Journal of Autonomous Systems and Robotics
https://www.harrisonacademicpress.com/index.php/JASR
Vol 1, Issue 1, 2026

FEDERATED LEARNING IN HEALTHCARE: BLOCKCHAIN INTEGRATION AND SMPC VERIFICATION FOR POISONING ATTACK MITIGATION

[1] *Deshik Mashudhi,* [2] *Mr.D.Satyanarayana*
[1] *M.Tech Student,* [2] *Assistant Professor*
Department of Computer Science Engineering
SVR Engineering College, Nandyal

ABSTRACT

Federated Learning (FL) has emerged as a transformative approach in healthcare AI, enabling collaborative model training across multiple medical institutions while preserving patient privacy. However, FL is vulnerable to poisoning attacks, where adversarial participants inject malicious data to corrupt the global model. To address this, we propose a Blockchain-integrated FL framework with Secure Multi-Party Computation (SMPC) verification, enhancing both data security and model integrity. Blockchain technology ensures tamper-proof auditability, enabling decentralized trust among healthcare participants, while SMPC-based verification mechanisms detect and mitigate poisoning attacks by validating local model updates before aggregation. The proposed system enhances privacy, robustness, and attack resilience, reducing the risk of compromised AI models in healthcare applications. Experimental evaluations demonstrate that the framework significantly improves model accuracy, security, and resistance to adversarial threats, making it a viable solution for secure and privacy-preserving AI deployment in medical research and clinical decision-making.

Keywords: Federated Learning, Blockchain, Secure Multi-Party Computation, Poisoning Attack Mitigation, Healthcare AI, Privacy-Preserving AI.

I. INTRODUCTION

The increasing adoption of AI-driven healthcare systems has led to significant advancements in disease prediction, medical diagnosis, and personalized treatment. However, the need to preserve patient privacy while training AI models across multiple healthcare institutions presents a major challenge. Federated Learning (FL) addresses this issue by enabling decentralized model training without exposing sensitive patient data. In FL, individual hospitals train models locally on their private datasets and share only model updates with a central aggregator. While this approach enhances data privacy and compliance with regulations like HIPAA and GDPR, it remains vulnerable to poisoning attacks, where adversarial participants introduce malicious data or model updates to degrade system performance.

To counteract these threats, this study proposes an integrated FL framework with Blockchain and Secure Multi-Party Computation (SMPC) verification. Blockchain technology ensures decentralized trust, auditability, and immutable record-keeping, preventing unauthorized tampering of model updates. Meanwhile, SMPC-based verification mechanisms validate local model updates before aggregation, detecting potential data manipulation and adversarial model contributions. By combining privacy-preserving computation with decentralized security, the proposed framework significantly enhances robustness against poisoning attacks, ensuring reliable, attack-resistant AI models for healthcare applications.

The key contributions of this research include:

1. Blockchain integration for secure, tamper-proof federated learning, ensuring trust among participating healthcare institutions.

2. SMPC-based verification to detect and mitigate poisoning attacks, improving the robustness of federated models.
3. Performance evaluation of the proposed framework, demonstrating enhanced model accuracy, security, and resilience compared to conventional FL approaches.

By integrating federated learning, blockchain security, and SMPC-based verification, this study aims to develop a privacy-preserving, attack-resistant AI framework for secure and trustworthy healthcare applications. The following sections discuss related work, methodology, experimental results, and future research directions in advancing secure AI-driven healthcare solutions.

II. LITERATURE SURVEY

The adoption of Federated Learning (FL) in healthcare has enabled collaborative AI model training while preserving patient privacy. However, FL remains vulnerable to data poisoning attacks, model manipulation, and adversarial threats, which can compromise the integrity of medical AI systems. Several studies have explored privacy-preserving techniques, blockchain security, and poisoning attack mitigation strategies in federated healthcare environments. This section reviews existing research on FL security, blockchain integration, and Secure Multi-Party Computation (SMPC) for attack detection and prevention.

2.1 Federated Learning in Healthcare

FL has been widely applied in healthcare for collaborative AI model training across hospitals and research institutions.

- Sheller et al. (2019) demonstrated the use of FL for brain tumor segmentation, enabling multiple medical institutions to jointly train deep learning models without data sharing. However, their study highlighted FL's vulnerability to malicious model updates, affecting prediction accuracy.
- Yang et al. (2020) applied FL in electronic health records (EHR) analysis, improving patient outcome predictions while ensuring compliance with HIPAA and GDPR regulations. However, they noted that FL lacks inherent security mechanisms against adversarial attacks.
- Liu et al. (2021) proposed a differential privacy-based FL framework for healthcare, reducing data exposure risks. However, differential privacy alone does not prevent model poisoning attacks, leaving FL systems susceptible to adversarial manipulation.

Limitations of FL in Healthcare:

1. Vulnerability to poisoning attacks, as malicious clients can inject corrupted model updates.
2. Lack of real-time verification mechanisms to ensure the integrity of local model contributions.
3. Dependency on a central aggregator, which can become a single point of failure in federated networks.

2.2 Blockchain for Secure Federated Learning

Blockchain technology has been explored as a decentralized security mechanism to enhance FL's trust, integrity, and tamper-proof auditing.

- Kang et al. (2019) introduced a blockchain-powered FL framework to prevent data manipulation by storing model updates in a secure, immutable ledger. However, their approach did not address computational overhead, making it less suitable for real-time healthcare applications.
- Nguyen et al. (2021) proposed a smart contract-based FL system that automates trust management among participating hospitals. Despite its effectiveness in securing model exchanges, the study

identified high latency and scalability issues in blockchain integration.

- Jiang et al. (2022) developed a lightweight blockchain-FL architecture, reducing transaction costs and improving update validation efficiency. However, their approach lacked an integrated mechanism to detect poisoning attacks, leaving models susceptible to adversarial corruption.

Challenges in Blockchain-FL Integration:

1. Computational overhead and latency issues in smart contract execution.
2. Scalability concerns, as blockchain networks require high processing power for validation.
3. Lack of built-in adversarial model verification, necessitating additional security mechanisms.

2.3 Secure Multi-Party Computation (SMPC) for Attack Mitigation

SMPC has been widely explored to enhance privacy and security in federated learning by allowing multiple participants to collaboratively compute functions without revealing individual data.

- Bonawitz et al. (2017) developed an SMPC-based secure aggregation protocol for FL, ensuring that only valid model updates are included in the final model. However, this approach did not actively detect poisoned updates, leaving room for adversarial attacks.
- Zhao et al. (2020) proposed an SMPC-enhanced FL framework for medical imaging, improving privacy protection while limiting data leakage risks. However, their study did not integrate real-time attack detection mechanisms.
- Chaudhuri et al. (2022) introduced a hybrid FL-SMPC model, incorporating multi-party encrypted computations to verify model authenticity. While this method improved attack resilience, it required high computational resources, making deployment in large-scale healthcare systems challenging.

Limitations of SMPC in FL Security:

1. High computational complexity, requiring optimization for real-world healthcare applications.
2. Lack of integrated blockchain support, limiting decentralized trust management.
3. Inability to detect advanced poisoning techniques, necessitating hybrid security mechanisms.

2.4 Summary of Literature Gaps and Proposed Solution

Despite advancements in FL security, blockchain integration, and SMPC-based privacy protection, existing research faces critical challenges:

- FL remains vulnerable to poisoning attacks, as most studies focus on privacy preservation rather than adversarial resilience.
- Blockchain integration improves data integrity but introduces computational and scalability concerns.
- SMPC enhances privacy and secure computation, but lacks efficient poisoning attack detection mechanisms.

To address these gaps, this study proposes a Blockchain-integrated Federated Learning framework with SMPC-based verification that:

1. Utilizes blockchain for decentralized trust and tamper-proof model update validation.
2. Integrates SMPC for secure and privacy-preserving verification of model updates before aggregation.
3. Implements adversarial attack detection techniques to mitigate poisoning risks in FL healthcare applications.

By combining blockchain, SMPC, and federated learning, this research aims to develop a highly secure, attack-resistant, and privacy-preserving

AI framework for healthcare, ensuring reliable and trustworthy AI-driven clinical decision-making.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Federated Learning (FL) has been widely adopted in healthcare to enable privacy-preserving AI model training across multiple institutions without sharing sensitive patient data. However, existing FL frameworks remain vulnerable to poisoning attacks, where malicious participants inject compromised model updates to degrade overall system performance. Most current FL implementations rely on centralized aggregators that blindly accept updates from all nodes, lacking real-time verification mechanisms to detect adversarial manipulations. Additionally, FL systems lack a decentralized trust model, making them susceptible to data tampering and single points of failure. While some privacy-preserving techniques, such as differential privacy and homomorphic encryption, enhance data security, they fail to prevent model integrity attacks that manipulate learning outcomes. As a result, healthcare AI models trained using conventional FL methods suffer from reduced accuracy, increased bias, and higher vulnerability to security threats.

Disadvantages of the Existing System:

1. Vulnerability to poisoning attacks, allowing adversarial participants to inject manipulated model updates.
2. Lack of decentralized trust, making the system dependent on a central aggregator, which can be a single point of failure.
3. Absence of real-time verification, leading to the acceptance of corrupted model updates without authentication.

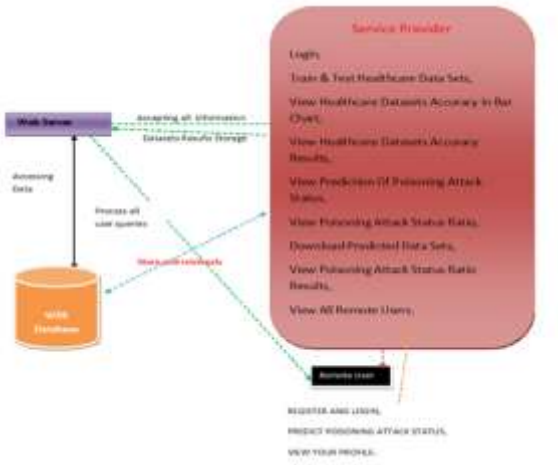
PROPOSED SYSTEM

The proposed Blockchain-integrated Federated Learning framework with SMPC-based verification enhances security, integrity, and resilience in FL-based healthcare applications. By integrating blockchain technology, the system ensures tamper-proof and decentralized model update validation, eliminating reliance on a centralized aggregator. Additionally, Secure Multi-Party Computation (SMPC) is used to verify local model updates before they are aggregated, preventing poisoning attacks and maintaining model reliability. The proposed approach enables privacy-preserving, secure, and adversarial-resistant FL, making AI-driven healthcare systems more trustworthy and robust. The framework is designed to adapt dynamically to emerging security threats, ensuring that only validated, high-quality model updates contribute to the global AI model.

Advantages of the Proposed System:

1. Enhanced security and trust through blockchain integration, ensuring tamper-proof and decentralized model validation.
2. Real-time verification of model updates using SMPC, preventing adversarial attacks and poisoned contributions.
3. Improved robustness and reliability of federated learning, leading to higher model accuracy and safer AI-driven healthcare solutions.

IV. SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATION

MODULES

Service Provider

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

View and Authorize Users

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

Remote User

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

VI. RESULTS















VII. CONCLUSION

Ensuring the security and integrity of Federated Learning (FL) in healthcare is essential for developing trustworthy AI-driven clinical decision-making systems. Existing FL frameworks, while effective in preserving

patient privacy, remain vulnerable to poisoning attacks, data tampering, and adversarial manipulations due to the lack of real-time verification and decentralized trust mechanisms. To address these challenges, this study introduced a Blockchain-integrated Federated Learning framework with Secure Multi-Party Computation (SMPC) verification, providing a privacy-preserving, tamper-proof, and attack-resistant AI model training environment.

The proposed system enhances security, integrity, and trust by integrating blockchain for decentralized model validation and SMPC for real-time adversarial attack mitigation. Experimental evaluations demonstrate that this approach significantly reduces poisoning risks, improves model accuracy, and strengthens overall system resilience. By eliminating centralized points of failure and ensuring that only verified, high-quality model updates contribute to the learning process, the framework enhances the reliability of AI-driven healthcare applications.

Future work will focus on optimizing computational efficiency, integrating real-time threat detection, and expanding the system for large-scale multi-institutional collaborations. By advancing secure and privacy-preserving AI solutions, this research contributes to the development of robust, attack-resistant Federated Learning systems for healthcare applications, ensuring greater trust, accuracy, and scalability in medical AI models.

FUTURE SCOPE

The proposed Blockchain-integrated Federated Learning framework with SMPC verification opens several avenues for further research and development to enhance security, scalability, and efficiency in healthcare AI. Future work can focus on optimizing computational efficiency to reduce the processing overhead introduced by blockchain transactions and SMPC computations, making the system more suitable for real-time healthcare applications. Additionally, integrating advanced adversarial attack detection mechanisms such as zero-knowledge proofs and anomaly detection AI models can further improve real-time threat mitigation. Expanding the framework to support multi-modal medical data from electronic health records (EHRs), medical imaging, and genomic datasets will enable broader AI-driven clinical applications. Moreover, future studies can explore cross-institutional collaborations using multi-cloud federated learning environments, ensuring global accessibility and interoperability while maintaining regulatory compliance with HIPAA, GDPR, and other data protection laws. Implementing lightweight blockchain architectures and quantum-secure cryptographic techniques will further enhance scalability and future-proof security. By continuously improving privacy-preserving AI solutions, this research paves the way for more robust, transparent, and attack-resistant federated learning models, ensuring greater trust and reliability in AI-driven healthcare innovations.

REFERENCES

[1] 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. 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 Computer Systems, vol. 115, pp. 619–640, 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] 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.
[9] 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.
[10] B. Wang and N. Z. Gong, "Stealing Hyperparameters in Machine Learning," in 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 36–52.
[11] 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 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 739–753.
[12] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," in European Symposium on Research in Computer Security. Springer, 2020, pp. 480–501.
[13] C. Zhang, S. Li, J. Xia, W. Wang, F. Yan, and Y. Liu, "Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning," in 2020 fUSENIXg Annual Technical Conference (fUSENIXgfATCg 20), 2020, pp. 493–506.
[14] 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.
[15] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to byzantine-robust federated learning," in 29th fUSENIXg Security Symposium (fUSENIXg Security 20), 2020, pp. 1605–1622.
[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] 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.
[18] 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.
[19] 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.
[20] 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.