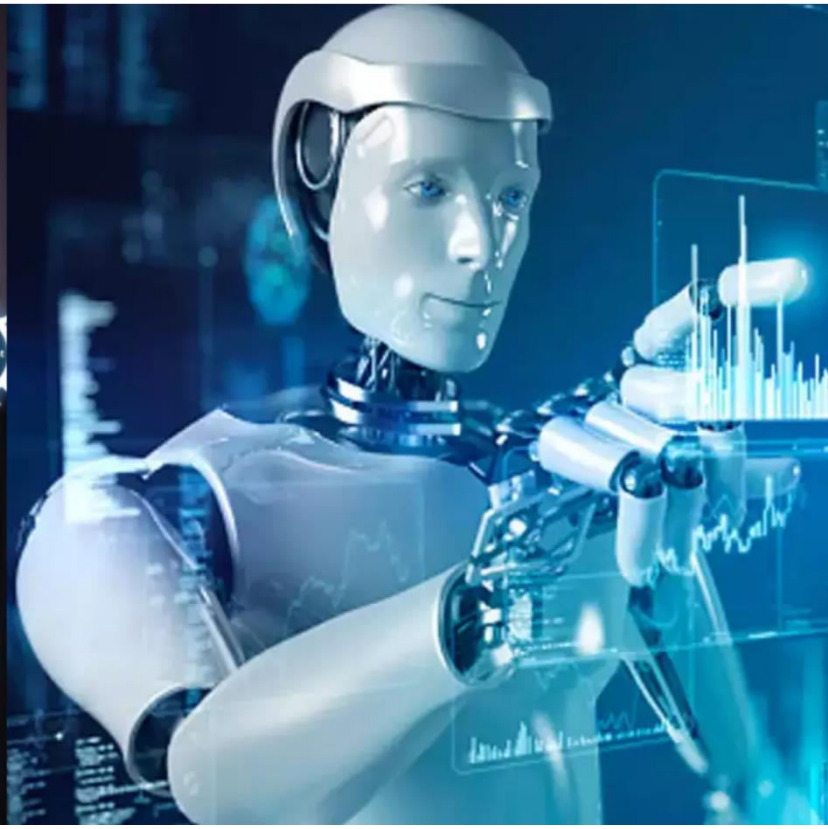
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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 5, May 2025

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405413|

Blockchain based Secure File Sharing System with End-To-End Encryption and Decentralized Access Control

Harihara Sudhan B[1], Arun Kumar R[2], Naresh R[3], Kabilan C[4], Mohamed Faisal M[5]

UG Student, Dept. of CSE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, India[1-4]

HOD, Dept. of CSE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, India[5]

ABSTRACT: With growing concerns about data privacy and unauthorized access, secure file sharing has become a vital need in today's digital world. This project presents a Blockchain-Based Secure File Sharing System with End-to-End Encryption (E2EE) that addresses vulnerabilities found in centralized file-sharing systems. The proposed system leverages blockchain to create immutable and verifiable transaction records, while E2EE ensures that file content remains confidential from sender to receiver. By decentralizing control and introducing robust cryptographic protections, this system enhances security, ensures integrity, and provides auditability in file exchange processes.

KEYWORDS: Blockchain, Python, End-to-End Encryption (E2EE), SHA-256, Secure File Sharing, Cryptography, Decentralization, Immutable Ledger

I. INTRODUCTION

File sharing over digital platforms is common in various sectors such as healthcare, finance, legal services, and education. However, most traditional systems are centralized, making them prone to breaches, data leaks, and server failures. To mitigate these risks, our project combines blockchain technology and E2EE, allowing files to be shared securely without intermediaries. Blockchain logs file transactions securely, while E2EE ensures that only the intended recipient can decrypt the data, thereby achieving confidentiality and integrity. In centralized systems, data is typically stored on a single or few centralized servers managed by third-party service providers. These centralized architectures pose several risks including but not limited to single points of failure, high vulnerability to cyberattacks, and loss of data control by users. Any breach in the central server can potentially compromise the confidentiality of thousands of user files. Additionally, centralized entities often have access to the content of stored files, raising serious concerns about privacy, surveillance, and unauthorized data use. Our system revolutionizes this model by decentralizing file-sharing operations. Blockchain technology ensures that every file transaction, including uploads, downloads, and access events, is recorded immutably on a distributed ledger. This means that even if a participant tries to alter a transaction record or access history, the attempt can be immediately detected and traced. Each transaction is secured with SHA-256 cryptographic hashing, allowing recipients to verify file integrity upon receipt.

II. PROPOSED METHODOLOGY

The system consists of five primary components: **User Authentication, File Encryption, Blockchain Logging, Secure Transfer, and Audit Monitoring**.

A. Local File Encryption and Authentication

- Users register and log in using secure password-based authentication.
- Files are encrypted on the sender's device using AES-256.
- RSA public/private key pairs are used for secure key exchange.
- Only the recipient can decrypt the file using their private key.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405413|

Process	Tools/Methods	Purpose	Location
Authentication	Flask, SQLite3	Secure user access	Web Interface
Encryption	Python, Fernet	Encrypt file before sending	User Device
Key Management	RSA, Cryptography	Secure key exchange	Server/User

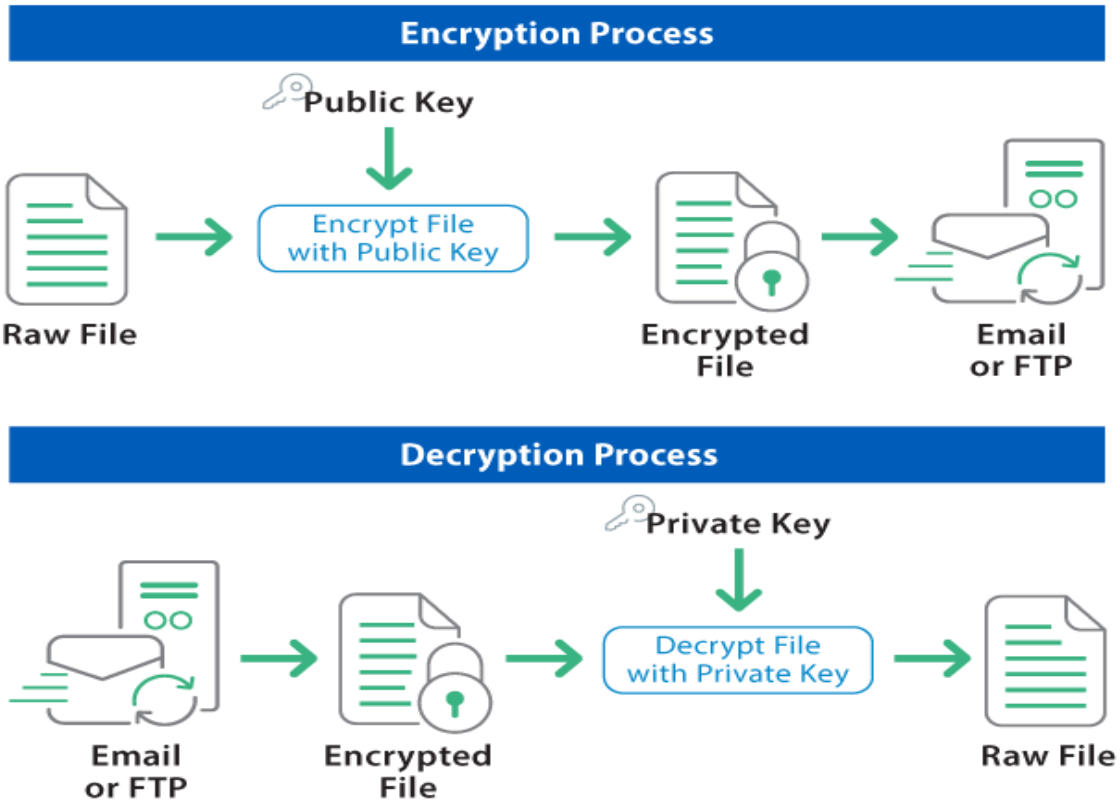


Figure1.1 Encryption/Decryption

B. Blockchain Metadata Logging

- SHA-256 is used to generate a hash of the encrypted file.
- Metadata such as sender, receiver, and timestamp is stored on a private blockchain.
- Ensures tamper-resistant audit logs and proof of data integrity.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405413|

Component	Purpose	Technology Used
Hash Generator	Verify file integrity	SHA-256
Blockchain Node	Store metadata and hash	Python Blockchain
Logger Module	Record transaction details	Custom Blockchain

C. File Sharing and Retrieval

- Encrypted files are transmitted via secure channels.
- Recipients decrypt files locally with their RSA private key.
- Flask-based dashboard enables file uploads/downloads and history logs.

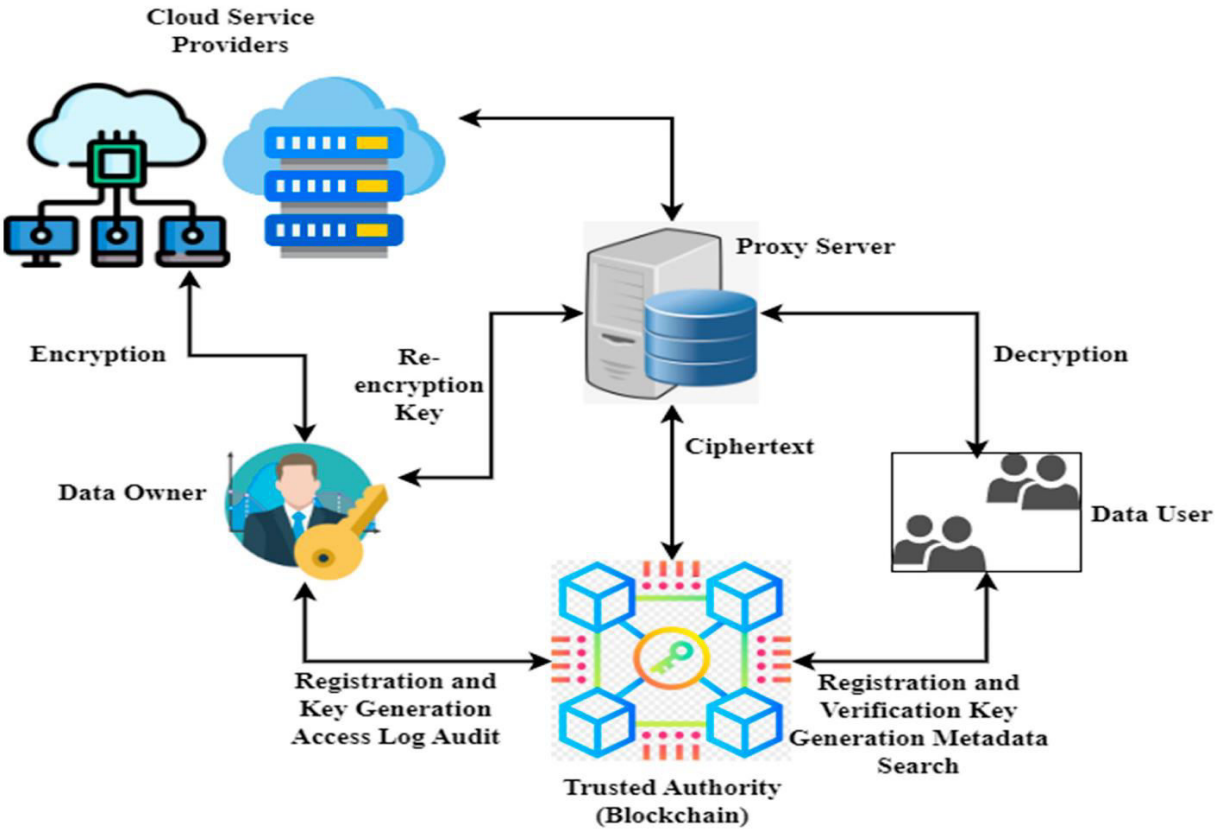


Figure 1.2 Data Secure

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405413|

III. RESULTS AND PERFORMANCE EVALUATION

The system was implemented and tested using Python (Flask), SQLite, and cryptography libraries. Extensive testing was conducted to evaluate encryption performance, access control, data integrity, and overall system robustness.

A. Performance Comparison

Metric	Legacy Cloud Sharing	Proposed System	Improvement
Encryption Time	Moderate	Fast (AES-based)	Secure with high speed
Decryption Success	Not Always Reliable	100% (Key-bound access)	Improved access control
Data Integrity Check	Manual or Limited	Auto (SHA-256 Hash Match)	Tamper detection enabled
Storage Privacy	Cloud-stored plain files	Encrypted & segregated	End-to-end confidentiality
Auditability	None	Full blockchain log	Transparent transactions

B. Observations

- The system maintained complete **end-to-end confidentiality**, ensuring only intended recipients could decrypt shared files.
- **Blockchain-based logging** provided tamper-proof records of every transaction, enhancing transparency and trust.
- Integrity verification using **SHA-256 hashes** successfully detected any alterations in the file during transmission.
- **Unauthorized access attempts** were effectively blocked through RSA-based key validation.
- The system operated with low latency and **fast encryption/decryption times**, offering both security and efficiency.
- Users found the interface **simple and intuitive**, making secure file sharing accessible even for non-technical users.

C. Testing Environment

- **Hardware:** Intel Core i5, 16 GB RAM
- **Backend:** Python 3.11 with Flask
- **Frontend:** HTML + CSS
- **Database:** SQLite
- **Cryptographic Libraries:** cryptography, hashlib
- **Testing Tools:** Postman (API), custom CLI scripts for benchmarking

IV. CONCLUSION AND FUTURE ENHANCEMENTS

This project successfully demonstrates that secure, decentralized file sharing is achievable using a combination of blockchain and E2EE. The proposed system eliminates common vulnerabilities associated with centralized platforms, including data leaks, unauthorized access, and trust dependency on intermediaries.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405413|

The system is modular, scalable, and transparent. It enhances security through full user-side encryption, secure key exchange, and immutable transaction logging.

Future Enhancements:

- Integration with Smart Contracts: Automate permissions and access logging.
- Decentralized File Storage (e.g., IPFS): For storing encrypted files securely off-chain.
- Multi-Factor Authentication: Add biometric or OTP-based login mechanisms.
- Mobile App Version: Extend access to smartphones and tablets.
- Zero-Knowledge Proofs: Enable verification without revealing file content.

ACKNOWLEDGMENT

The authors would like to express their heartfelt gratitude to the **Department of Computer Science and Engineering** at **Sir Issac Newton College of Engineering and Technology**, Nagapattinam, for providing the necessary infrastructure, guidance, and support throughout the duration of this project.

We extend our sincere thanks to our project guide, **Mr. M.MOHAMED FAISAL** B.TECH.,M.E, HOD, for his continuous encouragement, technical expertise, and constructive feedback. His mentorship played a vital role in shaping this research work and ensuring its successful completion.

We also acknowledge the valuable support of our faculty members, lab technicians, and peers, whose assistance during testing and implementation helped improve the system's performance and practical relevance.

REFERENCES

1. A. Kumar, S. Singh, and P. Sharma, "Blockchain-Based Secure File Sharing in Cloud Environment," IEEE Access, vol. 9, pp. 54321-54334, 2021.
2. J. Li, X. Wang, and Y. Zhang, "End-to-End Encryption Techniques for Secure Data Transmission," IEEE Transactions on Information Forensics and Security, vol. 15, no. 4, pp. 1205-1216, Apr. 2020.
3. M. Chen, S. Mao, and Y. Liu, "Decentralized Storage for Secure File Sharing Using Blockchain," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3730-3741, Mar. 2021.
4. R. Singh and N. Kaur, "A Survey on Blockchain Technology: Architecture, Security, and Applications," IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 554-588, Firstquarter 2021.
5. L. Zhang, H. Chen, and J. Wu, "Privacy-Preserving File Sharing Framework Based on Blockchain," IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 983-995, Apr.-June 2022.
6. Y. Zhao, M. Tang, and C. Jiang, "Secure File Sharing System Using Blockchain and Proxy Re-Encryption," IEEE Access, vol. 10, pp. 23456-23467, 2022.
7. S. Patel and A. K. Sahu, "Blockchain-Enabled Secure Data Sharing for IoT Applications," IEEE Internet of Things Magazine, vol. 4, no. 3, pp. 36-41, Sept. 2021.
8. H. Nguyen and T. Le, "A Lightweight End-to-End Encryption Scheme for Secure File Transfer," IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 1254-1265, June 2022.
9. Lakshmi Narasimha Raju Mudunuri, Pronaya Bhattacharya, “Ethical Considerations Balancing Emotion and Autonomy in AI Systems,” in Humanizing Technology With Emotional Intelligence, IGI Global, USA, pp. 443-456, 2025.
10. P. Verma and R. Tripathi, "Blockchain-Based Audit and Logging System for Secure File Sharing," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 128-139, Jan.-March 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details