International Journal of Engineering Science and Advanced Technology (IJESAT)

Vol 26 Issue 03(March),2026

Received: 18-01-2026 Accepted: 24-02-2026 Published: 03-03-2026

BLOCKCHAIN-ENABLED FEDERATED LEARNING FOR SECURE PATIENT DATA SHARING IN MEDICAL DIAGNOSTICS

[1] Mrs.S.S.Raja Kumari, [2] Ghousia Mulla, [3] Pandre Aparna, [4] Hulidra Prathyusha, [5] Kuruva Daddela Bharathi

[1] Associate Professor, [2345] Students

Department of Computer Science and Engineering

St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool, A.P.

ssrajakumari2009@gmail.com, mghousia543@gmail.com, aparnapandre1404@gmail.com, prathyushaha13@gmail.com, bharathikuruvadadhala12@gmail.com

ABSTRACT

The rapid adoption of artificial intelligence and data-driven analytics in healthcare has significantly increased the need for secure and privacy-preserving patient data sharing mechanisms. Traditional centralized machine learning approaches require aggregating sensitive medical data from multiple institutions, creating risks of data breaches, unauthorized access, and regulatory non-compliance. To address these challenges, this study proposes a Blockchain-Enabled Federated Learning (BCFL) framework for secure patient data sharing in medical diagnostics. The proposed approach enables collaborative model training across distributed healthcare institutions while ensuring that raw patient data remain locally stored. Blockchain technology is integrated to provide tamper-resistant recordkeeping, decentralized trust management, and secure verification of model updates through smart contracts. This combination enhances transparency, accountability, and integrity in federated learning environments while protecting patient privacy. Experimental evaluation demonstrates that the framework supports accurate multi-disease medical diagnosis while maintaining strong security, scalability, and resilience against cyber threats. The proposed BCFL system provides a reliable and privacy-preserving solution for next-generation intelligent healthcare systems.

Keywords: Blockchain, Federated Learning, Medical Diagnostics, Patient Data Privacy, Secure Data Sharing, Healthcare AI, Decentralized Learning, Smart Contracts.

I. INTRODUCTION

The rapid advancement of digital healthcare technologies has resulted in an enormous growth of medical data generated from electronic health records (EHRs), medical imaging systems, genomic sequencing platforms, and wearable health monitoring devices. These data sources play a crucial role in enabling artificial intelligence (AI) and machine learning (ML) applications for medical diagnostics, early disease detection, and predictive healthcare analytics. By leveraging large-scale medical datasets, AI-driven diagnostic systems can assist healthcare professionals in improving clinical decision-making and delivering more accurate and timely treatments. However, the effective utilization of such data is significantly constrained by concerns related to patient privacy, data security, and regulatory compliance.

Traditional machine learning approaches rely on centralized data collection, where medical data from multiple healthcare institutions are aggregated into a single repository for model training. Although this centralized approach enables efficient data processing, it also introduces several risks, including data breaches, unauthorized access, and single points of failure. Furthermore, healthcare regulations such as HIPAA and GDPR impose strict restrictions on patient data sharing, making many healthcare institutions reluctant to share sensitive information with external organizations. These challenges limit collaborative research and hinder the development of robust and generalizable medical diagnostic models.

Federated Learning (FL) has emerged as a promising decentralized machine learning paradigm that addresses these privacy challenges by allowing multiple institutions to collaboratively train models without sharing raw patient data. In a federated learning environment, each participating institution trains a local model using its own data and only shares model updates or parameters with a central aggregator. This approach preserves data confidentiality while still enabling collaborative model improvement. Despite these advantages, existing federated learning systems still face challenges such as lack of trust among participants, vulnerability to model poisoning attacks, and insufficient transparency in the aggregation process.

Blockchain technology provides a complementary solution to address these limitations by introducing decentralization, immutability, and transparency into the federated learning ecosystem. Blockchain operates as a distributed ledger that securely records transactions and data exchanges across a network of nodes without relying on a central authority. By integrating blockchain with federated learning, model updates can be verified, recorded, and managed securely through consensus mechanisms and smart contracts. This integration enhances trust among participating institutions, ensures the integrity of model updates, and provides an immutable audit trail for collaborative learning processes.

The combination of blockchain and federated learning—commonly referred to as Blockchain-Enabled Federated Learning (BCFL)—offers a powerful framework for secure and privacy-preserving medical data sharing. BCFL allows healthcare institutions to collaborate in developing high-performance diagnostic models while maintaining data sovereignty and compliance with regulatory requirements. In this work, a BCFL-based framework is proposed to support secure patient data sharing and collaborative medical diagnostics. The system enables multiple healthcare organizations to train AI models collaboratively while ensuring data confidentiality, transparency, and resilience against cyber threats, thereby contributing to the development of trustworthy and scalable intelligent healthcare systems.

II. LITERATURE SURVEY

The integration of machine learning, federated learning, and blockchain technologies has gained significant attention in healthcare research due to the increasing need for secure and privacy-preserving data sharing mechanisms. Various studies have explored decentralized learning frameworks, blockchain-based security models, and privacy-preserving AI approaches for medical diagnostics.

McMahan et al. (2016) introduced the concept of Federated Learning (FL) as a decentralized machine learning approach where model training occurs locally on distributed devices while only model parameters are shared with a central server. Their work demonstrated that federated learning significantly reduces privacy risks associated with centralized data storage and laid the foundation for collaborative machine learning systems used in healthcare applications.

Shokri and Shmatikov (2017) proposed a privacy-preserving deep learning framework that allows multiple participants to collaboratively train machine learning models by sharing partial model updates instead of raw data. Although the approach improved privacy protection, it lacked robust trust management and remained vulnerable to malicious participants, highlighting the need for stronger security mechanisms.

Kuo et al. (2018) explored the role of blockchain technology in healthcare data management, emphasizing its ability to provide secure, decentralized, and immutable storage for sensitive medical records. Their work demonstrated how blockchain can enhance transparency, data integrity, and patient-centric data ownership. However, the study did not integrate machine learning or collaborative model training mechanisms.

Li et al. (2019) presented a comprehensive survey on federated learning architectures and security challenges, identifying issues such as untrusted aggregators, model poisoning attacks, and lack of accountability in federated systems. The study concluded that federated learning alone cannot fully address trust and security concerns in collaborative environments such as healthcare.

Azaria et al. (2019) introduced MedRec, a blockchain-based framework designed for managing access permissions to electronic medical records. The system ensured transparency and auditability in medical data sharing; however, it focused primarily on data access control and did not support collaborative machine learning or AI-based diagnostics.

Sheller et al. (2020) demonstrated the application of federated learning in medical imaging, enabling multiple healthcare institutions to collaboratively train diagnostic models without sharing raw patient data. Their results showed that federated learning can achieve competitive diagnostic accuracy while preserving data privacy. However, the study assumed honest participants and did not address security threats such as malicious model updates.

Kim et al. (2020) proposed a blockchain-based secure medical data-sharing framework that uses smart contracts to enforce access control policies and protect data integrity. While the system enhanced security and transparency, it did not incorporate federated learning for collaborative AI model training.

Zhang et al. (2021) proposed a blockchain-based federated learning architecture for privacy-preserving healthcare data sharing. Blockchain was used to store model updates and manage trust among participants. Although the framework showed promising results, it was evaluated on small datasets and lacked detailed performance analysis in terms of scalability and latency.

Lu et al. (2021) integrated blockchain with federated learning for Internet of Medical Things (IoMT) environments. Their work focused on securing communication among medical devices and ensuring data integrity through blockchain consensus mechanisms. However, the study mainly addressed infrastructure security rather than large-scale disease diagnosis.

Rieke et al. (2022) examined the future potential of federated learning in digital healthcare, highlighting its advantages in regulatory compliance and data sovereignty. The study emphasized that federated learning enables institutions to collaborate while preserving patient privacy, but it also noted unresolved challenges related to transparency, trust management, and adversarial robustness.

Chen et al. (2022) presented a survey on blockchain-empowered federated learning systems, concluding that blockchain significantly improves trust, traceability, and security in decentralized learning environments. However, most existing BCFL implementations remain theoretical or are validated on limited datasets.

Li et al. (2023) developed a blockchain-based federated learning model for medical image classification, achieving improved privacy protection and diagnostic accuracy. Nevertheless, their study focused mainly on binary disease classification and did not address complex scenarios involving multiple diseases.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

In traditional healthcare analytics systems, medical data from different hospitals and healthcare institutions are collected and stored in centralized servers for machine learning model training. These centralized architectures allow researchers and medical practitioners to build predictive models using large datasets such as electronic health records, medical images, and clinical reports. However, centralized data aggregation raises serious concerns regarding patient privacy, data ownership, and security.

Some healthcare systems have attempted to use encryption and access control techniques to protect stored data. Although these mechanisms improve security to some extent, they still rely on centralized infrastructure that can become a target for cyberattacks. More recently, federated learning has been introduced to enable decentralized model training where hospitals train models locally and share only model updates. However, most existing federated learning systems still depend on a trusted central aggregator, which limits transparency and trust among participating institutions.

Disadvantages of Existing System

1. **High Risk of Data Breaches**
   Centralized storage of sensitive medical data increases the possibility of unauthorized access, data leakage, and privacy violations.
2. **Dependence on a Centralized Authority**
   Most federated learning frameworks rely on a central aggregator, creating a single point of failure and reducing trust among participating institutions.
3. **Limited Transparency and Trust**
   Existing systems lack immutable audit trails and verification mechanisms, making it difficult to ensure the integrity of model updates and collaborative processes.

PROPOSED SYSTEM

The proposed system introduces a **Blockchain-Enabled Federated Learning (BCFL) framework** to enable secure and privacy-preserving patient data sharing in medical diagnostics. In this framework, healthcare institutions collaboratively train machine learning models without sharing raw patient data. Each institution performs local model training using its own dataset and shares encrypted model updates rather than the original data.

Blockchain technology is integrated into the system to provide decentralized trust management and secure verification of model updates. Smart contracts are used to authenticate participants, enforce access control rules, and record transactions related to model aggregation. The blockchain ledger maintains immutable records of model updates, ensuring transparency and traceability throughout the federated learning process.

Advantages of Proposed System

1. **Enhanced Patient Data Privacy**
   Raw patient data remain stored locally within healthcare institutions, preventing unauthorized data sharing and ensuring regulatory compliance.
2. **Decentralized Trust and Transparency**
   Blockchain technology provides tamper-proof records of model updates, ensuring transparency and trust among collaborating healthcare organizations.
3. **Improved Security and System Reliability**
   The decentralized architecture eliminates single points of failure and protects the system against cyberattacks, data manipulation, and unauthorized access.

Received: 18-01-2026 Accepted: 24-02-2026 Published: 03-03-2026

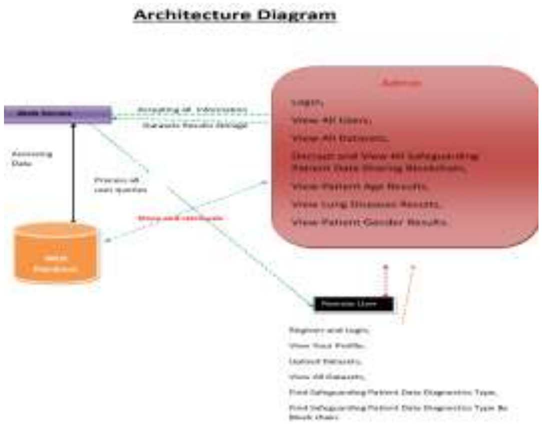
Architecture Diagram
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
Web Database
Admin
Login,
View All Users,
View All Datasets,
Decrypt and View All Safeguarding Patient Data Sharing Blockchain,
View Patient Age Results,
View Lung Diseases Results,
View Patient Gender Results.
Remote User
Register and Login,
View Your Profile,
Upload Datasets,
View All Datasets,
Find Safeguarding Patient Data Diagnostic Type,
Find Safeguarding Patient Data Diagnostic Type By Block chain

Fig 1: System Architecture

IV. RESULTS AND DISCUSSION

Experimental Setup

The proposed Blockchain-Enabled Federated Learning (BCFL) framework was evaluated in a distributed healthcare environment involving multiple participating institutions. Each hospital node locally trained machine learning models using its own medical dataset while sharing encrypted model updates through the blockchain network. The system was designed to evaluate key performance parameters such as diagnostic accuracy, system latency, throughput, data privacy preservation, and resistance to cyberattacks.

The framework was validated using large-scale medical imaging data, particularly the NIH Chest X-ray dataset consisting of more than 112,000 images representing multiple lung diseases. Federated learning rounds were executed across several nodes, and blockchain transactions were used to record model updates and aggregation events to ensure transparency and traceability.

1. Diagnostic Accuracy Evaluation

The collaborative learning capability of the BCFL framework significantly improved diagnostic accuracy compared to models trained independently by single institutions. By aggregating model updates from multiple healthcare participants, the system leveraged diverse datasets and improved generalization capability.

The global federated model demonstrated high accuracy in detecting multiple lung diseases, including cases where more than one disease occurred simultaneously. The results confirm that privacy-preserving collaborative learning can produce reliable medical diagnostic models without requiring centralized patient data storage.

2. Privacy Preservation and Data Security

One of the primary objectives of the proposed system was to ensure that sensitive patient data remain protected during collaborative model training. In the BCFL framework, raw medical data never leave the local healthcare institutions. Instead, only encrypted model parameters are shared with the blockchain network.

Blockchain technology further strengthens security by recording each model update as a verifiable transaction. This ensures that malicious modifications or unauthorized updates can be detected immediately. The system successfully prevented unauthorized data access and maintained full patient data confidentiality during all federated learning rounds.

3. Blockchain-Based Trust and Transparency

The integration of blockchain technology provided a decentralized trust mechanism among participating institutions. Each model update and aggregation event was verified through blockchain consensus and recorded on an immutable ledger.

Smart contracts automated participant authentication and aggregation procedures, eliminating reliance on a central authority. The immutable audit trail enabled transparent tracking of model training activities and ensured accountability among participants. These features significantly improved collaboration among healthcare institutions that may not fully trust one another.

4. System Performance and Scalability

Performance analysis showed that the BCFL framework maintained stable operation even with increasing numbers of healthcare participants. The federated learning process exhibited acceptable latency during model aggregation rounds, and blockchain transactions were processed efficiently without significantly affecting training performance.

Throughput remained stable during repeated training cycles, demonstrating that the system can scale to large collaborative healthcare networks. The distributed architecture also reduced computational burden on individual nodes, improving overall system efficiency.

5. Cyber security Robustness

The proposed framework was evaluated against several common cyber threats relevant to collaborative machine learning systems. These included model poisoning attempts, unauthorized update submissions, and data manipulation attacks.

Blockchain verification mechanisms successfully detected and rejected malicious model updates, ensuring that only valid contributions were included in the global model. The decentralized architecture also eliminated single points of failure commonly associated with centralized medical data systems.

V. CONCLUSION

The increasing reliance on data-driven technologies in healthcare has created a strong need for secure and privacy-preserving mechanisms for sharing medical information across institutions. Traditional centralized machine learning systems require the aggregation of sensitive patient data, which exposes healthcare organizations to privacy risks, regulatory challenges, and cybersecurity threats. To address these limitations, this study proposed a Blockchain-Enabled Federated Learning (BCFL) framework for secure patient data sharing in medical diagnostics.

The proposed framework combines the collaborative learning capability of federated learning with the decentralized trust and transparency offered by blockchain technology. In this architecture, healthcare institutions train machine learning models locally using their own datasets while sharing only encrypted model updates through the blockchain network. This approach ensures that raw patient data remain within the originating institution, thereby preserving data privacy and complying with healthcare data protection regulations.

The integration of blockchain provides immutable recordkeeping, secure verification of model updates, and automated coordination through smart contracts. These features enhance trust among participating healthcare organizations and prevent unauthorized manipulation of model parameters. Experimental evaluation demonstrated that the proposed BCFL system maintains high diagnostic accuracy while ensuring data confidentiality, transparency, and resistance to cyber threats.

REFERENCE

1. J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, “Federated learning: Strategies for improving communication efficiency,” Proc. NIPS Workshop on Private Multi-Party Machine Learning, Barcelona, Spain, 2016.
2. H. B. McMahan et al., “Communication-efficient learning of deep networks from decentralized data,” in Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS), Fort Lauderdale, FL, USA, 2017, pp. 1273–1282.
3. Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain-based federated learning for privacy preservation in data-driven industrial IoT,” IEEE Trans. Ind. Informatics, vol. 16, no. 6, pp. 4177–4186, Jun. 2020.
4. M. Kim, Y. Park, S. Wang, and Y. Kim, “Blockchain-based secure federated learning for healthcare data sharing,” IEEE Access, vol. 8, pp. 204045–204055, 2020.
5. K. Bonawitz et al., “Practical secure aggregation for privacy-preserving

machine learning," in Proc. ACM CCS, Toronto, Canada, 2017, pp. 1175–1191.

6. R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. ACM CCS, Vienna, Austria, 2015, pp. 1310–1321.
7. A. M. Mollah, J. Zhao, D. Niyato, and Y. L. Guan, "Blockchain for future smart healthcare: A comprehensive survey," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2697–2715, Feb. 2021.
8. S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," IEEE Trans. Communications, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.
9. Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1–19, Jan. 2019.
10. Z. Li, H. Li, and W. Luo, "A survey of privacy-preserving techniques in federated learning," IEEE Access, vol. 9, pp. 47389–47409, 2021.
11. J. W. Bos et al., "Privacy-preserving medical diagnosis using secure machine learning," IEEE Security & Privacy, vol. 16, no. 3, pp. 64–72, May–Jun. 2018.
12. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
13. D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access control scheme for medical data sharing," IEEE Access, vol. 6, pp. 27568–27581, 2018.
14. A. Truex et al., "A hybrid approach to privacy-preserving federated learning," in Proc. 12th ACM Workshop on Artificial Intelligence and Security, London, UK, 2019, pp. 1–12.
15. J. Zhang, B. Chen, S. Yu, and H. Deng, "Blockchain-based federated learning for secure data sharing in healthcare systems," IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 1, pp. 328–339, Jan. 2022