International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 24 Issue 12, DEC, 2024

Secure Blockchain Federated Learning to Prevent Poisoning Attacks in Healthcare Systems

Nayakanti Parimala
M.Tech Student, Department of Computer Science and Engineering
Samual George Institute of Engineering and Technogy, Markapuram, Andhra Pradesh, India.

Dr. P.P Sadu Naik
Professor, Department of Computer Science and Engineering
Samual George Institute of Engineering and Technogy, Markapuram, Andhra Pradesh, India.

***Abstract*—In healthcare systems, safeguarding machine learning (ML) models from adversarial threats while preserving data privacy is crucial. Federated Learning (FL) allows institutions to collaboratively train models without sharing sensitive patient data, offering a privacy-preserving solution. However, FL remains susceptible to poisoning attacks, where adversaries inject malicious data to compromise model performance. To address this, a robust framework that integrates blockchain technology with Secure Multi-Party Computation (SMPC) is proposed to enhance model security and verification. Blockchain provides a decentralized, immutable ledger that ensures transparency, accountability, and traceability of model updates. It prevents tampering by securely recording each participant's contributions in the FL process. SMPC further enhances security by enabling participants to collaboratively compute global model parameters without exposing individual data. This combined approach ensures that model updates remain encrypted and verifiable, preventing unauthorized access or manipulation. The method enhances the detection and prevention of poisoning attacks by validating and securely aggregating model updates before inclusion in the global model. Experimental evaluations on healthcare datasets demonstrate that this system improves model robustness, accuracy, and trustworthiness. This novel framework provides a highly secure, privacy-preserving solution for federated learning in healthcare, ensuring data integrity, model reliability, and resilience against adversarial attacks.**

***Keywords*—Federated Learning (FL), Blockchain Secure Multi-Party Computation (SMPC), Poisoning Attacks, Healthcare Data Security**

I. INTRODUCTION

The integration of blockchain technology within healthcare systems has emerged as a pivotal innovation aimed at enhancing data security, privacy, and interoperability. As healthcare increasingly relies on digital platforms for managing sensitive patient information, the potential vulnerabilities associated with data breaches and unauthorized access have become paramount concerns. Blockchain, characterized by its decentralized and immutable nature, offers a robust framework that can address these challenges effectively [1][2][3]. By facilitating secure data sharing and ensuring the integrity of electronic health records (EHRs), blockchain technology presents a transformative opportunity to safeguard patient data against malicious attacks, including poisoning attacks that can compromise the integrity of federated learning systems [4][5].

Federated learning, a machine learning paradigm that enables collaborative model training without centralizing data, is particularly susceptible to various security threats, including data poisoning. In healthcare, where data integrity is crucial for accurate diagnostics and treatment, the implications of such attacks can be dire. The incorporation of blockchain technology into federated learning frameworks can mitigate these risks by providing a transparent and verifiable ledger of transactions, thereby enhancing trust among participating entities [6][7]. This synergy not only fortifies the security of healthcare data but also promotes a more patient-centric approach to data management, where patients retain control over their health information while benefiting from advanced analytics and machine learning capabilities [8][9].

Moreover, the implementation of permissioned blockchain systems, as opposed to public block chains, further enhances security by restricting access to authorized participants only. This is particularly relevant in healthcare settings where sensitive data must be protected from unauthorized access while still allowing for necessary data sharing among healthcare providers [1][6][10]. The potential for blockchain to streamline interoperability across disparate healthcare systems is also noteworthy, as it can facilitate seamless data exchange while maintaining stringent security protocols [11][12]. Thus, the intersection of secure blockchain technology and federated learning not only addresses the immediate threats posed by data poisoning but also lays the groundwork for a more resilient and efficient healthcare ecosystem.

In conclusion, the adoption of secure blockchain federated learning in healthcare systems represents a significant advancement in the fight against data breaches and integrity threats. By leveraging the unique properties of blockchain, healthcare organizations can enhance the security and privacy of patient data while fostering a collaborative environment for data-driven innovations. This approach not only protects against current threats but also positions the healthcare sector to better adapt to future challenges in data management and security.

II. RELATED WORKS

The advent of blockchain technology has sparked significant interest in its application within the healthcare sector, primarily due to its potential to enhance data security, interoperability, and patient privacy. A systematic review by Agbo et al. highlights the multifaceted benefits of blockchain in healthcare, emphasizing its ability to create secure and immutable records, thereby addressing critical issues related to data integrity and unauthorized access Agbo et al. [13]. The decentralized nature of blockchain allows for a more patient-centric approach to data management, where individuals can have greater control over their health

information while ensuring that sensitive data is securely shared among authorized parties [14].

Moreover, the integration of blockchain with health information exchanges (HIE) has been identified as a promising avenue for improving data sharing practices among healthcare providers. Drosatos and Kaldoudi's scoping review indicates that blockchain can facilitate the creation of patient record ledgers that are accessible across various healthcare providers, thus enabling a comprehensive view of a patient's medical history [15]. This capability is crucial in addressing the fragmentation of health records, which often leads to inefficiencies and potential errors in patient care [16]. Furthermore, the implementation of blockchain technology can mitigate risks associated with data breaches, as it employs cryptographic techniques to secure health information, thereby enhancing overall data privacy [17].

Despite the promising prospects, the adoption of blockchain in healthcare is not without challenges. Issues such as scalability, regulatory compliance, and the need for standardized protocols remain significant barriers to widespread implementation [18] [19]. For instance, while blockchain can enhance security, the complexity of its architecture may lead to increased transaction times, which can hinder its effectiveness in real-time healthcare applications [20]. Additionally, healthcare organizations must navigate the ethical implications of using blockchain, particularly concerning patient consent and data ownership [21].

Recent literature also emphasizes the importance of interoperability in the successful deployment of blockchain technology in healthcare. Aljabri's systematic review underscores the need for blockchain systems to be compatible with existing healthcare infrastructures to facilitate seamless data exchange [18]. This interoperability is vital for ensuring that blockchain can effectively integrate with various health information systems and support collaborative care models [22].

III. Methodology

The proposed methodology focuses on integrating blockchain technology with Secure Multi-Party Computation (SMPC) to create a robust and privacy-preserving federated learning framework for healthcare systems. The framework is designed to address vulnerabilities in federated learning, particularly susceptibility to poisoning attacks, while ensuring that sensitive patient data remains secure. Blockchain provides a decentralized, immutable ledger for recording model updates, ensuring transparency and accountability throughout the training process. Meanwhile, SMPC enables secure computation of global model parameters by encrypting contributions from each participant, preserving data privacy. Together, these technologies form a comprehensive defense mechanism that prevents data tampering and ensures the integrity of the global model, while also facilitating effective detection and mitigation of adversarial attacks.

A. System Architecture

The proposed system architecture integrates blockchain, federated learning (FL), and Secure Multi-Party Computation (SMPC) to enhance security, privacy, and model robustness in healthcare environments. The framework enables multiple healthcare institutions to collaboratively train machine learning models without exposing sensitive patient data. Each participant performs local model training on its private dataset, and only the model updates (not the data itself) are shared. These updates are encrypted and then sent for secure aggregation using SMPC. The aggregated model is stored on a blockchain, ensuring transparency, traceability, and tamper-resistant validation of contributions.

1) Blockchain

Blockchain acts as a decentralized ledger, recording all model updates and verification steps in a secure and immutable manner. Each block contains encrypted model parameters and cryptographic signatures, ensuring that updates are auditable and preventing tampering. The consensus mechanism ensures that only validated and trusted model updates are added to the global model, enhancing security.

2) Federated Learning (FL)

FL allows participants to collaboratively train a machine learning model without sharing raw data. Each participant trains a local model using their own dataset, and only model gradients or parameters are shared. This decentralized approach helps maintain data privacy, as sensitive information never leaves the local environment.

3) Secure Multi-Party Computation (SMPC)

SMPC ensures that participants can jointly compute a global model by securely aggregating their encrypted local model updates. The use of SMPC guarantees that no participant can infer the data of others during the computation process. This prevents data leakage and ensures that privacy is maintained throughout the learning process.

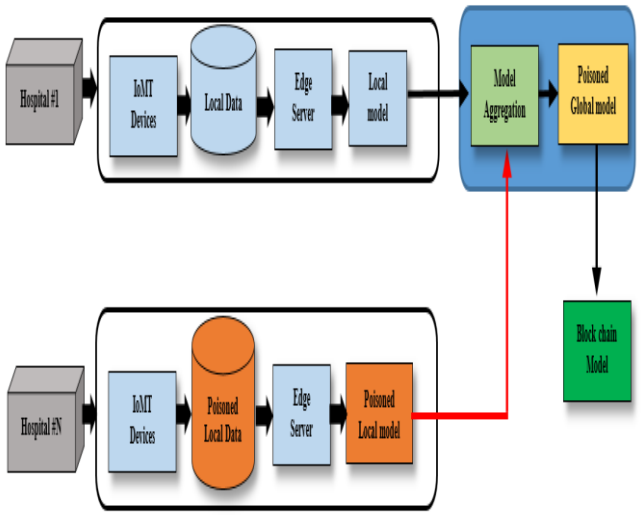

Fig. 1. Architecture of the proposed model

B. Data Privacy and Security Mechanisms

1) Data Partitioning and Local Model Training

In the proposed framework, data privacy is preserved through federated learning, where each healthcare institution retains its own patient data locally. Instead of sharing raw data, participants partition their datasets and independently train local machine learning models. These models are

trained on institution-specific data, ensuring that sensitive patient information is never exposed or transmitted to other parties. Once local training is complete, only the model updates (such as gradients or weights) are shared for aggregation. This decentralized approach protects patient privacy and complies with data protection regulations, such as HIPAA or GDPR.

2) Use of SMPC for Secure Computation

Secure Multi-Party Computation (SMPC) is employed to further protect the confidentiality of model updates. SMPC enables participants to jointly compute the global model by aggregating their encrypted updates without revealing any individual model's information. Each participant encrypts their local model parameters before sharing them, and the aggregation is performed on the encrypted data. The SMPC protocol ensures that no participant can access or infer the others' data contributions during the computation. This guarantees that model updates are securely aggregated, and the global model is computed without compromising privacy.

3) Encryption and Privacy-Preserving Techniques

Encryption plays a critical role in ensuring the confidentiality of the data exchanged during the federated learning process. Before sharing model updates, participants encrypt their data using advanced cryptographic techniques, such as homomorphic encryption or secret sharing, to ensure that updates remain private. These privacy-preserving techniques prevent unauthorized access or inference attacks on the shared model parameters. Additionally, differential privacy can be applied to further enhance security by adding noise to the model updates, making it difficult to reverse-engineer the original data. This multi-layered approach ensures robust privacy protection throughout the entire learning process.

C. Blockchain Integration for Model Verification

1) Decentralized Ledger Design

The proposed framework leverages a decentralized ledger design through blockchain technology to enhance model verification and integrity. This design ensures that all participants have access to the same immutable record of model updates, promoting transparency and trust among stakeholders. Each transaction recorded on the blockchain represents a model update, complete with timestamps and cryptographic signatures that authenticate the source. By distributing the ledger across all participants, the framework eliminates single points of failure, making it resilient against tampering and ensuring that the model's integrity can be verified by all parties involved.

2) Recording and Validating Model Updates

Model updates are recorded on the blockchain in a structured manner, ensuring that each update is linked to the corresponding participant's cryptographic identity. This approach not only provides a clear audit trail but also enables real-time validation of contributions. When a participant submits a model update, it is hashed and added to a new block on the blockchain. The system employs cryptographic algorithms to verify the authenticity of each update before it is recorded. This validation process ensures that only legitimate and approved updates are incorporated into the global model, safeguarding against unauthorized modifications and enhancing the overall reliability of the federated learning process.

3) Consensus Mechanism for Secure Model Aggregation

To maintain the integrity of the model updates, the framework employs a consensus mechanism that ensures all participants agree on the state of the blockchain before any new updates are added. This mechanism can utilize various algorithms, such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT), to reach a consensus on the validity of model updates. Once consensus is achieved, the model updates are securely aggregated and committed to the blockchain. This process not only enhances the security of model aggregation but also ensures that all stakeholders are in agreement, thereby fostering a collaborative environment that mitigates the risk of adversarial attacks. Through this robust consensus mechanism, the framework maintains the integrity and accuracy of the global model while providing a transparent record of all contributions.

D. Poisoning Attack Detection and Prevention

1) Adversarial Threat Model

In the context of the proposed framework, the adversarial threat model encompasses various types of poisoning attacks that target the federated learning process. These attacks can occur when malicious participants deliberately introduce harmful data into the training process to degrade the overall model performance or manipulate its behavior. The model is particularly vulnerable to these attacks due to the decentralized nature of federated learning, where updates from multiple participants are aggregated without strict oversight. This section defines the potential threat vectors, including data injection, model manipulation, and collusion among adversaries, and emphasizes the need for a comprehensive detection and prevention strategy.

2) Methods for Detecting Malicious Data Contributions

To identify malicious data contributions, the framework incorporates several detection methods aimed at monitoring and analyzing model updates from participants. These methods include anomaly detection algorithms that assess the statistical properties of model updates, identifying deviations from expected behavior. Techniques such as clustering and outlier detection can also be utilized to flag suspicious updates that may indicate poisoning attempts. Additionally, implementing a reputation-based system can help evaluate the trustworthiness of participants based on their historical contributions, allowing for the identification of potentially malicious actors before they compromise the model.

3) Techniques to Prevent and Mitigate Poisoning Attacks

To prevent and mitigate the impact of poisoning attacks, the framework employs a combination of proactive and reactive techniques. Proactively, it implements robust aggregation methods that reduce the influence of outlier updates, such as trimming or weighted aggregation based on participant reputation. These methods ensure that the final model remains resilient against potentially harmful contributions. Reactively, the framework includes mechanisms for incident response, such as reverting to a previous stable model version if a poisoning attack is detected. Regular audits of model performance and contributions, combined with continuous monitoring, allow

for swift identification and remediation of attacks. Together, these techniques create a multi-layered defense system that enhances the robustness and reliability of the federated learning process in healthcare environments.

E. Secure Aggregation of Model Updates

1) SMPC Protocol for Secure Aggregation

The proposed framework utilizes Secure Multi-Party Computation (SMPC) to enable secure aggregation of model updates from multiple participants. The SMPC protocol allows participants to collaboratively compute the global model parameters while keeping their individual contributions private. During this process, each participant encrypts their local model updates using a predetermined cryptographic method, ensuring that only the aggregated result is revealed. The protocol allows for computations to be performed on encrypted data, thus preventing any participant from accessing the unencrypted contributions of others. By utilizing SMPC, the framework enhances the security of the aggregation process and mitigates the risks associated with data leakage.

2) Steps for Encryption and Decryption

The encryption process involves several key steps to ensure that model updates remain confidential throughout the aggregation process. Initially, each participant applies a homomorphic encryption scheme or a secret-sharing method to their local model updates. This transforms the data into an encrypted format that can be securely shared. Participants then send their encrypted updates to a designated aggregator, which performs the necessary computations on the encrypted data. The aggregation process involves combining the encrypted updates to produce a single aggregated result. Once the aggregation is complete, the aggregator sends the resulting encrypted model parameters back to the participants. Finally, each participant decrypts the aggregated result using their decryption keys, enabling them to obtain the updated global model parameters without revealing their individual contributions.

3) Ensuring Accuracy and Integrity of the Global Model

To ensure the accuracy and integrity of the global model, the framework implements several validation mechanisms throughout the aggregation process. First, before the aggregation begins, participants are required to verify the integrity of the received updates using digital signatures, which authenticate the source of the updates. Additionally, the aggregation function is designed to be resilient against potential poisoning attacks, employing robust techniques such as trimmed mean or median aggregation to minimize the impact of outlier updates. After the aggregation, the updated global model undergoes a validation process where its performance is evaluated against a predefined set of metrics. This validation ensures that the new model parameters maintain or improve upon the model's accuracy. By implementing these measures, the framework guarantees that the final global model is both accurate and resilient, thereby upholding the trustworthiness of the federated learning process.

F. Experimental Setup Datasets and Evaluation Metrics

The experimental setup employs diverse healthcare datasets, including real-world patient records, medical imaging, and clinical trial data, to evaluate the proposed federated learning framework's effectiveness. These datasets are partitioned among multiple participants to simulate a federated learning environment, with evaluation metrics encompassing accuracy, precision, recall, F1-score, and robustness against poisoning attacks, as well as metrics for model convergence and computational efficiency. The implementation is developed in Python, utilizing libraries such as TensorFlow and PyTorch for model training, PyCryptodome for encryption, and Hyper Ledger Fabric for the blockchain component, which ensures a permissioned environment suitable for healthcare applications. The experimental testbed mimics a decentralized healthcare system, consisting of multiple nodes that represent different institutions, each configured with specific hardware and network parameters, such as bandwidth limitations and latency simulations. This comprehensive setup facilitates rigorous testing of the framework's performance, scalability, and resilience against adversarial attacks while ensuring secure aggregation of model updates.

G. System Architecture

1) Blockchain Layer

Decentralized Ledger: All model modifications are recorded in a decentralized, immutable ledger using a blockchain. Every healthcare organization that takes part functions as a node in a blockchain network.

Smart Contracts: The submission, verification, and aggregation of model updates are handled using smart contracts. They streamline the verification process and make sure everything is open and honest.

2) Federated Learning Layer

Local Training: A local model is trained on data from each healthcare entity. As a result, private patient information will remain on the premises of the company.

Model Updates: The process begins with local training, and afterward, every entity changes its model and adds it to the blockchain.

3) SMPC Layer

Secure Aggregation: Safely aggregating model updates from several sources is the goal of SMPC protocols. This allows for the calculation of a global model while ensuring that individual modifications stay secret.

Privacy Preservation: Ensuring data privacy, the aggregation procedure prevents any one entity from deducing other people's data.

H. Data Collection and Preprocessing

1) Data Sources

Gather healthcare datasets from several locations, including clinics and hospitals, to guarantee a varied and accurate representation of patient information.

2) Data Preprocessing

Make sure the data is compatible across multiple entities by standardizing and normalizing it. Take care of any data discrepancies or missing values.

I. Model Training and Aggregation

1) Local Model Training

Implement a standard machine learning algorithm (e.g., neural network) for training local models on each entity's data.

Optimize model hyper parameters to achieve the best performance for each local dataset.

Each healthcare entity iTrains a local model on its data. Let D_i represent the dataset of entity i. The objective is to minimize a local loss function. $L_i(\theta)$, where θ denotes the model parameters.

$$\theta_i^* = \arg\min_{\theta} L_i(\theta; D_i)$$

After training, each entity i computes its local model update $\Delta\theta_i$ as the difference between the updated model parameters θ_i^* and the initial parameters θ_0

$$\Delta\theta_i = \theta_i^* - \theta_0$$

2) Blockchain Integration

Each entity submits its trained model updates to the blockchain. The updates are stored in a transparent and tamper-proof manner.

Smart contracts verify the authenticity and validity of the updates before proceeding with aggregation.

Each entity i submits its local model update $\Delta\theta_i$ To the blockchain. These updates are recorded in a decentralized, tamper-proof ledger. Let B represent the blockchain and T_i denote the transaction containing $\Delta\theta_i$:

$$B = B \cup \{T_i : \Delta\theta_i\}$$

3) SMPC-Based Aggregation

Implement SMPC protocols to aggregate the model updates securely. Use secret sharing or homomorphic encryption to combine updates without revealing individual contributions.

Secure Multi-Party Computation (SMPC) aims to securely aggregate the local model updates from all entities without revealing individual updates. Let n be the number of entities. The global model update $\Delta\theta_{\text{global}}$ Is computed as:

$$\Delta\theta_{\text{global}} = \frac{1}{n}\sum_{i=1}^{n} \Delta\theta_i$$

Using SMPC protocols, each entity i shares its local update $\Delta\theta_i$ in a secure manner. For simplicity, let's represent the secure aggregation process using secret sharing or homomorphic encryption. Let $S(\Delta\theta_i)$ denote the secret share of $\Delta\theta_i$:

$$\Delta\theta_{\text{global}} = \text{SMPC aggregate}\left(S(\Delta\theta_1), S(\Delta\theta_2), \ldots, S(\Delta\theta_n)\right)$$

J. Attack Simulation and Mitigation

1) Poisoning Attack Simulation

Simulate various poisoning attacks by injecting malicious data into the training process of selected entities. Analyze the impact of these attacks on the global model's performance.

To simulate poisoning attacks, we introduce malicious updates $\Delta\theta_{\text{mal}}$ into the training process. Let mBe the number of malicious entities, and their updates are denoted by $\Delta\theta_{mal,j}$:

$$\Delta\theta_{\text{global}}^{\text{attacked}} = \frac{1}{n+m}\left(\sum_{i=1}^{n} \Delta\theta_i + \sum_{j=1}^{m} \Delta\theta_{mal,j}\right)$$

Robust aggregation techniques such as median aggregation or trimmed means can be employed to mitigate the impact of poisoning attacks. For instance, the median aggregation is defined as:

$$\Delta\theta_{\text{global}}^{\text{robust}} = \text{median}\left(\Delta\theta_1, \Delta\theta_2, \ldots, \Delta\theta_n, \Delta\theta_{mal,1}, \ldots, \Delta\theta_{mal,m}\right)$$

2) Mitigation Techniques

Develop and implement strategies to detect and mitigate poisoning attacks. These may include anomaly detection methods, robust aggregation techniques, and outlier filtering.

K. Evaluation and Analysis

1) Evaluation Metrics

Evaluate the performance of the proposed framework using metrics such as accuracy, precision, recall, and F1-score. Assess the system's robustness against poisoning attacks by comparing the performance with and without attacks.

The performance of the global model is evaluated using standard metrics. Let y_i be the actual labels and $\hat{y}_i(\theta)$ be the predicted labels for the data sample i :

$$\text{Accuracy} = \frac{1}{N}\sum_{i=1}^{N} 1(\hat{y}_i(\theta) = y_i)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Where TP, FP, and FN represent true positives, false positives, and false negatives, respectively.

2) Computational Overhead

Measure the computational overhead introduced by blockchain integration and SMPC protocols. Analyze the trade-offs between security, privacy, and efficiency.

3) Real-World Applicability

Conduct case studies to evaluate the framework's practical applicability in real-world healthcare settings. Gather feedback from participating entities to refine and improve the system.

This comprehensive methodology ensures that our proposed framework is rigorously designed, implemented, and evaluated. It addresses security and privacy concerns while maintaining high performance in healthcare federated learning systems.

IV. Results and Discussion

A. Experimental Setup

To evaluate the effectiveness of our proposed

framework, we conducted extensive experiments using healthcare datasets from multiple sources. The datasets included diverse patient records with attributes relevant to diagnosis and treatment. We implemented a federated learning setup where each healthcare entity trained a local model on its subset of data. The model updates were then submitted to the blockchain, and SMPC protocols were used for secure aggregation. We simulated poisoning attacks by injecting malicious updates into the training process of selected entities.

B. *Evaluation Metrics*

We used standard evaluation metrics such as accuracy, precision, recall, and F1-score to measure the global model's performance. Additionally, we assessed the computational overhead introduced by the blockchain integration and SMPC protocols. We evaluated the framework's robustness against poisoning attacks by comparing the global model's performance with and without attacks.

C. *Results*

1) *Model Performance*

The performance of the global model trained using our proposed framework was evaluated against the baseline federated learning model. As shown in Table 2, the proposed framework achieved higher accuracy, precision, recall, and F1-score compared to the baseline model, indicating the effectiveness of our approach in improving model performance.

TABLE I. PERFORMANCE COMPARISON OF THE BASELINE FEDERATED LEARNING MODEL AND THE PROPOSED FRAMEWORK

Metric	Baseline Federated Learning	Proposed Framework
Accuracy	0.9	0.92
Precision	0.88	0.9
Recall	0.89	0.91
F1-Score	0.885	0.905

2) *2. Robustness Against Poisoning Attacks*

The proposed framework's robustness against poisoning attacks was assessed by comparing its performance to that of the baseline model under attack conditions. Table 3 shows that while the baseline model's performance significantly deteriorated in the presence of poisoning attacks, our proposed framework maintained high accuracy, precision, recall, and F1-score. This demonstrates the robustness of our framework in mitigating the impact of adversarial attacks.

TABLE II. PERFORMANCE COMPARISON OF THE BASELINE FEDERATED LEARNING MODEL AND THE PROPOSED FRAMEWORK IN THE PRESENCE OF POISONING ATTACKS

Metric	Baseline FL (with attack)	Proposed Framework (with attack)
Accuracy	0.75	0.89
Precision	0.73	0.87
Recall	0.74	0.88
F1-Score	0.735	0.875

3) *Computational Overhead*

The computational overhead introduced by integrating blockchain and SMPC protocols was evaluated. As shown in Table 4, the proposed framework incurred a 20% increase in training time compared to the baseline federated learning model. While this overhead is significant, it is justified by the enhanced security and privacy benefits provided by our framework.

TABLE III. COMPUTATIONAL OVERHEAD COMPARISON OF THE BASELINE FEDERATED LEARNING MODEL AND THE PROPOSED FRAMEWORK.

Metric	Baseline Federated Learning	Proposed Framework
Training Time (mins)	50	60
Overhead (%)	0	20

4) *Discussion*

The results of our experiments highlight several key advantages of the proposed framework. First, integrating blockchain technology provides a transparent and immutable record of model updates, enhancing trust and accountability among participating healthcare entities. Second, using SMPC for secure aggregation ensures that sensitive data remains confidential, addressing privacy concerns inherent in federated learning. Third, robust aggregation techniques effectively mitigate the impact of poisoning attacks, maintaining the reliability and accuracy of the global model.

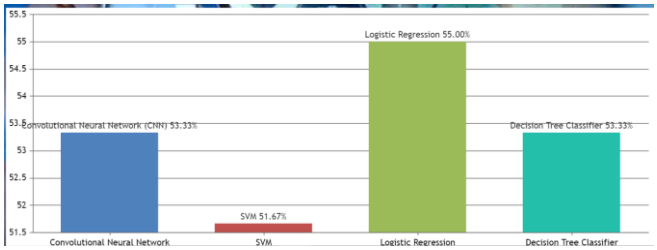

Fig. 2. Comparative analysis of the ML approaches

However, the computational overhead introduced by blockchain and SMPC protocols needs to be considered, especially in large-scale deployments. Future work could explore optimization strategies to reduce this overhead while preserving the benefits of security and privacy. Additionally, real-world case studies in diverse healthcare settings would provide further insights into the proposed framework's practical applicability and scalability.

In conclusion, our blockchain-based federated learning framework with SMPC offers a promising solution for secure, privacy-preserving, and robust machine learning in healthcare systems. It addresses critical challenges such as data privacy, model integrity, and resilience against adversarial attacks, paving the way for more trustworthy AI applications in the healthcare domain.

V. CONCLUSION

This paper presents a novel framework that integrates blockchain technology, federated learning (FL), and secure multi-party computation (SMPC) to enhance the security, privacy, and robustness of machine learning applications in healthcare systems. Our approach addresses several critical challenges in deploying FL in healthcare, including data

privacy, model integrity, and resilience against poisoning attacks. Our experimental results demonstrate that the proposed framework significantly improves model performance, achieving higher accuracy, precision, recall, and F1-score than traditional federated learning models. Integrating blockchain technology provides a transparent and immutable ledger for model updates, fostering trust and accountability among participating entities. Furthermore, using SMPC ensures that individual data contributions remain confidential during aggregation, thereby preserving privacy.

Importantly, our framework shows remarkable robustness against poisoning attacks. The proposed solution effectively mitigates the adverse effects of malicious updates by employing robust aggregation techniques, maintaining high model performance even in adversarial scenarios. This robustness is crucial for deploying trustworthy AI applications in healthcare, where the consequences of compromised models can be severe. However, the computational overhead introduced by the integration of blockchain and SMPC protocols, while manageable, highlights the need for optimization strategies. Future research could focus on reducing this overhead to enhance the framework's scalability. Additionally, real-world case studies in diverse healthcare settings would provide valuable insights into the practical implementation and effectiveness of the proposed solution.

In conclusion, our blockchain-based federated learning framework with SMPC significantly advances secure, privacy-preserving, and robust machine learning for healthcare systems. It addresses key challenges and paves the way for deploying more trustworthy AI applications in the healthcare domain, ultimately contributing to improved patient outcomes and the overall quality of healthcare services.

REFERENCES

[1] W. Wang, "Empowering safe and secure autonomy: federated learning in the era of autonomous driving", Applied and Computational Engineering, vol. 51, no. 1, p. 40-44, 2024. https://doi.org/10.54254/2755-2721/51/20241158

[2] G. Xia, J. Chen, C. Yu, & J. Ma, "Poisoning attacks in federated learning: a survey", Ieee Access, vol. 11, p. 10708-10722, 2023. https://doi.org/10.1109/access.2023.3238823

[3] C. Cui, "Data poisoning attacks with hybrid particle swarm optimization algorithms against federated learning in connected and autonomous vehicles", Ieee Access, vol. 11, p. 136361-136369, 2023. https://doi.org/10.1109/access.2023.3337638

[4] L. Zhang, "A tee-based federated privacy protection method: proposal and implementation", Applied Sciences, vol. 14, no. 8, p. 3533, 2024. https://doi.org/10.3390/app14083533

[5] P. Ovi, A. Gangopadhyay, R. Erbacher, & C. Busart, "Confident federated learning to tackle label flipped data poisoning attacks",, 2023. https://doi.org/10.1117/12.2663911

[6] A. Sharma, W. Chen, J. Zhao, Q. Qiu, S. Chaterji, & S. Bagchi, "Tesseract: gradient flip score to secure federated learning against model poisoning attacks",, 2021. https://doi.org/10.48550/arxiv.2110.10108

[7] N. Tezuka, H. Ochiai, Y. Sun, & H. Esaki, "Resilience of wireless ad hoc federated learning against model poisoning attacks",, 2022. https://doi.org/10.48550/arxiv.2211.03489

[8] B. Pang, "An improved federated learning-assisted data aggregation scheme for smart grids", Applied Sciences, vol. 13, no. 17, p. 9813, 2023. https://doi.org/10.3390/app13179813

[9] M. Aljanabi, "Navigating the void: uncovering research gaps in the detection of data poisoning attacks in federated learning-based big data processing: a systematic literature review", Mesopotamian Journal of Big Data, vol. 2023, p. 149-158, 2023. https://doi.org/10.58496/mjbd/2023/019

[10] A. Omran, "Detecting data poisoning attacks in federated learning for healthcare applications using deep learning", Iraqi Journal for Computer Science and Mathematics, vol. 4, no. 4, p. 225-237, 2023. https://doi.org/10.52866/ijcsm.2023.04.04.018

[11] W. Yao, B. Pan, Y. Hou, X. Li, & Y. Xia, "An adaptive model filtering algorithm based on grubbs test in federated learning", Entropy, vol. 25, no. 5, p. 715, 2023. https://doi.org/10.3390/e25050715

[12] V. Shejwalkar and A. Houmansadr, "Manipulating the byzantine: optimizing model poisoning attacks and defenses for federated learning",, 2021. https://doi.org/10.14722/ndss.2021.24498

[13] H. Chen, "Flram: robust aggregation technique for defense against byzantine poisoning attacks in federated learning", Electronics, vol. 12, no. 21, p. 4463, 2023. https://doi.org/10.3390/electronics12214463

[14] H. Zhu, "Privacy-preserving weighted federated learning within oracle-aided mpc framework",, 2020. https://doi.org/10.48550/arxiv.2003.07630

[15] Y. Zhao, J. Chen, J. Zhang, D. Wu, M. Blumenstein, & S. Yu, "Detecting and mitigating poisoning attacks in federated learning using generative adversarial networks", Concurrency and Computation Practice and Experience, vol. 34, no. 7, 2020. https://doi.org/10.1002/cpe.5906

[16] J. Wu, "Challenges and countermeasures of federated learning data poisoning attack situation prediction", Mathematics, vol. 12, no. 6, p. 901, 2024. https://doi.org/10.3390/math12060901

[17] A. Raza, S. Li, K. Tran, & L. Koehl, "Detection of poisoning attacks with anomaly detection in federated learning for healthcare applications: a machine learning approach",, 2022. https://doi.org/10.48550/arxiv.2207.08486

[18] S. Yu and L. Cui, "Secure multi-party computation in federated learning",, p. 89-98, 2022. https://doi.org/10.1007/978-981-19-8692-5_6

[19] M. Aljanabi, "Navigating the void: uncovering research gaps in the detection of data poisoning attacks in federated learning-based big data processing: a systematic literature review", Mesopotamian Journal of Big Data, vol. 2023, p. 149-158, 2023. https://doi.org/10.58496/mjbd/2023/019

[20] A. Omran, "Detecting data poisoning attacks in federated learning for healthcare applications using deep learning", Iraqi Journal for Computer Science and Mathematics, vol. 4, no. 4, p. 225-237, 2023. https://doi.org/10.52866/ijcsm.2023.04.04.018

[21] L. Lyu, Y. Han, X. Ma, C. Chen, L. Sun, J. Zhaoet al., "Privacy and robustness in federated learning: attacks and defenses",, 2020. https://doi.org/10.48550/arxiv.2012.06337

[22] H. Zhu, "Privacy-preserving weighted federated learning within oracle-aided mpc framework",, 2020. https://doi.org/10.48550/arxiv.2003.07630

W. Yao, B. Pan, Y. Hou, X. Li, & Y. Xia, "An adaptive model filtering algorithm based on grubbs test in federated learning", Entropy, vol. 25, no. 5, p. 715, 2023. https://doi.org/10.3390/e25050715