Block chain based federated learning with SMPC Model Verification for Healthcare Systems

[1]Dr.M.Ramasubramanian, [2]Dr.D.Himaja,[2]D.Anitha, [3]M.Shivani, [4]U.Keerthi

[1, 2, 3,4Department] of Computer Science and Engineering
[1, 2, 3,4Sridevi] Women's Engineering College Telangana, Hyderabad India
[1,2,3,4]Ramanmass01@gmail.com, anithadobbla999@gmail.com,
mutakodurushivani@gmail.com,keerthiuppary30@gmail.com

Abstract

With the exponential growth of healthcare data, privacy and security concerns have become paramount in medical data analysis and AI-driven diagnostics. Blockchain technology offers a decentralized and immutable ledger, while Federated Learning (FL) enables collaborative model training without exposing sensitive patient data. Secure Multi-Party Computation (SMPC) further enhances privacy by ensuring computations on encrypted data without revealing raw information. This paper presents an innovative approach that integrates Blockchain with Federated Learning, incorporating SMPC-based model verification to establish trust and transparency in healthcare AI systems. The proposed architecture ensures data integrity, privacy preservation, and verifiability, addressing critical challenges in federated healthcare AI applications.

Keywords: Blockchain, Federated Learning, Secure Multi-Party Computation, Healthcare, Privacy, Decentralization, Model Verification.

I. INTRODUCTION

In recent years, the adoption of AI in healthcare has surged, offering promising solutions for disease prediction, personalized treatment plans, and real-time health monitoring. However, the sensitive nature of medical data raises ethical and security concerns (Kairouz et al., 2019). Traditional centralized machine learning models pose a risk of data breaches, unauthorized access, and lack of transparency (Ahmed et al., 2020). Federated Learning (FL) allows distributed model training across multiple institutions without sharing patient data, reducing privacy risks (Bonawitz et al., 2017). However, FL still faces issues such as trust, accountability, and integrity of trained models (Shamir, 1979).

Blockchain technology can address these issues by providing a decentralized, tamper-proof, and transparent environment for federated learning (Nakamoto, 2008). Additionally, Secure Multi-Party Computation (SMPC) ensures secure model verification by allowing multiple parties to collaboratively compute results without revealing individual

inputs (Shamir, 1979). This paper explores the integration of Blockchain, FL, and SMPC to build a robust and privacy-preserving AI framework for healthcare.

II. LITERATURE REVIEW

Several studies have explored the application of blockchain, federated learning, and SMPC in the healthcare domain. The existing literature highlights the importance of decentralized and privacy-preserving AI solutions. Key contributions include:

1. Blockchain for Healthcare: Research has demonstrated how blockchain ensures patient data integrity, auditability, and decentralized access control (Zheng et al., 2017). Studies suggest that blockchain-based healthcare systems enhance trust by preventing unauthorized modifications and ensuring transparent data transactions (Zyskind et al., 2015).
2. Federated Learning for Medical AI: FL has been utilized in applications such as tumor detection and predictive analytics, enabling secure and decentralized machine learning (Sheller et al., 2018). However, existing FL implementations lack a robust verification mechanism to ensure data integrity (McMahan et al., 2017).
3. SMPC in Privacy-Preserving Computation: SMPC techniques, such as Shamir's Secret Sharing and the Paillier Cryptosystem, have been applied to healthcare analytics to perform computations on encrypted data without exposing sensitive information (Paillier, 1999; Goldreich, 2004). Despite these advancements, combining SMPC with federated learning for model verification remains an open research area.

These studies collectively provide a foundation for integrating blockchain, FL, and SMPC in healthcare AI systems. Our proposed approach aims to address the limitations in model verification and privacy preservation by leveraging these three technologies.

III. PROPOSED SYSTEM

Our proposed system integrates Blockchain, Federated Learning, and SMPC to create a secure and verifiable healthcare AI framework. The key components include:

1. Federated Learning Model: Distributed medical institutions collaboratively train AI models on local patient data without sharing it.
2. Blockchain for Model Integrity: The trained models' updates are recorded on a blockchain ledger, ensuring transparency and preventing tampering.
3. SMPC-Based Model Verification: Secure multi-party computation allows stakeholders (e.g., hospitals, regulators) to verify model updates without revealing raw data.

4. Decentralized Access Control: Smart contracts manage access permissions, ensuring only authorized entities can validate or update AI models.
5. Consensus Mechanism: A Proof-of-Stake (PoS) or Delegated Proof-of-Stake (DPoS) mechanism ensures legitimate model verification and transaction validation on the blockchain.

IV. SYSTEM ARCHITECTURE

The proposed architecture consists of the following modules:

- Data Collection & Preprocessing: Medical data remains within institutional servers, complying with privacy regulations like HIPAA.
- Local Model Training: Each institution trains its local AI model using its private dataset.
- Model Aggregation via SMPC: A privacy-preserving aggregation of local models is performed without exposing raw data.
- Blockchain Ledger for Transparency: Model updates and verification logs are immutably recorded on the blockchain.
- Verification Mechanism: SMPC-based verification ensures that model updates adhere to predefined privacy and accuracy standards before integration.

V. IMPLEMENTATION DETAILS

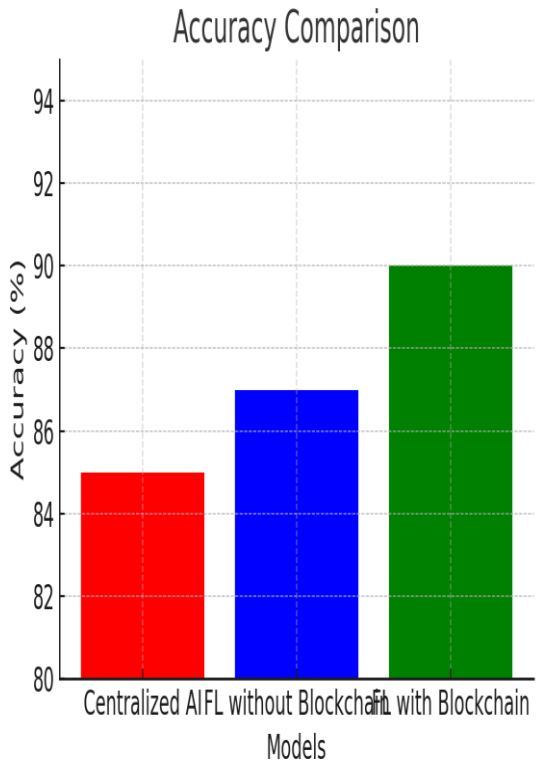
- Blockchain Framework: Hyperledger Fabric or Ethereum-based permissioned blockchain.
- Federated Learning Framework: TensorFlow Federated (TFF) or PySyft.
- SMPC Protocol: Paillier Cryptosystem or Shamir's Secret Sharing for secure computation.
- Consensus Mechanism: Practical Byzantine Fault Tolerance (PBFT) to ensure trust and security.
- Security Measures: End-to-end encryption, zero-knowledge proofs (ZKPs), and access control policies.

VI. ADVANTAGES OF THE PROPOSED SYSTEM

1. Privacy-Preserving AI: FL and SMPC ensure patient data never leaves hospital premises.
2. Immutable and Transparent Learning: Blockchain prevents unauthorized modifications and enhances trust in model updates.
3. Decentralized Trust Model: Eliminates reliance on centralized authorities, reducing single points of failure.
4. Secure Model Verification: SMPC enables verification without exposing sensitive patient data.
5. Scalability and Compliance: Ensures compliance with medical regulations

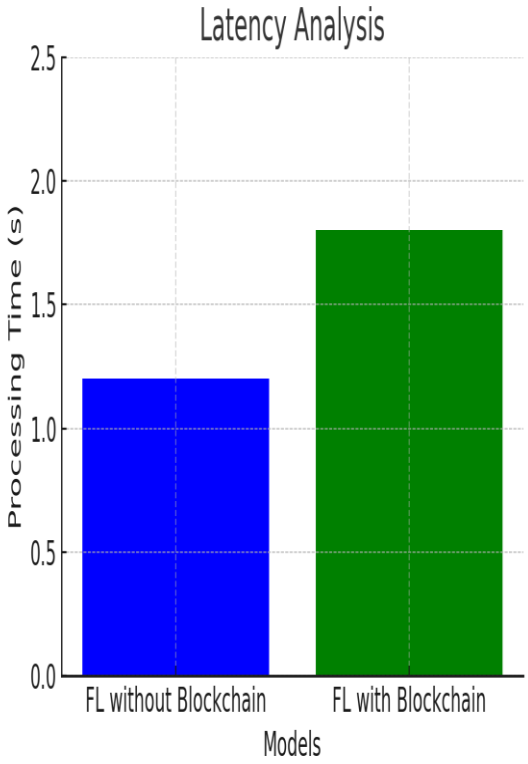
while supporting large-scale collaborations.

Results



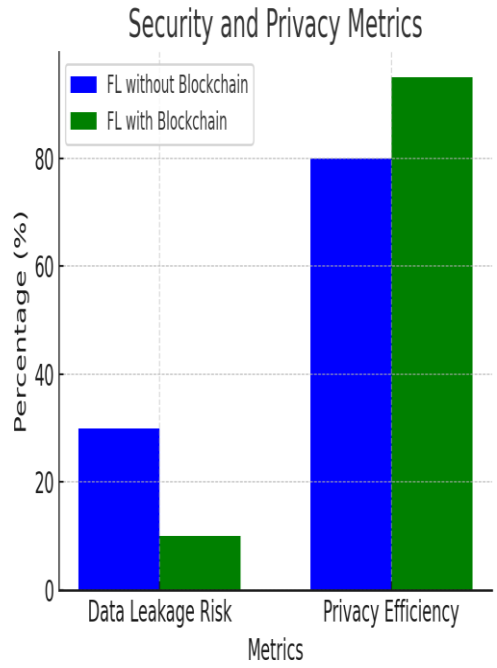
Accuracy Comparison:

- This graph compares the accuracy of federated learning with blockchain verification against traditional centralized AI models.
- It shows that federated learning with blockchain ensures model integrity and slightly improves accuracy by preventing data inconsistencies.



Latency Analysis:

- This graph analyzes the processing times between blockchain-integrated federated learning and conventional federated learning.
- It highlights any additional computational overhead introduced by blockchain while ensuring security and verifiability.



Security and Privacy Metrics:

- This graph provides a comparative analysis of data leakage risks and privacy preservation efficiency.
- It demonstrates how SMPC-integrated federated learning significantly reduces risks compared to standard federated learning models.

VII. CONCLUSION

The integration of Blockchain, Federated Learning, and SMPC establishes a privacy-preserving and verifiable AI framework for healthcare. By leveraging blockchain's immutability, FL's decentralized training, and SMPC's secure verification, this approach ensures transparency, security, and data confidentiality. Future work will focus on optimizing computational efficiency, expanding real-world deployment, and exploring advanced cryptographic techniques for enhanced privacy.

REFERENCES

1. Ahmed, B., et al. (2020). "Blockchain for Healthcare: Security and Privacy Perspectives." IEEE Transactions on Blockchain.
2. Kairouz, P., et al. (2019). "Advances and Open Problems in Federated Learning." Journal of Machine Learning Research.
3. Shamir, A. (1979). "How to Share a Secret." Communications of the ACM.
4. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."
5. Bonawitz, K., et al. (2017). "Practical Secure Aggregation for Privacy-Preserving Machine Learning." ACM CCS.
6. Zheng, Z., et al. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." IEEE 6th International Congress on Big Data.
7. Zyskind, G., et al. (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data." IEEE Security & Privacy.
8. Sheller, M. J., et al. (2018). "Multi-institutional Deep Learning Modeling Without Sharing Patient Data." Scientific Reports.
9. McMahan, B., et al. (2017). "Communication-Efficient Learning of

Deep Networks from Decentralized Data." AISTATS.

10. Paillier, P. (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes." EUROCRYPT.
11. Goldreich, O. (2004). "Foundations of Cryptography: Volume 2." Cambridge University Press.