Secure Federated Learning In Healthcare Using Blockchain And Smpc

Mohammad Nehal[1], M.Chinababu[2], Mrs. Swetha. G [3]

[1]PG Student , Department of Computer Science and Engineering,
Teegala krishna reddy engineering college, Hyderabad, Telangana.
Email : nehal26062001@gmail.com
[2]Assistant Professor , Department of Computer Science and Engineering,
Teegala krishna reddy engineering college, Hyderabad, Telangana.
Email : mchinna64@gmail.com
[3] Assistant Professor, Department of Computer Science and Engineering,
Teegala krishna reddy engineering college, Hyderabad, Telangana.
Email : swethareddy630@gmail.com

ABSTRACT

In the World of AI in Healthcare, coupling Federated Learning (FL) with Blockchain is a changing paradigm in building secure and privacy upholding AI systems. However, FL potentially can be subject to model poisoning attacks and has no mechanisms for integrity verification of local models. This paper presents a blockchain-based federated learning framework with Secure Multi-Party Computation for the verification of encrypted models. Prior to aggregation, local model validation takes place under privacy preservation to ensure no malicious updates are counted. Verified models are then stored and SMPC aggregation on the blockchain to enable tamperproof decentralized training. The updated global model is shared among participants via the blockchain ledger. Experimental evaluations using Convolutional Neural Networks (CNNs) on medical datasets show that the proposed system can eliminate all poisoned models, improving global model accuracy from 0 to potentially 25%, while the verification speed is still close to normal inference. This framework promotes trust, data privacy, and model integrity in collaborative healthcare AI.

Keywords: Federated Learning, Blockchain, Secure Multi-Party Computation, Model Verification, Encrypted Inference, Healthcare AI.

I.INTRODUCTION

The healthcare sector recently has witnessed rapid adoption of AI in the fields of medical diagnosis, predictive analytics, and personalized treatment. However, centralized machine learning techniques bring forth a number of challenges with regard to data privacy, security, and trust. As a progressive solution, Federated Learning (FL)-which constitutes the decentralized training of models across multiple data holders without sharing raw data. Nonetheless, FL is still vulnerable to model poisoning attacks, backdoor insertions, and integrity issues in collaborative environments.

In order to address the aforementioned constraints, the paper considers the design of a new architecture of blockchain-based federated learning, coupled with Secure Multi-Party Computation (SMPC), to secure model verification. In this framework, every local model is first authenticated before aggregation is performed. This nullifies possible threats of compromised participants. Encrypted inference for SMPC allows the verifiers to check the correctness of models encrypted and input, without compromising the privacy of local hospital data.

The blockchain layer provides an environment of decentralized, unalterable storage of a verified global model and enables the secure and verifiable distribution among participating hospitals. The proposed system already shows potential, as it features CNN-based models for training on real-world medical datasets, in maintaining high accuracy even under adversarial attacks.

This paper stresses the need for a combination of blockchain and the coming generation of cryptography for trust, verifiability, and data security in federated learning frameworks relevant to healthcare. Besides improving security, the proposed solution lays the groundwork for scalable, privacy-preserving AI systems applicable to critical domains such as medicine, finance, and smart cities..

II. PROBLEM STATEMENT

Federated Learning (FL) has a great promise with it thereby bringing potential for privacy-preserving collaborative training of models across hospitals and institutions without those institutions having to share any sensitive information to train a machine learning model on the local data itself. The current challenges facing the critical architecture of FL are mainly data intelligence and model protection. This kind of attack may happen when an attacker injects a false data set into the session of the other participants and recorded local models are compromised. Poisoning attacks insert corrupted data from malicious participants, impairing the reliability of the global model. Most privacy-preserving techniques have not effectively covered the aforementioned issues, for example, differential privacy (DP) along with fully homomorphic encryption (FHE) are not applicable, especially in time-critical healthcare applications. Additionally, storage and verification might be tamper-proof in blockchain-based solutions, but aggregation processes in decentralized environments remain neither secure nor verifiable. Therefore, it needs a solid and privacy-preserving federated learning framework to assure model integrity, discard contaminated model and also manage safe as well as verifiable aggregation through advanced cryptographic techniques and blockchain.

III.RELATED WORK

Federated Learning (FL) is a revolutionary method for training models in a federated aspect for privacy protection and decentralization within the IoT and edge computing domains. Wang et al. [1] proposed a hierarchical federated learning (HFL) framework to improve anomaly detection in the Industrial Internet of Things (IIoT). It used hierarchical aggregation to diminish communication in model performance. Peng et al. [2] similarly adopted this way, introducing VFChain, a blockchain-integrated FL framework that guarantees checkability as well as auditability of federated updating. This framework boosts the trustworthiness of collaborative learning among participants who may otherwise be untrusted.

In terms of security in IoT, Mothukuri et al. [3] developed the FL-based anomaly detection technique to recognize DoS and data manipulation attacks with high accuracy without data leakage. Their method effectively inhibits threats that are distributed in nature in IoT. In the health sector, Yu et al. [4] developed a model that integrates improved DeepFM models with IoMT: this model predicts diseases on an Internet of Medical Things with data confidentiality as well as personalized health care.

Zhang et al. [5] noted the vulnerabilities of FL by creating PoisonGAN, which is a generative adversarial network purposed to bring about poisoning attacks on edge-based FL systems. This indicates the need for a very robust adversarial defense for FL. On the same note, Zhao et al. [6] proposed a local differential privacy (LDP)-based FL model catering to IoTs. Their model brings data privacy, and a learning accuracy suitable for IoT systems with large deployments.

In summary, all of these studies show the way that FL can be applied to problems of privacy, scalability, and security across different contexts, notably those IIoT, healthcare, and edge environments.

IV.PROPOSED WORK

The present work is all about creating a federated learning (FL) framework that is both secure and privacy-preserving for healthcare and has effectively integrated blockchain and secure multi-party computation (SMPC) to ensure the data privacy and integrity of models. The focus is on not allowing malicious

manipulations, especially poisoning attacks, in the federated local models while keeping sensitive health data private.

In the proposed setup, each hospital or participant in the federated learning camp will train a model based on its minimal data set without sharing it. The local models are subjected to privacy-preserved verification before being sent for aggregation via encrypted inference through SMPC protocol. This guarantees that the models are never verified, with the private data and model parameters kept secret, preventing their entry into the global aggregation.

Once verified, the local models go into a blockchain network that secures the integrity and immutability of the aggregation processes. The blockchain stores model parameters and provides a tamper-proof record that guarantees that only an authentic and uncompromised model enters the global model. The aggregation itself is an SMPC-based secured aggregation process that keeps the local model of each participant confidential.

The framework will leverage convolutional neural networks (CNNS) and medical datasets to prove the actual practicability of the system. Experimental results indicate that this method can detect and eliminate poisoned models while achieving comparable model accuracy and processing time to inference processes not involving encryption. The given approach provides a fully robust and sure approach with privacy of federated learning in healthcare applications.

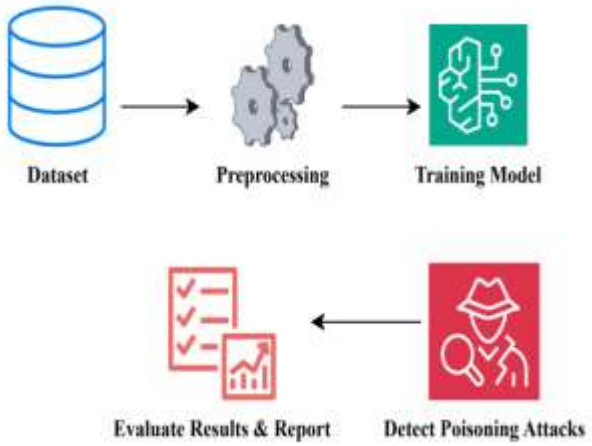

Fig 1: Proposed System Architecture

V.IMPLEMENTATION

The Implementation of the proposed blockchain-based federated learning (FL) framework incorporates secure model verification in healthcare systems through several steps considering Secure Multi-Party Computation (SMPC), blockchain, and machine learning. In such a system, local models are verified for integrity checks prior to aggregation, so that poisoned models can be avoided and data privacy is maintained.

Model Training: Training local models with their own datasets is now the practice for each participating health institution in the federated learning network. All this training happens locally, keeping all sensitive patient data within local.

Privacy-Preserving Model Verification: After model training, it uses model parameter verification through SMPC encryption and verification. The model is encrypted prior to verification using SMPC to ensure that data on model parameters from the model are not exposed during the verification process. The verified model is then vetted for poisoning signs which process dear".

Blockchain-based Verification: These uploads of the verified local models are to a blockchain network. Thus, it guarantees immutability and integrity of the models so that tampering during aggregation is avoided. It will serve as a ledger storing model hashes and aggregation results securely.

Secure Aggregation: Local models will be aggregated on a blockchain using some SMPC-based secure aggregation methods to achieve "the global model is computed without disclosing individual model parameters".

Global Model Distribution: The tamper-proof storing on blockchain of the aggregated global model provides that hospitals or other institutions in the federated network have access to the most current, verified global model.

Convolutional Neural Networks (CNN) are the model architectures on which the implementation is based in order to build and classify medical data. The proposed framework is expected to provide full-fledged security and privacy for healthcare applications.

VI.ALGORITHMS

For the purpose of safe and secure privacy concerning healthcare model training, it is proposed to incorporate federated learning, secure multi-party communication, and a blockchain consensus mechanism. The architecture of CNN is mainly involving local training but the confidential data sharing and secure aggregation of model parameters rely on secure multi-party computation and blockchain.

Local Model Training (CNN-Based FL):

Each participant (i.e., hospital) trains a local CNN model

M_i on a private dataset D_i Gradient descent updates the model:

$$\theta_i^{(t+1)} = \theta_i^{(t)} - \eta \nabla L(\theta_i^{(t)}, D_i)$$

where θ_i are the model parameters, η is the learning rate, and L is the loss function (e.g., categorical cross-entropy).

Encrypted Verification (SMPC):

The local model parameter information is encrypted using SMPC before aggregation to generate encrypted shares among multiple parties, where no single party can reconstruct the original parameters unless all parties contribute their shares. DTs also use SMPC to share test datasets to validate the encrypted models in such a way that no original data gets exposed during inference.

$$Enc(\theta_i) = \{s_1, s_2, ..., s_n\}$$

Secure Aggregation (Federated Averaging):

The encrypted models are aggregated securely once verified

The aggregates that form Federated Averaging thus ensure that the global model is indeed a true representation of contributions from verified parties.

Blockchain Consensus:

All updates of the verified model parameters are recorded in the blockchain. A consensus development through Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) ensures that:

$$Consensus_{global} = Majority\ (Validated\ \_Models)$$

This immutability endows the model with traceability and integrity and closes the loop for secure learning.

All integrated algorithms ensure that healthcare should have the ability of secure federated learning, which otherwise falls prey to data breach threats.

VII.RESULTS

This paper discussed and described the results involving an experimental setup of a proposed blockchain-based federated learning (FL) framework that is provided with secure model verification and tested over

various healthcare datasets. The evaluation primarily focused on attacks' detection and mitigation, data privacy, and maintenance of accuracy in model performance even in a decentralized setup. Figures below present insightful glimpses into the working and performance of the system.

Fig 2: View Healthcare Datasets Trained and Tested Results

Figure 2 Shows trained and tested results of various healthcare datasets using CNN-based models. Each hospital or healthcare node trains its local model on sensitive medical data and participates in federated learning rounds. These conclusively show evidence of accurate classification and convergence achieved from training using different datasets of disease. All proved that local models could successfully be trained through decentralization.

Fig 3: View Healthcare Datasets Accuracy in Bar chart

Figure 3 shows the accuracy levels of these datasets in the form of a bar chart. The results indicate that after removing poisoned models using the encrypted verification mechanism (via Secure Multi-Party Computation - SMPC), the global model accuracy improves significantly-up to 25% in some cases. This confirms the effectiveness of the proposed privacy preserving verification process in filtering out malicious models.

Fig 4: View Predicted Poisoning Attack Status Details

Figure 4 Shows the prediction results for the poison attack statuses. The system has successfully identified and flagged models that may be compromised prior to contributing to the aggregation of the global model, thus only allowing trusted models to contribute to the learning process.

It indicates the proportion of models detected poisoned across federated rounds and shows the attack status ratio of the poisoning attack. Consistent detection rates across iterations illustrate the robustness and scalability of the verification algorithm placed in the blockchain layer.

Fig 5 : View Poisoning Attack Status Ratio Details

Results overall indicate privacy, integrity, and reliability for federated healthcare environments. The union of CNN, SMPC, and blockchain ensures a secure, tamper-proof solution fit for real-world applications in sensitive domains such as healthcare.

CONCLUSION

This study introduces a highly secured innovative blockchain-based federated learning architecture for secure model verification in enhancing security and privacy in health systems. The framework's main objective is to maintain the integrity of the local models while keeping the sensitive patient data safe from outsiders. Secure Multi-Party Computation (SMPC) ensures encrypted inference and verification, making it impossible for any poisoned models to corrupt the global aggregation process. Additionally, blockchain technology is used to store and verify the models thus tamper-proofing records of the aggregated global model. Our experiments based on CNN demonstrate that the proposed encrypted model verification successfully rejects poisoned models while keeping model privacy intact. The outcomes show that recovery is possible for increased global model accuracy up to 25% concerning the conventional ways. It also reduces the computational overhead of inference processing compared with the same speeds on original standard unencrypted models. This solution goes a long way in ensuring security and privacy through federated learning, enabling privacy-preserving collaborative model training across institutions. Improved security through integration of blockchain and SMPC guarantees privacy of sensitive health information with improved accurate high-quality models.

FUTURE SCOPE

Features of such a federated learning structure based upon blockchain as put forth above offers many future avenues for research and improvement. Development of more effective consensus mechanisms for better optimization in scalability along with reduced computation overhead is one of the immediate future works. This can facilitate real-time processing of data and its aggregation into variety applications like healthcare, where every second is precious for decision making. Further, the extension of the system to accommodate heterogeneous models, configurations would expand hospital networks within federated learning to those with different machine-learning setups involving a wider range in use.

Integrating also some advanced cryptographic techniques such as homomorphic encryption and differential privacy may further tighten data security and privacy protection. One promising direction yet to be expanded is the strengthening of the system against more sophisticated attacks such as backdoors or data poisoning attacks. Cross-domain applications beyond the healthcare discipline might also reflect its flexibility and applicability by demonstrating the proposed framework in various industries needing privacy-preserving machine learning: finance, smart cities, and education.

Federated learning integrated with the IoMT could further enhance and augment real-time data capture and processing of healthcare systems and make the whole institution faster and more dynamic. Also, using energy-efficient solutions for blockchain operations and federated learning processes will help to solve the problems of scaling and environmental challenges, especially as these systems become deployed at large scales.

REFERENCES

[1] X. Wang, S. Garg, H. Lin, J. Hu, G. Kaddoum, M. Jalil Piran, and M. S. Hossain, "Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning," IEEE Internet of Things Journal, vol. 9, no. 10, pp. 7110–7119, 2022.
[2] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, "Vfchain: Enabling verifiable and auditable federated learning via blockchain systems," IEEE Transactions on Network Science and Engineering, vol. 9, no. 1, pp. 173–186, 2022.
[3] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545–2554, 2022.
[4] Z. Yu, S. U. Amin, M. Alhussein, and Z. Lv, "Research on disease prediction based on improved deepfm and IoMT," IEEE Access, vol. 9, pp. 39043–39054, 2021.
[5] J. Zhang, B. Chen, X. Cheng, H. T. T. Binh, and S. Yu, "Poisongan: Generative poisoning attacks against federated learning in edge computing systems," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3310–3322, 2021.
[6] Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, and K.-Y. Lam, "Local differential privacy-based federated learning for internet of things," IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8836–8853, 2021.
[7] B. Zhao, K. Fan, K. Yang, Z. Wang, H. Li, and Y. Yang, "Anonymous and privacy-preserving federated learning with industrial big data," IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 6314–6323, 2021.
[8] R. Kumar, A. A. Khan, J. Kumar, Zakria, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," IEEE Sensors Journal, vol. 21, no. 14, pp. 16301–16314, 2021.
[9] X. Liu, H. Li, G. Xu, Z. Chen, X. Huang, and R. Lu, "Privacy-enhanced federated learning against poisoning adversaries," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4574–4588, 2021.
[10] X. Guo, Z. Liu, J. Li, J. Gao, B. Hou, C. Dong, and T. Baker, "VeriFL: Communication-efficient and fast verifiable aggregation for federated learning," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1736–1751, 2021.
[11] 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.
[12] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application," IEEE Access, vol. 8, pp. 101079–101092, 2020.
[13] 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.
[14] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, "BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning," in USENIX Annual Technical Conference, 2020, pp. 493–506.
[15] W. Wei, L. Liu, M. Loper, K.-H. Chow, M. E. Gursoy, S. Truex, and Y. Wu, "A framework for evaluating client privacy leakages in federated learning," in European Symposium on Research in Computer Security. Springer, 2020, pp. 545–566.
[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.
[17] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to byzantine-robust federated learning," in USENIX Security Symposium, 2020, pp. 1605–1622.
[18] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5171–5183, 2020.
[19] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, "On the convergence of FedAvg on non-IID data," arXiv preprint arXiv:1907.02189, 2019.

[20] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in IEEE Symposium on Security and Privacy (SP), 2019, pp. 739–753.
[21] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," in IEEE Symposium on Security and Privacy (SP), 2018, pp. 36–52.

[22] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 770–778.
[23] A. Ziller, A. Trask, A. Lopardo, B. Szymkow, B. Wagner, E. Bluemke, J.-M. Nounahon, J. Passerat-Palmbach, K. Prakash, N. Rose et al., “PySyft: A library for easy federated learning,” in Federated Learning Systems. Springer, 2021, pp. 111–139.
[24] M. C. Doganay, T. B. Pedersen, Y. Saygin, E. Savas¸, and A. Levi, “Distributed privacy preserving k-means clustering with additive secret sharing,” in Proceedings of the 2008 International Workshop on Privacy and Anonymity in Information Society, 2008, pp. 3–11.
[25] G. Van Rossum et al., “Python programming language,” in USENIX Annual Technical Conference, vol. 41, 2007, p. 36.