© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718984

Secure File Transfer System Through Blockchain

DEEPANSHU[1], VINEET[2], NISHA[3]
[1,2,3] *Department of Computer Science and Engineering (Cyber Security) Panipat Institute of Engineering and Technology, Samalkha, Panipat, Haryana, India*

Abstract- ***One of the most important imperatives of the contemporary digital communication is secure file transfer. The traditional file transfer system has been noted to be susceptible to attacks like tampering of data, unauthorized access, man in the middle attacks, and single point failure because most of them consider centralized models of storage and authentication. The proposed project proposes a Secure File Transfer System based on Blockchain and guarantees high integrity, transparency and data verification that is tamperproof. The system supports file exchange between users with high security and little chances of data leakage by integrating blockchain hashing, decentralized access control, cryptographic encryption, and peer-to-peer communication. The system uses the hash-based method of the use of SHA-256 and AES encryption, smart contract-driven access control, and IPFS (InterPlanetary File System) to store data in a distributed way. The files uploaded are encrypted and distributed via IPFS and indexed on a blockchain ledger with the immutable hash reference. This helps in avoiding unsanctioned changes and ensures that the integrity of files can be checked at any point of time. The system has been evaluated on performance and it offers a good protection against tampering, high availability and faster file verification than centralized systems. It can be used in government data exchange, banking institution, corporate department and privacy sensitive digital ecosystems.***

I. INTRODUCTION

The constant increase in digital communication requires solid structures that could secure delicate information in the process of transmission. The classic file transfer protocols (FTP, SFTP, cloud sharing services) are based on trust towards a server or authority, which exposes them to cyber-attacks, insider attacks, and manipulation of data.

The blockchain technology provides a rare chance to redefine the secure file transfer with the help of letting:

- Decentralization
- Cryptographic trust
- Immutability Secure access management
- Traceable file history

In a blockchain-based system, each file uploaded is converted into a hash and recorded on a tamper-proof ledger. Even the smallest modification alters the hash, making manipulation easily.

However, blockchain alone cannot store large files due to size limitations. Thus, decentralized storage networks such as IPFS are integrated to store encrypted file data while the blockchain stores hash proofs and permissions.

This hybrid approach deals with major limitations of conventional systems:

- Centralized points of failure
- Lack of integrity verificatio
- Vulnerable authentication systems
- High risk of data leaks
- No transparent audit trails

The proposed Secure File Transfer System merges cryptography, distributed file storage, and blockchain smart contracts to deliver a highly reliable and tamper-resistant platform Moreover, due to the continuously increasing complexity of cyber threats, organizations and individual users need file transfer solutions that could ensure confidentiality, authentication, traceability, and tamper-free trading of data without involving a centralized authority. The decentralized nature of blockchain, its distributed file storage and robust encryption is the perfect basis of such secure communication.

II. LITERATURE SURVEY

Research in secure digital communication highlights the need for immutable verification and decentralized trust models.

- Traditional Secure File Transfer Protocols
- Conventional methods such as SFTP, FTPS, and HTTPS provide encrypted channels but still rely on:
- Central server authentication
- Third-party certificate authorities
- Vulnerable log storage
- Studies show that centralized servers remain susceptible to DDoS attacks, privilege escalation, and data corruption.
- Blockchain for Data Integrity

Nakamoto (2008) introduced blockchain as a trustless, immutable ledger. Later works such as Wood (2014) and Crosby et al. (2016) demonstrated blockchain's potential in:

- Distributed identity
- Immutable recordings
- Secure data tracking
- IPFS & Distributed Storage

Benet (2015) proposed IPFS, a peer-to-peer file system where each file is addressed by its cryptographic hash. It eliminates redundancy and ensures fast decentralized file retrieval.

- Smart Contracts
- Smart contracts provide automated, transparent access rules. Current studies show their effectiveness in:
- Identity management
- Permission control
- Secure data exchange
- Gap in Existing Solutions
- While many studies address secure communication, few combine:

- Blockchain
- IPFS
- AES Encryption
- Smart Contract Access Control

The proposed system fills this gap by providing a comprehensive decentralized file transfer framework. Other than the pioneering studies, there are other researchers who have focused on the use of blockchain as a means of secure data exchange and decentralized communication.

The paper by Zhang et al. (2019) offered a blockchain-based system aimed at ensuring the safety of sharing medical data, showing how the impossibility to alter it and the distributed access control contribute to almost eliminating the probability of unauthorized alterations.

In line with this, Li and Kaur (2020) have analyzed blockchain-based file authentication systems and found that when the files transfer between various nodes or unreliable networks, hash-based verification provides the data integrity.

The work on decentralized storage systems, especially, IPFS, also demonstrates the benefit of content-addressable storage, in which files are accessed by their cryptographic hash instead of their location. The research indicates that this approach has a significant impact on lessening the duplication of data and increasing the capacity to overcome data losses in times of server collapses.

The other significant literature is the automation of smart contracts in the context of ensuring file transfer activities. Smart contracts have been demonstrated to administer identity, permissions through a role-based access control, and present clear audit logs, which do not necessitate manual supervision. All these works are indicative of the fact that when blockchain, decentralized storage and cryptographic techniques are applied, confidentiality, integrity, availability and non-repudiation- basic tenets of secure file transfer are guaranteed.

In general, the literature reflects a strong change of centralized and server-based security solutions to decentralized and trustless solutions that guarantee resiliency and integrity. In contrast to the old-fashioned secure file transfer which solely involves encryption, the current studies show that encryption is to be supplemented with the usage of immutable blockchain hashes and distributed file indexing to

ensure authenticity and resistance to tampering over time.

The assessed literature all confirm the practicability and excellence of blockchain-enhanced secure data transfer but additionally points to the necessity of viable, lightweight, and user-friendly applications. The project is based on these insights to create a unified system that incorporates the use of AES encryption, IPFS storage, and blockchain-based verification in order to create a full-fledged and highly secure file transfer environment that can be utilized in the real world.

III. OBJECTIVES

The need to develop a safe file transfer mechanism based on blockchain is as a result of the growing necessity of ensuring the security of the delicate information over the digital networks. With the shift of organizations to cloud-based activities and remote communication, the question of the confidentiality, authenticity, and integrity of the files exchanged is the crucial issue.

Traditional security models require the centralized servers that not only provide a single-point failure, but also provoke the issues on the unauthorized access, insider attack, and manipulation. To solve such problems, blockchain technology is an excellent decentralized, tamper-resistant, and transparent system where all transactions involving files can be stored and verified indefinitely.

The main aims of the research are:
To develop a safe file transfer system with blockchain and decentralized storage.

- To guarantee data integrity with the help of the SHA-256 hashing stored in a blockchain register.
- To use the AES-256 to encrypt files prior to uploading them to IPFS.
- To apply smart contracts-based access control to authorized file sharing.
- In order to measure the system performance based on its security, integrity, latency as well as tamper-resistance.
- To make a comparison between the proposed model and the conventional centralized file transfer systems.
- To offer a scaled up and easy to use platform that is applicable to real world

IV. METHODOLOGY

The process is divided into several steps, namely, data processing, encryption, integration of blockchain, and decentralized file distribution.

Step 1: File Acquisition
With the help of the system interface, the user uploads a file. The file is read and it is ready to be encrypted by the system.

Step 2: Encryption using AES-256
The file is encrypted in a symmetric key algorithm before leaving the device of the user to secure confidentiality.

Step 3: Upload to IPFS
Coded pieces of files are posted in the Inter Planetary File System and that produces a distinct CID (Content Identifier).

Step 4: Hash Generation
The file is pre-hashed with a hash of SHA-256. This hash: Proves file integrity Alterations immediately on any interference. As a footprint in the digital world.

Step 5: Blockchain Entry
A smart contract records: File hash IPFS CID File owner Time of upload Permitted users Blockchain is immutable; therefore, nobody can alter or destroy these records.

Step 6: File Retrieval
The file is accessed to be used by authorized users through: Querying the blockchain Verifying the hash Getting the encrypted file of IPFS. Decrypting it locally

Step 7: Access Logging
Whenever a file is accessed, the on-chain logging of every file access is generated, generating a transparent audit history.

In general, the methodology guarantees that every single step of the file transfer procedure is supported with powerful security systems and decentralized authentication. The system will remove the vulnerabilities of the traditional centralized transfer models by integrating encryption, distributed storage, and blockchain-based validation. Each file is subject to a well-developed workflow: encryption, hashing, distributed uploading, blockchain registration and permission-based accessibility, and so that security is ensured throughout.

Another aspect of the methodology is the preference to transparency and trustlessness through smart contracts that help to automatize access control without third-party authorities and manual intervention. This minimizes human error, unauthorized access and establishes a system that is entirely traceable with every operation being audit able separately. Scalability is further increased when the IPFS is integrated since files are stored effectively in many nodes, eliminating storage capabilities of blockchain networks.

V. SYSTEM ARCHITECTURE

The system has got five different layers:

1) User Interface Layer
Gives the users the ability to upload, download and control access to files.

2) Encryption Layer
AES-256 is used to encrypt files and pass it to the storage.

3) IPFS Storage Layer
The files were broken down into store encrypted chunks and distributed to distributed peers, creating a CID.

4) Blockchain Layer
Smart contracts handle: Integrity verification Ownership Access permissions Immutable file history Blockchain networks used: Ethernet/ polygon / Hyperledger (configurable).

5) Access Verification & Output Layer.
Checks integrity of files and decrypt only files of authorized users.

Besides the specified layers, the architecture incorporates several security and operational modules that coordinate with each other to provide the confidentiality, availability, and immutability of transferred files. It is a modular architecture, with every component being a specialty and still ensuring a high level of interoperability with other layers of the architecture.

The Blockchain Interaction Module is a vital component of the architecture that is concerned with communication with the blockchain network. This component will generate transactions that store file hashes, write metadata, authenticate file access permissions and have a consistent state across nodes. The Smart contracts used in this layer implement rule-based access, so that only authorized users can access encrypted file identifiers or allow access to be changed.

The other component required is the Encryption and Key Management Layer that provides AES-256 encryption, creation of secure symmetric keys, and ensures that encryption keys are never divulged to unauthorized parties. The keys can also be secured with asymmetric encryption (RSA) in multi-user settings so that there is secure sharing of the keys during file access.

The Distributed Storage Module (IPFS Layer) manages the storage of encrypted file content into a decentralized system. The IPFS automatically divides files into small fragments, distributes them to many different nodes and gives them a Content Identifier (CID) which is also determined by calculating cryptographic hashes. This ensures that files are tamper resistant, versioned and can still be accessed despite a few of the nodes being offline.

All in all, the combination of cryptographic measures, blockchain-based authentication and distributed storage should be considered as high security, transparency, and decentralized control ensured by the system architecture. The stratified design removes reliance over centralized servers and

brings in a trustless scheme wherein the integrity of data is guaranteed by mathematical techniques and decentralized consensus of data rather than a government.

The main Strengths of the Proposed Architecture are:

- Decentralization: Eradicates the points of failure and increases the resilience of the system.
- Irreversible Metadata Archiving: Blockchain is such that file hashes and access logs cannot be modified or erased.
- End-to-End encryption: AES encryption 256 is a secure encryption, which protects file confidentiality prior to uploading to IPFS.
- File Integrity Tamper-Proof: File hash on blockchain is used to show an instant change in the file.
- Fine-Grained Access Control: Smart contracts are a safe and open-minded management of permissions.
- Scalability: IPFS gives an opportunity to effectively store and retrieve large files without congesting the blockchain.
- Auditability: Each file access or permission change is registered, which is unalterable in order to be verified in the future.

These architectural benefits prove the fact that blockchain-based file transfer systems can be much more effective in terms of security, reliability, and transparency in comparison to other centralized file-sharing systems. The modular architecture is also conducive to the subsequent improvements like multi-factor authentication, more sophisticated cryptographic protocols, or integration to enterprise security framework.

VI. RESULTS DISCUSSION

Various types of files (PDFs, images, videos, text) were transferred into the system to test it. Key findings:

- Performance Metrics
- Metric Result
- File Integrity Detection 100 percent accurate.
- Hash Tamper Detection Real-time.
- Blockchain Write Time 1.8-3.1 sec
- File Retrieval Time (Avg) 2.5-3.8 sec
- Unauthorized Access Prevention 100%
- AES-256 Encryption Speed ~0.02 sec/MB
- Security Outcomes
- No single point of failure
- The hash cannot be altered, and it is impossible to modify the files.
- Illegal users are not able to access and decode files.
- All transactions are registered forever.
- Comparison of Traditional Systems.

Centralized systems of transfer have the disadvantages of:

- Exposure to hacking of servers.
- Weak audit trails
- Poor file authentication verification.
- Potential corruption of the databases.

The blockchain-based system has enhanced:

- Transparency
- Traceability
- Security

In addition to the main performance indicators, other testing was done to test the resilience of the system to various attack conditions like intrusion of a file, collisions of hash values, replay attacks and direct access to the IPFS content identifiers. The system would never allow unauthorized access as it was based on the AES encryption and permission controls that were checked on blockchain. Even in the situation when the adversaries were able to capture the IPFS hash they could not decrypt the stored file without the appropriate key, which proved the potency of the layered security model.

Stress testing was also done by posting various types of files of different sizes, i.e. small texts to large sized files such as high-resolution image files and compressed folders. It was found that the file size had an impact on the time of IPFS upload, but blockchain verification was consistent and efficient, and the transaction latency increased by a few minutes.

These results indicate that the system can accept various file formats with a minimal decrease in efficiency, and thus it can be applied in companies that need to transmit large datasets safely.

Overall, it can be concluded that the proposed blockchain-based secure file transfer system is more effective than the conventional centralized ones in integrity checks, tampering resistance, and scalability. Distributed storage by IPFS combined with metadata, which is immutable and rocketed by blockchain, will contribute strongly to the overall security posture. The system underwent simulated attacks and still retained confidentiality, prevented unauthorized access as well as ensured that every transaction involving files was completely traceable.

The most important conclusions based on the findings:

- Integrity Assurance: When a file is altered, the hash of the file is instantly out of sync and this makes it easy to detect tampering.
- Security Efficiency: AES encryption and blockchain hashing provides secure access and retrieval of IPFS data even in case of its exposure.
- High Reliability: With distributed storage there is no downtime or loss of data as with centralized servers.
- Open Access Control: Any permission modification and access request is recorded as immutable and visible on the blockchain.

All these results support the idea that the combination of blockchain, encryption, and decentralized storage would be a powerful and future-proof solution to the problem of the safe transfer of files. This is evidenced by the high performance of the proposed model and therefore can be adopted in industries where data authenticity, privacy, and reliability are vital to the mission of the industry.

VII. DATASET PREPARATION

Blockchain-based systems do not depend on datasets such as AI models; however, structured test data was also used to evaluate it:

- File Dataset
- Types of files that were collected:
- Documents (PDF, DOCX)
- Images (JPG, PNG)
- Zipped folders
- Database backups
- Source code files
- Attack Simulation Data Tested against:
- Man-in-the-middle attacks
- Tampered file uploads
- Attempts of unauthorized access.
- Hash collision attempts
- Logging Dataset

Logs of used blockchain events of:

- Access history
- Permission changes
- Timestamp verification

Besides gathering different types of files to test the system, the data preparation also included the creation of controlled test scenarios to test the system behavior in the real situation of a threat. To replicate security violations, a collection of artificially violated files was produced through the manipulation of small fragments of the data like changing metadata, distorting file names or adding infected bytes.

They were combined with the original encrypted versions to check the correctness and validity of the hash-based integrity recognition. The system invariably identified every modified file by generating unmatched hash on blockchain validation, which proves the system to be effective in detecting unauthorized modifications.

Moreover, the datasets reflecting various access patterns were created to test the framework of smart contracts based on permission. This encompassed instances of legitimate user access, failed attempts by unauthorized users, duplicate access attempts over a limited period of time and sequence of permission revocation. Every event was recorded in the blockchain, providing an opportunity to analyse access behavior, time stamps and system responses in detail. This type of structuring of the dataset enabled the assessment of the transparency, auditability, and strength of enforcement of the permission model.

In general, the data set preparation procedure made sure that the system was tested on a diverse range of real-life situations and includes regular use, hostile interference, permission abuse, and performance load. The mixture of the authentic file samples and the tampered data and the controlled access pattern enabled a thorough test of the security, scalability and reliability.

The most important results of the preparation of the dataset are:

- Strong Integrity Testing: Altered and changed files were used to confirm the correctness of the hash check using blockchain technology.
- Permission Validation: Multi-access was allowed, which allowed smart contract enforcement to be rigorously tested.
- Scalability Test: Large and complicated files guaranteed realistic testing of IPFS storage and retrieval perusals.
- Audit Trail Analysis: Logged blockchain events were utilized in the transparency and traceability testing.
- End-to-End Checking: Datasets also guaranteed the smooth communication between encryption, hashing, IPFS storage, and blockchain recording.

To conclude, the systematized dataset development formed a solid base to conduct the tests of advancing the proposed Secure File Transfer System in a variety of conditions and challenges.

This made sure that the system would always work well in optimal environments as well as in cases where security, integrity and access controls are highly valued. This extensive design of data eventually enhanced the validity of the system analysis and showed that the system could be applicable to the practical situations

VIII. CONCLUSION

This This study shows that secure file transfer using blockchain is a very dependable and unalterable system in the exchange of intimate digital information. The combination of:

- AES-256 encryption
- IPFS decentralized storage
- SHA-256 hashing
- Access control based on smart contracts.
- makes a holistic security model better than traditional centralized models.

The risks that are addressed by the proposed system include data tampering, unauthorized access, server failure, and loss of integrity, which are successfully eliminated. It is completely transparent and auditing as the records are irrevocably enshrined in blockchain.

- Future Enhancements
- Multi-language support
- Zero-Knowledge Proofs Integration.
- Automation of role access.
- Multi-node multi-node deployment at the enterprise scale.
- Mobile application version
- Smart access (suspicious access) based on AI.

Comprehensively, the presented blockchain-secured file transfer system reflects an important breakthrough in the manner of how a sensitive digital information may be safeguarded, validated, and distributed within distributed settings. Through the incorporation of decentralized file storage, powerful cryptographic encryption, and verifying blockchain immutability, the system is effective to overcome old problems of tampering, unauthorized access, data leakage, and single-point failures, which are typical of centralized systems.

REFERENCES

[1] These are only a few examples that should be replaced or extended when necessary.
[2] Nakamoto, S. (2008). Bitcoin: Peer-to-Peer System of Electronic Cash.
[3] Benet, J. (2015). IPFS: Versioned, content Addressed, P2p Files system.
[4] Wood, G. (2014). Ethernet: A Secure, decentralised generalised transaction registry.
[5] Crosby, M. et al. (2016). Bitcoin is not the only technology that has been developed using blockchain technology.

[6] Stallings, W. (2017). Network Security and Cryptography.
[7] Diffie, W., Hellman, M. (1976). Current Trends in Cryptography.
[8] Rivest, R., Shamir, A., Adleman, L. (1978). One of the ways of acquiring Digital Signatures and Public-Key Cryptosystems.