

**Federated Learning for Privacy-Preserving Healthcare Systems A Literature
Review**

Student Preparation

ABDULRAHMAN MOHAMMED ALJAMAAN

Under the supervision of

د. محمد عنبر

2026

1. Problem Statement

1.1 Problem Domain

Healthcare systems are undergoing rapid digital transformation through the adoption of Electronic Health Records (EHRs), medical imaging technologies, wearable devices, Internet of Medical Things (IoMT), and Artificial Intelligence (AI). These technologies generate massive volumes of sensitive patient data that are valuable for developing intelligent clinical decision-support systems and predictive healthcare models. However, healthcare data are typically distributed across multiple hospitals and medical institutions, making centralized data collection difficult due to strict privacy regulations, ethical concerns, and organizational policies. Federated Learning (FL) has emerged as a promising distributed machine learning paradigm that enables collaborative model training without requiring institutions to exchange raw patient data (Kairouz et al., 2021; Li et al., 2020).

1.2 Description of the Problem

Although Federated Learning offers an attractive solution for privacy-preserving collaborative learning, several technical and practical challenges remain unresolved. Healthcare datasets are inherently heterogeneous because hospitals differ in patient demographics, disease prevalence, imaging equipment, and clinical practices. This non-independent and non-identically distributed (non-IID) nature of healthcare data significantly reduces the accuracy and convergence of federated learning models. Furthermore, communication overhead, limited computational resources in healthcare institutions, security vulnerabilities such as model inversion and poisoning attacks, and difficulties in maintaining fairness among participating organizations continue to hinder the large-scale deployment of FL in real-world healthcare systems (Yang et al., 2019; Nguyen et al., 2022).

1.3 Significance of the Problem

Protecting patient privacy while enabling collaborative medical research is one of the most critical challenges in modern healthcare. Privacy breaches can result in legal penalties, financial losses, and reduced public trust in healthcare organizations. At the same time, restricting access to distributed healthcare data limits the development of robust AI models capable of improving disease diagnosis, treatment planning, and personalized medicine. Therefore, identifying effective Federated Learning strategies that preserve privacy while maintaining high predictive performance has become an important research priority for both healthcare providers and AI researchers (Rieke et al., 2020; Sheller et al., 2020).

1.4 Existing Solutions

Researchers have proposed numerous techniques to improve the security and performance of Federated Learning in healthcare. These include secure aggregation protocols, differential privacy, homomorphic encryption, blockchain integration, personalized federated learning, adaptive aggregation algorithms, and communication-efficient optimization methods. Several healthcare applications have successfully demonstrated the use of FL in disease diagnosis, medical image analysis, cancer detection, COVID-19 prediction, and electronic health record analytics. While these approaches have shown promising results, each addresses only specific aspects of the overall problem and introduces trade-offs between privacy, computational efficiency, communication cost, and model accuracy (McMahan et al., 2017; Li et al., 2020; Rieke et al., 2020).

1.5 Justification for the Research

Despite the growing body of literature on Federated Learning for healthcare, existing studies remain fragmented and often focus on individual techniques or specific medical applications. There is limited comprehensive analysis that systematically compares current privacy-preserving methods, identifies their strengths and weaknesses, examines implementation challenges, and highlights future research directions. Consequently, a comprehensive literature review is needed

to synthesize current knowledge, evaluate recent developments, identify research gaps, and provide recommendations for designing more secure, efficient, scalable, and trustworthy Federated Learning systems for healthcare environments. Such a review will assist researchers and practitioners in understanding the current state of the field and guide future innovations in privacy-preserving healthcare AI.

2. Research Objectives

Primary Research Objective

To critically review and synthesize the existing literature on Federated Learning for privacy-preserving healthcare systems in order to identify current approaches, challenges, research gaps, and future research directions.

Specific Research Objectives

1. To review the fundamental concepts, architecture, and principles of Federated Learning in healthcare systems.
2. To identify the major privacy, security, and data-sharing challenges addressed by Federated Learning in healthcare applications.
3. To analyze the existing Federated Learning techniques, frameworks, and privacy-preserving mechanisms proposed in the healthcare literature.
4. To evaluate the strengths, limitations, and performance trade-offs of current Federated Learning approaches with respect to privacy protection, model accuracy, scalability, communication efficiency, and security.
5. To identify the current research gaps and unresolved challenges affecting the adoption of Federated Learning in real-world healthcare environments.
6. To recommend potential future research directions for improving privacy-preserving Federated Learning systems in healthcare.

References

- Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). *Advances and open problems in federated learning*. Foundations and Trends® in Machine Learning, 14(1–2), 1–210.
- Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). *Federated learning: Challenges, methods, and future directions*. IEEE Signal Processing Magazine, 37(3), 50–60.
- McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). *Communication-efficient learning of deep networks from decentralized data*. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 1273–1282.
- Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., Poor, H. V., & Dobre, O. (2022). Federated learning for healthcare informatics. *ACM Computing Surveys*, 55(3), 1–37.
- Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M. N., Landman, B. A., Maier-Hein, K., Ourselin, S., Sheller, M., Summers, R. M., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). *The future of digital health with federated learning*. NPJ Digital Medicine, 3(119), 1–7.
- Sheller, M. J., Edwards, B., Reina, G. A., Martin, J., Bakas, S., Patel, P., Chellappa, V., & Pati, S. (2020). *Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data*. Scientific Reports, 10(12598), 1–12.
- Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). *Federated machine learning: Concept and applications*. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.