IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems

Ms. Ankitha S[1], Shwetha M D[2], Nisarga[3], Rakshitha B k[4], Chandana S[5]

Assistant Professor, Dept. of Computer Science MMK and SDM MMV[1]

III BCA, Dept. of Computer Science MMK and SDM MMV[2-5]

Abstract: Healthcare systems generate large amounts of sensitive patient information through hospitals, labs, wearable devices, diagnostic centres, and electronic medical records. Traditional centralized machine learning approaches require sharing raw healthcare data to train intelligent models. This raises significant concerns about privacy, security, and following regulations. Federated Learning (FL) addresses these issues by allowing multiple healthcare institutions to work together to train machine learning models without transferring raw patient information. However, federated learning environments are still at risk of poisoning attacks, where malicious actors submit altered model updates that harm model performance and reliability. This research presents a secure framework called Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems. The framework combines Federated Learning, Secure Multi-Party Computation (SMPC)-based verification, and Blockchain technology to create a reliable collaborative platform for healthcare intelligence. Healthcare institutions train models locally and share only model parameters instead of patient records. Local model updates undergo SMPC-based verification to flag suspicious contributions before aggregation. Verified updates are combined using federated learning techniques, while malicious updates are discarded. Blockchain technology maintains unchangeable logs to enhance transparency, traceability, and accountability. The proposed system is implemented as a Flask-based web application supported by an SQLite database. This database manages healthcare participants, federated rounds, verification records, global model information, and blockchain event history. The framework strengthens privacy preservation, boosts security against poisoning attacks, and builds trust in distributed healthcare artificial intelligence systems. Experimental implementation shows that combining federated learning with blockchain and verification methods offers a dependable and scalable solution for secure healthcare collaboration.

Keywords - Blockchain Technology, Federated Learning, Healthcare Artificial Intelligence, Secure Multi-Party Computation (SMPC), Poisoning Attack Detection, Privacy Preservation, Distributed Machine Learning, Healthcare Security, Model Verification, Blockchain Auditability.

I. INTRODUCTION

Healthcare organizations increasingly rely on artificial intelligence for disease diagnosis, patient monitoring, medical image classification, treatment prediction, and clinical decision support systems. Effective healthcare AI models need large and diverse datasets. However, healthcare data is highly sensitive due to privacy regulations, institutional restrictions, and ethical concerns. Traditional centralized machine learning systems collect healthcare data into a common repository. This increases the risks of unauthorized access, privacy breaches, and cyberattacks. Federated Learning (FL) has emerged as a privacy-friendly approach where participating healthcare institutions train machine learning models locally and share only model updates instead of raw patient records. This distributed method allows for collaboration while keeping data confidential. Despite its privacy benefits, federated learning is still vulnerable to poisoning attacks. Malicious participants can intentionally alter local model updates to corrupt the global model. Such attacks can significantly lower prediction accuracy and endanger patient safety. To address these challenges, this work suggests a framework that combines Federated Learning, Secure Multi-Party Computation (SMPC)-based verification, and Blockchain technology. The SMPC-inspired verification checks model updates before aggregation, while blockchain ensures transparent and tamper-proof logging of training activities. This integration creates a secure and privacy-oriented collaborative learning framework specifically designed for healthcare systems.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

II. LITERATURE SURVEY

1. Privacy-Preserving Collaborative Learning in Healthcare

Healthcare organizations produce a vast amount of sensitive patient data from medical records, diagnostic systems, and healthcare databases. Traditional machine learning methods rely on centralized data collection, creating issues regarding privacy, security, and compliance. Recent research suggests collaborative AI methods that allow healthcare institutions to build models together without directly sharing patient data. Distributed learning can improve model accuracy using data from multiple institutions. However, centralized systems still face risks such as data breaches and unauthorized access.

Implication for Proposed System: A privacy-preserving framework is essential for secure healthcare collaboration while protecting patient information.

2. Federated Learning for Secure Healthcare Intelligence

Federated Learning (FL) is a distributed machine learning approach where healthcare institutions train local models and share only model updates instead of raw data. This method supports privacy preservation and allows hospitals to collaborate securely. Federated Learning is used in healthcare areas like disease prediction, medical image analysis, and clinical decision support. However, challenges such as poisoning attacks, malicious participants, and information leaks still exist.

Implication for Proposed System: Federated Learning enhances privacy but requires additional security and verification mechanisms for trustworthy healthcare collaboration.

3. Poisoning Attack Detection and Secure Model Verification

Poisoning attacks are significant security threats in distributed machine learning systems where malicious participants send manipulated model updates to decrease model accuracy or produce biased results. Even a small number of malicious updates can harm collaborative learning performance. Researchers are using techniques like verification methods and Secure Multi-Party Computation (SMPC) to bolster security. SMPC enables safe collaboration without revealing private information and helps lessen the impact of harmful updates.

Implication for Proposed System: Incorporating SMPC-based verification boosts federated learning security and enhances defence against poisoning attacks.

III. EXISTING SYSTEM

Current healthcare artificial intelligence systems primarily rely on either centralized machine learning or traditional federated learning methods. In centralized learning, healthcare institutions transfer patient data to a shared server for model training. While this improves data availability, it poses privacy risks, security issues, and regulatory challenges due to the storage of sensitive healthcare information in one place. To address these problems, traditional Federated Learning approaches allow hospitals and healthcare organizations to train models locally and share only model updates. This helps maintain privacy by avoiding direct patient data sharing.

However, existing federated learning systems still encounter significant challenges. Many frameworks accept local model updates without adequate verification, leaving them open to poisoning attacks where malicious participants can submit altered updates that affect global model performance. Current systems also provide limited mechanisms for ensuring participant trust, lack unchangeable audit records, and rely heavily on centralized aggregation servers, raising security and reliability concerns. These issues reduce current systems' effectiveness in healthcare settings where privacy, transparency, accountability, and protection against attacks are crucial. Thus, a secure framework is needed to enhance verification, build trust, and improve security in collaborative healthcare learning systems.

IV. PROPOSED METHODOLOGY

1. Project Framework and Core Components

By combining Federated Learning (FL), Secure Multi-Party Computation (SMPC), and Blockchain Technology, the

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

suggested solution aims to create a safe and private healthcare collaborative learning environment. Healthcare organizations can collaborate to develop machine learning models without directly exchanging private patient data thanks to the platform.

The system's major goal is to improve healthcare AI security by thwarting poisoning assaults while upholding openness and privacy. Blockchain technology keeps unchangeable records of system activity, SMPC-based verification validates local model modifications, and Federated Learning facilitates cooperative training. Hospitals can safely engage in joint intelligence development while maintaining patient confidentiality thanks to this integration, which establishes a reliable environment.

2. Multi-Layer Secure Verification Framework

The proposed methodology adopts a multi-stage workflow to improve security and reliability.

Stage 1: Registration and Authentication of Healthcare Institutions

Healthcare organizations that participate register with the platform and are issued secure authentication credentials. Each institution serves as a federated client and trains its own local model.

This phase guarantees entry to the collaborative learning space only to authorized users.

Stage 2: Training of Local Model

Healthcare institutions train machine learning models on their own systems, using their own patient data. Raw healthcare data never leaves the organization, nor the organization.

The output is only the model parameters or model updates, for collaborative processing.

This stage guarantees:

- Patient confidentiality protection
- Reduced risk of data leakage
- Addressing health care security needs

Stage 3: Model Verification with SMPC

This step is the main security part of the framework.

Local updates are verified by an SMPC-based verification mechanism prior to model aggregation. The verification module is used to identify suspicious or manipulated model updates received from malicious participants.

The verification process is complete:

- Validate model update
- Suspicious update detection
- Preventing poisoning attacks
- Confirm secure contribution

Only verified updates are passed to aggregation.

Stage 4: Federated Aggregation and Blockchain Logging

The global health care model is developed by combining the verified updates using the Federated Averaging (FedAvg) methods.

Blockchain technology also logs:

- Variations of federated learning

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

- Verification results
- Global model building activities
- History of activity for participants

This will increase transparency, accountability and trust between the health care institutions involved.

3. System Functional Components

The proposed framework consists of the major operational modules:

Authentication Module

- Login for users and approval of participants

Health Care Client Management Module

- Registration and monitoring of healthcare institutions

Module for Federated Learning

- Training a local model and aggregating collectively

SMPC Verification Module

- Detection of poisoning attack and model validation

Module for Blockchain Logging

- Immutable event recording and audit trailing

Dashboard & Monitoring Module

- Healthcare collaboration analytics and system monitoring

4 . DATABASE DESIGN

In the proposed system, the database design is crucial for supporting blockchain event trackin g, federated learning activities, healthcare coll aboration, and verification procedures. The database is built to provide data consisten cy, safe storage, and effective retrieval of infor mation needed for system functions.
For prototype development, the suggested fra mework makes use of a relational database str ucture that is implemented using SQLite.
The database is made up of several linked tabl es that support various system functional comp onents.

User Table: Holds user identification informat ion for safe system access, including user ID, username, email address, password, and access role**.**

Healthcare Client Table:

Information regarding participating healthcare facilities, such as institution ID, organization n ame, registration data, and participation statusi s kept up to date in the Healthcare Client Table

Federated Round Table:

Holds data from collaborative learning rounds including round ID, clients involved, training s tate, and aggregation specifics.

Verification Table:

Keeps track of accepted or rejected model upd ate records and SMPC-
based verification results.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

Global Model Table:

After federated learning is finished, tableholds data about aggregated global machine learning models.

Blockchain Event Log Table:

Preserves unchangeable records of system audi t data, federated learning activities, verificatio n events, and aggregation results.

The database design guarantees scalability for future improvements and practical implementa tion while promoting privacy protection, trans parency, traceability, and safe collaborative he althcare intelligence.

5. STRATEGY FOR TECHNICAL ARCHITECTURE AND IMPLEMENTATION

System Architecture

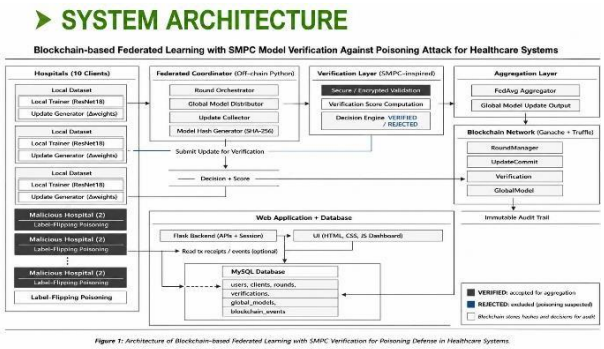


Figure 1: Architecture of Blockchain-based Federated Learning with SMPC Verification for Poisoning Defense in Healthcare Systems

A modular design is used in the suggested system to increase security and scalability.

Component	Technology	Purpose
Frontend	HTML, CSS, JavaScript	User interaction and dashboard
Backend	Python Flask	Business logic and workflow processing
Database	SQLite	Data storage and management
Machine Learning	Federated Learning	Collaborative model training
Security Layer	SMPC Verification	Secure model validation
Blockchain Layer	Blockchain Logging	Transparency and auditability

Algorithm

The suggested method uses a structured algorithm to carry out collaborative learning in healthcare settings in a safe and private manner. To facilitate local model training, model update verification, poisoning attack detection, global model aggregation, and secure event recording, the framework combines Federated Learning, Blockchain technology, and Secure Multi-Party Computation (SMPC)-based verification. The algorithm starts with the development of a federated learning round after user identification and healthcare institution registration. Using internal datasets, healthcare participants train local models and submit model updates for validation. Before aggregation, harmful or suspicious updates are detected via SMPC-based verification. The global model is created by combining verified model updates using the Federated Averaging (FedAvg) method, and blockchain recording documents significant system operations for auditability and transparency. This algorithmic method enhances security against poisoning and preserves privacy.

Experimental Result & Analysis:

Figure 1: Interface for User Registration To gain safe access to the system, users can create an account through the User Registration Interface. Users input the necessary information for registration and authentication. The page guarantees a safe and simple onboarding process for users.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

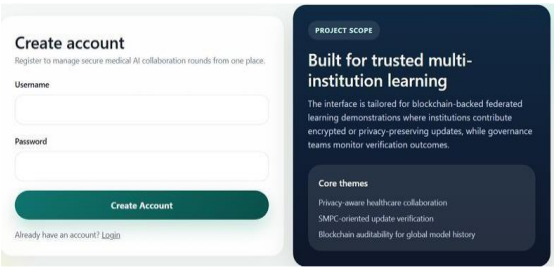


Figure 2: Dashboard

The Flask-based healthcare application's primary user interface is the Dashboard. Users can monitor system activity, view results, and organize training rounds. To guarantee safe and open healthcare collaboration, the platform makes use of blockchain logging and SMPC certification.

Figure 3: Predicting Images

For the purpose of validation and analysis, the Image Prediction module determines the most likely source of an input medical image collection. It facilitates dataset consistency checks and aids in the classification of medical image categories. This enhances the precision and dependability of healthcare data processing.

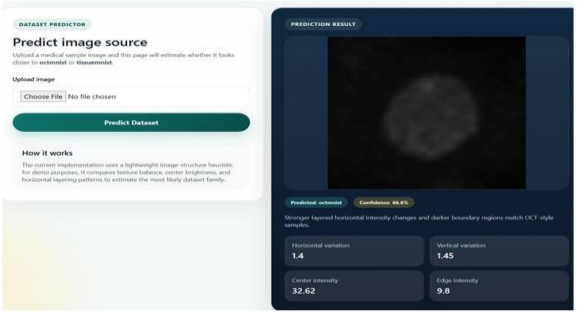
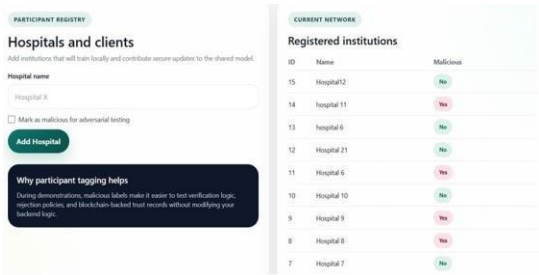


Figure 4: Registry of Participants

Healthcare organizations taking part in the federated learning system are managed by the Participant Registry. Users can add participants and keep an eye on their activity. The module facilitates coordinated and safe network communication.



IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2026

DOI: 10.17148/IARJSET.2026.13586

V. CONCLUSION AND FUTURE WORK

A safe and private foundation for cooperative healthcare intelligence is offered by the suggested Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems. Healthcare organizations can create machine learning models without disclosing private patient data because to the system's integration of Federated Learning, Secure Multi-Party Computation (SMPC), and Blockchain technology. While blockchain guarantees openness and auditability, the verification mechanism aids in identifying malicious changes and strengthens defence against poisoning assaults. The created framework is appropriate for secure healthcare artificial intelligence systems since it enhances security, privacy, and trust.

Future Work

For practical implementation, the suggested system can be expanded by incorporating actual hospital datasets and extensive healthcare networks. Stronger poisoning attack detection methods and sophisticated cryptographic verification procedures might enhance security even more. Cloud deployment, smart contract integration, support for deep learning frameworks like TensorFlow and PyTorch, and switching to scalable databases like MySQL or PostgreSQL are further potential future improvements. The system may become more effective, scalable, and appropriate for practical healthcare applications as a result of these enhancements.

REFERENCES

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proceedings of Artificial Intelligence and Statistics (AISTATS)*, 2017.

[2] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marce done, H. B. McMahan, S. Patel, and K. Seth, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2017.

[3] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. Bhagoji, and S. Zhao, "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[5] 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.