International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 06-02-2026 Accepted: 13-03-2026 Published: 20-03-2026

BLOCKCHAIN-BASED FEDERATED LEARNING WITH SMPC MODEL VERIFICATION AGAINST POISONING ATTACK FOR HEALTHCARE SYSTEMS

[1]G. NAGAPPA, [2]JALVADI RAJASEKAR, [3]SANJANOLLA SRIRAM, [4]M SUBASH
[1]Associate Professor, [234]Student
DEPT OF CSE
St.Johns College of Engineering and Technology (Affiliated by JNTUA)
nagappasgcsesjcet@gmail.com, rajashekarj2026@gmail.com, ramusriramu0@gmail.com, mandesubash2550@gmail.com

ABSTRACT

Due to the rising awareness of privacy and security in machine learning applications, federated learning (FL) has received widespread attention and applied to several areas, e.g., intelligence healthcare systems, IoT-based industries, and smart cities. FL enables clients to train a global model collaboratively without accessing their local training data. However, the current FL schemes are vulnerable to adversarial attacks. Its architecture makes detecting and defending against malicious model updates difficult. In addition, most recent studies to detect FL from malicious updates while maintaining the model's privacy have not been sufficiently explored. This paper proposed blockchain based federated learning with SMPC model verification against poisoning attacks for healthcare systems. First, we check the machine learning model from the FL participants through an encrypted inference process and remove the compromised model. Once the participants' local models have been verified, the models are sent to the blockchain node to be securely aggregated. We conducted several experiments with different medical datasets to evaluate our proposed framework.

I. INTRODUCTION

The Internet of Things (IOT) has been applied in various services, including the healthcare domain. The integration of IOT in the healthcare system is also known as the Internet of Medical Things (IOMT). With the development of IOMT, many healthcare devices are interconnected, allowing devices to exchange information among medical experts and Artificial Intelligence (AI) based services. This interconnectivity helps healthcare industries like hospitals to improve the efficiency and quality of their services. In the medical diagnosis field, medical imaging devices facilitate the process of early diagnosis and treatment for medical staff.

Due to this interconnectivity, medical image retrieval is made easy, resulting in extensive data with wide variations. Consequently, medical image analysis has become a challenging task for medical experts and is prone to human error. In recent years, the success of Deep Learning (DL) in computer vision tasks has provided a significant breakthrough in medical image classification tasks. Several studies of DL in medical imaging fields have shown promising results by providing accurate and efficient diagnoses [1].

As shown in Figure 1, cloud computing is one paradigm that emerged to solve the availability of computing and storage resources. Therefore, the cloud is usually used to deploy the DL model for training and data inference. However, sending the raw data from the IOMT cluster to the cloud will be very expensive. This is where edge computing, like edge servers, will be advantageous to process the data before sending it to the cloud.

It is known that a high-performing Deep Learning (DL) model requires a large and diverse dataset for its training. This large-scale dataset is often obtained from multi-institutional or multi-national data accumulation and voluntary data sharing in the healthcare industry. While massive data collection is essential for the deep learning process, sharing patients' data raises privacy concerns and relative regulations such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA). Due to the rising concerns, healthcare institutions may be prevented from sharing their medical datasets. In some cases where sharing is possible, some restrictions are applied, resulting in inadequate data sharing.

In recent studies, [2] proposed a federated learning model that allows parties to collaboratively train a model by sharing local model updates with a parameter server. Intuitively, this method is safer than centralized training because machine learning models learn from healthcare IOMT data without relying on a third-party cloud to hold their data [3]. However, federated learning also presents some challenges that may limit its applications in real-world case scenarios. For example, federated learning remains vulnerable to various attacks that may result in leakage of private data [4] or poisoned learning model [5]. Also, the participants in the current FL setup cannot verify the authenticity of the machine learning model. To protect FL participants' privacy, the existing defense method mainly focuses on ensuring the confidentiality of the machine learning gradients. Differential Privacy (DP) [6], [7] is one of the commonly used methods to preserve the privacy of the learning model. Adding DP to a federated learning scenario can improve the privacy of the participants models. However, adding noise into machine learning gradients will reduce the learning model accuracy [7]. DP is also ineffective in mitigating poisoning attacks while maintaining model performance resulting in a faulty global model. To tackle the poisoning attack, existing research on anomaly detection [8],[9] has been explored. However, the existing methods cannot eliminate all the poisoned models and cause the accuracy of the global model to be reduced. Also, they perform the anomaly detection method in a plaintext model. This will lead to another issue where the attacker can perform a parameter stealing attack [10] and a membership inference attack [11]. Thus, a verifiable and secure anomaly detection method for federated learning scenarios is needed.

This paper proposes a privacy-preserving verification method to eliminate poisoned local models in a federated learning scenario. The proposed method eliminates the compromised local model while guaranteeing the privacy of the local model's parameters using an SMPC-based encrypted inference process. Once the local model is verified, the verified share of the local model is sent to the blockchain for the aggregation process. SMPC-based aggregation is used to perform the secure aggregation between the blockchain and the hospital. After the aggregation process, the global model is stored in tampered-proof storage. Later, each hospital receives the global model from the blockchain and verifies the authenticity of the global model. The contributions of our work are summarized as follows:

_ Propose a new block chain-based federated learning architecture for healthcare systems to ensure the security of the global model used for classifying disease.

_ Design a privacy-preserving method for local model anomaly detection in a Federated learning scenario with SMPC as the underlying technology. Our encrypted model verification method eliminates the poisoned model while protecting the local model privacy from membership inference attacks and parameter stealing.

_ Propose an SMPC-based secure aggregation in the block chain as a platform to decentralize the aggregation process.

_ We present a verifiable machine learning model for federated learning participants using block chain in the IOMT scenario.

PROBLEM SCENARIO AND DESIGN GOALS

A. Problem Scenario

To discuss and highlight the current issues with current federated learning, we use an IOMT-enabled hospital scenario (see Fig. 2). Assume that several smart hospitals are placed in different regions with varying patient demographics and diseases. Each smart hospital is equipped with a cluster of IOMT devices. The IOMT devices will be used to scan the patient to detect a severe disease. In The current IOMT scenario, IOMT devices will act as data sources since the IOMT devices are resource-constrained and cannot perform any machine learning algorithm. Hence, each hospital has an edge server with computing resources to execute the machine learning tasks using the local datasets. Nevertheless, due to dataset limitations, the machine learning model accuracy generated from the local datasets is relatively low. Therefore the edge server from each hospital participates in the federated learning platform. In the federated learning platform, locally trained models from the hospital's edge server are collected and aggregated to produce a highly accurate machine learning model without sending private datasets to the cloud provider. Later, the aggregated or global model is sent back to the edge server for another round of federated learning processes. Once

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 06-02-2026 Accepted: 13-03-2026 Published: 20-03-2026

the global model reaches the desired accuracy, it will be used to recognize the disease more accurately.

II. LITERATURE SURVEY

"Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application,"

L. Sun, X. Jiang, H. Ren, and Y. Guo,

With the booming development of medical informatization and the ubiquitous connections in the fifth generation mobile communication technology (5G) era, the heterogeneity and explosive growth of medical data have brought huge challenges to data access, security and privacy, as well as information processing in Internet of Medical Things (IoMT). This article provides a comprehensive review of how to realize the timely processing and analysis of medical big data and the sinking of high-quality medical resources under the constraints of the existing medical environment and medical-related equipment. We mainly focus on the advantages brought by the cloud computing, edge computing and artificial intelligence technologies to the IoMT. We also explore how to rationalize the use of medical resources and the security and privacy of medical data, so that high-quality medical services can be provided to patients. Finally, we discuss the current challenges and possible future research directions in the edge-cloud computing and artificial intelligence related IoMT.

"On the convergence of fedavg on non-iid data,"

X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang,

Federated learning enables a large amount of edge computing devices to jointly learn a model without data sharing. As a leading algorithm in this setting, Federated Averaging (FedAvg) runs Stochastic Gradient Descent (SGD) in parallel on a small subset of the total devices and averages the sequences only once in a while. Despite its simplicity, it lacks theoretical guarantees under realistic settings. In this paper, we analyze the convergence of FedAvg on non-iid data and establish a convergence rate of O(1 T) for strongly convex and smooth problems, where T is the number of SGDs. Importantly, our bound demonstrates a trade-off between communication-efficiency and convergence rate. As user devices may be disconnected from the server, we relax the assumption of full device participation to partial device participation and study different averaging schemes; low device participation rate can be achieved without severely slowing down the learning. Our results indicates that heterogeneity of data slows down the convergence, which matches empirical observations. Furthermore, we provide a necessary condition for FedAvg on non-iid data: the learning rate η must decay, even if full-gradient is used; otherwise, the solution will be $\Omega(\eta)$ away from the optimal.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

In FL, data privacy is achieved by sending the model to the client and performing local training. Later, the locally trained model will be collected by the central server and aggregated into a global model. With this method, the participants only shared the local model and did not send any datasets. However, FL itself is not sufficient to provide a privacy guarantee. Some research has been performed to secure the FL architecture. The author in [6] and [7] enhance the data privacy in FL with differential privacy (DP) by adding noise in the local datasets. In [7], also anonymize the end-user by adding a proxy server. However, the experiment result show there is a significant accuracy reduction. This privacy-preserving method is unsuitable for FL in healthcare systems since accuracy is essential for the inference process.

Zhang et al. [13] use fully homomorphic encryption (FHE) to perform aggregation and training processes by performing a batch encryption method. However, all the homomorphic encryption methods are unusable for healthcare scenarios since the training process takes significant time. Authors in [14], [15], and [16] have successfully performed an adversarial attack on FL architecture. The authors have demonstrated a poisoning attack on the local client's datasets. The poisoned model will be generated and impact the global model. Based on the existing attack, DP and FHE method is insufficient against the poisoning attack. In [17], the author proposed a privacy-enhanced FL against poisoning adversaries. To secure the machine learning model, they encrypt the model using linear homomorphic encryption. Since they encrypt the model from the first round of FL, the training process will take longer than regular machine learning. After the participants finish the encrypted training process, The local model will send to the server for encrypted aggregation. Based on the results of their experiments, their aggregation method reduces the accuracy of the machine learning model.

Blockchain is known for its immutability and is used for tampered-proof storage. The use of blockchain can track the local or global model for audibility purposes. Combining blockchain with FL can ensure the machine learning model's integrity. Author in [18] proposed verifiable aggregation for FL. Their method follows the concept of blockchain, where they use the hash to compute the digest for verification. Nonetheless, the aggregation and hashing process is performed on a single server. The correct utilization of blockchain technology can overcome the problem. In tackling the issue, [19] proposed decentralized privacy using blockchain-enabled FL. They use blockchain to store and verify the model using cross-validation, but the participant is connected to the same blockchain. In their framework, the participant can use other's local models, which leads to privacy issues.

The work on [20] uses a smart contract to verify the global model. The use of smart contracts can audit the authenticity of the global model. However, they did not perform any checks on the local or global model. Also, the local model is not sent to the blockchain, and not possible to perform any audit process. From the proposed work, they can not handle any poisoning attack.

Disadvantages

- The system didn't implement a verifiable Federated Learning (FL) scenario that leverages SMPC to perform an encrypted local model verification process and secure aggregation on the blockchain node.

- The federated learning scenario not allows each participant to collaboratively train the machine learning model locally with their local datasets. Later the machine learning model will send to the cloud for the model aggregation process.

PROPOSED SYSTEM

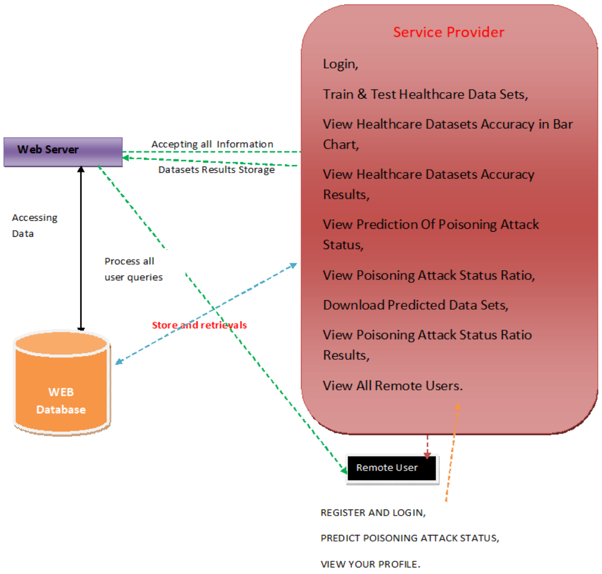
The system proposes a privacy-preserving verification method to eliminate poisoned local models in a federated learning scenario. The proposed method eliminates the compromised local model while guaranteeing the privacy of the local model's parameters using an SMPC-based encrypted inference process. Once the local model is verified, the verified share of the local model is sent to the blockchain for the aggregation process. SMPC-based aggregation is used to perform the secure aggregation between the blockchain and the hospital. After the aggregation process, the global model is stored in tampered-proof storage. Later, each hospital receives the global model from the blockchain and verifies the authenticity of the global model

Advantages

- Propose a new blockchain-based federated learning architecture for healthcare systems to ensure the security of the global model used for classifying disease.

  Design a privacy-preserving method for local model anomaly detection in a Federated learning scenario with SMPC as the underlying technology. Our encrypted model verification method eliminates the poisoned model while protecting the local model privacy from membership inference attacks and parameter stealing.
- Propose an SMPC-based secure aggregation in the blockchain as a platform to decentralize the aggregation process.
- We present a verifiable machine learning model for federated learning participants using blockchain in the IoMT scenario.

IV. SYSTEM ARCHITECTUTRE


Service Provider
Login,
Train & Test Healthcare Data Sets,
View Healthcare Datasets Accuracy in Bar Chart,
View Healthcare Datasets Accuracy Results,
View Prediction Of Poisoning Attack Status,
View Poisoning Attack Status Ratio,
Download Predicted Data Sets,
View Poisoning Attack Status Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT POISONING ATTACK STATUS,
VIEW YOUR PROFILE.

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 06-02-2026 Accepted: 13-03-2026 Published: 20-03-2026

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Train & Test Healthcare Data Sets, View Healthcare Datasets Accuracy in Bar Chart, View Healthcare Datasets Accuracy Results, View Prediction Of Poisoning Attack Status,View Poisoning Attack Status Ratio, Download Predicted Data Sets, View Poisoning Attack Status Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT POISONING ATTACK STATUS, VIEW YOUR PROFILE.

V. CONCLUSION

This paper proposes block chain-based federated learning with a secure model verification for securing healthcare systems. The main objective is to ensure the local model is poisoned-free while maintaining privacy and providing verifiability for the federated learning participants.

In this framework, we perform a privacy-preserving verification process on the local model before the aggregation process. To preserve privacy on the local model, the verification is performed through an encrypted inference supported by SMPC protocol. This method allows the verifier to check the model with encrypted models and images. Once the local model is verified, the verified share of the local model is sent to the block chain node. Block chain and the hospital will perform SMPC-based secure aggregation. Once the majority of nodes have the same result, the global model is stored in the block chain. Later, the tamper-proof storage will distribute the updated global model to every hospital that joins the federated learning round.

In the experiment, we use Convolutional Neural Network (CNN) based algorithms with several medical datasets to generate local models and aggregate them under FL settings. Our experiment results show that the model encrypted verification process can eliminate all the participants' poisoned models while maintaining the privacy of the local model. In addition, we can recover up to 25% for the global model accuracy. It is essential to mention that our secure inference processing time is almost similar to the original inference process.

In the future, we plan to develop an efficient consensus mechanism for block chain-based aggregation. In this paper, we assume that all hospitals use the homogeneous model and use the same setup to generate their respective local models. However, we plan to broaden our work in the future to support a heterogeneous model in block chain-based federated learning.

REFERENCES

[1] Babburi, S. (2025). Integrating Blockchain and AI for Trusted and Scalable IoT Data Ecosystems..

[2] Banda Saikumar. (2025). Integrating azure network rules for storage account through terraform in CI/CD pipelines: automating storage account access restrictions to public IP. Journal of Scien+B112ce &amp; Technology, 10(2), 15–22. https://doi.org/10.46243/jst.2025.v10.i02.pp15-22.

[3] Prodduturi, S. M. K. (2025). Opportunities and Challenges for iOS Developers in Exploring the Integration of Augmented Reality Technologies. International Journal of Engineering Science and Advanced Technology (IJESAT), 25(4), 200-207.

[4] Gaddam, S. (2024). Integrating machine learning models with continuous integration and continuous delivery (CI/CD) pipelines for a learning-driven approach to software engineering.

[5] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," Future Generation Computer Systems, vol. 115, pp. 619–640, 2021.

[6] Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic

Received: 06-02-2026 Accepted: 13-03-2026 Published: 20-03-2026

Analysis. Journal of Computational Analysis & Applications, 35(1).

[7] Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s), 1270–1285. https://doi.org/10.12732/ijam.v38i4s.685.

[8] Todupunuri, A. (2024). Develop Machine Learning Models to Predict Customer Lifetime Value for Banking Customers, Helping Banks Optimize Services. International Journal of All Research Education &amp; Scientific Methods, 12(10), 1254–1259. https://doi.org/10.56025/ijaresm.2024.1210241254.

[9] Ganji, M. (2025). Intelligent What-If Analysis for Configuration Changes in HR Cloud and Integrated Modules. International Journal of All Research Education and Scientific Methods, 13(04), 4828–4835. https://doi.org/10.56025/ijaresm.2025.1304254828.

[10] Todupunuri, A. (2023). The Role of Artificial Intelligence in Enhancing Cybersecurity Measures in Online Banking Using AI. International Journal of Enhanced Research in Management &amp; Computer Applications, 12(01), 103–108. https://doi.org/10.55948/ijermca.2023.01015.

[11] Reddy, S. K. R. (2025). Tailoring Loyalty Rewards Systems across Industries: Cloud vs On-Prem Solutions. International Journal of All Research Education and Scientific Methods (IJARESM).

[12] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, “Data poisoning attacks against federated learning systems,” in European Symposium on Research in Computer Security. Springer, 2020, pp. 480–501.

[13] The Future of Conversational AI in Banking: A Case Study on Virtual Assistants and Chatbots*: Exploring the Impact of AIPowered Virtual Assistants on Customer Service Efficiency and Satisfaction. (2024). International Research Journal of Economics and Management Studies, 3(10). https://doi.org/10.56472/25835238/irjems-v3i10p124.

[14] Poojari, R. (2025). A Comparative Analysis of Fine-Tuning Versus Retrieval-Augmented Approaches for Enhancing Healthcare-Centric Large Language Models.

[15] Kalae, U. K. (2021). Enhancing data analytics and reporting efficiency using Power BI and SQL in cloud computing environments. Journal of Computational Analysis and Applications, 29(6), 2021. https://doi.org/10.48047/jocaaa.2021.29.06.48.

[16] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, “How to backdoor federated learning,” in International Conference on Artificial Intelligence and Statistics. PMLR, 2020, pp. 2938–2948.