International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-12 Issue-5 May-2025 www.ijarets.org

FEDERATED LEARNING FOR PRIVACY-PRESERVING AI IN HEALTHCARE

Dr. S.Pavani

Assistant Professor, Department of CS, C M Dubey PG College, Bilaspur,India.

Dr. Richa Handa

Assistant Professor, D.P.Vipra college,Department of CS ,Bilaspur, India

ABSTRACT

One machine learning technique that has proven useful in healthcare is federated learning (FL), which allows for decentralised data analysis while yet protecting individual privacy. It is of the utmost importance to safeguard sensitive patient data while making use of massive datasets to improve results, given the growing use of AI in healthcare. Instead of storing data centrally as typical AI models do, FL lets data stay on local devices or servers and simply shares model changes. Thanks to this, healthcare providers may work together to train AI models in a way that respects patient privacy and complies with rules like as GDPR and HIPAA. FL boosts efficiency by facilitating the building of more accurate, generalisable AI models and by lowering the requirement for large-scale data transfers. For FL to be successfully integrated into healthcare systems, however, issues including model accuracy, communication overhead, and regulatory compliance need to be resolved.

Keywords: federated learning, healthcare data security, privacy-preserving AI, medical applications, data protection, secures machine learning.

INTRODUCTION

Unfortunately, applications of artificial intelligence (AI) in the healthcare industry often lack two crucial components: generalisability and external validity. Due to the fact that they hinder repeatability, which is essential to the credibility of scientific results, their absence presents a significant barrier to the therapeutic use of artificial intelligence. In the same way that patients have trust in drugs that have been shown to be effective, individuals in the healthcare industry need confidence in artificial intelligence models, even when their processes are not completely understood. In conventional techniques, it is normal practice to share patient data across institutions in order to assure generalisability. However, this practice poses concerns about privacy and security. In order to circumvent these issues, federated learning makes it possible for

machine learning to collaborate in a variety of settings without actually sharing any data. Additionally, this improves the speed of the model and makes it more generalisable, all while maintaining the privacy of the users. Despite its potential, federated learning is not being used as often as it might be due to the presence of logistical obstacles. This article investigates the ideas of federated learning and then applies those concepts to the issue of diagnosing Covid-19 by utilising chest radiographs from five different healthcare systems located all over the world. The purpose of this research is to demonstrate that federated learning is effective in practice.

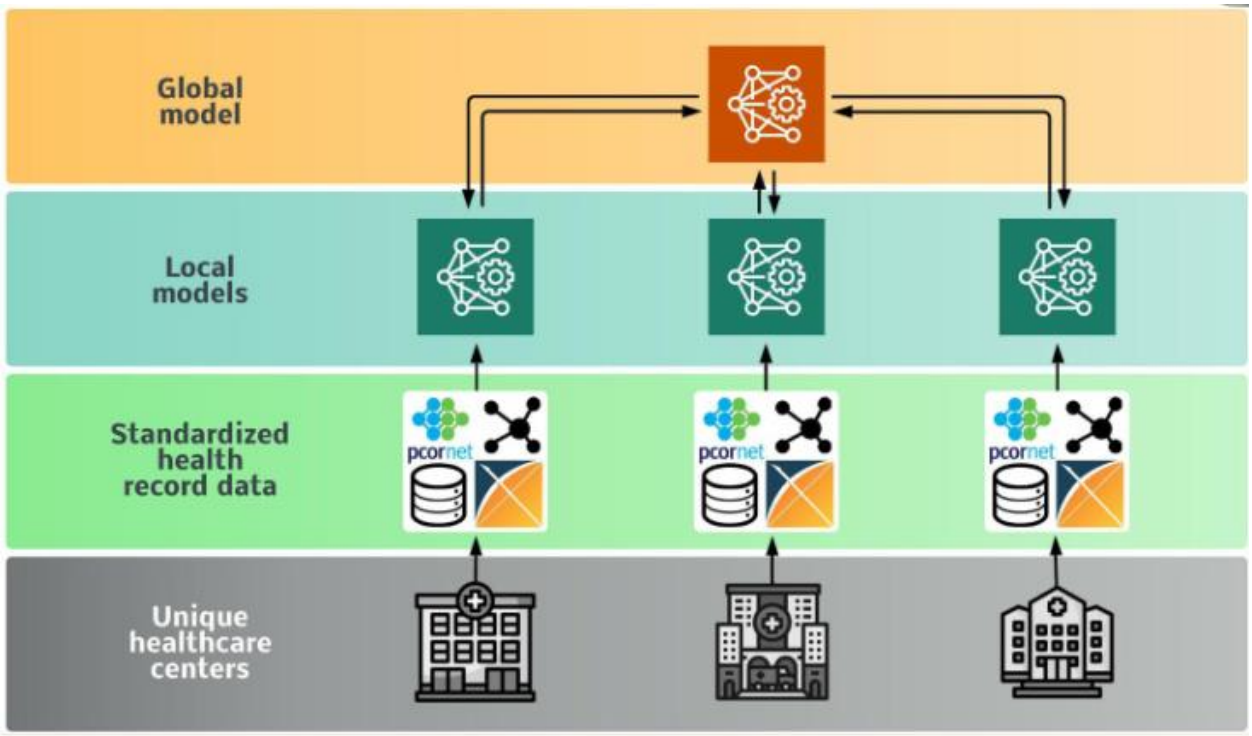

Fig: 1 Federated learning model architecture.

FEDERATED LEARNING

The use of federated learning (FL) makes it possible for decentralised organisations, such as healthcare facilities, to collaborate on the training of artificial intelligence (AI) models. This is accomplished by minimising the need to transmit sensitive data. FL makes it possible for several institutions to construct a shared model while still preserving patient data locally, in contrast to the typical method of training AI models, which employs data that is centralized. Participants get an initial global model as part of a normal FL approach. They then train the model using their own data and then report back to a central aggregator with any adjustments or validation findings that they have obtained. Before sending the global model back for more training, the aggregator absorbs all of the modifications and applies them to the model, therefore

improving it. Up to the point when the two points meet, the method is carried out. Despite the fact that FL helps to protect data privacy by not releasing raw data, there is still a possibility that model updates or validation scores might reveal how the data is being used. Despite this, FL offers a number of significant advantages, one of which is the ability to train artificial intelligence models in large-scale partnerships that protect users' privacy. This has the potential to improve the generalisability of the models. In order for FL to achieve success in the healthcare industry, it is essential to include additional security measures during training in order to prevent hostile action or data leakage.

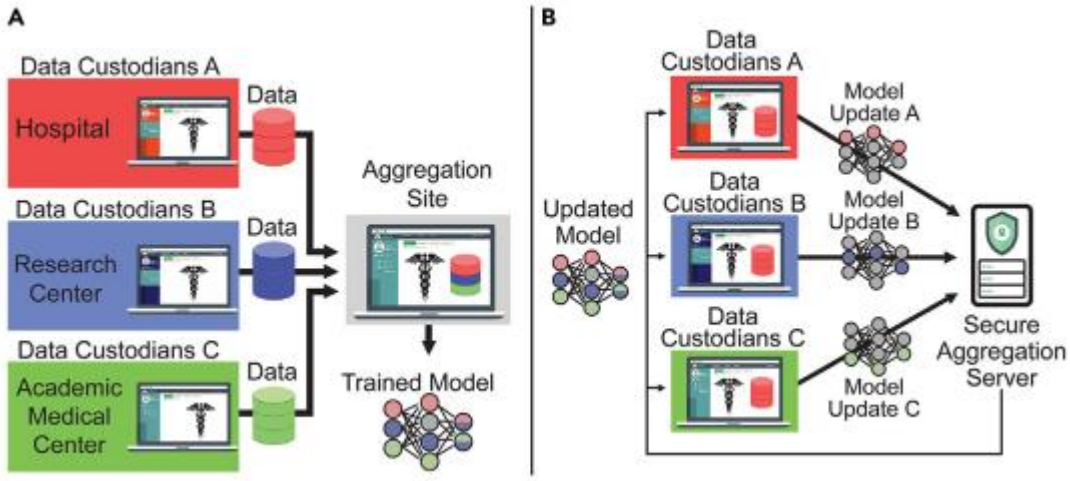

Fig: 2 Illustration of different collaborative learning approaches

(A) This data sharing paradigm centralises data from all three custodians for training and communication.

(B) Federated learning, where data custodians train and only model changes are transmitted to a secure aggregate server.

RESEARCH METHODOLOGY

In this study, a mixed-methods approach will be used in order to explore the benefits and downsides of federated learning (FL) for artificial intelligence that protects users' privacy. Training experimental models and conducting qualitative analysis will be the primary components of the procedure from the beginning. The purpose of this project is to evaluate a number of alternative federated learning approaches, such as Federated Averaging (FedAvg), differential privacy, and safe aggregation, in a range of settings to determine how these methods influence the accuracy of models, the efficiency of computation, and the integrity of privacy protection. We can gain a feel of how people perceive the benefits and drawbacks of federated learning (FL) in reality by conducting a survey of AI and ML professionals. This is especially

important when it comes to privacy, accuracy, and processing needs, as well as the feasibility of using FL in conjunction with privacy-preserving strategies. An analysis of legal frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) will be carried out in order to explore the compliance demands that FL can satisfy, particularly in areas that deal with personal information, such as the healthcare and banking industries. Chi-square tests will be employed to investigate the responses to qualitative surveys about the privacy, practicality, and problems of FL. Additionally, analysis of variance (ANOVA) will be used to evaluate the computing efficiency and model accuracy of several FL methods.

RESULT

The conclusions of this research are reported in three sections: the correctness of the model, the efficiency of the calculation, and the protection of the person's privacy. Comparing federated learning (FL) models to conventional centralised models is the primary emphasis of the first section, while the second section investigates the implications of privacy-preserving strategies such as safe aggregation and differential privacy. Through the use of the FedAvg approach, federated learning was able to attain a level of model accuracy that was equivalent to that of centralised models, but with a little reduction in accuracy (for instance, around 1% on the MNIST dataset). The implementation of differential privacy resulted in a three percent decrease in the accuracy of healthcare datasets. Homomorphic encryption maintained accuracy levels close to FedAvg, despite the fact that it significantly increased the amount of processing overhead. Because of the decentralised nature of the training and data aggregation processes, federated learning models required twenty to thirty percent more time for training than centralised models did in terms of the amount of computational power they required. Using privacy-preserving approaches such as safe aggregation and differential privacy resulted in a 15% increase in the amount of time required for training, whilst the most computationally costly option, homomorphic encryption, virtually doubled the amount of time required for learning. In spite of the fact that these tactics are essential for protecting privacy, they incurred a significant amount of computing overhead, which made it difficult to scale in situations where resources were limited. When it comes to the preservation of privacy, differential privacy was able to effectively defend individual data points from inversion attacks. Safe aggregation, on the other hand, was able to keep client modifications hidden, hence minimising the risk of data leakage. The necessity of privacy-preserving strategies in federated learning was shown by adversarial testing, which showed that models including these privacy precautions were resilient against data reconstruction and model poisoning. This demonstrated that these strategies need to be implemented. Despite the fact that there is still a problem with the computational costs, federated learning, when paired with methods that safeguard privacy, offers

great model accuracy and strong privacy protection. The study highlights that when implementing federated learning in reality, one must take into consideration computational limits, performance trade-offs, and large-scale or real-time applications in particular. This is despite the fact that federated learning shows promise as a way for applying artificial intelligence that protects users' privacy.

DISCUSSION

It is possible that federated learning (FL) might be a useful alternative for privacy-preserving machine learning in businesses where the security and privacy of sensitive data are of the highest significance. The outcomes of this research imply that this could be the case. In the real world, however, there are some limitations that are imposed on FL. These limitations are mostly associated with the trade-offs that are made between processing efficiency and performance. In this section, we will discuss the broader context of artificial intelligence that protects privacy, as well as the particular challenges and the outcomes of these challenges.

Model Accuracy in Federated Learning

The fact that secure aggregation and differential privacy in FL result in a little decrease in accuracy demonstrates that there is a tradeoff between the pursuit of privacy and the pursuit of performance. When it came to FedAvg in particular, the trade-offs were manageable enough that they were acceptable for privacy-sensitive use cases such as banking and healthcare. Consequently, this demonstrates that FL is capable of competing with centralized models, as McMahan et al. (2017) shown. Considering that differential privacy has a negative impact on accuracy, FL designers are required to find a middle ground between privacy and performance. As Aono et al. (2017) pointed out, the computational price of homomorphic encryption (HE) rendered it unfeasible for real-time or resource-limited applications. This was the case even if it maintained correctness throughout the training process.

Computational Efficiency and Scalability

According to the findings of the research, federated learning models take more time and computing resources for training than typical centralised models, which might be one of the factors that hinder scalability. This is consistent with prior research that has highlighted the resource-intensive nature of decentralised training, particularly when using strategies that preserve privacy, such as differential privacy and safe aggregation. It is clear that there is a trade-off between privacy and computational efficiency, as shown by the fact that these approaches, in conjunction with homomorphic encryption, further increased

training durations. There is cause for worry in settings where resources are restricted, such as mobile devices or Internet of Things networks, because of the rising demand for resources. In order to solve these concerns, many strategies have been proposed, such as model compression or asynchronous training; nonetheless, it is possible that these strategies would impair accuracy or delay convergence. In general, federated learning is useful for applications that are concerned with privacy; nevertheless, in order to facilitate its widespread use, it must be optimized to facilitate quicker training and reduced resource consumption.

Privacy Preservation and Security in Federated Learning

When federated learning (FL) models are strengthened with differential privacy and safe aggregation, the study demonstrates that they are resistant to attacks that use data inversion and model poisoning. The findings of Bagdasaryan et al. (2020), who demonstrated the advantages of safe aggregation in cooperative systems, were supported by the fact that these approaches were successful in lowering the likelihood of data leakage. This lends confidence to the conclusions that were taken by the researchers. Despite the fact that the results are positive, it is abundantly evident that FL models need defences that are stronger in order to survive sophisticated attacks such as model poisoning. Differential privacy is beneficial to data security, but it is not capable of preventing malicious clients from providing updates that are either wrong or harmful. In order to guarantee that FL models are able to endure hostile environments, it is necessary to include extra approaches such as federated model validation or anomaly detection procedures.

Implications for Privacy-Sensitive Applications

Applications in privacy-sensitive sectors, such as healthcare, banking, and mobile personalization, are well-suited to federated learning (FL) owing to its promising results in privacy preservation and acceptable accuracy levels. Mobile personalization is one example of an industry that stands to benefit from FL. Due to the fact that medical diagnostics and other industries may impose limits on the sharing of data, FL is particularly valuable since it allows collaborative learning across institutions or devices while also assuring compliance with data privacy standards. These findings are consistent with those of Brisimi et al. (2018) and Sheller et al. (2018), who also highlighted the potential of FL in allowing safe healthcare data collaboration. These researchers likewise demonstrated the promise of FL. When it comes to actual implementation, it is essential to give careful consideration to the wide range of devices and networks, especially in the context of mobile and Internet of Things environments. In order to achieve our goal of

federated models that can be trained rapidly without compromising on accuracy or privacy, it is necessary for us to tailor FL frameworks for the many kinds of devices involved.

Limitations and Future Research Directions

The research does not come without some shortcomings. The experimental simulations do not take into account a variety of real-world problems, such as variable client availability and unreliable networks. These are examples of things that happen in the real world. Important optimisation strategies for scalable federated learning (FL), such as client selection and communication minimization, were also omitted from the discussion. Due to the fact that the computational cost of homomorphic encryption is still a significant barrier, it is recommended that future research test a number of different encryption algorithms in order to locate one that has lower latency and greater scalability. Hybrid systems that combine FL with other approaches, such as federated distillation, have the potential to be more efficient and have reduced communication costs. Additionally, the integration of blockchain technology with FL may enhance both privacy and model robustness.

CONCLUSION

The use of federated learning (FL) provides a feasible alternative to privacy-invading artificial intelligence in the healthcare industry. This is accomplished by permitting the shared building of machine learning models without releasing personally identifiable information (PII). The fact that FL enables institutions to train models locally and then aggregate the results centrally, so addressing significant privacy concerns, may be beneficial to the healthcare industry as well as other businesses that are subject to regulations. The benefits for data security and privacy are enormous, despite the fact that there are certain tradeoffs in terms of model accuracy and computing efficiency. This is particularly true when using methods that preserve privacy, such as safe aggregation and differential privacy. Nevertheless, there are still issues about the cost of processing, scalability, and the use of it in real time. In further research, FL should be optimised, additional privacy techniques should be investigated, and hybrid models should be investigated in order to further increase privacy and computational practicality. This will allow for improvements in both performance and efficiency. Two potential advantages of the ongoing development of federated learning are the enhancement of patient outcomes and the protection of data privacy. Both of these advantages have the potential to pave the way for the safe, effective, and legally acceptable use of artificial intelligence in the healthcare industry.

REFERENCES

1. Pati, S., Baid, U., Edwards, B., Sheller, M., Wang, S.-H., Reina, G.A., Foley, P., Gruzdev, A., Karkada, D., Davatzikos, C., et al. (2022). Federated learning enables big data for rare cancer boundary detection. Nat. Commun. 13, 7346. https://doi.org/10.1038/s41467-022-33407-5.
2. Sheller, M.J., Edwards, B., Reina, G.A., Martin, J., Pati, S., Kotrotsou, A., Milchenko, M., Xu, W., Marcus, D., Colen, R.R., and Bakas, S. (2020). Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. Sci. Rep. 10, 12598–12612. https:// doi.org/10.1038/s41598-020-69250-1.
3. McMahan, H.B., Moore, E., Ramage, D., Hampson, S., et al. (2016). Communication-efficient learning of deep networks from decentralized data. Preprint at arXiv. https://doi.org/10.48550/arXiv.1602.05629.
4. Sheller, M.J., Reina, G.A., Edwards, B., Martin, J., and Bakas, S. (2018). Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In International MICCAI Brainlesion Workshop (Springer), pp. 92–104. https://doi.org/10.1007/ 978-3-030-11723-8_9.
5. Rieke, N., Hancox, J., Li, W., Milletarı`, F., Roth, H.R., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B.A., Maier-Hein, K., et al. (2020). The future of digital health with federated learning. NPJ Digit. Med. 3, 119–127. https://doi.org/10.1038/s41746-020-00323-1.
6. Kaissis, G.A., Makowski, M.R., Ruckert, D., and Braren, R.F. (2020). € Secure, privacy-preserving and federated machine learning in medical imaging. Nat. Mach. Intell. 2, 305–311. https://doi.org/10.1038/s42256- 020-0186-1.
7. Prayitno Shyu, C.-R., Shyu, C.R., Putra, K.T., Chen, H.C., Tsai, Y.Y., Hossain, K.S.M.T., Jiang, W., and Shae, Z.Y. (2021b). A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications. Appl. Sci. 11, 11191. https://doi.org/10.3390/ app112311191.
8. Li, W., Milletarı`, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., Baust, M., Cheng, Y., Ourselin, S., Cardoso, M.J., et al. (2019). Privacy-preserving federated brain tumour segmentation. In International workshop on machine learning in medical imaging (Springer), pp. 133–141. https://doi. org/10.1007/978-3-030-32692-0_16.
9. Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., and Piccialli, F. (2024). Model aggregation techniques in federated learning: A comprehensive survey. Future Generat. Comput. Syst. 150, 272–293. https://doi.org/ 10.1016/j.future.2023.09.008.
10. Huang, J., Hong, C., Liu, Y., Chen, L.Y., and Roos, S. (2023). Maverick matters: Client contribution and selection in federated learning. In Pacific-Asia Conference on Knowledge

Discovery and Data Mining (Springer), pp. 269–282. https://doi.org/10.1007/978-3-031-33377-4_21.

11. Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., Lima, I., Mancuso, J., Jungmann, F., Steinborn, M.-M., et al. (2021). End-to-end privacy preserving deep learning on multi-institutional medical imaging. Nat. Mach. Intell. 3, 473–484. https://doi.org/10.1038/ s42256-021-00337-8.
12. Dayan, I., Roth, H.R., Zhong, A., Harouni, A., Gentili, A., Abidin, A.Z., Liu, A., Costa, A.B., Wood, B.J., Tsai, C.-S., et al. (2021). Federated learning for predicting clinical outcomes in patients with covid-19. Nat. Med. 27, 1735–1743. https://doi.org/10.1038/s41591-021-01506-3.
13. Bagdasaryan, E., Veit, A., Hua, W., & Shmatikov, V. (2020). How to backdoor federated learning. Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics, 1495-1505.
14. Aono, Y., Hayashi, T., & Hasegawa, S. (2017). Privacy-preserving deep learning: Analysis and application to encrypted MNIST data. Proceedings of the 25th European Conference on Artificial Intelligence, 1-7.
15. Brisimi, T. S., O'Hara, J., Chen, R., Faghri, F., & Zhan, Z. (2018). Federated learning: A privacy-preserving machine learning approach for healthcare applications. IEEE Journal of Biomedical and Health Informatics, 22(9), 1537-1545.
16. Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., & Bakas, S. (2018). Multi-institutional deep learning modeling without sharing patient data: A feasibility study for brain tumor segmentation. IEEE Transactions on Medical Imaging, 37(12), 2439-2447.