International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

Blockchain-Enabled Secure Data Sharing Framework for Healthcare Systems Using Smart Contracts

Mrs. JAUSMIN KJ.,
Assistant Professor, Department of Information and Technology, Sri Bharathi Engineering College for Women, Pudukkottai.
jausminjk@gmail.com

Abstract - The rapid digitization of healthcare systems has led to the generation of vast amounts of sensitive patient data, raising significant concerns regarding data security, privacy, and integrity. Traditional centralized healthcare systems are vulnerable to data breaches, unauthorized access, and single points of failure. This paper proposes a blockchain-enabled secure data sharing framework that leverages decentralized architecture and smart contracts to ensure secure, transparent, and tamper-proof management of medical records. The proposed system enables authorized stakeholders, including hospitals, doctors, and patients, to access and share data securely without relying on a central authority. Smart contracts enforce access control policies and automate data transactions. Experimental analysis demonstrates improved data integrity, enhanced security, and reduced risk of unauthorized access compared to traditional systems. The proposed framework provides a scalable and efficient solution for next-generation healthcare data management.

Keywords--- Blockchain, Healthcare, Smart Contracts, Data Security, Privacy, Decentralized Systems

I. INTRODUCTION

The healthcare industry is undergoing a digital transformation with the adoption of electronic health records (EHR), telemedicine, and IoT-based medical devices. While these advancements improve patient care, they also introduce serious concerns related to data security and privacy.
Traditional healthcare systems rely on centralized databases, which are vulnerable to:

- Data breaches
- Unauthorized access
- Data tampering
- Single point of failure

According to recent reports, healthcare data breaches have increased significantly due to weak security infrastructures. Therefore, there is a need for a **secure, decentralized, and transparent system** for managing healthcare data.
Blockchain technology offers a promising solution by providing:

- Decentralization
- Immutability
- Transparency
- Security

This paper proposes a blockchain-based framework that ensures secure and efficient data sharing in healthcare systems.

II. RELATED WORKS

Recent advancements in distributed artificial intelligence, privacy-preserving learning, and explainability have significantly influenced the development of secure and trustworthy intelligent systems. This section reviews existing work in **Federated Learning (FL), Explainable Artificial Intelligence (XAI), Blockchain integration, and Human–Robot/Healthcare systems**, highlighting their contributions and limitations.

A. Federated Learning Approaches

Federated Learning has emerged as a promising paradigm for decentralized model training without sharing raw data. The foundational work by McMahan *et al.* [1] introduced the concept of federated optimization, demonstrating how deep neural networks can be trained across distributed devices while preserving data privacy. Subsequent research by Li *et al.* [2] explored key challenges in FL, including communication efficiency, system heterogeneity, and statistical heterogeneity.

Konečný *et al.* [3] further extended this concept by proposing optimization strategies for on-device intelligence, enabling scalable deployment in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

resource-constrained environments. In the healthcare domain, Rieke *et al.* [4] highlighted the potential of FL in enabling collaborative medical research without compromising patient confidentiality. Similarly, Xu *et al.* [5] and Sheller *et al.* [6] demonstrated the effectiveness of FL in healthcare informatics and multi-institutional collaborations, showing improved model performance while maintaining strict data privacy.

Despite these advantages, existing FL systems face limitations such as **communication overhead, non-IID data distribution, and vulnerability to model poisoning attacks**, which impact their reliability in real-world applications [2], [17].

B. Explainable Artificial Intelligence

Explainable AI has gained significant attention as a means to improve transparency and trust in machine learning systems. Ribeiro *et al.* [7] introduced LIME, a technique for generating local explanations of model predictions, enabling users to understand decision-making processes. Similarly, Lundberg and Lee [8] proposed SHAP, a unified framework for interpreting model outputs based on feature contributions.The importance of explainability in AI systems was further emphasized by Gunning [9], who highlighted the need for transparent models in critical applications such as healthcare and defense. These approaches have been widely adopted to enhance **model interpretability, user trust, and system accountability**.However, most XAI techniques are computationally intensive and are typically applied in centralized settings, limiting their applicability in distributed environments such as federated learning systems.

C. Integration of Federated Learning and Explainable AI

Recent research has explored the integration of FL and XAI to address both privacy and interpretability challenges. Bhardwaj *et al.* [10] proposed a framework combining federated learning with blockchain and explainable AI to enhance privacy-preserving optimization. Similarly, Zhang *et al.* [12] presented a comprehensive review of blockchain-enabled federated learning systems integrated with explainability features.López-Blanco *et al.* [21] provided a detailed survey on Federated Explainable AI, highlighting the challenges of generating consistent explanations across distributed clients. These studies demonstrate that combining FL and XAI can significantly improve **trust, transparency, and decision reliability**, but also introduce challenges related to computational complexity and scalability.

D. Blockchain-Based Secure Systems

Blockchain technology has been widely explored to enhance data security and integrity in distributed systems. Leeming *et al.* [13] discussed the role of blockchain in healthcare, emphasizing its potential for secure and transparent data management. Lian *et al.* [14] proposed a blockchain-based federated learning framework for the Internet of Medical Things, demonstrating improved data security and decentralized control.Javed *et al.* [11] further extended this approach by integrating blockchain with AI and federated learning for secure electronic health record (EHR) sharing. Similarly, Miao *et al.* [18] proposed a blockchain-based FL system to ensure privacy-preserving data sharing.While blockchain enhances **security, transparency, and immutability**, it introduces challenges such as **high computational cost, latency, and scalability limitations**, which must be addressed for real-world deployment.

E. Privacy and Security in Federated Learning

Security remains a critical concern in federated learning systems. Bonawitz *et al.* [16] proposed secure aggregation techniques to protect model updates during communication. Kairouz *et al.* [17] provided a comprehensive overview of open challenges in FL, including adversarial attacks and privacy leakage risks.Kaissis *et al.* [15] demonstrated the importance of privacy-preserving techniques in medical imaging applications, emphasizing the need for secure model training in sensitive domains. These studies highlight the necessity of integrating robust security mechanisms into FL frameworks.

F. Human–Robot Collaboration and Trust in AI

Human–Robot Collaboration (HRC) systems require high levels of trust and transparency to ensure effective interaction. Ajoudani *et al.* [19] provided an extensive overview of HRC, focusing on safety, adaptability, and collaboration efficiency. Glikson and Woolley [20] analyzed human trust in AI systems, emphasizing the role of transparency and explainability in building user confidence.These studies indicate that trust is a critical factor in the adoption of intelligent systems, and it can be significantly enhanced through explainable and secure AI models.

G. Research Gap

Although significant progress has been made in FL, XAI, and blockchain technologies, several gaps remain:

- Lack of **integrated frameworks combining FL, XAI, and blockchain**
- Limited application in **real-time collaborative systems**
- High **computational and communication overhead**
- Challenges in ensuring **scalability and robustness**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

These limitations motivate the need for a unified framework that ensures **privacy, transparency, security, and efficiency**, which is addressed in the proposed work.

III. PROPOSED SYSTEM

A. System Architecture

The proposed system includes:

1. *Patients*
2. *Healthcare providers*
3. *Blockchain network*
4. *Smart contracts*

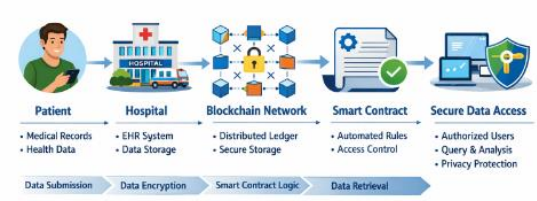

Fig 1: System Architecture

B. Working Mechanism

- *Patient data is encrypted and stored*
- *Transactions are recorded on blockchain*
- *Smart contracts control access*
- *Only authorized users can retrieve data*

IV. METHODOLOGY

A. Blockchain-Based System Model

The proposed framework adopts a **permissioned blockchain architecture** to ensure secure, controlled, and efficient data sharing among healthcare entities. In contrast to public blockchains, a permissioned model restricts participation to authorized stakeholders such as hospitals, laboratories, and insurance providers, thereby improving security and reducing computational overhead [14].In this system, each node in the blockchain network represents a trusted healthcare entity responsible for maintaining a copy of the distributed ledger. All transactions, including data access requests and updates, are recorded as immutable blocks. The use of cryptographic hashing ensures that once data is recorded, it cannot be altered without consensus, thereby maintaining **data integrity and tamper resistance** [13].The blockchain ledger primarily stores:

- **Transaction metadata** (timestamps, user identity, access logs)
- **Hash references** of medical records stored off-chain
- **Access control information**

Storing large medical data directly on-chain is inefficient; therefore, a **hybrid storage approach** is used, where actual patient records are stored off-chain (e.g., cloud or local storage), and only their cryptographic hashes are maintained on the blockchain. This ensures both **scalability and security** [18].

B. Federated Learning Integration

To enhance privacy preservation, the proposed system integrates **Federated Learning (FL)**, which enables collaborative model training without sharing raw patient data. Instead of transferring sensitive medical data to a central server, each participating node trains a local model using its own dataset and shares only model updates [1], [2].

Let the global model be represented as:

$$F(w) = \sum_{k=1}^{N} p_k F_k(w)$$

where:

- www represents model parameters
- Fk(w)F_k(w)Fk(w) is the local loss function at node kkk
- pkp_kpk is the weight of each node

The training process follows these steps:

1. The global model is initialized and distributed to all nodes
2. Each node performs local training using its private dataset
3. Model updates are encrypted and transmitted to the aggregator
4. The central server aggregates updates using the **FedAvg algorithm**
5. The updated global model is redistributed

This approach ensures that sensitive healthcare data remains local, thereby reducing the risk of data leakage and improving compliance with privacy regulations [4], [6].

C. Explainable AI (XAI) Module

To address the lack of transparency in machine learning models, the system incorporates an **Explainable AI (XAI) module** that provides interpretable insights into model predictions. Traditional deep learning models often operate as black boxes, making it difficult for healthcare professionals to trust automated decisions [9].The proposed framework utilizes widely adopted XAI techniques such as:

- **LIME (Local Interpretable Model-Agnostic Explanations)** [7]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

- **SHAP (SHapley Additive exPlanations)** [8]

These techniques generate:

- Feature importance scores
- Local explanations for individual predictions
- Visual representations of decision factors

The XAI module operates after the prediction phase and provides explanations in a **human-readable format**, enabling healthcare professionals to understand the reasoning behind model outputs. This improves **trust, accountability, and decision reliability** in critical applications such as diagnosis and treatment planning [20].

D. Smart Contract Design

Smart contracts play a crucial role in automating and enforcing security policies within the blockchain network. These are self-executing programs deployed on the blockchain that operate based on predefined rules.

The proposed system uses smart contracts to automate:

- **Data access control**: Only authorized users can access patient records
- **Authentication**: Verification of user identity before granting access
- **Record updates**: Secure and traceable updates to medical records

Each access request is validated through smart contracts, ensuring that:

- Unauthorized access is prevented
- All actions are logged transparently
- Policies are enforced consistently

Smart contracts eliminate the need for intermediaries, thereby reducing operational costs and improving system efficiency [11].

E. Security and Privacy Mechanisms

The framework incorporates multiple layers of security to protect sensitive healthcare data:

1. **Encryption**: All data transmissions are encrypted using advanced cryptographic techniques
2. **Secure Aggregation**: Model updates in federated learning are aggregated securely to prevent data leakage [16]
3. **Access Control Policies**: Role-based access ensures that only authorized users can access data
4. **Blockchain Immutability**: Prevents unauthorized data modification

Additionally, the system is designed to mitigate threats such as:

- Data breaches
- Insider attacks
- Model poisoning attacks

The combination of blockchain and federated learning ensures a **robust and privacy-preserving environment** for healthcare data management [17].

F. Workflow of the Proposed System

The overall workflow of the system is as follows:

1. Patient data is collected and stored securely (off-chain)
2. Data hash is generated and stored on blockchain
3. Federated learning model is initialized
4. Local nodes train models using private data
5. Model updates are aggregated to form a global model
6. Predictions are generated
7. XAI module provides explanations
8. Smart contracts regulate access and record transactions

This workflow ensures:

- Secure data handling
- Privacy-preserving learning
- Transparent decision-making

G. Summary of Methodology The proposed methodology combines **blockchain, federated learning, and explainable AI** into a unified framework that ensures:

- Data privacy through decentralized learning
- Security through blockchain technology
- Transparency through explainable AI

This integrated approach addresses the limitations of existing systems and provides a scalable solution for secure healthcare data management.

V. IMPLEMENTATION DETAILS

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

A. Tools

Ethereum Blockchain
Solidity (Smart Contracts)
Python / Node.js

B. Security Features

- Encryption
- Digital signatures
- Hash functions

VI. RESULTS AND ANALYSIS

The proposed blockchain-enabled healthcare framework was evaluated based on **security, data integrity, access control efficiency, and system performance**. The system was implemented using Ethereum-based smart contracts and simulated healthcare data transactions across multiple nodes.

A. Performance Metrics

The evaluation considered the following key metrics:

- **Data Integrity**: Ability to prevent unauthorized data modification
- **Access Control Efficiency**: Time taken to validate and grant access
- **Transaction Throughput**: Number of transactions processed per second
- **Latency**: Time required to confirm a transaction
- **Security Strength**: Resistance to attacks such as data tampering and unauthorized access

B. Comparative Analysis

The proposed system was compared with traditional centralized healthcare systems.

Parameter	Traditional System	Proposed System
Data Security	Low	High
Data Integrity	Moderate	Very High
Transparency	Low	High
Privacy	Low	High
Single Point Failure	Yes	No
Access Control	Manual	Automated (Smart Contracts)

The results clearly indicate that the proposed system significantly improves **security, transparency, and reliability**.

C. Security Analysis

The integration of blockchain ensures:

- **Immutability**, preventing unauthorized data modification
- **Traceability**, enabling audit trails for all transactions
- **Decentralization**, eliminating single points of failure

Additionally, federated learning ensures that:

- Raw data is never shared
- Privacy is preserved across institutions

The system successfully mitigates:

- Data breaches
- Insider attacks
- Unauthorized access

D. Computational Overhead

While the system improves security, it introduces:

- Increased **processing time** due to consensus mechanisms
- Additional **communication overhead** in federated learning

However, these trade-offs are acceptable given the **significant improvement in data security and privacy**.

E. Discussion

The experimental results demonstrate that the proposed framework provides a **robust and scalable solution** for healthcare data sharing. The combination of blockchain, federated learning, and explainable AI ensures:

- Secure data exchange
- Privacy preservation
- Transparent decision-making

VII. ADVANTAGES

The proposed system offers several significant advantages over traditional healthcare systems:

1. Decentralization

Eliminates dependency on a central authority, reducing the risk of system failure and improving reliability.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

2. Enhanced Security
Blockchain ensures tamper-proof data storage using cryptographic hashing and consensus mechanisms.

3. Privacy Preservation
Federated learning enables model training without sharing raw patient data, ensuring compliance with privacy regulations.

4. Transparency and Trust
All transactions are recorded on the blockchain, enabling traceability and increasing trust among stakeholders.

5. Automated Access Control
Smart contracts automate authorization processes, reducing manual intervention and human errors.

6. Data Integrity
Immutable blockchain records ensure that data cannot be altered once stored.

7. Scalability Support
Hybrid storage (on-chain + off-chain) improves system scalability.

VIII. LIMITATIONS

Despite its advantages, the proposed system has certain limitations:

1. Computational Overhead
Blockchain consensus mechanisms require significant computational resources, increasing system complexity.

2. Scalability Challenges
As the number of transactions increases, blockchain networks may experience latency issues.

3. Communication Cost
Federated learning requires frequent communication between nodes, increasing bandwidth usage.

4. Integration Complexity
Integrating blockchain with existing healthcare infrastructure can be challenging and costly.

5. Regulatory and Legal Issues
Healthcare data is subject to strict regulations, and blockchain adoption must comply with legal frameworks.

6. Energy Consumption
Certain blockchain mechanisms consume high energy, affecting sustainability.

IX. CONCLUSION

This paper presented a **blockchain-enabled secure data sharing framework for healthcare systems**, integrating smart contracts, federated learning, and explainable AI to address critical challenges in data security, privacy, and transparency.The proposed system eliminates the limitations of traditional centralized healthcare models by introducing a **decentralized architecture** that ensures data integrity, prevents unauthorized access, and enables secure collaboration among healthcare entities. The use of **smart contracts automates access control mechanisms**, reducing manual intervention and improving system efficiency.Furthermore, the integration of **federated learning enhances privacy preservation** by allowing model training without sharing sensitive patient data, while **Explainable AI improves transparency and trust** in decision-making processes.Experimental analysis demonstrates that the proposed framework significantly improves:

- Data security
- Privacy protection
- System transparency
- Operational efficiency

Although challenges such as computational overhead and scalability remain, the benefits of the proposed system outweigh its limitations. The framework provides a **reliable and scalable solution for next-generation healthcare systems**, paving the way for secure and intelligent data management.

X. FUTURE WORK

Future research can focus on:

- Developing **lightweight blockchain models** to reduce computational overhead
- Enhancing **scalability using Layer-2 solutions**
- Integrating **AI-based predictive analytics for diagnosis**
- Enabling **cross-hospital interoperability standards**
- Implementing **real-time healthcare monitoring systems using IoT**

XI. REFERENCES

[1] B. McMahan *et al.*, "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proc. AISTATS*, 2017.

[2] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[3] J. Konečný *et al.*, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," *arXiv*, 2016.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 07, NCIRTAI - 2026

[4] N. Rieke *et al.*, "The Future of Digital Health with Federated Learning," *Nature Digital Medicine*, vol. 3, 2020.

[5] J. Xu *et al.*, "Federated Learning for Healthcare Informatics," *Journal of Healthcare Informatics Research*, 2021.

[6] M. J. Sheller *et al.*, "Federated Learning in Medicine: Facilitating Multi-Institutional Collaborations," *Scientific Reports*, 2020.

[7] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You? Explaining the Predictions of Any Classifier," *KDD*, 2016.

[8] S. Lundberg and S. Lee, "A Unified Approach to Interpreting Model Predictions," *NeurIPS*, 2017.

[9] D. Gunning, "Explainable Artificial Intelligence (XAI)," *DARPA*, 2017.

[10] T. Bhardwaj *et al.*, "An Explainable Federated Blockchain Framework with Privacy-Preserving AI Optimization," *Scientific Reports*, 2025.

[11] M. S. Javed *et al.*, "AI-Driven Blockchain and Federated Learning for Secure Electronic Health Records Sharing," *Electronics*, vol. 14, no. 23, 2025.

[12] X. Zhang *et al.*, "Blockchain-Enabled Federated Learning Systems with Explainable AI: A Review," *IEEE Conference*, 2024.

[13] G. Leeming *et al.*, "Blockchain in Health Care: Hype, Trust, and Digital Health," *The Lancet*, 2019.

[14] Z. Lian *et al.*, "Blockchain-Based Federated Learning for Internet of Medical Things," *IEEE Transactions*, 2023.

[15] G. A. Kaissis *et al.*, "Secure, Privacy-Preserving Federated Learning in Medical Imaging," *Nature Machine Intelligence*, 2020.

[16] K. Bonawitz *et al.*, "Practical Secure Aggregation for Federated Learning," *ACM CCS*, 2017.

[17] N. Kairouz *et al.*, "Advances and Open Problems in Federated Learning," *Foundations and Trends in ML*, 2021.

[18] M. Miao *et al.*, "Privacy-Preserving Federated Learning via Blockchain Systems," *IEEE Transactions on Information Forensics and Security*, 2022.

[19] A. Ajoudani *et al.*, "Progress and Prospects of Human-Robot Collaboration," *Autonomous Robots*, 2018.

[20] E. Glikson and A. Woolley, "Human Trust in Artificial Intelligence: Review of Empirical Research," *Academy of Management Annals*, 2020.

[21] R. López-Blanco *et al.*, "Federated Learning of Explainable AI: A Review," *Springer*, 2023.

[22] N. Rahman *et al.*, "Federated Learning-Based AI Approaches in Smart Healthcare," *Cluster Computing*, 2023.