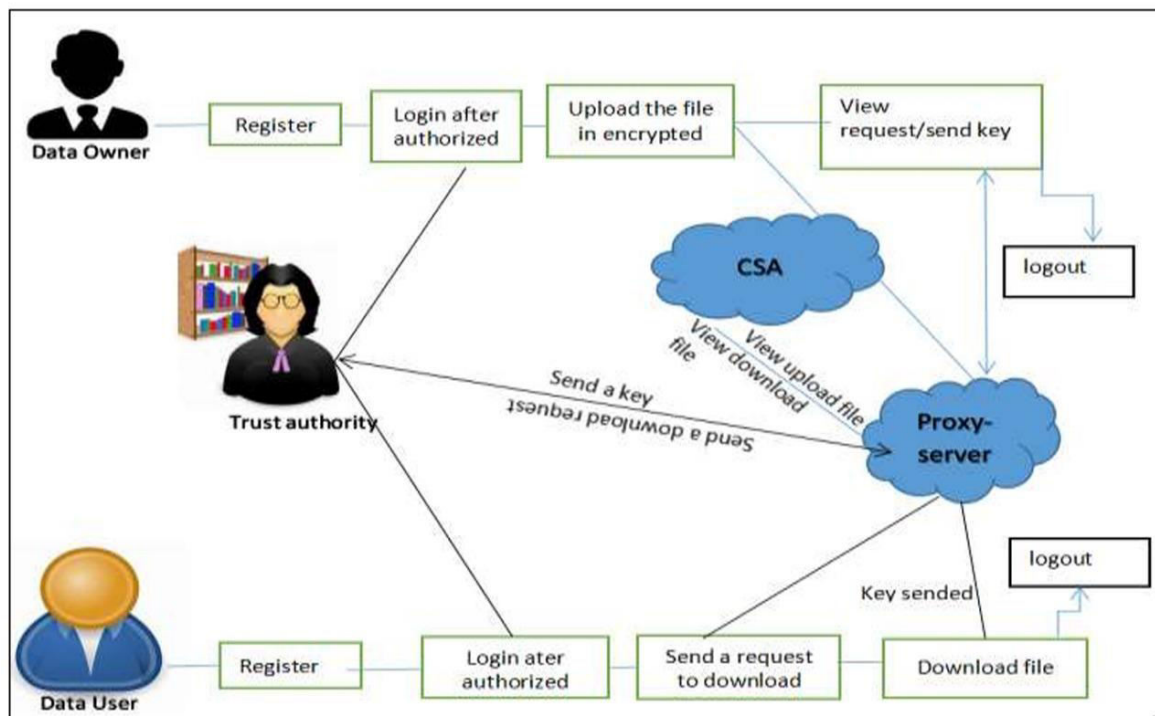
**5. Decryption by Recipient**

The recipient downloads the re-encrypted file and decrypts it using their private ECC key. The original symmetric AES key is used to retrieve the original content securely.

## 6. Audit and Revocation

All key generation, re-encryption, and access events are recorded immutably on the blockchain. The data owner retains full control to revoke or update access rights by modifying or removing the ReKey, ensuring real-time dynamic access control.

### System Architecture:



## IV. ALGORITHM DESIGN

- Step 1: Owner encrypts data with symmetric key (AES-256)
- Step 2: Owner encrypts AES key with their public key
- Step 3: Owner generates ReKey using:  

$$\text{ReKey} = \text{ReEncrypt}(\text{OwnerPrivateKey}, \text{RecipientPublicKey})$$
- Step 4: Proxy transforms encrypted AES key using ReKey
- Step 5: Recipient decrypts AES key with their private key
- Step 6: Recipient uses decrypted AES key to access original data

## V. TESTING AND EVALUATION

The system was tested to evaluate its effectiveness in secure data sharing, proxy-based access delegation, and blockchain-backed traceability. Testing was conducted in both **simulated and controlled environments** using sample data across multiple user roles.

#### A. Testing Scenarios

Test Case	Description
TC1: Valid Data Access	Authorized recipient successfully decrypts shared data using ReKey.
TC2: Unauthorized Access Attempt	Unauthorized user fails to access data without a valid ReKey.
TC3: ReKey Revocation	Revoked ReKey prevents recipient from decrypting data post revocation.
TC4: Tamper Detection	Modified encrypted data fails hash verification on the blockchain.
TC5: Concurrent Access	Multiple authorized users accessing data simultaneously via separate ReKeys.

#### Performance Metrics

- **Access success rate:** 100% for authorized users using valid ReKeys
- **Average re-encryption time:** ~120ms per data block, with minimal overhead

#### Challenges

- **Latency due to blockchain write delays** (e.g., ReKey registration, access logging)
- **Complexity in managing dynamic key revocation** across multiple recipients

## VI. RESULTS

### Registration Page:

#### Data User Register

Name :	Email :
<input type="text" value="Enter Your Name"/>	<input type="text" value="Enter Your Email"/>
Dob :	Gender :
<input type="text" value="dd-mm-yyyy"/>	<input type="text" value="Select Your Gender"/>
Phone No :	Address :
<input type="text" value="Enter Your Phone No"/>	<input type="text" value="Enter Your Address"/>
Password :	
<input type="text" value="Enter Your Password"/>	

Sign Up


### Login Page :

User Login

Email :
<input type="text" value="Enter Your Email"/>
Private key :
<input type="text" value="Enter Your Private Key"/>
Password :
<input type="text" value="Enter Your Password"/>


LoginRegister!

Gmail :



**proxyservermailgroupno1@gmail.com**  
Hi, adityaYour Data User Registration is Approved Private Key : IMir4M4sZxA=

---



**proxyservermailgroupno1@gmail.com**  
to me ▾

Filename : new.txt  
Re-Decryption key: 7JvSV/bUDXO0u3Y4HLhMsA==

↩ Reply
➡ Forward
😊

File upload :

Upload File

File Keyword :

**Convert PDF to Text here**

Select File :

Preview File :

```
HOCHwMBtkwDC1+Zdxu5VGt3OFTCXxtwmDbdGHhqaLMe8PUuRPyx
f5jpCOpmYa4jvQn4KYyu1Yq82Jq5o3ra8Je7qycLD/r1mDvGNEep+3+b
pkZua21Uk+T0htOWTtjG3XN5154BdigoX6Lv8DiuPw==
```

File Access control :

### Requested Files

File Name	User Name	Requested Time	Status	Approve	Reject
new.txt	aditya	2025/02/02 22:57:28	Approved	<input type="button" value="Approve"/>	<input type="button" value="Reject"/>
new.txt	aditya	2025/02/02 22:58:35	waiting	<input type="button" value="Approve"/>	<input type="button" value="Reject"/>
new.txt	aditya	2025/02/02 22:58:41	waiting	<input type="button" value="Approve"/>	<input type="button" value="Reject"/>
new.txt	aditya	2025/02/02 22:58:46	waiting	<input type="button" value="Approve"/>	<input type="button" value="Reject"/>
ms office key.txt	sneha	2025/02/03 12:56:52	Approved	<input type="button" value="Approve"/>	<input type="button" value="Reject"/>



File download :

### Download Files

File ID	File Name	Requested Time	Status	Action
1	new.txt	2025/02/02 22:57:28	Approved	<a href="#">Download</a>
2	new.txt	2025/02/02 22:58:35	Approved	<a href="#">Download</a>
3	new.txt	2025/02/02 22:58:41	Approved	<a href="#">Download</a>
4	new.txt	2025/02/02 22:58:46	Approved	<a href="#">Download</a>

### VII. CONCLUSION

The integration of blockchain and proxy re-encryption (PRE) offers a robust solution for secure and scalable data sharing in decentralized systems. Blockchain ensures transparency, immutability, and integrity, while PRE enables fine-grained, privacy-preserving access control. This combination eliminates key challenges like single points of failure and poor key management. It allows dynamic delegation and revocation of access, making it ideal for sensitive domains such as healthcare, finance, and IoT. The system supports trustless collaboration among multiple parties without compromising data confidentiality. Both theoretical and experimental evaluations confirm its effectiveness, scalability, and efficiency. Overall, the proposed framework advances secure data sharing by blending the strengths of blockchain and PRE. It sets the stage for building privacy-aware, decentralized data ecosystems suited for real-world applications.

### VIII. FUTURE SCOPE

In the future, lightweight blockchain methods can be used to save energy and improve performance. AI can help monitor the system, detect threats, and manage access automatically. Strong encryption techniques can keep data private even while sharing. The system can be improved to work across different platforms and cloud services. Easy-to-use tools for key management will help more people use the system. It can also be updated to follow data protection laws like GDPR and HIPAA. Smart contracts can be added to automate data sharing and access control. These changes will make the system more secure, flexible, and user-friendly.

### REFERENCES

1. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. EUROCRYPT, Springer, 1998, pp. 127–144.
2. B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Proc. NDSS, vol. 4, 2004, pp. 5–6.
3. R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in Proc. EUROCRYPT, Springer, 2004, pp. 207–222.
4. N. Fotiou and G. C. Polyzos, "Securing content sharing over ICN using identity-based proxy re-encryption," arXiv preprint arXiv:1707.03230, 2017.
5. T. Salman et al., "Security services using blockchains: A state of the art survey," arXiv preprint arXiv:1810.08735, 2018.
6. R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," arXiv preprint arXiv:2005.14282, 2020.



7. M. Ul Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," arXiv preprint arXiv:2112.06089, 2021.
8. T. Vo and D. Nguyen, "Decentralized key management using blockchain for encrypted data," International Journal of Computer Applications, vol. 183, no. 2, pp. 1–6, 2021.
9. M. Li, Y. Chen, C. Lal, M. Conti, and M. Alazab, "Eunomia: Anonymous and secure vehicular digital forensics based on blockchain," IEEE Transactions on Intelligent Transportation Systems, 2023.
10. H. Zhang, M. Xiong, and W. Liu, "Blockchain-based scalable and secure EHR data sharing using proxy re-encryption," The International Arab Journal of Information Technology, vol. 20, no. 4, pp. 523–531, 2023.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details