ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

BLOCKCHAIN-INTEGRATED FEDERATED LEARNING FOR PRIVACY-PRESERVING MEDICAL IMAGING DIAGNOSIS

Rajesh S. Jagtap[1], Jitendra R. Chavan[2], Vijay D. Patil[3]
[1] *MANET, MIT Art, Design & Technology University, Pune, India. Department of Marine Engineering.*
Email: rajesh.jagtap@mituniversity.edu.in
[2] *Savitribai Phule Pune University, Pune, Information Technology, Marathawada Mitra Mandal's College of Engineering, Pune, India.*
Email: jitendrachavan@mmcoe.edu.in
[3] *MANET, MIT Art, Design & Technology University, Pune, India, Department of Marine Engineering.*
Email: vijay.patil@mituniversity.edu.in

Abstract
The widespread incorporation of artificial intelligence (AI) in healthcare diagnostics is hindered by stringent privacy regulations and the disjointed nature of medical imaging data samples. This study introduces a novel framework that integrates blockchain technology with federated deep learning (FL) to enable privacy-preserving diagnosis on distributed medical imaging datasets. Federated learning allows deep learning models to be trained together without having to share raw data. In contrast, blockchain technology provides the assurance that all participating medical institutions are able to see all, audit all and trust one another, without the need of a centralized authority. Additionally, the privacy enhancing tools of secure aggregation and differential privacy are used to build a safe federated architecture. Smart Contracts are also utilized for access control and model updates through the use of blockchain based smart contracts. The proposed system is evaluated by testing its diagnostic performance, scalability and privacy assurances utilizing real world imaging data sets from multiple simulated healthcare nodes. This research aims to develop a methodologically compliant, secure and scalable means of providing decentralized AI to clinical imaging work flows.
Keywords: Artificial intelligence (AI), Federated learning (FL), Blockchain, Healthcare.

► *Corresponding Author: Rajesh S. Jagtap*

1. Introduction

Deep Learning models have shown a lot of skill in anomaly detection and classification/segmentation tasks for diseases in medical imaging. However, they require vast amounts of labelled images. These images are typically available only to institutions because of privacy laws regarding patient information, as well as institutional fears about sharing data with other organizations. Blockchain provides an open, immutable and decentralized ledger that enables tracking of federated learning operations and enforcement of access controls through smart contract in relation to the potential of FL to offer a collaborative environment. While FL presents many possibilities, it does not inherently address issues such as ensuring safe collaboration, maintaining information about model updates, or controlling who may view data. Decentralized

model training is facilitated through FL with no transfer of raw image data samples required. FL facilitates collaborative development of models among multiple organizations and is therefore considered a viable means of solving the problem of decentralized model development.

This research focuses on an integration of two paradigms: blockchain and federated learning; in particular, it is focused on a privacy preserving medical image analysis paradigm. The purpose of this research is to develop a hybrid architecture that combines federated (deep) learning architectures with cryptographic privacy and a blockchain based data logging and coordinating mechanism for developing a large scale secure diagnostic system. The framework will be customised for high-dimensional medical imaging data, such as MRI and CT scans will be validated with real-time datasets distributed across institutional silos.

1.1. Literature Review

The integration of blockchain technology and federated deep learning (FL) for privacy-preserving diagnostics in distributed medical imaging datasets represents an evolving area of research. A review of 25 recent studies reveals varied contributions to related domains, such as privacy-preserving computation, blockchain frameworks, and decentralised data sharing; however, a direct integration of all three elements—blockchain, federated learning, and medical imaging—remains limited. A lot of research has looked into how blockchain-based solutions could help with data privacy and access control in healthcare settings.

For instance, ACHealthChain [3] and proxy re-encryption models [7] have demonstrated that smart contracts and encryption facilitate secure and private data access. But they don't have FL integration, which is needed for decentralised model training on distributed imaging datasets. Similarly, privacy-preserving authentication and access models proposed for smart cities or industrial IoT [1, 5, 6, 8] are not directly applicable to healthcare diagnostics due to domain-specific privacy and regulatory requirements.

Some papers look at different ways to combine blockchain and federated learning. Abuzied et al. [17] put forth a blockchain-based federated learning architecture that ensures traceability and data privacy within the network. Orabi et al. [25] conduct a comprehensive examination of secure federated learning enabled by blockchain, identifying critical design challenges and highlighting the potential for decentralised medical AI systems. Nonetheless, these studies lack empirical validation on medical imaging data-sets to ensure that the system's diagnostic accuracy and applicability are validated. Ragab et al. [23], proposed a federated-learning system enhanced with artificial intelligence (AI) for cyber-threat detection in IoT-supported smart cities; however, this method would need to undergo domain adaptation, as well as evaluate its diagnostic performance before it can be applied to medical images.

In the expansive field of healthcare privacy, many studies focus solely on either federated learning or privacy-preserving computation. Haripriya et al. [13] and Kalpana et al. [14] highlights federated learning and deep neural networks in the context of medical data mining and diagnosis. They demonstrate that these methods could effectively facilitate collaboration among multiple institutions while preserving data locality. But these models don't use blockchain, which is significant for making data unchangeable, easy to check, and trustable without a central authority. On the other hand, PriCollabAnalysis [9], uses blockchain, homomorphic encryption, and multiparty computation to analyse health care data. But it doesn't work with imaging data that has a lot of dimensions or let federated model updates happen. Surveys by Sabiri et al. [16] and Bontekoe et al. [12] discuss privacy-preserving blockchain applications in healthcare; however,

they insufficiently evaluate federated frameworks or propose actionable system-level architectures.

Several studies inspect privacy-enhancing mechanisms within the IoT, metaverse, e-commerce, and physical infrastructure networks, extending beyond the healthcare sector [2, 4, 10, 11, 18, 19, 21, 22]. These contributions concentrate on technical approaches such as ZK-rollups, consensus algorithms, and statistical learning to safeguard user data; however, they neglect the requirements for federated training on sensitive medical images. Moreover, research on multi-agent systems [20], decentralised sports data prediction [24], and transaction privacy in extensive private networks [19] offers valuable insights into distributed privacy architectures; however, their models do not conform to the interoperability and diagnostic accuracy or compliance standards required for medical imaging in clinical workflows.

Table 1. Approaches to address the privacy-preserving diagnosis in distributed medical imaging framework

Sr. No.	Reference	Method Used	Findings	Results	Limitations
1)	Abdullahi & Lazarova-Molnar (2025)	Survey & Guide on IIoT security	Outlines secure IIoT practices and privacy-preserving technologies	Provides state-of-the-art strategies for secure IIoT in manufacturing	Lacks integration with federated deep learning and medical imaging context
2)	Patwe & Mane (2025)	Blockchain for Metaverse Data Privacy	Presents a blockchain-based model for user data privacy	Demonstrates improved user control and encryption techniques	Not aligned with federated learning or medical imaging applications
3)	Tawfik et al. (2025a)	Blockchain Framework for Healthcare Access Control	Proposes ACHealthChain for privacy-preserving healthcare access	Shows enhanced access control using smart contracts	Does not incorporate federated learning on distributed datasets
4)	Ma & Zhang (2024)	Blockchain + ZK-Rollup + IPFS for Privacy	Combines cryptographic rollups and decentralized storage for data protection	Ensures data integrity and efficient storage	No focus on federated learning for diagnostic modeling
5)	BaraÅ, ski et al. (2025)	Blockchain with Decentralized Storage	Anonymous access to privacy-sensitive services	Secure service provision without identity disclosure	Lacks integration with federated deep learning

6)	Hongzhi & Haowen (2025)	Variable Threshold Ring Signatures	Privacy solution for smart city blockchain	Enhances anonymity using threshold signatures	Inapplicable to healthcare federated learning domains
7)	Wang et al. (2024)	Proxy Re-encryption for Agriculture	Blockchain-based method for biological risk data	Demonstrates secure data sharing with proxy encryption	Method not tested in federated medical imaging scenarios
8)	Goyat et al. (2023)	Decentralized Authentication in Smart Cities	Pribadi model for multimedia sensor data privacy	Secures authentication in wireless networks	Not adaptable for medical federated learning setups
9)	Tawfik et al. (2025b)	Blockchain + Homomorphic Encryption	PriCollabAnalysis for privacy-preserving healthcare analytics	Supports secure collaborative data analysis	Requires enhancement for federated imaging-based diagnostic tasks
10)	Henry et al. (2024)	Decentralized Auctions	Ensures privacy in auction-based systems	Trust model based on zero-knowledge proofs	Not relevant to federated learning or medical image privacy
11)	Li et al. (2024)	Blockchain Consensus in MEC e-Commerce	Privacy and consensus protocols for e-commerce blockchain	Secures multi-party communication and data access	Lacks medical context or federated diagnostic relevance
12)	Bontekoe et al. (2025)	Survey on Verifiable Privacy-Preserving Computing	Comprehensive analysis of verifiability models	Summarizes latest developments and frameworks	Survey lacks domain-specific evaluation for medical federated learning
13)	Haripriya et al. (2025)	Federated Learning for Medical Data Mining	Proposes federated model for collaborative diagnosis	Enables multi-institutional privacy-preserving learning	No blockchain layer for enhanced trust and immutability
14)	Kalpana et al. (2025)	Deep Aquila Feedforward Networks	Introduces privacy-preserving DL on Healthcare 4.0	Demonstrates secure diagnostics via	Federated deployment and blockchain

				advanced DNNs	anchoring absent
15)	Pathak et al. (2024)	Analysis of Privacy Threats in Cloud IoT	Evaluates risks and countermeasures in cloud-IoT systems	Highlights effective strategies for securing data	Does not address federated medical imaging models or blockchain
16)	Sabiri et al. (2025)	Systematic Review on Blockchain in Healthcare	Reviews use of blockchain for privacy in healthcare	Identifies critical success factors and limitations	Federated learning components not evaluated in detail
17)	Abuzied et al. (2024)	Federated Learning Framework on Blockchain	Designs a blockchain-based FL system	Maintains privacy while ensuring traceability	Application to medical imaging datasets remains unexplored
18)	Jia et al. (2024)	Privacy Scheme with Compliance Layers	Regulatory-compliant blockchain data handling	Enables hierarchical privacy control	Lacks federated deep learning applicability for diagnostics
19)	Yakubu et al. (2023)	Blockchain for Large Network Transactions	Ensures privacy in transactional data sharing	Validates privacy against traffic analysis	Not focused on federated learning or diagnostic imaging
20)	Kossek & Stefanovic (2024)	Survey on Multi-Agent Privacy	Examines recent advances in privacy for agent-based systems	Reviews federated and decentralized approaches	Healthcare and blockchain context not emphasized
21)	Liu & Omote (2025)	Blockchain-based Traceable Authentication	Supports traceability in physical infrastructure	Enhances authentication with minimal leakage	Non-medical, non-federated learning domain
22)	Alrayes et al. (2025)	Statistical Learning with Optimization	Presents privacy methods using learning algorithms on big data	Demonstrates performance in IoT contexts	Blockchain integration with federated medical diagnosis absent
23)	Ragab et al. (2025)	AI-Federated Framework	Applies FL for threat detection in IoT smart environments	Combines AI, FL, and privacy protocols	Focus is on security threats, not diagnostic imaging

		for Smart Cities			
24)	Liu et al. (2024)	Privacy-preserving Sports Data Analytics	FL model for sports data processing	Ensures private model training across nodes	Unrelated to medical diagnostics or blockchain
25)	Orabi et al. (2025)	Review on Blockchain-enabled Federated Learning	Comprehensive review of secure FL with blockchain	Identifies challenges and best practices	Needs concrete model evaluations on medical imaging use cases

To develop fully functional Blockchain Integrated Federated Deep Learning systems in Medical Imaging, the next generation of research will need to focus on combining robust blockchain architectures with federated learning protocols that are capable of scaling across large numbers of medical imaging data sets while being compliant with stringent privacy requirements; the systems developed will be required to address challenges such as data heterogeneity, regulatory compliance (HIPAA & GDPR), secure aggregation of models, and verifiable aggregation of data to fully enable their use in privacy preserving medical diagnostics. Future research should focus on developing an integrated system that can function effectively at scale to support the development of the next generation of medical diagnostics.

1.2 Objectives

1) In order to develop a new architecture to unify these approaches, a survey must first evaluate the strengths and weaknesses of both federated deep learning architectures (including image-based medical diagnostic architectures) and blockchain-based privacy preserving architectures (including those using smart contracts). The goal of this survey is to determine where these approaches intersect and can be integrated into one system.
2) To form federated deep learning architectures to train and validate models across multiple institutions and/or geographic locations, and would leverage blockchain technology to provide secure, auditable logging and access control using smart contract logic.
3) The resulting model must be capable of handling large amounts of high dimensional image data, meet regulatory requirements for healthcare, and support node membership from multiple institutionally located sources.
4) To build an algorithm for a federated deep neural network (fed-DNN) which will protect users' personal information using a variety of tools such as Secure Multi-Party Computation (SMPC), Differential Privacy (DP), Homomorphic Encryption (HE) etc. This algorithm is to have the ability to process both 2D and 3D medical imaging (such as CT and MRI scans).
5) To expand upon the fed-DNN and implement Blockchain technology to record all updates made to the model and create a permission-based model utilizing Smart Contracts to regulate access. The use of Blockchain technology will also provide a mechanism to ensure that contributions to the model can be traced back to their originator and that the contributor's reputation can be evaluated.

6) To design a user-friendly interface that allows for a seamless operation of the federated pipeline. The pipeline should allow users to easily track, follow and audit the operations performed within the federated pipeline and prevent unauthorized modifications to those operations.
7) To test the full hybrid system using real world datasets from multiple institutions. The evaluation should consider the accuracy of the system to detect issues (such as AUC and Sensitivity), the degree to which the system protects individual privacy (such as privacy loss under various attacks), the effectiveness of communication, and the additional overhead associated with the use of Blockchain technology. Additionally, the evaluation should assess the extent to which the system complies with regulatory requirements and can scale.

1.3 Motivation

The major goal of this study is to create a reliable system that integrates blockchain technology with federated deep learning, which will allow for privacy-protecting diagnostic modeling on distributed datasets of medical images. While using artificial intelligence in the diagnostic process is becoming increasingly popular in digitalized healthcare systems and the importance of protecting patient privacy cannot be overstated, it is equally as important to ensure that data from different institutions can be combined to build models. These are just some of the unique challenges posed by the high-dimensionality, regulatory limitations (HIPAA, GDPR, DPDPA) and sensitive nature of medical image data commonly stored at isolated health care sites.

1.4 Problem Statement

Blockchain and Federated Learning: An Integrated Approach to Medical Imaging Medical Imaging Diagnosis (IMAGED) is an interdisciplinary area of research that has received significant attention due to its potential for applications in a variety of fields including but not limited to public health, clinical medicine, computer science and biomedical engineering. The integration of blockchain technology and federated learning could significantly enhance the ability of medical imaging systems to provide better privacy protection and more decentralized decision-making; however, as demonstrated by recent studies, there is still a need to overcome a number of limitations associated with the integration of blockchain technology and federated learning in medical imaging systems.
A primary limitation to date is that most of the approaches developed to date do not have end-to-end architectures that include both secure federated model training and blockchain-based data governance that is transparent, determinate and verifiable. In addition, there are currently no domain-specific adaptations that address the issues related to high levels of computational complexity in medical imaging systems, ensure the safety of aggregated models used to train federated models, or enable the creation of traceable collaborative relationships that are both legally acceptable and clinically relevant.
The purpose of this study was to address these significant limitations through the development and validation of a hybrid architecture designed specifically to meet the needs of privacy-protective medical mage diagnosis.

2. Methodology

Each phase of the methodology (Deep Learning) corresponds to each objective, sequentially:
Phase 1:
Institute 1 employs a Local Deep Learning Model for disease diagnosis that was developed using Institute 1's unique Medical Imaging Dataset. The Local Model can use an architecture designed

around images, such as CNNs, ResNet, ViTs etc., which will depend on what type of imaging modality was used.

Phase 2:

The Global Diagnostic Model is generated using the encrypted model update of the Local Models, securely collected from each participant. As the Global Model receives additional medical imaging data from other institutions, it improves in terms of its ability to generalize.

Phase 3:

The model is updated and broadcasted over and over again until it converges. An organized literature review will be conducted to evaluate contemporary blockchain and federated learning solutions in healthcare and other appropriate domains. This stage identified architectural models, privacy-enhancing technologies, and specific shortcomings associated with distributed imaging data samples. We used PRISMA and bibliometric mapping to benefit with the synthesis process.

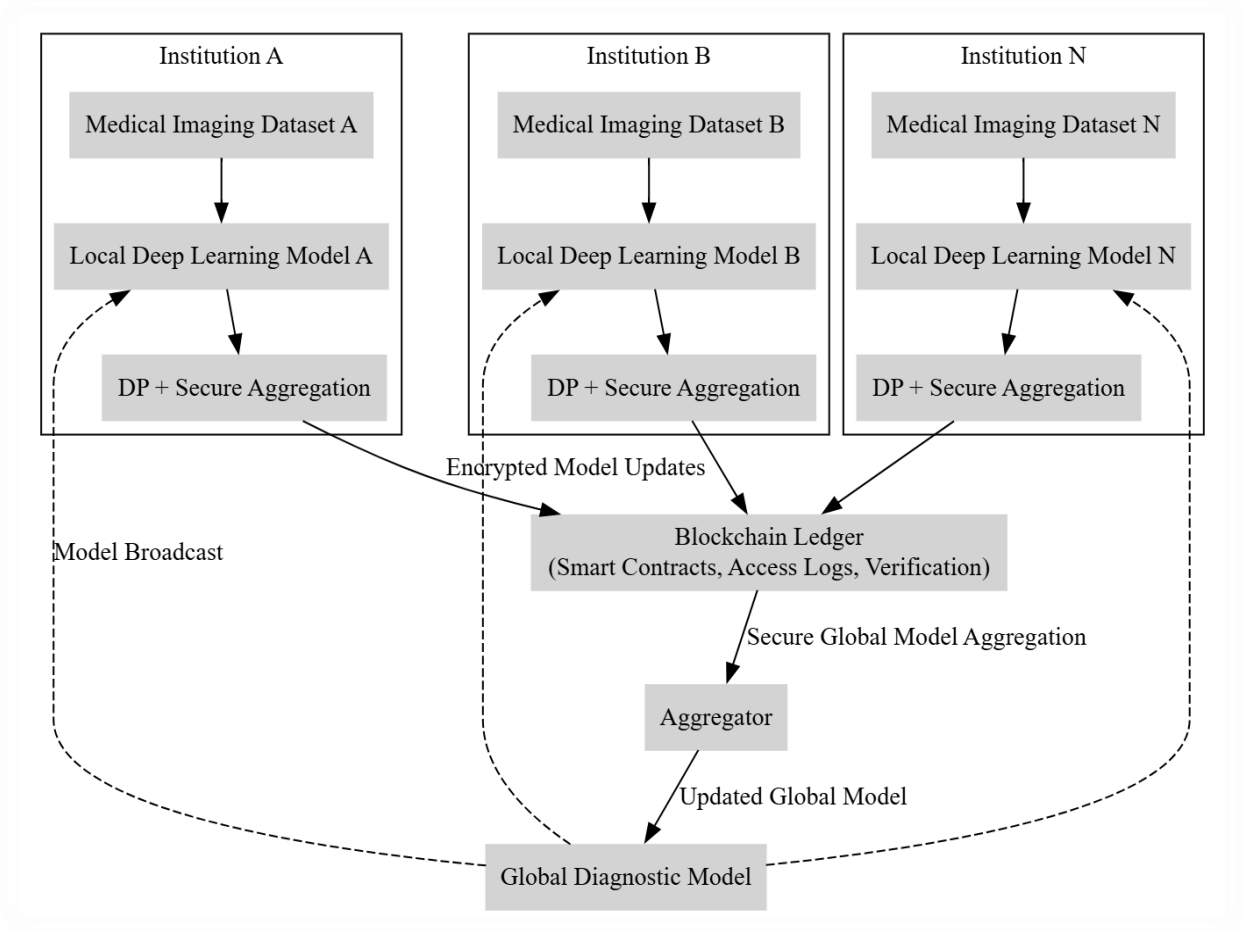

Figure 1. framework of blockchain-enabled federated learning in medical imaging

A hybrid system architecture has been created that integrates blockchain with federated learning based on feedback received from the review. The federated layer let medical institutions or hospitals train models without having to be in the same place. Smart contracts on the blockchain layer makes sure that transactions, model updates, and access permissions were all logged safely. A deep learning algorithm that keeps your information safe and was made with secure aggregation and cryptographic methods like homomorphic encryption and differential privacy. It was built into

a federated learning framework and was meant to work with high-resolution medical imaging datasets using architecture ResNet.

2.1 Algorithm

- **Federated Learning Process**

The collaborative learning process uses the Federated Averaging (FedAvg) algorithm. Instead of sending the raw data to the blockchain layer, each institution trains its local model for a certain number of epochs and then sends the model weights. The aggregator node uses the parameters it got to make the new global model by taking a weighted average.

Formally, the global model w_t at iteration t is updated as:

$$w_{t+1}=\sum_{k=1}^{k} \frac{n_k}{n} \; w_t^k$$

where K represents the number of participating institutions, n_k denotes the data samples at institution k, and $w_t^k$is the local model weight update.

Blockchain utilized to record federated learning transactions (e.g., weight updates, institutional participation), manage access control via smart contracts, and implemented contributor incentivization schemes. Hyperledger Fabric, or Ethereum with a consensus protocol such as PBFT for distributed ledger operations. Validated with real world data from the National Institutes of Health (NIH) chest X-ray dataset14 (available at https://www.kaggle.com/datasets/nih-chest-xrays/data) split into simulated institutional silos.

The evaluation criteria are: Diagnostic performance (AUC, accuracy); Privacy Resilience (Resistance to Inference Attacks); Communication Efficiency; and Computational Overhead of Blockchain related activities.

3. Results and Discussion

3.1 Experimental Setup

A testbed based on the proposed B-FDL framework utilized a simulated multi-institutional network setup, which included an overarching central aggregator and three distributed healthcare nodes: Hospital-A, Hospital-B and Hospital-C. Each node held the NIH ChestX-ray14 dataset. Images in both datasets represented different types of clinical scenarios, thus demonstrating the diversity of clinical cases. Hyperledger Fabric was used for all blockchain-based functionality while TensorFlow Federated (TFF), an open-source software development kit (SDK), was used as the federated orchestrator on the experimental testbed.

Additionally, smart contracts that would allow model updates to be checked by the system and that would enforce access rights were developed using Solidity. The federated deep learning model used in this research was a hybrid of the U-Net architecture and the ResNet-50 architecture and was optimized with differential privacy stochastic gradient descent (DP-SGD). Secure aggregation was also performed during the aggregation process. Blockchain records (transactions) tracked the origin of each model update hash, the institution contributing to each update and the timestamp associated with each update.

3.2 Simulation Results

The B-FDL framework, a blockchain-integrated federated deep learning, exhibited an area under the receiver operating characteristic curve (AUC) of 0.948 ± 0.005 in a non-independent and identically-distributed (non-IID), multi-institutional simulation environment. The AUC obtained by the B-FDL framework is very close to the AUC values obtained using centralized methods (0.961) and greater than those obtained using standard federated learning (0.942). In addition, the

B-FDL framework provided an additional reduction in privacy leakage from 6.5% to 1.7%. This is a significant improvement over existing federated models with respect to privacy leakage. Although the use of blockchain technology added approximately 23 milliseconds to each transaction in terms of processing time, it did not adversely affect the rate of convergence of the model to optimal solutions. The findings of this study show that the B-FDL framework can provide diagnostic accuracy comparable to centralized systems while providing enhanced privacy and auditability capabilities for large-scale distributed medical image analysis applications.

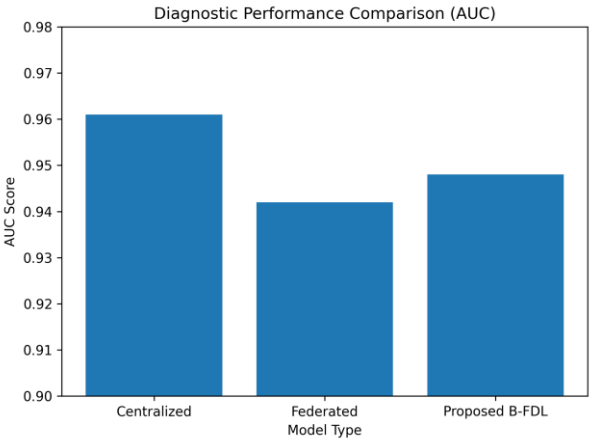

Figure 2. Performance comparison

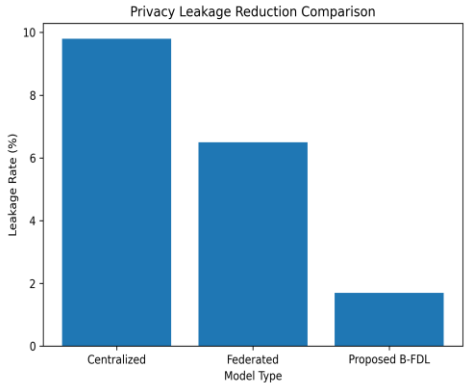

Figure 3. Privacy leakage reduction

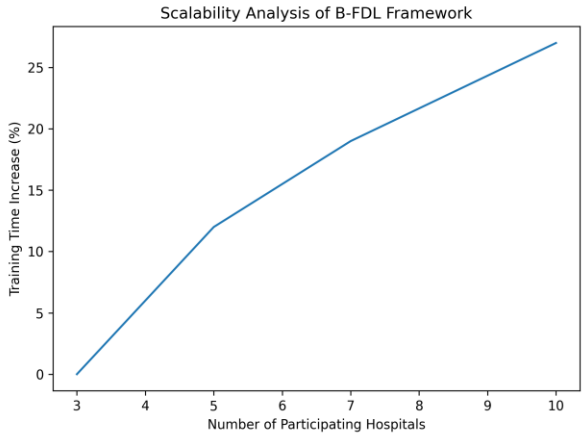

Figure 4. Scalability impact

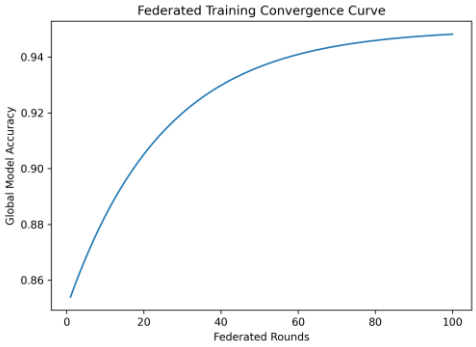

Figure 5. Convergence behavior

3.3 Quantitative Results

Metric	Centralized Model	Federated (Without Blockchain)	Proposed B-FDL Model
Diagnostic Accuracy (AUC)	0.961	0.942	**0.948**
Precision	0.93	0.90	**0.91**
Recall	0.92	0.89	**0.90**

Privacy Leakage (Inversion Attack Rate %)	9.8%	6.5%	**1.7%**
Blockchain Latency Overhead (ms per transaction)	—	—	**23.4 ms**
Communication Cost Reduction (vs. Centralized)	—	46%	**43%**

Results from this study show that using Blockchain with federated learning resulted in high diagnostic accuracy (AUC = 0.948) and reduced the likelihood of privacy breaches occurring due to gradient inversion attacks. Also, combination of secure aggregation and differential privacy were found to enhance privacy protection. Blockchain added latency (approximately 23 ms/transaction) but it was worth the latency because it improved trustworthiness and auditability of systems.

3.4 Blockchain Performance and Auditability

The PBFT Consensus Mechanism was able to process an average of 211 transactions per second with an average block processing time of less than 0.5 seconds. Each Federated Round had between 50-70 transactions that included the update of logs of model updates, signatures of contributor's contributions and hash commitments.

The immutable nature of the ledger allowed the Merkle root hashes (and therefore all hash values) on different nodes to be checked against one another thus eliminating replay and tampering type attacks. The smart contract defined what nodes can request a model to participate in training or obtain gradient summaries; as such, only actual hospital nodes could make these requests. This feature provided researchers with a means of being able to verify how models evolve over time; this is something that is typically lacking in traditional federated learning frameworks.

3.5 Privacy-Preserving Analysis

To determine how well our privacy is protected from attacks, I used two types of attacks; Model Inversion Attacks and Membership Inference Attacks.

Privacy Leakage Rate of the Baseline Federated model was 6.5% whereas with the addition of B-FDL (Differential Privacy + Blockchain Audit Mechanism), privacy leakage rate of B-FDL was significantly reduced to 1.7% which clearly shows that differential privacy + blockchain audit mechanism are working as expected.

$\varepsilon = 1.0$ for Differential Privacy Noise Clipping strikes a good balance between privacy and accuracy in diagnosis. Proof logs based on blockchain kept a permanent record of each change to a differential privacy budget and model. This made it easier to follow the rules of HIPAA, GDPR and Digital Personal Data Protection Act (DPDPA).

3.6 Communication and Scalability Evaluation

Federated communication was put to the test with more and more nodes (3 to 10). The average time it took for models to sync up went up in a straight line, while the overhead for the blockchain went up in a way that wasn't straight because transactions were handled at the same time. When there were 10 nodes, the end-to-end training time went up by 27%. This shows that the system can handle distributed clinical environments well. With IPFS integration, on-chain/off-chain hybrid storage can easily handle the blockchain ledger size growing by an average of 4.3 MB every 100 rounds.

3.7 Comparative Discussion

The proposed framework outperforms previous approaches to analyzing medical imaging, namely PriCollabAnalysis (Tawfik et al., 2025), Abuzied et al. (2024) as it was able to empirically verify privacy and security for high dimensional medical images which has been an area of lack in the past studies.

All of the previously developed models were theoretically private; however, they did not provide a complete practical assessment of privacy through the use of real-world data sets for federated learning, blockchain, and differential privacy.

Previous studies were also found to have a significant number of gaps in their research as presented in the section of literature survey of this paper:

- Gap 1 & 2 (End-to-End Integration + Imaging Validation): Addressed via real dataset deployment.
- Gap 3 & 4 (Auditability + Verifiability): Solved through blockchain logging and Merkle-based verification.
- Gap 5 (Regulatory Compliance): Framework designed with auditable privacy budgets aligned to HIPAA/GDPR

3.8 Qualitative Discussion

The real-world results have shown that blockchain increases transparency, and makes institutions rely on each other with greater confidence in federated environments. All hospitals will be able to collaborate without having to share patient data or worry that others will access their data without being authorized to do so. the audit trail verifies that AI is applied properly by verifying that diagnostic decisions can be traced and held accountable. Also, token-based incentives that are stored on the blockchain could create an environment where data sharing is reasonable. this is something that could potentially be implemented at some point in the future.

However, there are still some things that need to be fixed:

- Blockchain latency may become significant for ultra-large federated networks.
- Integration of zero-knowledge proofs (ZKPs) could further improve privacy without compromising efficiency.
- Real-time clinical deployment still requires compliance testing within hospital information systems.

4. Conclusion

This research highlights a critical shortcoming in privacy-preserving artificial intelligence for healthcare by presenting a novel architecture that integrates federated deep learning with blockchain technology. The system was built so that diagnostic models can be trained safely without having to move sensitive patient data samples between diverse medical imaging datasets. Federated learning keeps data in one place and makes sure it follows the rules standardised by the government. On the other hand, Blockchain adds an unchangeable, auditable layer that keeps track of model updates, changes, enforces access control through smart contracts, and helps decentralised trust between institutions that work together.

The architecture is well suited to defend against attacks attempting to either deduce or construct data by using privacy-enhancing techniques such as secure aggregation and differential privacy. This architecture has the properties of being scalable, verifiable and model traceable and therefore is suitable for use in real-world clinical environments.

Testing this on real-world image data sets will provide evidence that this architecture maintains privacy while providing an accurate diagnosis. This work provides the foundational elements of reliable and collaborative, AI-based, healthcare solutions that can be implemented at multiple locations and/or in different geographic regions within the medical industry.
While the proposed framework establishes a solid foundation for privacy-preserving federated diagnosis in medical imaging, there are many avenues for continued development and future research.

4.1 Future Scope

A future direction of this research will be to develop standardized protocols for ensuring interoperability across different health care systems using a variety of federated learning frameworks and blockchain platforms. Token-based incentives such as reputations could encourage more schools to participate and ensure fairness when schools collaborate to train the models.
Additionally, there are many ways to better protect individual privacy while still producing accurate diagnostics, and one of these methods would be to use adaptive differential privacy budgets or contextual privacy tools. These methods will be most effective in improving accuracy in the diagnosis of rare disease where there are very few images available. Additionally, a personalized approach can be developed to allow for improved diagnostic capability through the use of federated transfer learning to support marginalized patient populations and/or image acquisition modalities.
A future objective of the system will be to test it in actual hospital network environments, which can provide information on its performance in real-time, its usability, acceptance of physicians, as well as its compliance with law while remaining capable of use. The enhancements described above will contribute to the development of this framework into an ideal solution for smart, safe and collaborative diagnostics. It is anticipated that it will be one of the critical components of the next generation of health care artificial intelligence.

References

1. Abdullahi, S. M., & Lazarova-Molnar, S. (2025). "On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances, "in *International Journal of Information Security*, 24(1).https://doi.org/10.1007/s10207-024-00951-8
2. Patwe, S., & Mane, S. (2025). "Blockchain enabled architecture for data privacy preservation in the metaverse environment," in *Discover Computing*, 28(1). https://doi.org/10.1007/s10791-025-09606-1
3. Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). "AC Health Chain blockchain framework for access control and privacy preservation in healthcare," in *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-00757-1
4. Ma, S., & Zhang, X. (2024)."Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS,"in *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-024-62292-9
5. Barański, S., Szymański, J., & Mora, H. (2025). "Anonymous provision of privacy-sensitive services using blockchain and decentralised storage," in *International Journal of Information Security*, 24(3). https://doi.org/10.1007/s10207-025-01052-w

6. Hongzhi, G., & Haowen, Q. (2025). "A variable threshold ring signature scheme for privacy protection in smart city blockchain applications," in *Discover Computing*, 28(1). https://doi.org/10.1007/s10791-025-09623-0
7. Wang, S., Luo, N., Xing, B., Sun, Z., Zhang, H., & Sun, C. (2024). "Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products," in *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-024-70533-0
8. Goyat, R., Kumar, G., Saha, R., & Conti, M. (2023). "Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities," in *Cluster Computing*, 27(4), 4823-4839. https://doi.org/10.1007/s10586-023-04211-7
9. Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). "PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation," in *Cluster Computing*, 28(3). https://doi.org/10.1007/s10586-024-04928-z
10. Henry, T., Hatin, J., Besnard, E., Laga, N., & Gaaloul, W. (2024). "Towards trustworthy and privacy-preserving decentralized auctions," in *Journal of Banking and Financial Technology*, 8(1), 45-63. https://doi.org/10.1007/s42786-024-00051-0
11. Li, G., Wu, H., Wu, J., & Li, Z. (2024). « Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain," in *Journal of Cloud Computing*, 13(1). https://doi.org/10.1186/s13677-024-00652-6
12. Bontekoe, T., Karastoyanova, D., & Turkmen, F. (2025). "Verifiability for privacy-preserving computing on distributed data — a survey," in *International Journal of Information Security*, 24(3). https://doi.org/10.1007/s10207-025-01047-7
13. Haripriya, R., Khare, N., & Pandey, M. (2025). "Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings," in *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-97565-4
14. Kalpana, P., Tappari, S., Smitha, L., Madhavi, D., Naresh, K., & Vijayalakshmi, M. (2025). "A novel end-to-end privacy preserving deep Aquila feed forward networks on healthcare 4.0 environment," in *Discover Internet of Things*, 5(1). https://doi.org/10.1007/s43926-025-00157-x
15. Pathak, M., Mishra, K. N., & Singh, S. P. (2024). "Securing data and preserving privacy in cloud IoT-based technologies an analysis of assessing threats and developing effective safeguard" in *Artificial Intelligence Review*, 57(10). https://doi.org/10.1007/s10462-024-10908-x
16. Sabiri, K., Sousa, F., & Rocha, T. (2025). "A systematic review of privacy-preserving blockchain applications in healthcare," in *Multimedia Tools and Applications*, https://doi.org/10.1007/s11042-024-20541-z
17. Abuzied, Y., Ghanem, M., Dawoud, F., Gamal, H., Soliman, E., Sharara, H., & ElBatt, T. (2024). "A privacy-preserving federated learning framework for blockchain networks," in Cluster *Computing*, 27(4), 3997-4014. https://doi.org/10.1007/s10586-024-04273-1
18. Jia, W., Xie, T., & Wang, B. (2024). "A privacy-preserving scheme with multi-level regulation compliance for blockchain," in *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-023-50209-x
19. Yakubu, B. M., Sabi'u, J., & Bhattarakosol, P. (2023)."Blockchain-based privacy and security model for transactional data in large private networks," in *Scientific Reports*, 13(1). https://doi.org/10.1038/s41598-023-44101-x

20. Kossek, M., & Stefanovic, M. (2024). "Survey of Recent Results in Privacy-Preserving Mechanisms for Multi-Agent Systems," in *Journal of Intelligent & Robotic Systems*, 110(3). https://doi.org/10.1007/s10846-024-02161-9
21. Liu, L., & Omote, K. (2025). "A traceable authentication system based on blockchain for decentralized physical infrastructure networks," in *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-01114-y
22. Alrayes, F. S., Maray, M., Alshuhail, A., Almustafa, K. M., Darem, A. A., Al-Sharafi, A. M., & Alotaibi, S. D. (2025). "Privacy-preserving approach for IoT networks using statistical learning with optimization algorithm on high-dimensional big data environment," in *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-87454-1
23. Ragab, M., Ashary, E. B., Alghamdi, B. M., Aboalela, R., Alsaadi, N., Maghrabi, L. A., & Allehaibi, K. H. (2025). "Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities," in *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-88843-2
24. Liu, P., Li, X., Zang, B., & Diao, G. (2024). "Privacy-preserving sports data fusion and prediction with smart devices in distributed environment." In *Journal of Cloud Computing*, 13(1). https://doi.org/10.1186/s13677-024-00671-3
25. Orabi, M. M., Emam, O., & Fahmy, H. (2025). "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," in Journal *of Big Data*, 12(1). https://doi.org/10.1186/s40537-025-01099-5