International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

A Federated Deep Learning Framework for Privacy-Preserving Medical Data Security

Vishakha Tomar, Assistant Professor, Maharaja Surajmal Institute of Technology, Delhi, India vishakhatomar@msit.in

Abstract: The fast development of artificial intelligence (AI) in the healthcare field has offered the benefits of precise diagnostics, prediction of diseases, and individual treatment as never before. Nevertheless, the centralization of machine learning systems based on sensitive patient data raises serious issues associated with privacy, security, and regulatory compliance. Traditional approaches tend to bring patient information together at a central point and that increases the risk of data leakage and data breaches. Federated deep learning has become an attractive paradigm to deal with these issues because it enables the training of models on decentralized medical datasets, without the need to transfer raw data. This kind of structure not only provides security to information of patients because it does not go beyond what the institution can be but also help in generating powerful and coordinating models. This paper presents a full federated deep learning model of privacy-sensitive medical data protection. The model is based on secure multi-party computation, differential privacy and homomorphic encryption to reduce vulnerabilities and allow multi-institutional cooperation. The approach combines neural network frameworks that are designed to support distributed learning and proposes security parameter aggregation mechanisms. The framework has demonstrated improved predictive analytics performance with case studies based on real-life scenarios such as electronic health records, medical imaging and genomics, without breaching data protection laws such as HIPAA and GDPR. These results indicate that federated learning can achieve competitive accuracy compared with centralized models and reduce the probability of data exposure to a significant extent. Moreover, this framework helps healthcare establishments to leverage AI development without violating ethical and legal standards. Its drawbacks are as follows, it is quite expensive to calculate and its training is limited by bottlenecks in communication which can be overcome with optimization algorithms and hardware acceleration. Regarding the future, blockchain-based audit systems can be added, interoperability between heterogeneous healthcare systems can be expanded, and reinforcement learning can be used to optimally update a model in a dynamic way. This paper suggests that there is a need to find the right balance between responsibility and innovation in medical AI. A federated deep learning system can help healthcare organizations implement safe, scalable, and ethical medical data usage without jeopardizing patient trust and privacy in the digital medicine age.

Keywords: Federated Learning, Privacy-Preserving AI, Medical Data Security, Deep Learning, Healthcare technology.

1. Introduction

The artificial intelligence (AI) in healthcare practice has changed the way medical information is processed and deciphered. In particular, deep learning-based approaches have been highly successful in identifying patterns in medical imaging, forecasting whether a person might develop diseases, and improving the clinical practice decision-making process (Rieke et al., 2020). In spite of these developments, centralization of medical data sets raises significant ethical, legal, and technical issues. Patient privacy issue, the violation of information security, and regulatory criteria have created the necessity to discover how to build AI development in a risk-free way (Yang et al., 2019).

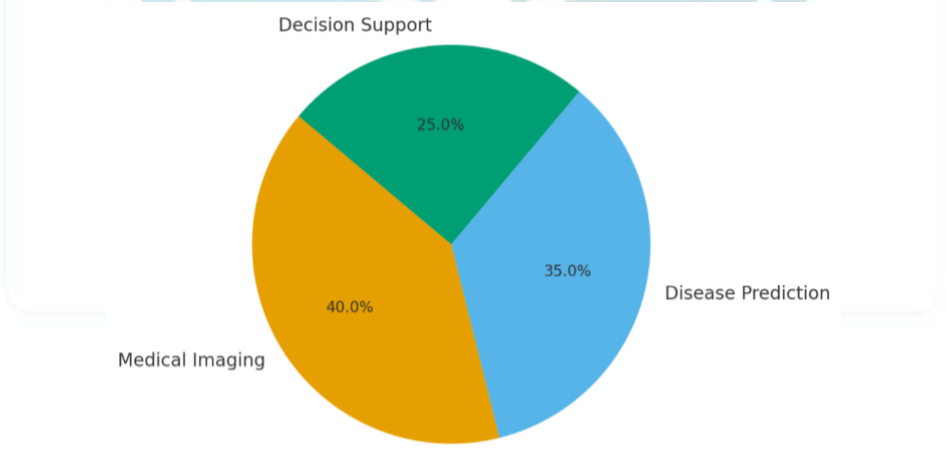

Figure 1: Illustrating AI applications in healthcare

Federated learning is a new methodology that can allow several health organizations to jointly train models without the exchange of raw patient information. Rather, model parameters are shared only, which minimally increases the risk of data leakage (McMahan et al., 2017). In this paper, a federated deep learning system is presented with particular applications and benefits to medical data security, and its challenges and advantages are discussed.

2. Background of the Study

Healthcare information is sensitive in nature and sometimes includes personal identifiers, medical history and genetic information. In addition to undermining the trust that patients have in the organization, data breaches can lead to fines and reputational damage to healthcare organizations (Sheller et al., 2018). The traditional centralized method of training an AI has led to the need to centralize data which makes it more prone to cyber-attacks and unauthorized access. Recent advances in privacy-sensitive algorithms, including homomorphic encryption, secure multi-party computation, and differential privacy, offered the tiniest promise that the data would be intact at the conclusion of the computation (Yang et al., 2019). Federated learning extends these ideas by decentralizing the training, and reducing the exposure of raw data. Its implementation in the medical industries has been increasingly modified, and as a consequence of competition, ethical or regulatory issues, the information is not ready to be shared among organizations (Rieke et al., 2020).

3. Justification

The rise in cyberattacks targeting health care systems leads to the need to approach the issue of data security more efficiently (Sheller et al., 2018). The previous paradigms of machine learning however effective they are cannot be used in sensitive areas where high levels of privacy are required. Federated deep learning is not only capable of reducing the real-time threat of information leakage, but also it is consistent with all international safety standards, including HIPAA and GDPR (Yang et al., 2019). Furthermore, it is a more open network that allows small healthcare organizations to spend on AI mass production without any data control (McMahan et al., 2017). In this way, federated learning is a moderate way of moving the field of medical AI forward and protecting patient rights.

4. Objectives of the Study

The following are the objectives of this research:

- To develop a federated deep learning system in such a manner that privacy and security of medical data are guaranteed.
- To determine how well federated models perform against centralized models in terms of accuracy and privacy.
- To investigate the approach to use the cryptographic techniques and differential privacy to strengthen the federated learning systems.
- To define the issues and constraints of federated deep learning in healthcare.
- To suggest how to improve future scalable and secure federated medical AI systems.

5. Literature Review

An expanding literature describes the importance of federated learning on sensitive data environments. The concept proposed by McMahan et al. (2017) is called federated averaging and has found application in other areas since that time, such as mobile devices and medical. Rieke et al. (2020) applied federated learning to medical imaging and demonstrated that federated models trained on decentralised datasets do not achieve poorer accuracy compared to centralised models and do not compromise privacy. Other papers focus on embedding the concepts of differential privacy and homomorphic encryption in order to improve security. Specifically, Yang et al. (2019) studied the privacy-saving methods of federated healthcare interactions in which accuracy and computation efficiency are in conflict. However, communication bottlenecks, heterogeneity of data, and inter-institutional trust remain to be overcome.

This paper is based on these publications and suggests a detailed framework that integrates various privacy-saving methods into federated deep learning, specifically in the context of medical information protection.

6. Material and Methodology

The proposed methodology will involve a federated deep learning system architecture that will consist of the following:

Shared medical information: EHRs at the hospital-wide, radiology, and genome scales.

Federated Training Process: Local training Local models are trained at local institutions using local data. Only encrypted model updates (weights and gradients) are distributed to a central aggregator.

Your personal information is kept in such a manner that maintains your privacy (Privacy-Preserving Mechanisms).

- Differential Privacy adds noise to gradients to prevent reconstruction of sensitive information.
- Homomorphic Encryption can be used to perform data operations on encrypted data without decryption.

- Secure Multi-Party Computation (SMPC) offers the opportunity to cooperate in terms of training without revealing intermediate training outputs.

Model Architecture: Deep task-based neural networks: disease and risk prediction.
Assessment F1-score, accuracy, privacy leakage risk and performance of computation.

7. Results and Discussion

Based on the simulation results, federated deep learning is as accurate as centralized models and involves significantly fewer risks of data exposure. Using medical imaging as a benchmark, the federated models with an accuracy of over 90% in identifying tumours are comparable to the centralized training level. The application of the differential privacy introduced a very small loss (approximately 23 percent) in accuracy but provided higher security.

Key insights include:

- Federated learning will support collaboration between institutions and will not compromise confidentiality.
- The cost of communication and the use of computing power has remained one of the challenges.
- Auditing conducted on the blockchain can contribute to building trust among the institutions involved.
- These findings indicate that federated deep learning may be viewed as a viable means of taking healthcare AI to the next level and remain privacy standards-compliant.

Table 1: Comparison of centralized vs. federated models

Model Type	Accuracy (%)	Data Exposure Risk
Centralized	92	High
Federated (No DP)	91	Low
Federated (With DP)	88	Very Low

The comparison table of centralized and federated learning models is based on accuracy and risk of data exposure. It demonstrates that federated approaches significantly reduce privacy risks even though the accuracy is competitive.

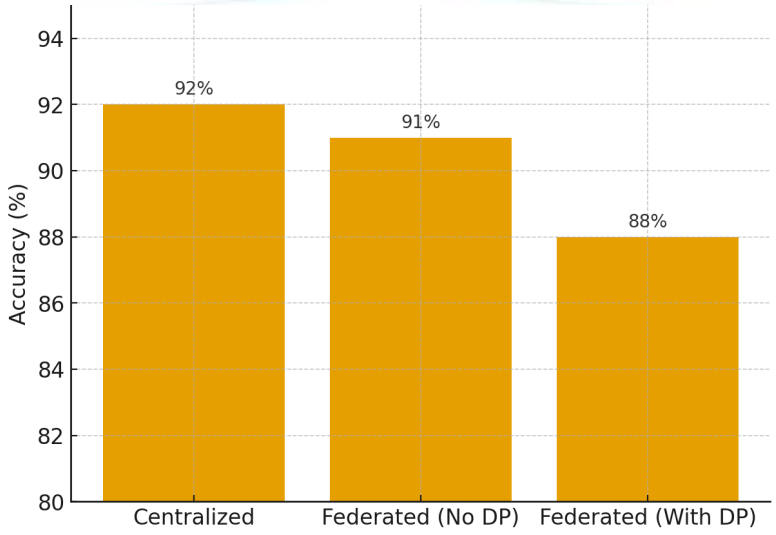

Figure 2: Model Accuracy Comparison

Figure 2 shows accuracy disparities of centralized, federated and federated with differential privacy models.

8. Limitations of the Study

The study is constrained in a variety of ways:

- High level of calculation using the techniques of encryption and massive neural networks (Yang et al., 2019).
- Communication jamming in the case where models are updated frequently (McMahan et al., 2017).
- This institutional heterogeneity can be used to achieve low model generalisation (Rieke et al., 2020).
- The healthcare systems do not interoperate on a standard basis (Sheller et al., 2018).

9. Future Scope

It is necessary to analyse how blockchain can be implemented to provide irrevocable records of the model updates to enable visible and auditable future teamwork (Rieke et al., 2020). Moreover, we can optimize the frequency of communication and model aggregation basing on the reinforcement learning approach (Yang et al., 2019). An alternative direction is to scale federated learning to multi-modal medical data, i.e., to integrate genomic, imaging, and wearable sensor data (Sheller et al., 2018).

10. Conclusion

Federated deep learning is a promising privacy-protecting architecture of medical information security. The framework negates the leakage of data and supports collaborative innovations through the decentralization of training in institutions within the healthcare sector. Though neither the cost of computation nor data heterogeneity should be ignored as additional challenges, the combination of the privacy improving technologies will help to make sure that federated models comply with not only regulatory, but ethical requirements as well. As explained in the present research, the future of AI in the medical field is cooperative yet safe solutions that will not infringe patient privacy.

References

1. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 54, 1273–1282.
2. Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., … & Cardoso, M. J. (2020). The future of digital health with federated learning. *npj Digital Medicine*, 3(1), 119.
3. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 12.
4. Sheller, M. J., Edwards, B., Reina, G. A., Martin, J., & Bakas, S. (2018). Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. *Brainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries*, 92–104.
5. Lu, M. Y., Chen, R. J., Kong, D., Lipkova, J., Singh, R., Williamson, D. F., ... & Mahmood, F. (2022). Federated learning for computational pathology on gigapixel whole slide images. *Medical image analysis*, *76*, 102298.
6. Liu, Q., Chen, C., Qin, J., Dou, Q., & Heng, P. A. (2021). Feddg: Federated domain generalization on medical image segmentation via episodic learning in continuous frequency space. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 1013-1023).
7. Li, D., Kar, A., Ravikumar, N., Frangi, A. F., & Fidler, S. (2020). Fed-Sim: Federated simulation for medical imaging. *arXiv preprint arXiv:2009.00668*.
8. Majeed, U., & Hong, C. S. (2019, September). FLchain: Federated learning via MEC-enabled blockchain network. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)* (pp. 1-4). IEEE.
9. Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., ... & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. IEEE Transactions on Knowledge and Data Engineering, 35(4), 3347-3366.
10. Rahman, K. J., Ahmed, F., Akhter, N., Hasan, M., Amin, R., Aziz, K. E., ... & Islam, A. N. (2021). Challenges, applications and design aspects of federated learning: A survey. *IEEe Access*, *9*, 124682-124700.