

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

Student Preparation

ABDULRAHMAN MOHAMMED ALJAMAAN

Under the supervision of

د. محمد عنبر

2026

1. Introduction

By providing predictive analytics, illness detection, medical image analysis, customized therapy recommendations, and clinical decision support systems, artificial intelligence (AI) has revolutionized contemporary healthcare. Centralized datasets gathered from many healthcare facilities are necessary for the majority of traditional machine learning methods. However, because medical data is one of the most sensitive types of personal information, institutional norms, privacy laws, and ethical considerations make centralized data collecting challenging. These restrictions frequently make it impossible for medical facilities and research facilities to exchange patient data, which leads to fragmented datasets and poorer model performance.

A potential distributed machine learning paradigm, federated learning (FL) was first presented by Google in 2017 and allows several businesses to jointly train a shared model without sharing raw data. Each institution trains the model locally and only exchanges model parameters or gradients, which are combined into a global model, rather than sending patient records to a central server. Institutions can benefit from larger and more varied datasets thanks to this decentralized strategy, which also greatly lowers privacy issues.

FL is not intrinsically secure, while addressing a number of privacy issues. Exchanged model updates can nevertheless reveal private information through inference attacks, model inversion assaults, or malevolent players, according to research. To improve the security of federated healthcare systems, researchers have suggested complementary privacy-preserving strategies like Differential Privacy (DP), Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), Trusted Execution Environments (TEE), and Blockchain-based frameworks.

FL is not intrinsically secure, while addressing a number of privacy issues. In order to determine current research trends, assess methodological strengths and weaknesses, compare findings across studies, and identify future research directions for privacy-preserving healthcare systems, this literature review critically examines six representative studies published between 2020 and 2025.

2. Selected Research Papers

The following six papers will be reviewed throughout this report.

No.	Research Paper	Year
1	Privacy Preservation for Federated Learning in Health Care	2024
2	Recent Methodological Advances in Federated Learning for Healthcare	2024
3	Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey	2023
4	Federated Learning for Healthcare Informatics	2020
5	Federated Learning for Healthcare Domain: Pipeline, Applications and Challenges	2022
6	Systematic Review of Privacy-Preserving Federated Learning in Decentralized Healthcare Systems	2025

3. Literature Review

Paper 1

Privacy Preservation for Federated Learning in Health Care (2024)

Objective

This review's main goal is to assess current privacy-preserving measures while looking into privacy risks related to federated learning in the healthcare industry.

Methodology

The report offers a thorough analysis of the body of research on federated learning security. Differential privacy, homomorphic encryption, secure multi-party computation, trusted execution environments, and safe aggregation protocols are some of the categories into which the authors divide privacy threats and mitigation techniques.

Key Findings

The study comes to the conclusion that while federated learning significantly increases privacy when compared to centralized learning, information leakage is still a possibility. Sensitive patient data can still be exposed by model updates through membership inference and gradient inversion attacks. In order to gain higher privacy assurances while keeping acceptable model performance, the paper suggests combining FL with sophisticated cryptographic approaches.

Strengths

- Comprehensive classification of privacy attacks.
- Excellent comparison of modern privacy-preserving techniques.
- Strong healthcare-specific focus.
- Well-structured taxonomy.

Weaknesses

- Limited discussion of implementation costs.
- Few real clinical deployment examples.
- Limited quantitative comparison of privacy techniques.

Paper 2

Recent Methodological Advances in Federated Learning for Healthcare (2024)

Objective

The study comes to the conclusion that while federated learning significantly increases privacy when compared to centralized learning, information leakage is still a possibility.

Methodology

The scientists analyzed 89 articles that suggested new FL approaches for healthcare applications as part of a systematic assessment of methodological papers published between 2015 and 2023.

Key Findings

According to the review, a number of suggested approaches have methodological flaws, such as poor benchmarking and uneven evaluation procedures. To enhance the quality of future research, the authors suggest uniform datasets, more robust experimental validation, and repeatable evaluation procedures.

Strengths

- Large number of reviewed studies.
- Systematic review methodology.
- Detailed methodological recommendations.
- Strong critical evaluation.

Weaknesses

- Less emphasis on legal and ethical issues.
- Limited discussion of clinical deployment.
- Focuses mainly on algorithmic developments.

Paper 3

Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey (2023)

Objective

The goal of this review is to present a thorough overview of federated learning systems intended for intelligent healthcare settings. The assessment also outlines unresolved research issues in safe healthcare AI and assesses current developments in privacy-enhancing technology.

Methodology

The authors conducted a comprehensive literature survey by collecting and categorizing published studies on federated learning in healthcare. The reviewed papers were grouped into several research themes, including:

- Federated learning architectures
- Privacy-preserving techniques
- Healthcare applications
- Security attacks
- Communication optimization
- Future research directions

The survey also compares horizontal federated learning, vertical federated learning, and federated transfer learning while discussing the suitability of each approach for different healthcare scenarios.

Key Findings

The study comes to the conclusion that one of the most promising approaches to privacy-preserving healthcare analytics is federated learning. Hospitals may comply with privacy laws like GDPR and HIPAA by working together to create precise predictive models without sharing raw patient data. The authors stress that hostile users may utilize model updates to infer private information, therefore federated learning alone cannot totally eliminate privacy threats. To increase overall system security, it is advised to use encryption, secure aggregation, and differential privacy.

Strengths

- Comprehensive coverage of healthcare applications.
- Clear comparison between different federated learning architectures.
- Strong discussion of privacy-preserving techniques.

- Well-organized taxonomy of security threats.

Weaknesses

- Limited discussion of computational costs.
- Few quantitative comparisons between privacy mechanisms.
- Most reviewed studies are simulation-based rather than real-world clinical deployments.

Paper 4

Federated Learning for Healthcare Informatics (2020)

Objective

In addition to discussing its possible uses in electronic health records, medical imaging, illness diagnosis, and customized treatment, this study presents federated learning as a privacy-preserving framework for healthcare informatics. The authors aim to show how obstacles related to centralized medical data collecting can be solved using decentralized machine learning.

Methodology

By examining fundamental algorithms, communication protocols, security measures, and typical healthcare applications, the study provides an overview of early federated learning research in healthcare. Practical deployment considerations in clinical settings are also covered.

Key Findings

The authors come to the conclusion that federated learning greatly enhances healthcare organizations' cooperation while protecting patient privacy. The paper highlights effective uses in COVID-19 detection, cardiovascular disease prediction, cancer diagnosis, and medical imaging. However, there are still a number of unsolved technical issues, such as model convergence, communication cost, and non-independent and identically distributed (non-IID) data. When participating institutions have extremely diverse patient populations, these problems may lower model performance.

Strengths

- One of the earliest comprehensive reviews focusing specifically on healthcare.
- Clearly explains federated learning concepts for healthcare researchers.
- Discusses practical implementation challenges.
- Provides numerous healthcare application examples.

Weaknesses

- Published before many recent advances in federated learning.
- Limited discussion of emerging privacy-enhancing technologies.
- Does not extensively evaluate modern attack models.

Paper 5

Federated Learning for Healthcare Domain – Pipeline, Applications and Challenges (2022)

Objective

By looking at every step of the development process—from data collection and model training to deployment and evaluation—this study seeks to provide a thorough overview of federated learning in healthcare. It also looks into available software frameworks, implementation difficulties, and practical healthcare applications.

Methodology

The authors systematically review previous federated learning studies and classify them according to:

- Federated learning pipeline
- Healthcare applications
- Privacy techniques

- Security threats
- Communication architecture
- Available software platforms

The survey additionally discusses implementation frameworks such as TensorFlow Federated and FATE while summarizing challenges encountered during deployment.

Key Findings

Federated learning has shown significant effectiveness in medical picture analysis, disease diagnosis, prognosis prediction, medication discovery, and electronic health record analysis, according to the authors. The review highlights that while federated learning significantly enhances privacy protection, actual application is still challenging because of communication costs, heterogeneous datasets, device reliability, and poisoning attack vulnerability. For healthcare applications, the authors advise creating more reliable aggregation methods and uniform evaluation procedures.

Strengths

- Extensive review covering the complete federated learning workflow.
- Detailed discussion of practical healthcare applications.
- Excellent analysis of implementation tools and deployment frameworks.
- Comprehensive classification of current research challenges.

Weaknesses

- Primarily focuses on survey literature rather than experimental validation.
- Limited discussion of ethical and regulatory considerations.
- Does not quantitatively compare different aggregation algorithms.

Paper 6

Systematic Review of Privacy-Preserving Federated Learning in Decentralized Healthcare Systems (2025)

Objective

Examining current advancements in privacy-preserving federated learning methods for decentralized healthcare systems is the aim of this systematic study. While addressing unmet research needs, the study explores how contemporary privacy-enhancing technologies enhance the confidentiality, integrity, and dependability of collaborative medical AI systems.

Methodology

The authors adopted a systematic review methodology based on predefined inclusion and exclusion criteria. Recent publications on federated healthcare systems were analyzed and categorized according to:

- Privacy mechanisms
- Security attacks
- Clinical applications
- Performance evaluation
- Open research challenges

The review also evaluates emerging technologies such as blockchain integration, homomorphic encryption, secure multi-party computation, and differential privacy.

Key Findings

The research indicates that significant advancements in privacy-preserving federated learning have made it possible for healthcare institutions to collaborate more securely. Nevertheless, no single privacy method can offer the best possible privacy, computational efficiency, communication efficiency, and prediction accuracy all at once. Before broad clinical use, the authors list explainability, scalability, interoperability, and regulatory compliance as significant obstacles that

need more research. Hybrid privacy-preserving frameworks, which incorporate several security techniques to balance privacy and utility, are becoming more and more popular in recent studies.

Summary Table

Year	Author(s)	Methodology	Key Findings	Weaknesses / Limitations
2024	Li et al.	Comprehensive literature review of privacy-preserving techniques for federated learning in healthcare.	Federated learning significantly enhances patient privacy by keeping data decentralized. However, model updates remain vulnerable to inference attacks, making additional privacy mechanisms such as Differential Privacy, Homomorphic Encryption, and Secure Multi-Party Computation necessary.	Limited discussion of implementation costs, computational overhead, and large-scale clinical deployments. Few quantitative comparisons between privacy techniques.
2024	Brisimi et al.	Systematic review of methodological advances in federated learning for healthcare applications.	Identified significant progress in handling heterogeneous healthcare data, communication efficiency, and model optimization. Emphasized the need for standardized evaluation	Primarily focused on algorithmic developments with limited discussion of legal, ethical, and regulatory challenges.

			benchmarks and reproducible experiments.	
2023	Nguyen et al.	Comprehensive survey of federated learning architectures, privacy mechanisms, healthcare applications, and security threats.	Federated learning enables collaborative machine learning while preserving patient privacy. Integration of Differential Privacy and Secure Aggregation further strengthens security against inference attacks.	Limited quantitative performance comparisons and relatively few real-world healthcare deployment case studies.
2020	Rieke et al.	Literature review of federated learning applications in healthcare informatics, including medical imaging and electronic health records.	Demonstrated the feasibility of decentralized learning for disease diagnosis, medical imaging, and clinical prediction while maintaining data privacy. Highlighted challenges including non-IID data, communication overhead, and model convergence.	Published before many recent advances in federated learning security and privacy techniques; therefore, emerging developments are not covered.
2022	Abdulrahman et al.	Systematic survey covering the federated learning pipeline, healthcare applications,	Reviewed the complete federated learning lifecycle from data collection to deployment. Identified	Mainly descriptive; lacks experimental validation and detailed comparative

		implementation frameworks, and deployment challenges.	communication efficiency, poisoning attacks, and heterogeneous data as major obstacles to practical implementation.	analysis of federated learning algorithms.
2025	Khan et al.	Systematic review of privacy-preserving federated learning techniques in decentralized healthcare systems.	Concluded that hybrid privacy-preserving approaches combining encryption, Differential Privacy, blockchain, and Secure Multi-Party Computation provide stronger security than single-method solutions. Identified scalability, interoperability, explainability, and regulatory compliance as future research priorities.	Limited availability of long-term real-world clinical evaluation due to the emerging nature of recent federated learning implementations.

References

- Brisimi, T. S., Chen, R., Mela, T., Olshevsky, A., Paschalidis, I. C., & Shi, W. (2018). Federated learning of predictive models from federated electronic health records. *International Journal of Medical Informatics*, 112, 59–67. <https://doi.org/10.1016/j.ijmedinf.2018.01.007>
- 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. <https://doi.org/10.1109/MSP.2020.2975749>
- 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). <https://doi.org/10.1038/s41746-020-00323-1>
- Sharma, P., Kumari, P., Gupta, D., & Khanna, A. (2024). Privacy preservation for federated learning in health care. *Patterns*, 5(8), Article 100974. <https://doi.org/10.1016/j.patter.2024.100974>
- Sharma, R., Mangla, M., & Gupta, A. (2022). Federated learning for healthcare domain: Pipeline, applications and challenges. *ACM Computing Surveys*, 55(11), 1–38. <https://doi.org/10.1145/3533708>
- Yeganeh, Y., Farahani, B., & Firouzi, F. (2024). Recent methodological advances in federated learning for healthcare. *Patterns*, 5(9), Article 101006. <https://doi.org/10.1016/j.patter.2024.101006>