Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Article

Privacy-Preserving Federated Learning: Advancements, Challenges, and Applications in Healthcare

Amit Walia [1*], Dr. Ravinder Singh Madhan [2]

[1] Ph.D., Research Scholar, Department of Computer Science and Engineering, IEC University, Baddi, Solan, Himachal Pradesh, India

[2] Associate Professor, Department of Computer Science and Engineering, IEC University, Baddi, Solan, Himachal Pradesh, India

Corresponding Author: * Amit Walia

DOI: https://doi.org/10.5281/zenodo.21023458

Abstract

This review delves into the evolving landscape of privacy-preserving federated learning, with a spotlight on its pivotal role and applications in healthcare. Federated learning, a decentralised machine learning approach, has emerged as a cornerstone for enabling model training across multiple devices or servers while maintaining data privacy. In the healthcare sector, preserving the confidentiality of sensitive patient data is paramount, necessitating innovative privacy-preserving techniques such as homomorphic encoding, differential privacy, and secure multi-party computation. The paper explores the integration of these techniques with disease prediction models, highlighting their potential to enhance remote patient monitoring, clinical decision support, and personalised medicine. Despite the promising advancements, the review identifies key challenges, including scalability, communication overhead, and ethical considerations, that need addressing to foster wider adoption. The paper concludes by projecting future directions, emphasising the continual development of privacy-preserving methods and their integration with emerging technologies to expand the applications of federated learning in healthcare. Through a comprehensive exploration, this review aims to shed light on the advancements, applications, and challenges, offering insights and recommendations for harnessing the potential of privacy-preserving federated learning in healthcare.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 02-02-2026
- **Accepted:** 27-03-2026
- **Published:** 30-03-2026
- **MRR:**4(3); 2026: 79-82

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Walia A, Madhan R S. Privacy-Preserving Federated Learning: Advancements, Challenges, and Applications in Healthcare. Indian J Mod Res Rev. 2026;4(3):79-82.

Access this Article Online

www.mrrjournal.in

KEYWORDS: Federated Learning, Privacy-Preservation, Healthcare Applications, Disease Prediction Models, Decentralized Learning, Data Security, Ethical Considerations.

INTRODUCTION

Federated Learning is a machine learning method that trains models on decentralised data, ensuring privacy and efficiency. It's applied in various fields, notably in healthcare, where it addresses privacy concerns related to personal health information (PHI). The method supports data privacy and security, reducing the risks of unauthorised access and the associated negative outcomes like identity theft and discrimination. It complies with legal standards like HIPAA, promoting trust and enabling patients to manage their health information securely. Privacy preservation in healthcare is vital for maintaining confidentiality in provider-patient communication and supporting public health initiatives by safely analysing large-scale health data [1][2].

The review focuses on the critical role of privacy preservation in healthcare, underscoring its impact on patients, providers, and organisations. It emphasises compliance with legal and ethical standards like HIPAA to protect personal health information and raises awareness about the risks of privacy breaches, including identity theft and discrimination. The review stresses the importance of maintaining trust in the healthcare system, secure communication, and supporting public health initiatives through confidential data analysis. Methodologically, it employs a multi-stage critical literature review using databases like Web of Science and Scopus, with an emphasis on Scopus for optimal results. Keywords were iteratively refined to capture relevant literature, assessing both quantitative and qualitative aspects to ensure thorough and reproducible research [1][3][4].

1. Federated learning concepts and principle

Federated learning is a cutting-edge machine learning paradigm that enables model training on decentralized data sources without the need to transfer raw data to a central server. This innovative approach addresses the challenges of data privacy, security, and communication costs associated with traditional centralized training methods. By keeping data local and private on individual devices while collaboratively training models, federated learning offers a privacy-preserving and efficient solution for machine learning tasks [1].

Concepts of Federated Learning:

Decentralised Training: Federated learning allows the distributed training of machine learning models across multiple devices or edge nodes without the need to aggregate or compromise the raw data. This decentralised approach ensures that sensitive data remains on local devices, reducing the risk of privacy breaches and unauthorised access [1],[5],[6]. Secure Aggregation Protocols: One key concept in federated learning is the use of secure aggregation protocols to protect data privacy during the model aggregation process. These protocols ensure that model updates from different devices are combined in a privacy-preserving manner, maintaining the confidentiality of individual data sources [1],[5], [8]-[13].

Principles of Federated Learning:

Privacy Preservation: The primary principle of federated learning is to preserve data privacy by keeping sensitive information local to each device. This approach minimises the risk of data exposure and unauthorised access, ensuring that individual data sources remain secure and confidential [1]. Data Efficiency: Federated learning leverages the collective knowledge and insights from distributed devices to improve model performance without the need for a centralised dataset. This data-efficient approach enhances the diversity and robustness of model training, leading to more accurate predictions [3],[4]. Computational Efficiency: Federated learning reduces the computational burden on individual devices and central servers by distributing the training process across multiple devices. This decentralised approach enhances computational efficiency and scalability, making it suitable for large-scale applications [1],[5],[8]-[13]. Personalised Models: Federated learning enables the creation of personalised models that capture device-specific characteristics and preferences. This customisation ensures that the trained models are tailored to individual devices, leading to more relevant and accurate predictions [1]. Communication Efficiency: In federated learning, only model updates are exchanged between devices, minimising the amount of data transmitted during the training process. This communication efficiency reduces bandwidth requirements and optimises the overall learning process [1],[5],[8]-[13].

2. Privacy preservation in healthcare [1],[5],[8]-[13]:

Privacy preservation in healthcare is a critical aspect of data management that focuses on safeguarding the confidentiality and security of sensitive patient information. With the increasing digitisation of healthcare data and the adoption of electronic health records (EHRs), protecting patient privacy has become paramount to ensure trust, compliance with regulations, and ethical standards.

Importance of Privacy in Healthcare Data:

Sensitive Nature of Medical Information: Healthcare data, including personal health information (PHI), is highly sensitive due to its intimate nature and potential risks associated with unauthorised access or disclosure. Privacy breaches can lead to the identification of individuals and compromise their sensitive information, even after de-identification processes. Legal and Ethical Obligation: Data protection laws and regulations exist worldwide to ensure the privacy and security of medical data. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the USA mandate the protection of PHI and impose strict guidelines for handling and storing healthcare information. Data Collection Challenges: The increasing volume of health data collected from EHRs, insurance claims, and health surveys necessitates robust analysis tools capable of handling and analysing large datasets while addressing data quality and privacy issues.

Regulatory Frameworks and Guidelines:
HIPAA and Data Privacy Laws: Regulatory frameworks like HIPAA play a crucial role in certifying the privacy and security of healthcare data. These laws protect individuals' privacy rights and regulate the processing of personal data to prevent unauthorised access and misuse. Rights Management Systems: Healthcare organisations implement rights management systems to control access to patient information and ensure that only authorised personnel can view or use sensitive data. This helps mitigate the risk of data misuse and unauthorised disclosures.

Implications of Privacy Breaches in Healthcare:
Identity Theft and Fraud: Unauthorized access to healthcare data can lead to identity theft, insurance fraud, and financial losses for individuals. Protecting patient privacy is essential to prevent these malicious activities and safeguard individuals' personal information. Reputational Damage: Privacy breaches in healthcare can result in reputational damage for healthcare organisations and individuals involved. Loss of public trust and legal consequences may follow such breaches, highlighting the importance of robust privacy preservation measures.

Role of Privacy Preservation in Healthcare:
Trust and Confidentiality: Preserving privacy in healthcare is crucial for maintaining trust between healthcare providers and patients. Patients must feel comfortable seeking medical care and sharing their information, knowing that their data is secure and confidential. Secure Communication: Privacy preservation enables secure and confidential communication between healthcare providers and patients, ensuring that sensitive information is not exposed to unauthorised parties. This confidentiality is essential for maintaining the integrity of healthcare services.

3. Challenges and Future Direction.

Challenges and future directions in privacy-preserving federated learning and healthcare applications encompass a range of technical, ethical, and regulatory considerations that impact the adoption and advancement of privacy-preserving techniques. Addressing these challenges and exploring future directions is crucial to enhancing data security, promoting ethical data practices, and maximizing the potential of federated learning in healthcare settings [7], [14], [18], [15]-[17].

Challenges in Privacy-Preserving Federated Learning:
1. Scalability: Challenge: Scaling federated learning to accommodate a large number of devices or participants while maintaining communication efficiency and model accuracy is a significant challenge. As the number of participants increases, managing communication overhead and ensuring model convergence become more complex. Solution: Developing scalable federated learning algorithms, optimising communication protocols, and implementing efficient model aggregation techniques can help address scalability challenges and improve the performance of federated learning systems.

2. Communication Overhead: Challenge: Federated learning involves frequent communication between devices or edge nodes to exchange model updates, which can lead to high communication overhead and latency issues. Managing communication costs while ensuring data privacy and security is a key challenge in federated learning. Solution: Implementing efficient communication strategies, such as compressed model updates, differential privacy mechanisms, and secure aggregation protocols, can help reduce communication overhead and enhance the efficiency of federated learning systems.

3. Ethical Considerations: Challenge: Ensuring ethical data practices, transparency, and accountability in privacy-preserving federated learning is essential to maintaining trust and compliance with regulatory standards. Addressing ethical considerations related to data collection, sharing, and model training is crucial for the responsible deployment of federated learning in healthcare. Solution: Promoting ethical guidelines, providing education on data ethics, and integrating ethical frameworks into federated learning systems can help mitigate ethical challenges and foster responsible data practices in healthcare applications.

Future Directions in Privacy-Preserving Federated Learning [14]-[17]**:**
1. Advancements in Privacy-Preserving Techniques: Direction: Future research in federated learning should focus on developing advanced privacy-preserving techniques, such as secure multi-party computation, differential privacy, and homomorphic encryption, to enhance data security and confidentiality in healthcare applications. Impact: By integrating cutting-edge privacy-preserving methods, federated learning systems can offer enhanced protection for sensitive patient data, enable secure data sharing, and support compliance with privacy regulations in healthcare settings.

2. Integration with Emerging Technologies: Direction: Federated learning can be integrated with emerging technologies like IoT, blockchain, cloud computing, and AI to enhance its capabilities in healthcare applications. This integration can facilitate secure data sharing, improve data governance, and enhance model performance in healthcare analytics. Impact: Leveraging synergies between federated learning and emerging technologies can lead to more efficient and secure healthcare data management, personalised medicine solutions, and remote patient monitoring systems, ultimately improving healthcare outcomes and patient care.

3. Expansion to New Healthcare Domains: Direction: Federated learning has the potential to expand beyond its current applications in healthcare to domains like genomics, personalised medicine, and population health management. Exploring new healthcare applications can drive innovation, improve healthcare outcomes, and advance patient-centric care. Impact: By expanding the scope of federated learning to new healthcare domains, researchers and practitioners can unlock

new opportunities for data-driven insights, predictive modelling, and personalised healthcare interventions, leading to advancements in patient care and public health initiatives.

CONCLUSION

This review delves into the integration of privacy-preserving federated learning in healthcare, highlighting its role in remote patient monitoring, clinical decision support, and personalized medicine, ensuring the protection of patient data. Despite the progress, challenges in scalability, communication efficiency, and compliance with ethical and regulatory standards persist. Future research is essential to leverage federated learning's full potential in healthcare. Ongoing developments in privacy techniques and technology integration herald new possibilities for improving healthcare through secure data practices. The review contributes to the academic dialogue, encouraging continued innovation in privacy-preserving federated learning within the healthcare sector.

REFERENCES

1. Crawshaw M. Multi-task learning with deep neural networks: a survey. arXiv. 2020 Sep 10. Available from: http://arxiv.org/abs/2009.09796
2. Ferreira MF, Camacho R, Teixeira LF. Using autoencoders as a weight initialization method on deep neural networks for disease detection. BMC Med Inform Decis Mak. 2020;20(Suppl 5):141. doi:10.1186/s12911-020-01150-w.
3. Abdelmageed S, Zayed T. A study of literature in modular integrated construction: critical review and future directions. J Clean Prod. 2020; 277:124044. doi: 10.1016/j.jclepro.2020.124044.
4. Bejani MM, Ghatee M. A systematic review on overfitting control in shallow and deep neural networks. Artif Intell Rev. 2021;54(8):6391-6438. doi:10.1007/s10462-021-09975-1.
5. Antunes RS, Costa CA, Küderle A, Yari IA, Eskofier B. Federated learning for healthcare: systematic review and architecture proposal. ACM Trans Intell Syst Technol. 2022;13(4):54. doi:10.1145/3501813.
6. The effect of training parameters and mechanisms on decentralized federated learning based on MNIST dataset. 2021 Aug. Available from: https://typeset.io/papers/the-effect-of-training-parameters-and-mechanisms-on-51kpl2f1ez
7. Privacy-preserving model aggregation for asynchronous federated learning. arXiv. 2023 May. doi:10.48550/arXiv.2305.17521.
8. Auer P, Burgsteiner H, Maass W. A learning rule for very simple universal approximators consisting of a single layer of perceptrons. Neural Netw. 2008;21(5):786-795. doi: 10.1016/j.neunet.2007.12.036.
9. Ganin Y. Natural image processing and synthesis using deep learning.
10. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. J Big Data. 2018;5(1):1. doi:10.1186/s40537-017-0110-7.
11. Brisimi TS, Chen R, Mela T, Olshevsky A, Paschalidis IC, Shi W. Federated learning of predictive models from federated electronic health records. Int J Med Inform. 2018; 112:59-67. doi: 10.1016/j.ijmedinf.2018.01.007.
12. Privacy and security concerns with healthcare data and social media usage. J Inf Priv Secur. 2017;13(2):49-50. doi:10.1080/15536548.2017.1322413.
13. Importance of data mining in healthcare: a survey. In: Proceedings of the International Conference on Advances in Social Networks Analysis and Mining. New York: ACM; 2015. p. 1057-1062. doi:10.1145/2808797.2809367.
14. Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. Federated learning for healthcare informatics. J Healthc Inform Res. 2021;5(1):1-19. doi:10.1007/s41666-020-00082-4.
15. Geirhos R, Jacobsen JH, Michaelis C, Zemel R, Brendel W, Bethge M, et al. Shortcut learning in deep neural networks. Nat Mach Intell. 2020;2(11):665-673. doi:10.1038/s42256-020-00257-z.
16. Choudhury O, et al. Anonymizing data for privacy-preserving federated learning. arXiv. 2020 Feb 20. doi:10.48550/arXiv.2002.09096.
17. Resource rationing for wireless federated learning: concept, benefits, and challenges. 2021 Apr. Available from: https://typeset.io/papers/resource-rationing-for-wireless-federated-learning-concept-51i7celkxh
18. Rauniyar A, et al. Federated learning for medical applications: a taxonomy, current trends, challenges, and future research directions. arXiv. 2023 Sep 20. doi:10.48550/arXiv.2208. 03392..