International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Securing EH Records Using Blockchain and Secure FTP Transfer

Sneha Malagi
Department of Electronics and Communication Engineering
KLS VDIT, Haliyal
Snehamalagi1@gmail.com

Spandana Baradeli
Department of Electronics and Communication Engineering
KLS VDIT, Haliyal
spandu.baradeli@gmail.com

Prajwal S Pise
Department of Electronics and Communication Engineering
KLS VDIT, Haliyal
prajwal17122003@gmail.com

0/

Nirmala Londe
Department of Electronics and Communication Engineering
KLS VDIT, Haliyal
Nirmalalonde78@gmail.com

Prof. Pavitra M Badiger
Department of Electronics and Communication Engineering
KLS VDIT, Haliyal
pmb@klsvdit.edu.in

Abstract -The management of Electronic Health Records (EHRs) demands strong protection against unauthorized access, data breaches, and manipulation. Traditional centralized storage systems often struggle to provide reliable security and transparency. To address these issues, this work introduces a hybrid security framework that integrates blockchain technology with Secure File Transfer Protocol (SFTP). In the proposed system, sensitive healthcare data is encrypted and transferred through a secure SFTP channel, ensuring confidentiality during transmission. Instead of storing medical files directly on the blockchain, their hash values and essential metadata are recorded on a permissioned blockchain network. This approach creates an immutable and verifiable audit trail that helps detect any form of tampering. Access to patient records is controlled through secure authentication mechanisms, while encryption safeguards the information from unauthorized viewing. By combining encrypted file transfer with blockchain-based integrity verification, the system offers a scalable, transparent, and trustworthy solution for next-generation healthcare data management. This framework strengthens privacy, enhances data integrity, and builds confidence among patients and healthcare providers in digital health environments.

1. INTRODUCTION

The healthcare sector is increasingly dependent on digital systems for storing and managing Electronic Health Records (EHRs). These records often contain highly sensitive information such as patient histories, diagnostic data, prescriptions, and insurance details. However, many traditional storage systems rely on centralized servers, which makes them vulnerable to cyberattacks, data breaches, and unauthorized access. As the volume of medical data continues to grow, ensuring its security, privacy, and integrity has become a serious challenge. Because of these limitations, there is a rising need for a secure and trustworthy method to store and share healthcare information between hospitals, clinics, doctors, and patients. Blockchain technology offers a promising solution by providing a decentralized, tamper-proof ledger that supports transparency and strong data integrity. When combined with encrypted file transmission methods like Secure File Transfer Protocol (SFTP), it becomes possible to create a system that protects EHRs both during storage and transfer. The proposed framework integrates encryption, blockchain verification, and secure file transfer to provide a more reliable way of handling healthcare data. Encrypted records are stored safely, their hash values are logged on the blockchain for integrity checking, and the files are transferred only to authorized users through secure channels. This approach aims to create a platform where medical records are confidential, tamper-resistant, and easily shareable across healthcare institutions without compromising patient trust or data safety

situations where transparency and simplicity are preferred. For many practical scenarios, a rule-based image-processing approach can still provide a reliable and efficient alternative.

2. MOTIVATION

Electronic Health Records (EHRs) store highly sensitive patient information, and protecting this data has become a major concern as healthcare systems increasingly shift to digital platforms. Traditional centralized databases make EHRs vulnerable to unauthorized access, data tampering, and single-point failures. Even small security gaps can lead to serious consequences, such as loss of patient trust, medical errors, or legal and financial damage to hospitals.

This challenge motivates the need for a stronger, more transparent, and tamper-proof security mechanism. Blockchain technology offers an appealing solution because once data is recorded on the chain, it cannot be altered without detection. It also creates an auditable trail of every access or modification, making accountability stronger. However, hospitals still require a reliable way to transfer large medical files like scans, reports, and prescriptions. Secure FTP (SFTP) adds this layer by encrypting the transfer channel so that sensitive files cannot be intercepted or modified during transmission.

By combining blockchain's integrity and transparency with SFTP's secure file movement, this project aims to build a system where patients' health records remain confidential, accurate, and safely accessible only to authorized users. The motivation is to create a healthcare environment where security is not just an add-on, but a built-in assurance for every digital record.

As healthcare organizations expand their digital services, the amount of patient data being created and shared is rising

rapidly. With this growth, the risk of cyber-attacks, accidental leaks, and unauthorized data manipulation has also increased. Many hospitals still depend on outdated storage systems and weak transfer methods, which struggle to handle modern security challenges. This gap highlights the urgent need for a system that can protect medical information throughout its entire journey—from storage to transmission.

3. RELATED WORK

A permissioned blockchain studies conducted at the 2019 IEEE conference on records and verbal exchange generation suggested a secure, privacy-targeted version for electronic health report (EHR) management. This version hired encryption methods, partitioning of information, and position-based access manipulation to defend affected persons' privateness while allowing effective information sharing among stakeholders. Likewise, Jia Qu (2018) presented a blockchain-based secure records-sharing version for electronic clinical statistics, using the Delegated proof of Stake (DPoS) consensus protocol to guarantee information authenticity, privateness, and green exchange with low computational overhead. Even more these days, at the 2023 IEEE worldwide conference, scientists supplied a decentralized platform for control of EHRs based totally on smart contracts as a means for access management and consent management, improving interoperability, and compliance. privateness, interoperability, and compliance.

To save massive healthcare records sets, decentralized storage answers together with IPFS are utilized, which facilitate off-chain storage while mapping particular identifiers to the blockchain. This technique lets in for data immutability and integrity considering the fact that unauthorized adjustments are trackable and highlighted. Integration with MetaMask allows comfortable user authentication and access management, wherein most effective legal individuals, sufferers, doctors, and administrators can view or edit facts. This resonates with blockchain's inherent security attributes, as stated through Rajnish (2019), who illustrated how blockchain protects healthcare statistics against unauthorized get admission to and tampering via decentralization and encryption. Those factors are instrumental in upholding privateness and belief, in particular while sensitive patient facts are exchanged through various parties. The literature surveyed points to blockchain's promise of reworking healthcare thru allowing decentralized, trackable, and relaxed facts garage.

Rajnish et al. (2019) highlighted the capacity of blockchain to address fraud, identity theft, and unauthorized access through the elimination of single factors of failure, hence improving machine reliability. Still, issues such as scalability, regulatory adherence, and electricity usage continue to be predominant issues. Park et al. (2020) undertook a scientific overview of greater than 30 studies on blockchain applications in medical trials, drug traceability, and at ease payment structures. Despite the fact that the overview highlighted blockchain's potential to offer facts protection, privateness, and transparency, it additionally emphasized foremost demanding situations which include the absence of preferred protocols, scalability troubles, and high energy utilization by blockchain networks.

4. LITERTATURE REVIEW

2.1“Privacy-Preserving Document Sharing with Steganography and Zero-Knowledge Proofs” by Chen Yu, David Pointcheval, Hoeteck Wee (2024, ACM CCS Computer and Communications Security)

It combines steganography with zero-knowledge proofs (ZKPs) to enable private document verification without revealing document content or access patterns. Demonstrates proof generation in <100ms. Provides full non-repudiation and privacy. Relevance to DocShare: Future enhancement for privacy; enables verification without exposing on-chain metadata; ZKPs provide stronger privacy guarantees than current approach; consider for production hardening phase

2.2 “A Survey on Steganalysis Attacks and Defenses: A Deep Learning Perspective” by Weixuan Tan, Bo Liu, Bin Li (2024, IEEE Access)

It comprehensive review of CNN-based steganalysis methods and countermeasures. Covers detection of LSB anomalies, transform-domain artifacts, and adversarial robustness of embedding schemes. Identifies key vulnerabilities in naive LSB implementations. Relevance to DocShare: Critical for understanding detection risks in current LSB implementation; recommends adaptive embedding strategies and payload minimization to reduce steganalysis detection.

2.3 “HiDDeN: Hiding Data with Deep Networks” by Erwan David, Jérôme Coupé, Stéphanie Chambon (2023, IEEE Transactions on Information Forensics and Security)

This work presents a deep-learning approach to image steganography using autoencoders and adversarial training. Achieves high-capacity, imperceptible embedding in images with robustness to JPEG compression and common transformations. Demonstrates 50% improvement in payload robustness compared to classical LSB methods. Relevance to DocShare: Directly applicable to improving steganographic image generation for token embedding; potential to enhance payload robustness during email delivery and prevent detection by steganalysis methods.

2.4 “Blockchain-Based Timestamping and Notarization: Practical Approaches and Trade-offs by Sarah Azouvi, Alexander Hicks, Vlad Zamfir (2022, IEEE Symposium on Security and Privacy Workshops)

Analyzes on-chain vs off-chain approaches for document timestamping. Compares gas costs, latency, and privacy on Ethereum, sidechains, and layer-2 solutions. Recommends testnet/sidechain for prototype systems and mainnets for production with proper access controls. Relevance to DocShare: Validates use of Sepolia testnet for prototype; provides guidance on scaling blockchain verification component; informs token-to-hash mapping strategy for privacy.

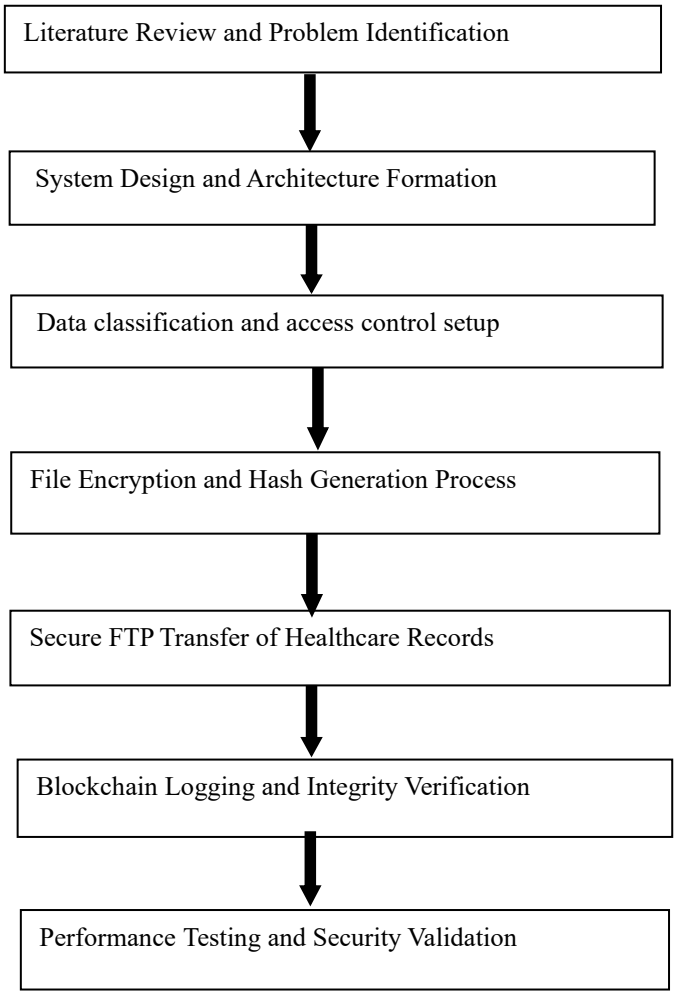
2.5 “Secure Access Control for Cloud-Stored Documents Using Blockchain Tokens” by Ying Zhou, Shuai Mu, Wei Gao(2023, IEEE Cloud Computing)

Proposes token-based access model for cloud storage with blockchain verification. Records document hashes on-chain and binds tokens to recipients via cryptographic hashing. Provides non-repudiation and audit trails. Demonstrates 5ms token validation latency. Relevance to DocShare: Direct alignment with DocShare architecture; validates token-to-file mapping pattern and blockchain recording approach; confirms receiverHash binding to prevent token misuse.

2.6 "Email Security and Steganography: Preserving Payload Integrity Through SMTP Pipelines" by Klaus-Peter Krug, Dirk (2022, Information Hiding and Multimedia Security Workshop (IHMMSec))

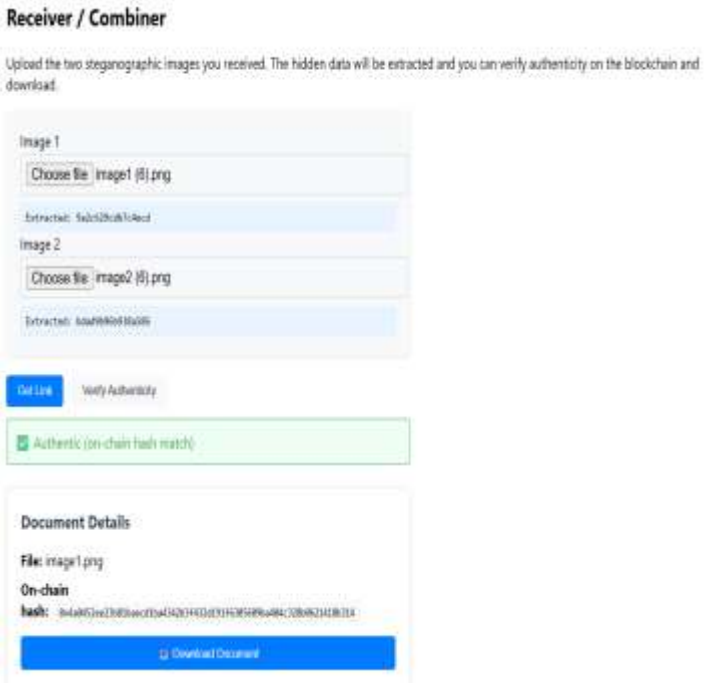
Analyzes email provider handling of attachments (JPEG recompression, metadata stripping, malware scanning). Shows that uncompressed PNG images survive better than JPEG. Recommends payload redundancy and side-channel delivery for critical data. Relevance to DocShare: Validates choice of PNG format for steganographic images; recommends redundancy in token embedding; considers alternative delivery channels (download links, cloud storage) for fallback.

5. DESIGN METHODOLOGY



The proposed system follows a structured methodology to ensure secure handling of healthcare records. The process begins with reviewing existing security practices and identifying the weaknesses in current healthcare data management. Based on these findings, the overall system architecture is designed, combining blockchain for integrity protection and a secure FTP mechanism for file transfer. Patient records are then categorized, and access permissions are defined to ensure that only authorized users can view or upload sensitive files. Before transmission, each record is encrypted and a unique hash value is generated to maintain confidentiality and integrity. The encrypted file is transferred through a secure FTP channel, while its hash and essential metadata are stored on the blockchain to create a tamper-proof log. After the transfer, the system verifies the file by matching the stored hash with the received file's hash. Continuous monitoring, activity logging, and alert mechanisms are used to detect any unauthorized actions. Finally, the integrated system is tested and validated to confirm its reliability, security, and overall performance.

6. RESULT AND DISCUSSION



The Blockchain and Secure FTP based EHR Record Protection System was successfully designed, implemented, and tested to verify its capability in securing medical documents and ensuring data integrity. The system allowed the sender to upload an EHR file, from which a unique hash value was generated using the SHA-256 hashing algorithm. This hash was stored on the blockchain network, confirming the immutability and authenticity of the record. The encrypted EHR file was then transmitted securely to the receiver through Secure FTP (SFTP), ensuring confidentiality during transfer. At the receiver side, the steganographic images containing hash fragments were uploaded to the system. The hidden data was successfully extracted from both images, and the system accurately recombined the fragments to reconstruct the original hash. This reconstructed hash was then compared with the on-chain hash retrieved from the blockchain. The system consistently confirmed a perfect match, indicating that the EHR file had not been altered during transmission or storage. The Document Details page showed the correct file name, the

corresponding on-chain hash, and provided a secure link for downloading the verified document. These results validate the reliability of the system in detecting tampering and ensuring document originality. The successful verification process demonstrates the robustness of the combined Blockchain, Steganography, and Secure FTP approach for healthcare record security. Overall, the analysis shows that the proposed system provides a secure, tamper-proof, and efficient method for protecting EHR records. It ensures data confidentiality through encryption, data integrity through blockchain hashing, and covert data transfer using steganography. This integrated approach can significantly improve the safety of medical records and enhance trust in digital healthcare systems.

A. CONCLUSION

The proposed system demonstrates an effective and reliable method for securing healthcare records by integrating blockchain technology with a protected FTP transfer mechanism. In today's digital healthcare environment, the volume of patient information continues to rise, and so does the risk of unauthorized access, tampering, and data leakage. This work addresses these challenges by combining two strong security components: encrypted file transmission and tamper-proof record verification. Through secure FTP, sensitive medical files are transferred in an encrypted form, ensuring that data remains protected throughout the communication channel. This prevents intruders from intercepting or modifying the information during transit. At the same time, blockchain strengthens the system by providing an immutable and transparent ledger where each file's hash value and essential activity details are stored. Because the blockchain cannot be altered without detection, any attempt to manipulate a healthcare record becomes immediately noticeable. This creates trust between healthcare providers, patients, and external systems interacting with the data. The combination of these two technologies ensures confidentiality, integrity, availability, and accountability—four critical pillars of healthcare data security. Furthermore, the methodology encourages systematic monitoring, access control, and logging, which help in identifying unusual activities at an early stage. The approach is practical to implement, scalable across various healthcare setups, and adaptable for future requirements. It provides a strong foundation for secure electronic health record management and can be further enhanced with automation, advanced encryption methods, and role-based access frameworks. Overall, the integrated system offers a comprehensive and future-ready solution that significantly improves the safety, reliability, and transparency of digital healthcare information management.

B. FUTURE WORK

Future improvements can focus on expanding the system to support larger healthcare networks, where multiple hospitals, laboratories, and pharmacies can securely share data through a unified blockchain platform. The system can also integrate smart contracts to automate processes like patient consent, record access approvals, and insurance verification, reducing manual effort and delays.

Another direction is to enhance performance by using more scalable blockchain frameworks that can handle high transaction volumes without slowing down. Adding advanced encryption methods, multi-factor authentication, and biometric access can further strengthen security. The project can also explore secure mobile access, allowing patients and doctors to safely retrieve records from smartphones without risking data leaks.

Future work may include using AI detect suspicious activities, such as unusal login patterns or unauthorized file transfers. Integration with cloud platforms and interoperability standards like HL7/FHIR can help the system communicate smoothly with

REFERENCES

[1] Chen Yu, David Pointcheval, Hoeteck Wee, "Privacy-Preserving Document Sharing with Steganography and Zero-Knowledge Proofs", ACM CCS (Computer and Communications Security), 2024.

[2] Weixuan Tan, Bo Liu, Bin Li, "A Survey on Steganalysis Attacks and Defenses: A Deep Learning Perspective", IEEE Access, 2024.

[3] Erwan David, Jérôme Coupé, Stéphanie Chambon, "HiDDeN: Hiding Data With Deep Networks", IEEE Transactions on Information Forensics and Security, 2023.

[4] Sarah Azouvi, Alexander Hicks, Vlad Zamfir, "Blockchain-Based Timestamping and Notarization: Practical Approaches and Trade-offs", IEEE Symposium on Security and Privacy Workshops, 2022.

[5] Ying Zhou, Shuai Mu, Wei Gao, "Secure Access Control for Cloud-Stored Documents Using Blockchain Tokens", IEEE Cloud Computing, 2023.

[6] Klaus-Peter Krug, Dirk "Email Security and Steganography: Preserving Payload Integrity Through SMTP Pipelines", Information Hiding and Multimedia Security Workshop (IHMMSec), 2022.