International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Decentralized Online Health Consultation System with Secure Blockchain Storage

Dr.P.Pavan Kumar [1],B. Venkata Bhargav[2], D. Harsha Vardhan[3], V. Sudhan Reddy[4]

[1]Assoc. Prof, Department of Computer Science and Engineering, CBIT, Proddatur, YSR, 516360
[2]UG Student, Department of Computer Science and Engineering-[AI&ML], CBIT, Proddatur, YSR
[3]UG Student, Department of Computer Science and Engineering-[AI&ML], CBIT, Proddatur, YSR
[4]UG Student, Department of Computer Science and Engineering-[AI&ML], CBIT, Proddatur, YSR

*Corresponding Author E-mail:venkatabhargav9398@gmail.com

Abstract

The rapid growth of digital healthcare platforms has improved access to medical consultation, especially in remote regions. However, centralized storage systems raise serious concerns regarding data privacy, unauthorized access, and record manipulation. Electronic Health Records (EHRs) contain highly sensitive information, and any compromise can reduce trust in digital healthcare services. This paper presents a decentralized online health consultation system that combines blockchain technology with Shamir Secret Sharing to strengthen confidentiality and reliability. Instead of storing complete medical records on a single node, the proposed approach divides sensitive data into cryptographic shares and distributes them across independent blockchain nodes. Only a predefined threshold of shares can reconstruct the original record, ensuring partial exposure does not reveal meaningful information. Experimental evaluation shows improved data protection and reduced storage overhead compared to traditional blockchain storage. The results indicate that the framework provides a practical and secure alternative for modern telehealth environments.

Keywords: Blockchain, Smart Healthcare, Electronic Health Records, Shamir Secret Sharing, Data Security

1. Introduction

Digital healthcare services have transformed how medical consultations are conducted and how patient records are maintained. Online consultation platforms allow patients to communicate with doctors without visiting hospitals, improving convenience and accessibility. Despite these

advantages, most systems still depend on centralized infrastructures, which introduce risks such as single points of failure, data breaches, and unauthorized internal access.

Electronic Health Records include medical history, prescriptions, diagnostic reports, and personal identification details. Protecting this information is both a technical and ethical responsibility. Cloud-based storage solutions offer scalability, yet they remain vulnerable to cyberattacks and insider misuse. A more secure and transparent storage approach is therefore necessary.

Blockchain technology provides a decentralized and tamper-resistant ledger that enhances accountability. However, storing complete medical records directly on blockchain networks is inefficient and expensive. To overcome this limitation, this study integrates Shamir Secret Sharing with blockchain storage. Medical data is divided into secure fragments and distributed across multiple nodes. No individual node contains the full record, strengthening confidentiality while maintaining availability when authorized access is granted.

2. Literature Review

Recent studies have explored blockchain applications in healthcare to improve integrity and patient privacy. Decentralized ledgers create immutable audit trails and reduce the risk of record alteration. Smart contracts have been proposed to automate consent verification and access control in telemedicine systems.[1]

Some approaches combine blockchain with cloud infrastructure to improve scalability. Although encryption is applied, encrypted data stored in centralized environments may still be exposed if encryption keys are compromised. Other research has focused primarily on logging and verification without addressing storage efficiency.[2]

The literature suggests that full data replication across nodes increases storage requirements and operational cost. There is a need for mechanisms that maintain confidentiality while

minimizing redundancy. The proposed system addresses this gap by incorporating threshold-based secret sharing within blockchain-supported healthcare storage.[3]

2.1 Expected System

In conventional blockchain-based healthcare systems, encrypted medical records are stored directly on-chain or linked storage systems, with each node maintaining a replica. While this improves transparency, it results in high storage consumption. If encryption keys are compromised, complete records may be exposed. Scalability also becomes challenging as medical datasets continue to grow.

2.2 Proposed System

The proposed framework enhances security by integrating Shamir Secret Sharing with blockchain. Instead of storing full records, each medical file is divided into multiple secret shares using a threshold algorithm. These shares are distributed among independent blockchain nodes.

Individual shares do not reveal meaningful information independently. Only when the predefined number of shares is combined can the original data be reconstructed. This approach prevents single-point data exposure and increases fault tolerance. Since nodes store only partial shares, storage overhead per node is reduced. The reconstruction process is mathematically reliable, ensuring accurate retrieval for authorized users.

3. Methodology & Architecture

The system architecture is designed to support secure storage and controlled sharing of EHRs without centralized control. It integrates blockchain, encryption, and decentralized storage components to ensure transparency and tamper resistance.

The architecture consists of four layers: user layer, application layer, blockchain layer, and decentralized storage layer. Patients and doctors interact through a web-based interface in the user layer. The application layer manages encryption, share generation, and request handling. The blockchain layer records transaction hashes and executes smart contracts to verify permissions. Decentralized storage components maintain encrypted data fragments created through secret sharing.

Several modules coordinate system operations. The EHR manager handles secure storage and verifies blockchain transactions. The administrator module initializes the network and deploys smart contracts. Smart contracts enforce access policies and validate patient consent before data retrieval. The data upload module encrypts records and generates secret shares before distribution. The data sharing module retrieves required shares and reconstructs the original record when authorization conditions are satisfied.

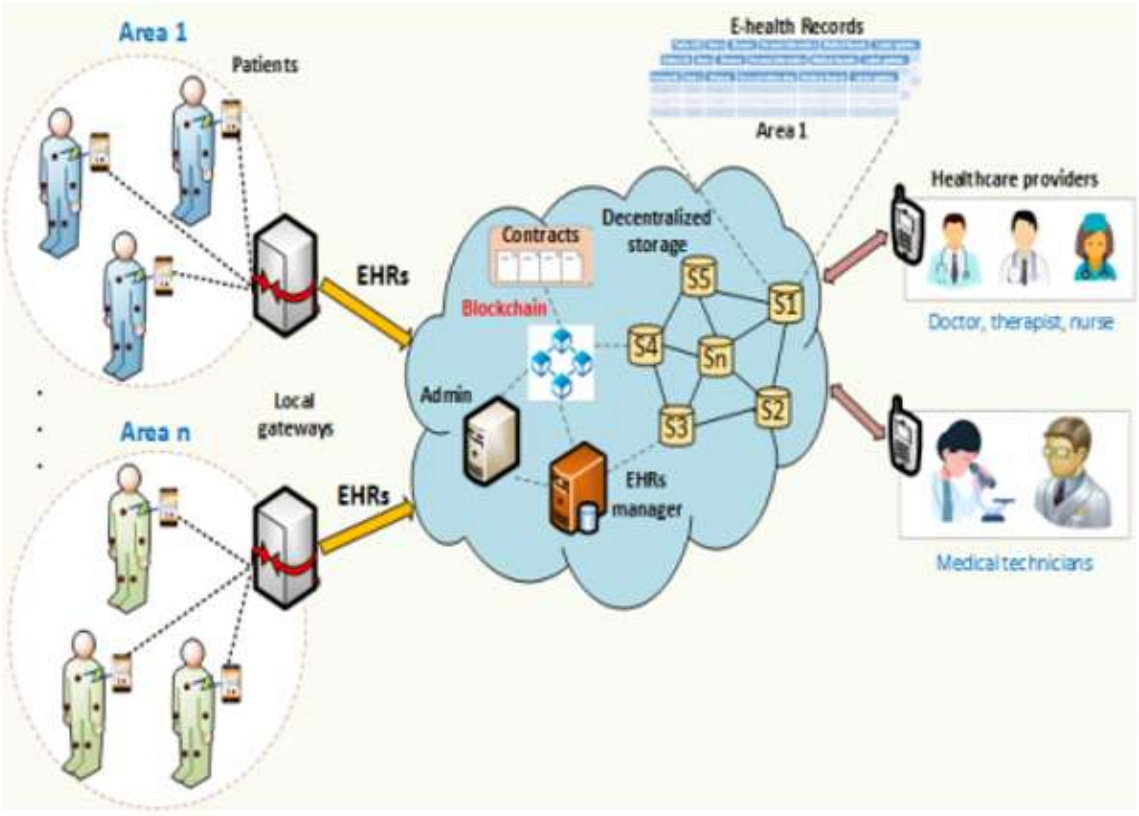

Fig.3.1: System Architecture of the Proposed Blockchain-Based Healthcare Model

3.2 Modules

The system is divided into the following functional modules:

EHR Manager: This module stores patient medical records and verifies blockchain transactions. It allows only authorized users to access the data and records every access securely.

Admin Module: The administrator deploys smart contracts, configures blockchain settings, and manages system initialization.

Smart Contract Module: Smart contracts are responsible for defining access control rules. They automatically verify patient consent before granting record access.

IPFS Module: This module stores encrypted patient data in decentralized storage and generates a unique content hash for blockchain recording.

Data Upload Module: Patients can securely upload medical records through this interface. The module performs encryption and initiates blockchain transactions.

Data Sharing Module: Authorized doctors retrieve medical records by accessing the blockchain-stored hash and fetching the corresponding encrypted file from IPFS.

4. Results and Discussion

The system was implemented and tested using multiple blockchain nodes to evaluate secure data distribution, reconstruction accuracy, and storage efficiency. Independent nodes were

successfully initialized, each maintaining its own ledger. Communication between nodes confirmed decentralized functionality.

For validation, sample data was provided as input. Instead of storing the complete value directly, the system generated secret shares and distributed them across nodes. Examination confirmed that the original input value was not visible in its full form, demonstrating effective confidentiality.

During reconstruction, the retrieval operation collected the required threshold of shares and successfully restored the original data. The reconstructed output matched the initial input, verifying correctness and reliability.

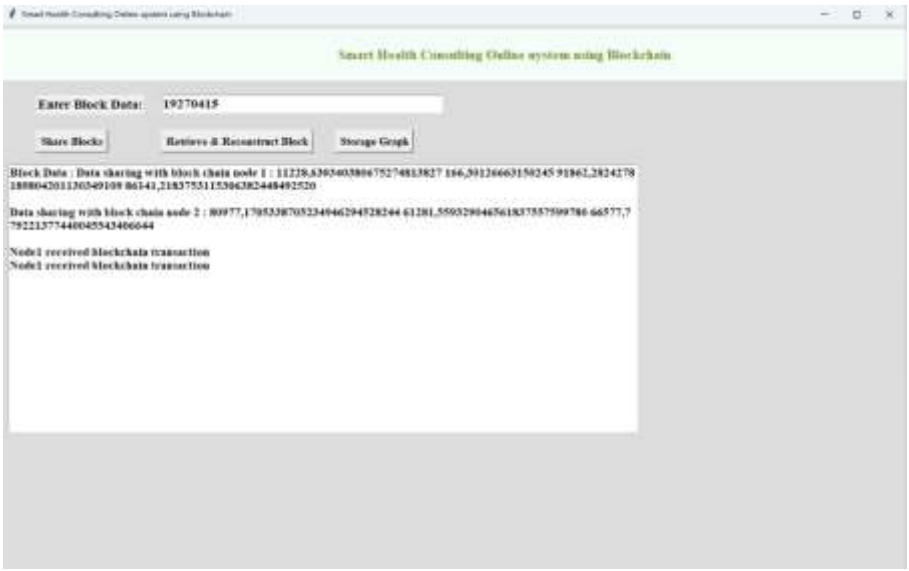

Fig. 4.1. Sharing of block data using Shamir Secret Sharing across blockchain nodes

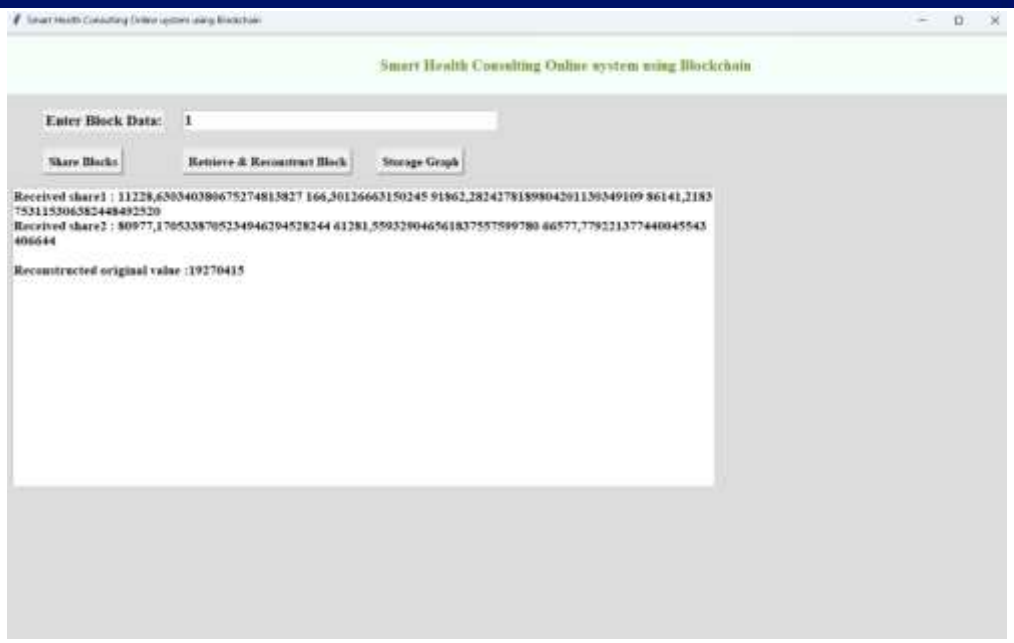

Fig. 4.2. Reconstruction of original block data using secret shares from blockchain nodes

Storage efficiency was also evaluated. Traditional blockchain storage replicates entire encrypted records across nodes, increasing storage consumption. In contrast, the proposed system stores only partial shares, significantly reducing storage overhead. This improvement supports scalability and makes the framework suitable for healthcare environments generating large volumes of medical data.

Overall, results indicate that the proposed system improves confidentiality, reliability, and storage efficiency compared to conventional blockchain storage models.

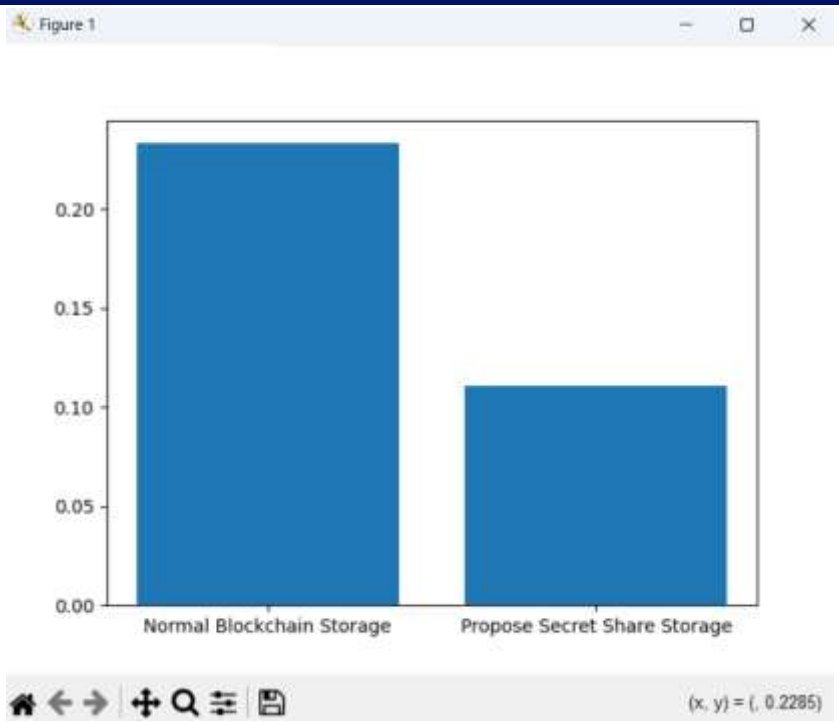

Fig. 4.3. Comparison of storage requirements between normal blockchain storage and proposed secret share storage

5. Conclusion

This study presented a decentralized online health consultation system integrating blockchain technology with Shamir Secret Sharing to enhance medical data security. By distributing secret shares across multiple nodes, the system strengthens confidentiality and eliminates single points of failure. Experimental results demonstrate accurate data reconstruction and reduced storage overhead. The framework provides a secure and practical solution for digital healthcare platforms. Future enhancements may include integration with real-time monitoring devices and refined access control mechanisms to further improve adaptability and performance.

Author's Contributions

- **V. Sudhan** – Worked on designing the system and building the main features of the

application, including the blockchain part.

- **D. Harsha Vardhan** – Focused on studying existing research, running experiments, and checking how well the system performs.

- **B. Venkata Bhargav** – Helped analyze the results and prepared the report and paper.

All Authors – Worked together on planning the system, discussing the results, and finalizing the paper.

References

[1]Shamir, A. (1979). How to share a secret. In *Communications of the ACM* (pp. 612–613).ACM. https://web.mit.edu/6.857/OldStuff/Fall03/ref/Shamir-HowToShareASecret.pdf

[2]IBM. (2023). What is blockchain technology? *IBM Documentation*. https://www.ibm.com/topics/blockchain

[3]Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE International Congress on Big Data* (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85

[4]Python Software Foundation. (2024). *Python 3 documentation*. Python.org. https://docs.python.org/3/

[5]Ahmad, M., Khan, A., & Ali, S. (2021). The role of blockchain technology in telehealth and telemedicine. *Journal of Medical Systems*, *45*(2), 1–12.

[6]Ehteshami, A., Rahman, M., & Noor, T. (2026). Application of blockchain in telemedicine: systematic review. *Healthcare Informatics Research*, *32*(1), 1–15.

[7]Ghosh, A., Sharma, P., & Das, R. (2023). Blockchain in healthcare: A comprehensive review. *Systems*, *11*(1), 38.