AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

Safeguarding Clinical Data Privacy through Block chain-Integrated For Multi-Disease Detection

Mr P Venkat[1]|Ammisetty Lavanya[2]|Shaik Masuda[3]|Derangula Uligi Nadha Uday Kumar[4]|Oburi Venu Madhav Kumar.

[1,2,3,4,5]Department of CSE-AIML, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India

Abstract: Medical healthcare systems are increasingly leveraging artificial intelligence to manage large-scale clinical data and improve disease diagnosis; however, traditional machine learning methods often compromise patient privacy due to centralized data sharing. This study proposes a secure and privacy-preserving framework that integrates Blockchain with Federated Learning, enabling multiple hospitals to collaboratively train models without sharing raw patient data. Each hospital trains a local RESNET-based model on its dataset and shares only encrypted model parameters, which are securely stored and aggregated via Blockchain to prevent tampering. The framework is validated on 15 lung diseases using the NIH Chest X-ray dataset, achieving an high accuracy, latency of 43.51 ms, and throughput of 10,034,017 bytes/s, demonstrating efficiency and scalability. The system also resists major cyber threats, including Double Spending, Transaction Malleability, and Endpoint Compromise attacks, highlighting its robustness. Overall, this work provides a practical and secure implementation of Blockchain-enabled Federated Learning for medical diagnostics while safeguarding patient data privacy.

Key Words: Safeguarding, Block chain, Federated Learning, RESNET, Patient Privacy, Medical Diagnostics, Secure AI, Healthcare Data Management, Cybersecurity

1. INTRODUCTION

The rapid growth of digital healthcare systems has generated vast amounts of medical data that can be effectively utilized for disease diagnosis using artificial intelligence techniques. Machine learning models, particularly deep learning approaches, have demonstrated strong performance in detecting complex diseases from medical images. However, traditional centralized learning methods require sharing sensitive patient data across institutions, which raises serious concerns regarding data privacy, security, and regulatory compliance. Federated Learning has emerged as a decentralized paradigm that enables multiple healthcare institutions to collaboratively train models without exposing raw data.

Despite its advantages, federated systems often rely on centralized aggregation servers, which remain vulnerable to attacks, tampering, and unauthorized modifications. To address these limitations, Block chain technology provides a secure and decentralized infrastructure for storing and validating model updates. By combining Blockchain with Federated Learning, it becomes possible to ensure transparency, immutability, and trust in collaborative medical model training. In this context, deep learning architectures such as Residual Networks enhance the accuracy of disease detection tasks. The integration of these technologies enables secure, efficient, and scalable healthcare solutions. This approach supports multi-institution collaboration while preserving patient confidentiality. The proposed framework focuses on improving diagnostic performance and strengthening data protection mechanisms. The system is evaluated using large-scale medical imaging datasets to ensure reliability and robustness in real-world healthcare environments. The system integrates Federated Learning with Blockchain technology to enable secure and collaborative disease diagnosis across multiple healthcare institutions. Each participating node trains a local deep learning model using a Residual Network architecture on its respective dataset. The trained model weights are encrypted using homomorphic encryption and submitted to a Blockchain network, where they are securely stored and verified using hash-based mechanisms. A consensus process ensures the integrity of transactions, and the global model is generated by aggregating local weights using averaging techniques. The Block chain provides immutability and traceability, preventing tampering and unauthorized changes. The global model is then distributed to participating nodes for accurate disease prediction. The system also incorporates security mechanisms to defend against attacks such as double spending, transaction manipulation, and endpoint compromise, ensuring a robust and trustworthy healthcare solution.

2. LITERATURE SURVEY

1. A. Rehman et al. (2022) The authors proposed a Healthcare 5.0 system that integrates Blockchain with Federated Learning to ensure secure medical data sharing. Their system enables hospitals to collaboratively train models without exposing sensitive patient information. Blockchain is used to provide transparency, immutability, and trust among participants. The study highlights improved data security and privacy preservation in distributed

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

healthcare environments. The framework also supports efficient data management across multiple institutions. This work establishes a strong foundation for secure AI-based healthcare systems. **2. A. P. Kalapaaking et al. (2024)** This research introduces a Blockchain-based Federated Learning system with Secure Multi-Party Computation (SMPC) for model verification. The proposed approach protects against poisoning attacks during collaborative model training. Blockchain ensures integrity and traceability of model updates. The system verifies the correctness of local models before aggregation. This improves trust among participating entities in healthcare systems. The study focuses on enhancing robustness against malicious contributions.

3. SYSTEM ARCHITECTURE

System Architecture represents the overall design and structure of the proposed system, showing how different components interact with each other to achieve secure federated learning. In this project, the architecture includes hospitals performing local model training, an encryption module for securing model weights, IPFS for decentralized storage, and a block chain network for maintaining tamper-proof records using smart contracts. The federated learning mechanism aggregates model weights to generate a global model, which is then shared back with hospitals for disease prediction. This architecture ensures data privacy, security, and integrity while enabling collaborative learning across multiple healthcare institutions.

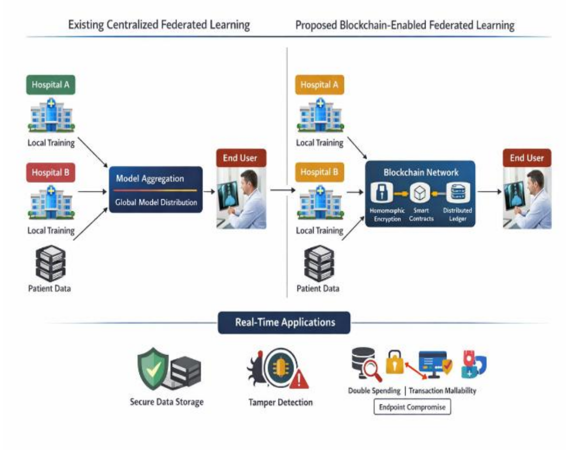

Fig1: System architecture

3.1 Methodology

The methodology of this research integrates both existing and proposed algorithmic approaches to safeguard patient privacy while enabling accurate disease diagnosis. Initially, the NIH Chest X-ray dataset is acquired and partitioned to simulate multiple hospital environments, providing diverse clinical data for analysis. Data preprocessing involves filtering relevant disease classes, encoding multi-label annotations, and resizing images to uniform dimensions, normalizing pixel values, and handling missing or inconsistent entries to ensure high-quality inputs for model training. For the existing approach, a standard deep learning model is trained centrally on the aggregated dataset to establish a performance baseline. In the proposed system, each hospital trains a local RESNET-based model independently, and encrypted model weights are securely stored and aggregated using Blockchain, implementing Federated Learning to preserve data privacy. Model evaluation is performed using metrics such as accuracy, precision, recall, and F1-score, while training performance is monitored through epoch-based accuracy and loss curves. Finally, the framework supports real-time disease detection by applying the aggregated global model to new patient X-rays, ensuring rapid and secure predictions across distributed hospital networks, thereby combining efficiency, privacy, and scalability in medical diagnostics.

3.2 Dataset Acquisition: The dataset is taken from the NIH Chest X-ray collection containing over 100,000 images with 15 lung disease labels and patient metadata. It is partitioned into multiple hospital nodes to simulate a federated learning environment while preserving data privacy and enabling decentralized training.

3.3 Data Pre-processing Images are resized, normalized, and encoded for multi-label classification, while irrelevant classes are removed. The dataset is split into simulated hospital nodes and prepared for RESNET input, ensuring consistency, quality, and suitability for federated learning.

3.4 Model Development: A centralized deep learning model is first trained as a baseline, followed by a RESNET-based federated learning model where each hospital trains locally. Encrypted model weights are shared via blockchain and aggregated using smart contracts for a secure global model.

3.5 Performance Evaluation: The proposed federated learning model outperforms the centralized approach in accuracy, precision, recall, and F1-score across 15 disease classes. It also ensures better privacy, scalability, and security while maintaining efficient real-time performance.

4. DESIGN AND CONSTRUCTION

The proposed system is designed as a secure and scalable framework for multi-disease diagnosis using Block chain-enabled Federated Learning. It follows a distributed architecture where multiple hospital nodes independently store data and train RESNET-based models. Each node prerocesses its

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

local dataset and performs model training without sharing raw data. The trained model weights are encrypted using homomorphic encryption to ensure privacy. These encrypted weights are shared through a Block chain network, where smart contracts handle secure aggregation. The global model is then updated and redistributed to all participating hospitals for further training. The system also includes a real-time prediction module for analysing new X-ray images. Overall, the design ensures data privacy, high accuracy, and efficient decentralized healthcare processing.

5. RESULTS AND DISCUSSION

The results show that the proposed Federated Learning and Blockchain-based system achieves effective and secure lung disease diagnosis. It attains strong accuracy, with improved performance in the global model, while maintaining data integrity through blockchain security and resisting common cyberattacks. Overall, the system ensures reliable classification, efficient storage, and robust performance suitable for real-world healthcare applications.

Fig 2: Building Smart Contract

Figure 2 show the Block chain Ethereum can store and retrieve data securely with the help of smart contracts and this contract contains functions which can called using python for data access.

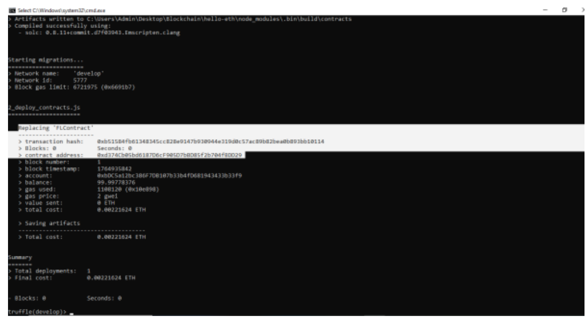

Fig 4: run Block chain

Figure 4 show the, got a contract address you can copy and paste in views.py at address

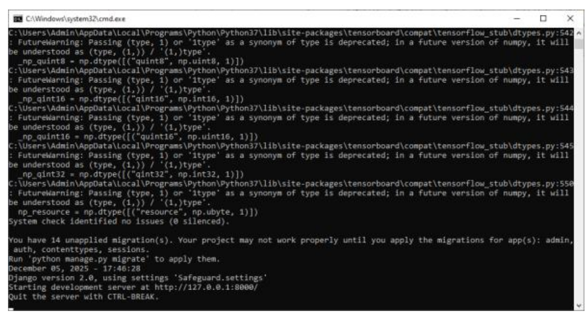

Fig 5: python server

Figure 5 show you run the python server using python manage.py runserver

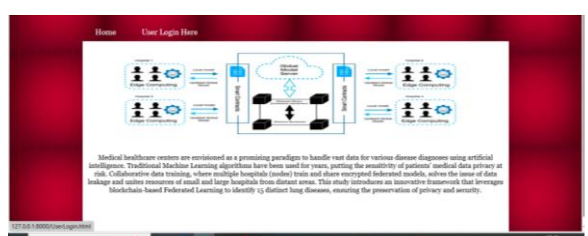

Fig 6: User Interface

Figure 6 got user interface after python server started and opening browser and enter URL as http://127.0.0.1:8000/index.html

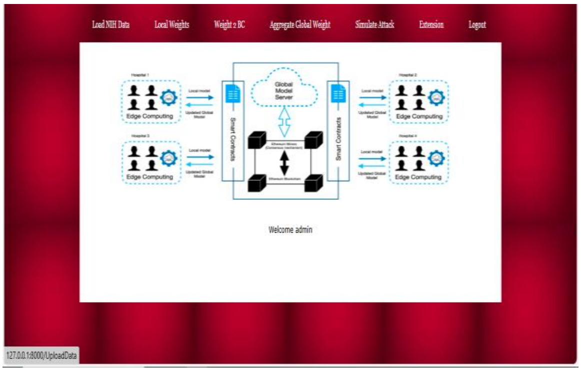

Fig7: Loading NIH Data

Figure 7 is the Load NIH Data Page allows authorized users to upload medical datasets from the National Institutes of Health.

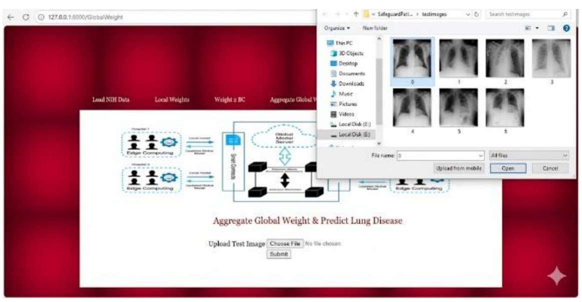

Fig8: Uploading Test Image

Figure 8 is the selecting and uploading test image to get Global weights from Blockchain and getting diagnosis result

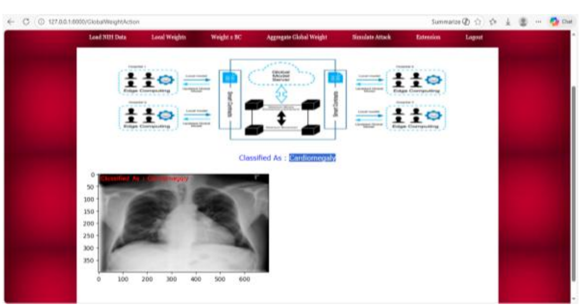

Fig 9: Diagnosis Prediction

Figure 9 is the uploaded image diagnose as 'Cardiomegaly' which can be seen in red and blue text.

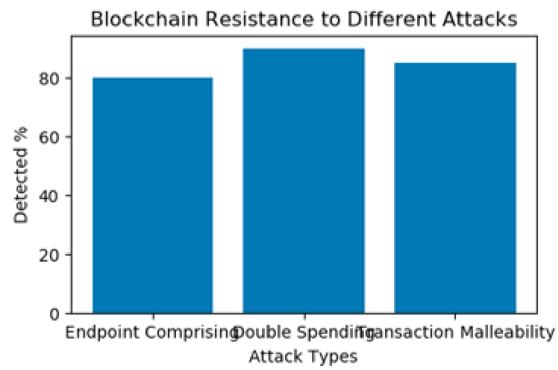

Fig10: Simulate Attack

Figure 10 illustrates the simulated attack evaluation process used to test the system's security against threats such as data tampering and model poisoning. It shows how effectively the system detects different types of attacks, with the block chain mechanism ensuring robust identification and prevention of malicious activities.

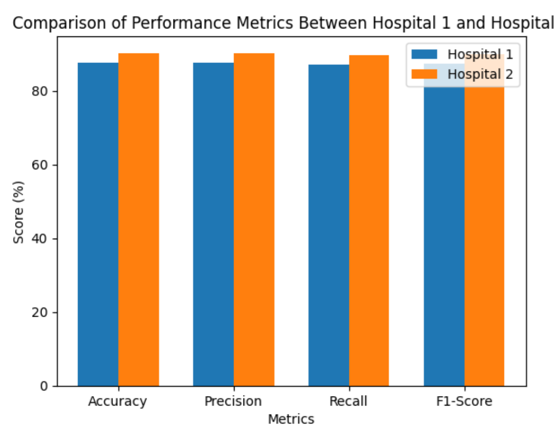

Figure 11: comparison of hospital 1 and 2

Figure 11 is the comparison bar plot showing Accuracy, Precision, Recall, and F1-Score for both Hospital 1 and Hospital 2.

Hospital 2 consistently performs slightly better across all metrics, which is clearly visible in the grouped bars for each evaluation measure.

6. CONCLUSION

The proposed system demonstrates an effective integration of Federated Learning and Blockchain technology to address critical challenges in medical data privacy, security, and collaborative model training. By enabling hospitals to train deep learning models locally using Residual Network architecture, the framework eliminates the need to share sensitive patient data while still achieving high diagnostic performance. The use of homomorphic encryption ensures that model weights remain protected during transmission, and Blockchain provides a decentralized, tamper-proof mechanism for storing and validating these weights. The experimental results confirm that the system achieves strong accuracy and reliable performance in detecting multiple lung diseases, while maintaining low latency and high throughput. The attack simulation further validates the robustness of the system against common cybersecurity threats, ensuring trust and integrity in the model aggregation process.

Future scope

The future scope of Blockchain-integrated Federated Learning for multi-disease detection is promising, as it can be extended to incorporate real-time patient monitoring and wearable device data, enabling continuous and personalized healthcare insights without compromising privacy. The framework can evolve to support larger-scale multi-institution collaborations across countries, integrating heterogeneous data sources such as genomic, imaging, and electronic health records for more accurate and early disease prediction. Additionally, advancements in lightweight encryption, edge computing, and adaptive model aggregation can further reduce latency and improve throughput, making the system suitable for telemedicine and remote diagnostics. With ongoing research in explainable AI, integrating interpretable models can also enhance clinician trust and regulatory compliance, paving the way for a fully secure, transparent, and scalable global healthcare data ecosystem.

REFERENCES

1. A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, “A secure Healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, 2022, Art. no. 106019.

2. A. P. Kalapaaking, I. Khalil, and X. Yi, "Blockchain-based federated learning with smpc model verification against poisoning attack for healthcare systems," *IEEE Trans. Emerg. Topics Comput.*, vol. 12, no. 1, pp. 269–280, First Quarter, 2024.

3. Z. Lian, Q. Zeng, W. Wang, T. R. Gadekallu, and C. Su, "Blockchain-based two-stage federated learning with non-IID data in IoMT system," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1701–1710, Aug. 2023.

4. A. Pathak, S. Sharma, A. Singh, S. Pandey, N. Yamsani, and R. Singh, "A study of deep learning and blockchain-federated learning models for COVID-19 identification utilizing CT imaging," in *Proc. IEEE World Conf. Appl. Intell. Comput.*, 2023, pp. 562–568.

5. V. Stephanie, I. Khalil, M. Atiquzzaman, and X. Yi, "Trustworthy privacy-preserving hierarchical ensemble and federated learning in Healthcare 4.0 with blockchain," *IEEE Trans. Ind. Inform.*, vol. 19, no. 7, pp. 7936–7945, Jul. 2023.

6. A. Lakhan, "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 664–672, Feb. 2023.

7. T. Hai, J. Zhou, S.R. Srividhya, S. J. Jain, P. Young, and S. Agrawal, "BVFLEMR: An integrated federated learning and blockchain technology for cloud-based medical records recommendation system," *J. Cloud Comput.*, vol. 11, 2022, Art. no. 22.