e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707249 |

Federated Instruction for Surgical Centers Using the SMPC Model and Blockchain Technology to PreventPoisoning Incidents

Sravanthi Kalal, Vinoothreddy D

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT : Due to heightened concerns regarding privacy and security in machine learning applications, federated learning (FL) has gained significant attention and has been applied across various domains such as intelligent healthcare systems, IoT-based industries, and smart cities. FL enables collaborative training of a global model without exposing local training data from clients. However, existing FL approaches are susceptible to adversarial attacks. The architecture of FL makes it challenging to detect and defend against malicious model updates. Moreover, research on detecting maliciousupdates in FL while preserving model privacy remains underexplored. This paperintroduces a novel approach: blockchain-based federated learning with Secure Multi- Party Computation (SMPC) model verification against poisoning attacks, specifically tailored for healthcare systems. Initially, the machine learning models from FL participants undergo encrypted inference to identify and eliminate compromised models. Once the local models of participants are verified, they are securely aggregated on the blockchain node. The proposed framework has been validated through experiments using diverse medical datasets to assess its efficacy.

KEYWORDS: SMPC, MEDICAL.

I. INTRODUCTION

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 block chain for the aggregation process. SMPC-based aggregationis used to perform the secure aggregation between the block chain 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 block chain and verifies the authenticity of the global model.

Federated learning allows multiple participants, such as hospitals, to collaboratively train a global machine learning model without sharing their local data. However, this decentralized approach introduces several challenges, including the risk of model poisoning attacks where acompromised participant can introduce a malicious local model to corrupt the global model. Additionally, there is a need to ensure the privacy of the local model parameters to prevent membership inference attacks and parameter stealing.

The primary goals of the proposed method are:

Security of the Global Model: Ensuring that the global model used for disease classification in healthcare systems is secure and free from poisoned local model.

Privacy Preservation: Protecting the privacy of local model parameters using SMPC to prevent any form of data leakage.

Decentralized Aggregation: Utilizing blockchain to decentralize the aggregation process, enhancing the security and transparency of the federated learning framework.

Verification of the Global Model: Ensuring that each participant can verify the authenticity of the global model received from the blockchain.

Previous research has explored various methods to enhance the security and privacy of federated learning. Techniques such as differential privacy and homomorphic encryptionhave been employed to protect data privacy. Blockchain technology has also been investigated as a means to provide a transparent and tamper-proof mechanism for aggregatinglocal models. However, integrating these technologies to address the specific challenges of model poisoning and parameter privacy in healthcare systems has been less explored.

II. 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 localmodel 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 trainingprocess 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 poisoningattack.

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 oftheir experiments, their aggregation method reduces the accuracy of the machine learning model. Our proposed method performs anomaly detection using an encrypted inference process to eliminate the poisoned local model. Later, we leverage the SMPC-based secure aggregation method. Our secure aggregation method will not affect the accuracy of machine learning. Also, we leverage blockchain for the aggregation process as part of the consensus mechanism to mitigate a single point of failure.Blockchain is known for its immutability and is used for tampered-proof storage. The use of blockchain can track the local or global modelfor 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 singleserver. The correct utilization of blockchain technology can overcome the problem.

In tackling the issue, [19] proposed decentralized privacy using blockchain-enabled FL. Theyuse 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.

III. DISADVANTAGES

Risks of local model security: In the current setup of federated learning, every party that sends their local model is sent to the cloud for the aggregation process without checking the model's validity. This traditional FL method introduces the risk of a local model being poisoned. For example, an attacker can perform a poisoning attack and train the model using poisoned data, leading to a faulty local model. Since healthcare data are critical, sending plaintext local models to the cloud can pose privacy risks. Therefore, validating and securing the local model is required to prevent it from various security aspects. Risks of generating a biased aggregated model: The model aggregation process of the local model is performed on the cloud services that can be tampered with and produce a biased global model. For example, an attacker can include a poisoned local model during the aggregation process that may lead the global model to have a false classification. Hence, a secure aggregation method is required to encounter the current security problem.Risk of receiving faulty global model: Inthe existing federated learning method, the global model generated from the cloud will be sent back to each edge server in the hospitals. However, the hospital can not verify the global model they received. The attacker can intercept and alter the global model. As a result, the hospital received a faulty global model. From this problem, a global model verification method is required to ensure the integrity of the global model.

Proposed System

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

Advantages

Robustness: The proposed work should have the ability to prevent the adversary from poisoning federated learning. This allows the federated learning participant to learn from a benign global model to improve their model accuracy. Also, a robust aggregation method needs to be developed to secure the aggregation process from an attacker. Privacy: The prior work [12] has shown that an attacker can perform a poisoning attack to decrease the global model accuracy by miss-classifying the machine learning model. To protect the federated learning participants, checking the participant's local learning model while maintaining the local model privacy itself is essential. Verifiability: The designed method should have the ability to verify the machine learning model, specifically the global model. Since the adversary may alter or poison the global model. In the current federated learning scenario, the participant received the global model from the cloud without knowing the model's authenticity.

IV. IMPLEMENTATION

Admin

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 Login, View All Users andAuthorize, View All Datasets, View All Datasets By Block chain IOMT Cluster, ViewPoisoning Attack Results, View Smoking Status Results.

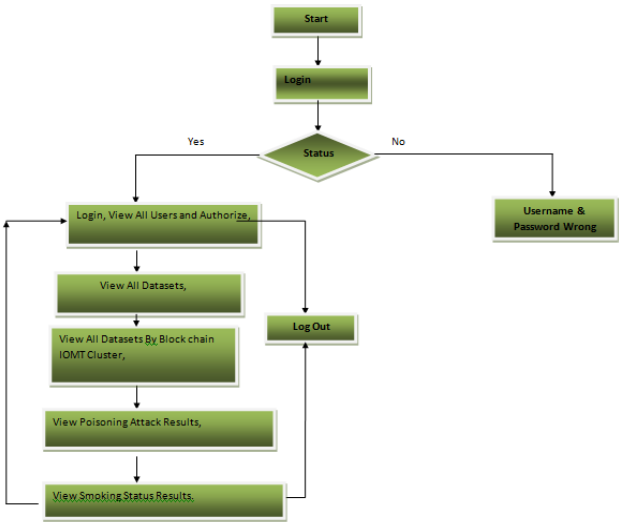
Start
Login
Yes
Status
No
Login, View All Users and Authorize,
Username & Password Wrong
View All Datasets,
Log Out
View All Datasets By Block chain IOMT Cluster,
View Poisoning Attack Results,
View Smoking Status Results.

Fig 2. Flow chart

View and Authorize Users

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

User

In this module, there are n numbers of users are present. User should register before doingany 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, View Profile, Upload Datasets, Find Poisoning Attack Type, Find Poisoning Attack Type By Hash code.

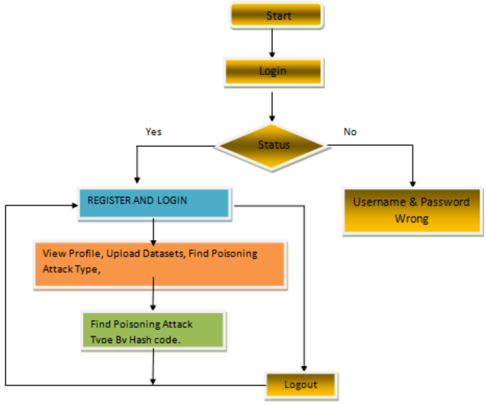
Start
Login
Yes
Status
No
REGISTER AND LOGIN
Username & Password Wrong
View Profile, Upload Datasets, Find Poisoning Attack Type,
Find Poisoning Attack Tvpe Bv Hash code.
Logout

Fig 3 Flow chart

V. RESULT

The results of implementing blockchain-based federated learning (FL) with secure multi- party computation (SMPC) model verification against poisoning attacks for healthcare systems are promising based on the conducted experiments with various medical datasets.

Initially, the encrypted inference process effectively detected and removed compromised models contributed by FL participants. This ensured that only authentic and trustworthy models proceeded to the next stage. The use of SMPC for model verification added a layer of security by allowing participants to validate model updates without revealing their local training data, thereby preserving privacy.Aggregation of verified local models on the blockchain node proved to be secure and transparent. Blockchain technology facilitatedtamper-resistant storage and management of aggregated models, enhancing overall data integrity and auditability.

VI. CONCLUSION

This paper proposes a blockchain-based federated learning framework with secure model verification designed to enhance security in healthcare systems. The primary goal is to ensurethat local models are free from poisoning attacks while maintaining participant privacy and providing verifiability.In this framework, we conduct a privacy-preserving verification of each local model before aggregation. To maintain model privacy, verification is performed using encrypted inference supported by the Secure Multi-Party Computation (SMPC) protocol. This method allows verifiers to assess models without accessing raw data or sensitive information. Once a local model is verified, the validated portion is sent to the blockchain node. The blockchain, in conjunction with hospitals, performs secure aggregation using SMPC. When a consensus is reached among the majority of nodes, the resulting global model is stored securely on the blockchain. This tamper-proof storage then distributes the updated global model to all participating hospitals in the federated learning round.In our experiments, we utilized Convolutional Neural Network (CNN) algorithms with variousmedical datasets to generate and aggregate local models within the federated learning framework. Our results demonstrate that the encrypted verification process effectively eliminates poisoned models while preserving local model privacy. Furthermore, we achievedup to a 25% recovery in global model accuracy. Importantly, the secure inference processing time was comparable to that of the original inference process.

REFERENCES

[1] L. Sun, X. Jiang, H. Ren, and Y. Guo, "Edge-cloud computing and artificial intelligencein internet of medical things: Architecture, technology and application," IEEE Access, vol. 8, pp. 101 079–101 092, 2020.

[2] 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.

[3] 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. 39 043–39 054, 2021.

[4] 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.

[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 ComputerSystems, vol. 115, pp. 619–640, 2021.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com