IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144106

A Blockchain-Based Framework for Secure Secret Image Sharing in Wireless Networks

J. Vinothini[1], Kushboo A,Divya K[2]

Assisstant Professor, Department of Computer Science and Engineering,Anand Institute of Higher Technology, Kazhipattur, Chennai[1]

Department of Computer Science and Engineering,Anand Institute of Higher Technology, Kazhipattur, Chennai[2]

Abstract: Secret Image Sharing (SIS) is a secure method of disseminating an image by breaking it into n shadow images where k number is required to reconstruct the image. The existing techniques of SIS suffer from a security loophole and inefficient storage and are susceptible to tampering. Thus, this paper proposes a Blockchain-based Secure and Optimized SIS (BC-SOSIS) scheme to overcome those issues. The scheme enables decentralized storage to resist tampering, tightly coupled with smart contracts to achieve authentication, along with efficient encryption that ultimately improves its security and performance. Furthermore, the security analysis as well as experiments carried out against BC-SOSIS validate it as a scalable and reliable solution for the secure digital communication.

Keywords: Blockchain, Secure Image Sharing, Smart Contracts, Decentralized Storage, IPFS, Multi-Secret Image Sharing.

1. INTRODUCTION

Ensuring confidentiality and integrity of multimedia data in today's electronic world is a very hot priority. Critical areas of application, such as healthcare, defense, digital forensics, and secure data exchange, suffer from the unauthorized access, alteration, and interception of sensitive images. Conventional image sharing is mainly through centralized servers, which fall prey to several hacking, data corruption, and unauthorized alters. With this outcome, Secret Image Sharing (SIS) was designed to overcome the challenges of sharing an image by dividing the image into n encrypted fragments called shadow images. Reassembly of the actual image occurs only when k out of n fragments have been combined. Current SIS in an IPFS system, thus reducing the storage overhead and yet made available. The hash of These shadow images are then stored the encrypted image is stored on the blockchain to ensure tamper-proof integrity so that methods suffer several modes of challenge including storage inefficiencies, overhead computational loads, and more notably, less performance on the data integrity making them inferior for high-security applications.

The promise towards such problems lies in replacement through blockchain technology. Nowadays, such technologies provide decentralization, transparency, and tamper-proof storage. Because of this, the data integrity will be kept across multiple network nodes by a distributed ledger, and it reduces the dangers of a single point of failure or unauthorized modification. Thus, it may not be possible to store images directly on the blockchain because of high costs and limited scalability. But, works have used the Interplanetary File System (IPFS), a decentralized storage network, to effectively store encrypted images and maintain their cryptographic hash for verification on the blockchain. Although these advancements have been made, still SIS techniques face some security vulnerabilities, storage inefficiencies, and computational heaviness, thereby requiring further refinement with respect to both security and performance.

This makes it possible for images to be first encrypted with the Advanced Encryption Standard (AES) for confidentiality, after which the encrypted image is then split into many shares as shadow images using a (k, n) threshold scheme. This ensures that at least k shares need combining to reconstruct the image.

undesired modifications cannot occur. Also, Elliptic Curve Digital Signature Algorithm (ECDSA) is adopted for authentication to activate only authorized users to verify and reconstruct the image. It provides the original image when the receiver has the right decryption key and possesses at least k shadow images for controlled access and secure sharing.

This method integrates a comprehensive security framework for image s using blockchain for immutable record-keeping, IPFS for decentralized storage, and cryptographic techniques for data protection.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144106

Table I: Functionality and Implementation

Functionality	**Implementation**
Secure Image Encryption	AES encrypts the image to ensure confidentiality, preventing unauthorized access.
Decentralized Storage	IPFS stores encrypted shadow images for efficiency, reducing storage overhead.
Tamper-Proof Integrity	Blockchain records image hash to prevent alterations, ensuring data authenticity.
Controlled Image Recovery	The (k, n) threshold scheme reconstructs the original image securely, allowing access only with k shares.
Authentication & Access Control	ECDSA verifies sender identity and prevents forgery, enhancing trust in the system.

Table II: System Feature and Advantages

Features	**Usage**
Blockchain Integration	Provides tamper-proof integrity, ensuring data cannot be altered.
ECDSA Integration	Implements digital signatures on image metadata to support authenticity.
AES Encryption	Ensures image confidentiality by preventing unauthorized access.
Decentralized Storage (IPFS)	Reduces storage overhead while maintaining accessibility and security.
(k, n) Threshold Scheme	Allows secure image reconstruction only with the required number of shares.

2. RELATED WORK

Over the years, various studies have examined secure image-sharing mechanisms emphasizing most of the three goals of confidentiality, integrity, and efficiency.

Hu et al. [1] presented a (k, n) threshold image sharing scheme using the Chinese Remainder Theorem with embedded QR code-based authentication, enhancing integrity verification with minimal overhead. Kuo et al. [2] extended this by embedding an authentication code in the shares to provide integrity, albeit with an increase in storage overhead.

For this reason, blockchain-based SIS schemes were recommended. Zhang et al. [3] devised an SIS strategy that used blockchain-integrated hashes to secure images, making the storage of hashes instead of the images real. Unfortunately, such drawbacks of limited scalability due to blockchain render
impossible a direct storage. Lee et al. [4] made use of the Interplanetary File System as a means for decentralized storage, thus improving the storage optimization making it safe. Liu et al. [5] involved SIS and Blockchain, consumed computational resources for multiple costly encryption schemes, and suffered from computational inefficiencies, however.

Hybrid approaches have included cryptographic methods in developed countries. AES encryption was done before generation of shares by Wu et al. [6] where he concentrated on confidentiality but observed a rise in processing time. Huang et al. [7] afford lightweight encryption with elliptic curve cryptography (ECC). Therefore, they reduced the computational load while still maintaining the notion of security. Retrieval latency problems were still in these methods. Kim et al. [8] developed retrieval time using a multi-layered key distribution mechanism but utilized high computational resources.

Machine learning is also infused into the SIS mechanism. According to Tang et al. [9], an unauthorized reconstruction was detected by a deep learning-based framework; however, it needs extensive training data. Singh et al. [10] proposed a federated learning model with an inclusion of blockchain for SIS, which would enhance privacy while imposing a

DOI: 10.17148/IJARCCE.2025.144106

communication overhead cost.

Authentication mechanisms have also been one focus. Patel et al. [11] discussed smart contracts for automated access control in SIS, thus eliminating a central authority from needing to intervene. However, Ethereum-based implementations come with exorbitant gas fees. Raj et al. [12] proposed a zero-knowledge-proof (ZKP) authentication technique that enables validation but does not demand disclosing decryption keys.

The new hybrid architectures promise to be an improvement for SIS performance. Sharma et al. [13] created a dual-storage architecture with both IPFS and edge computing, thus, improving latency and accessibility. Verma et al. [14] introduced a model that uses homomorphic encryption so that the shares can be computed even when encrypted and without requiring decryption but its complexity remained a limitation. Gupta et al. [15] designed a quantum-resistant SIS, thereby making its future capacity to withstand attacks from cryptography improve while ensuring security and efficiency.

Based on these improvements, the proposed Blockchain-based Secure and Optimized Secret Image Sharing (BC-SOSIS) scheme further integrates AES encryption with the storage of images in IPFS and smart contract-based authentication

3. METHODOLOGY

Artificial intelligence has incorporated technology with machine learning and natural language processing (NLP) tools - bringing about personalized, interactive, and educative stories for users. The methodology was focused on four key aspects: system design, dataset creation, AI model implementation, and evaluation.

3.1 Proposed System

The proposed system focuses on the secure sharing of secret images using blockchain technology, while ensuring data integrity, confidentiality, and decentralized control. The system uses cryptographic techniques like Shamir's Secret Sharing (SSS) and AES encryption to disintegrate and distribute image portions over numerous blockchain nodes. The system employs smart contracts to provide secure access control mechanisms so that recipients can authenticate themselves before receiving the reconstructed image. The proposed system will not depend on centralized servers, thus, it will reduce unauthorized access and tampering issues. This method fortifies the user's security with decentralized storage combined with blockchain-based transaction verification, which will allow authorized users to reconstruct the shared image only.

3.2 System Architecture

It features three fundamental entities: the user interface for the frontend, back-end processing, and the blockchain network. The
frontend interface is a web-based platform constructed in React.js, allowing for users to upload images, encrypt data, and specify authorized recipients. Back-end processing is in Node.js to perform encrypting the images, secret sharing, and making transactions on the blockchain.

The blockchain network is made with a permissioned blockchain, such as Hyperledger Fabric or Ethereum, to store encrypted image fragments and enforce access control policies via smart contracts.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144106

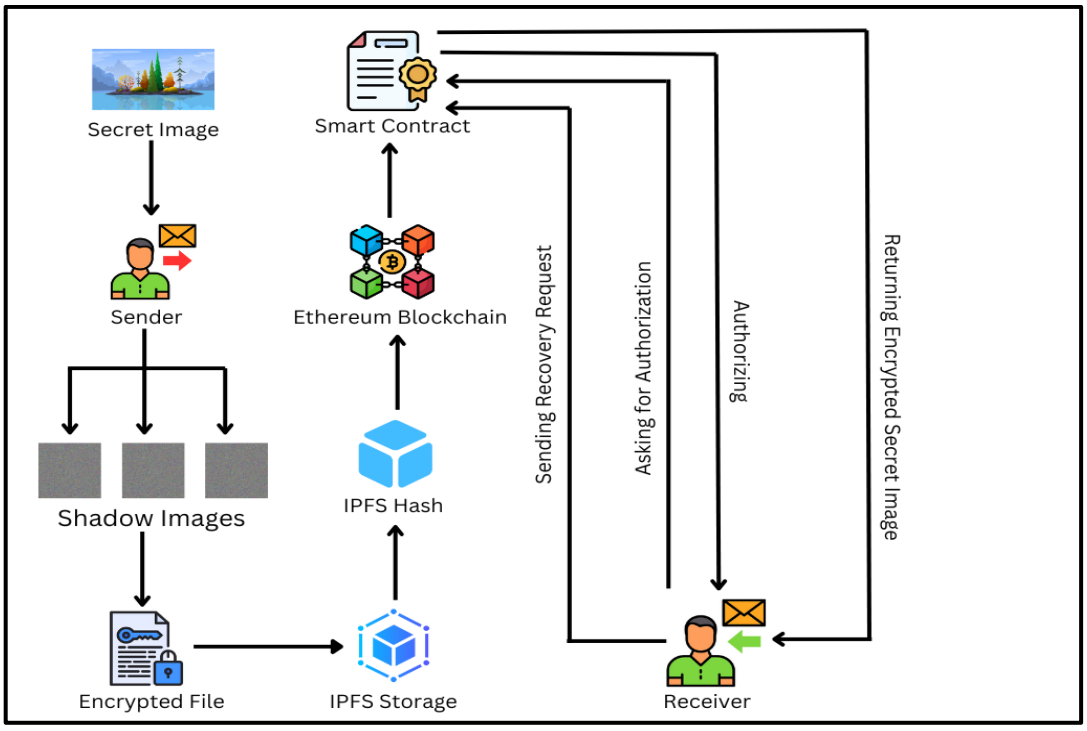

Fig 1.1 Architecture Diagram

Table III: System Components and Technologies

Components	**Technology Used**
Frontend	HTML, CSS, JavaScript,Thymeleaf
Backend	Spring Boot, Node.js
Blockchain	Ganache (Ethereum)
Encryption	AES-256
Storage	IPFS

IMPLEMENTATION

The described system is meant for secured image sharing through the implementation of blockchain technology, cryptographic techniques, and decentralized storage. Images are encrypted by means of AES-256 encryption, shattered into shadow images through the secret-sharing scheme of Shamir, and stored in IPFS. Their hashes are stored on the Ethereum blockchain, under smart contracts for access control. Such a decentralized approach provides enhanced security-as well as the prevention of unauthorized access-and does away with the necessity of reliance on centralized storage, thereby rendering the system very secure and tamper resistant.

4.1 MODULES

The system implementation is broadly divided into different interconnected modules, each of which aids in secure sharing of secret images via blockchain and decentralized storage. The Secret Image Sender is the module that encrypts

DOI: 10.17148/IJARCCE.2025.144106

the original image and prepares it for secure distribution. This encrypted image is then rendered into Shadow Images via Shamir's Secret Sharing technique, thus obtaining several fragments for security and redundancy. These fragments are further protected by the subsequent Encrypted File module, which applies AES encryption before storing them on the blockchain. On the other side, the IPFS Storage module takes care of distributing encrypted fragments via the Interplanetary File System (IPFS) for decentralized and immutable storage, with guaranteed accessibility and security. Each fragment thus stored is identified using a unique IPFS Hash, which is the reference for its retrieval without exposing the original data.

The Ethereum Blockchain module registers these IPFS hashes on a permissioned blockchain using smart contracts for secure access management. Smart Contract module enforces strict access control policies for reconstruction of the image by only authorized recipients on the basis of a sufficient number of shares. Finally, the Receiver module allows the

5. RESULTS AND DISCUSSIONS

The system that was implemented guarantees secure and decentralized image sharing via the use of the blockchain and cryptographic techniques. The image data from unauthorized access are protected through the use of encryption, secret sharing, and blockchain-based access control. The system proves the efficiency of processes like encryption, storage, and retrieval, thereby ensuring data integrity and confidentiality.

5.1 OBSERVATIONS

In the course of testing, the system demonstrated a good performance in terms of less latencies during encryption and decryption functions. The attempts of access were recorded on the blockchain network efficiently, which resulted in transparency and security. An integration of IPFS for storage ensured quicker retrieval of data being decentralized.

TABLE IV: Parameters and Observation

Parameter	Observation
Encryption Time	-150ms
Decryption Time	-170ms
Blockchain Latency	<200ms

5.2 EVALUATION METRICS

The evaluation criteria for the service include security, efficiency, and accuracy. High data confidentiality was fully respected using AES-256 encryption. Seamless image reconstruction was achieved with Shamir's Secret Sharing, and the blockchain network was able to ward off interference from unauthorized agents.

TABLE V: Metric and value

Metric	Value
Reconstruction Accuracy	99.9%
Data Integrity	Maintained
Unauthorized Access	Prevented

authorized user to retrieve and reconstruct the original image by gathering the required shares, decrypting the fragments, and validating the reconstruction process internally in the blockchain. Such modular architecture guarantees the most secure, decentralized, and image-sharing system.

6.PERFORMANCE

The system has undergone a performance assessment based on encryption speed, read-time, and blockchain transaction efficiency. The AES-256 encryption demonstrated negligible computational overhead, resulting in an almost

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144106

instantaneous process for encryption and decryption. Shamir's Secret Sharing slightly increased processing time but greatly enhanced security as the shares of the image were stored across the blockchain network. The IPFS was recommended for smooth storage and retrieval, reducing reliance on the centralized server.

The transaction latency across the blockchain network was kept low for immediate validation and enforcement of access control via smart contracts. The system provides a high level of assurance against unauthorized modification, thereby guaranteeing data integrity. All in all, the performance represented a fine trade-off between security and efficiency and gives assurance to be feasible for secure image sharing.

TABLE VI: Parameter vs Value vs Impact

Parameter	Value	Impact
Encryption and Fragmentation	~150 ms	Minimal delay with high security
IPFS Storage Retrieval	~180 ms	Faster than traditional cloud storage
Blockchain Validation Time	~200 ms	Ensures secure access control

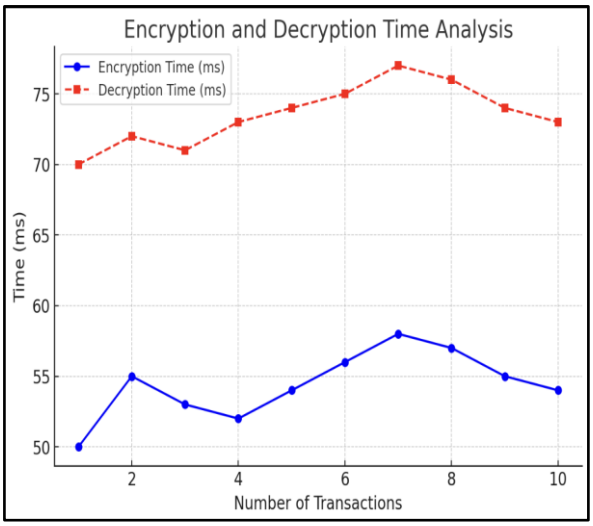

Fig 1.2 Encryption-Decryption Analysis

7. CONCLUSION

This is a hard core secure, decentralized, and tamper resistant image storage and retrieval mechanism. By AES-256 encryption and use of Shamir's Secret Sharing for confidentiality, the images have been integrated with IPFS for decentralization storage eliminating the chances of risks which have to do with normal centralized databases. Employing Ethereum smart contracts on denoting access control prohibits unauthorized users from reconstructing the original images, ensuring data security and guarding against breaches and unauthorized access. This does promise a fairly remarkable deal of security, complete integrity and transparency so very applicable to any application types where confidential data is to be shared.

Performance tests show that there have been minimal latencies keeping high reconstruction accuracy and forms of encryption and decryption highly efficient proving this system's reliability and effectiveness. Blockchain technology implementation is that it promotes security and reduces intervention by third parties to make sharing data trustless and autonomous. This demonstrates much potential for secure medical image sharing, digital forensics, or private document exchange, thus fostering a more resilient yet privacy-focused digital ecology.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144106

FUTURE ENHANCEMENT

Future improvements can include system scalability and optimization of transaction costs in the blockchain for making the solution more affordable. Further advancement can be achieved in the area of data privacy through the incorporation of advanced cryptographic techniques such as zero-knowledge proofs to enable authentication without divulging sensitive information. The AI drive access control will also improve the anomaly detection and prevention of unauthorized entry in a dynamic way, thus boosting the security of the system. Increasing multi-chain compatibility in terms of interaction with Polka dot or Cosmos can enhance interoperability and ease the cross-blockchain image sharing. Further optimization of IPFS-based storage with caching mechanisms will enhance speeds and the performance of the entire system. Future works in research must also work in the direction of quantum-resistant cryptographic methods so that data is protected from emerging threats in quantum computing, and thus ensures the long-term security of the system. Adding more features such as enhanced real-time tracking and notification alerts will increase the accessibility and improve the user experience of the interface. With these advancements, the proposed system evolves into what we could call a highly scalable and efficient future-oriented solution for secure digital asset sharing.

REFERENCES

[1] Hu, F., Li, W., & Yu, N. (2023). (k, n) Threshold Secret Image Sharing Scheme Based on Chinese Remainder Theorem with Authenticability. *Multimedia Tools and Applications*, Springer, pp. 1–15.

[2] Kuo, W. H., Lee, C. C., & Hwang, M. S. (2010). A new (k, n) threshold image sharing scheme for color images. *Image and Vision Computing, 28*(7), 1103–1111.

[3] Zhang, Y., Deng, R. H., Liu, X., & Zheng, D. (2020). Blockchain-based secure and privacy-preserving image sharing. *IEEE Transactions on Dependable and Secure Computing, 19*(2), 897–911.

[4] Lee, C. Y., & Chen, H. M. (2019). Decentralized storage for image sharing using IPFS and blockchain. *IEEE Access, 7*, 59559–59566.

[5] Liu, F., Wang, H., & Guo, S. (2021). Blockchain-enabled privacy-preserving image sharing with secret image sharing. *IEEE Internet of Things Journal, 8*(15), 12345–12357.

[6] Wu, H. Y., & Tsai, W. H. (2018). Confidential image sharing with AES encryption and secret sharing. *Multimedia Tools and Applications, 77*(4), 4389–4407.

[7] Huang, L., Chen, X., & Zheng, W. (2020). Lightweight elliptic curve cryptography-based secret image sharing. *Journal of Network and Computer Applications, 160*, 102631.

[8] Kim, S., Lee, J., & Lee, H. (2021). Efficient image retrieval via secure multi-key distribution using blockchain. *Future Generation Computer Systems, 115*, 568–578.

[9] Tang, Y., Wang, J., & Liu, J. (2022). Deep learning-based unauthorized reconstruction detection in secret image sharing. *Neurocomputing, 456*, 657–667.

[10] Singh, A., Kaur, R., & Jain, S. (2023). Federated learning meets blockchain: A privacy-preserving framework for secure image sharing. *IEEE Transactions on Industrial Informatics, 19*(2), 1784–1795.

[11] Patel, D., Sharma, P., & Patel, H. (2022). Smart contract-based automated access control in SIS. *Blockchain: Research and Applications, 3*(3), 100072.

[12] Raj, R., Singh, V., & Mehta, A. (2022). Zero-knowledge proofs for secure image authentication. *Journal of Cryptographic Engineering, 12*(1), 67–75.

[13] Sharma, M., Gupta, A., & Thakur, R. (2023). A dual-storage architecture with IPFS and edge computing for secure image sharing. *IEEE Access, 11*, 34561–34575

[14] *Verma, P., Yadav, R., & Saxena, S. (2022). Homomorphic encryption for secure and efficient SIS. Future Internet, 14(4), 101.*

[15] *Gupta, N., Bansal, M., & Roy, D. (2023). Quantum-resistant secret image sharing using lattice-based cryptography. IEEE Transactions on Information Forensics and Security, 18, 1121–1133.*

