

Chapter 9

Managing Sensitive Health Data Through Federated Learning and Generative AI: Advanced Privacy–Preserving Techniques for Secure Digital Healthcare

V. Vidhya

 <http://orcid.org/0009-0002-3859-6850>

*Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
India*

S. Sridevi

Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, India

B. Ramakrishna

CVR College of Engineering, India

T. Karpagam

R.M.K. College of Engineering and Technology, India

Dinesh M. G.

 <http://orcid.org/0009-0009-7643-5338>

Easa College of Engineering and Technology, India

DOI: 10.4018/979-8-3373-7426-0.ch009

Copyright © 2027, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

ABSTRACT

The rapid digitalization of healthcare has intensified the need for robust, privacy-preserving techniques to manage sensitive patient data. Federated Learning (FL) and Generative AI (GenAI) have emerged as transformative technologies that enable secure, collaborative model development without centralizing raw medical data. This chapter explores the foundational principles, privacy-preserving mechanisms, and integrated frameworks that combine FL and GenAI to support secure digital healthcare applications such as medical imaging, clinical decision support, genomics, and remote monitoring. It highlights key challenges including privacy leakage, data heterogeneity, adversarial threats, and regulatory complexities while identifying future research directions for scalable, trustworthy, and interoperable healthcare AI systems. The convergence of FL and GenAI represents a critical pathway toward secure, ethical, and data-driven healthcare innovation.

1. INTRODUCTION

1.1 Background and Motivation

The digitalization of the healthcare systems across the globe has caused an unprecedented increase in the amount, speed, and type of electronic health data. The electronic health records (EHRs), medical imaging, genomics, wearable devices, telemedicine platforms and remote monitoring systems all produce sensitive and highly personal health data. Although these data sources could have unparalleled potential in improving diagnostics, disease prediction, precision medicine, and clinical decision support, they have serious implications regarding patient privacy, misuse of data and compliance to regulations. The classical machine learning systems use centralized data storage whereby sensitive data is collected in one place to be used in training (Asha et al., 2026). Though it is effective to enhance the performance of the model, this method presents significant weaknesses, such as the possibility of cyberattacks, unauthorized data disclosure, and unintentional privacy breach. It is against this backdrop that the healthcare sector is in dire need of sophisticated technological systems that can be used to draw insights on distributed data without undermining security or breaking privacy of a patient.

Federated Learning (FL) and Generative AI (GenAI) are new tools that have become effective in solving these issues. Federated Learning allows the joint training of models in a number of decentralized healthcare facilities, including hospitals, laboratories, and clinics, without moving raw patient data outside the institution (Trivedi et al., 2023). Rather than the exchange of datasets, a model update or gra-

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/managing-sensitive-health-data-through-federated-learning-and-generative-ai/413689

Related Content

A Smart Grid Security Architecture for Wireless Advanced Metering Infrastructure (AMI)

Aftab Ahmad (2016). *International Journal of Information Security and Privacy* (pp. 1-10).

www.irma-international.org/article/a-smart-grid-security-architecture-for-wireless-advanced-metering-infrastructure-ami/154984

Improved Message Mechanism-Based Cross-Domain Security Control Model in Mobile Terminals

Zhiwei Cao, Zhijie Fan, Boan Chen, Zidong Cheng, Shijun Xuand Xin Li (2024). *International Journal of Information Security and Privacy* (pp. 1-27).

www.irma-international.org/article/improved-message-mechanism-based-cross-domain-security-control-model-in-mobile-terminals/347987

Memory-Based Antiforensic Tools and Techniques

Hamid Jahankhaniand Elidon Beqiri (2008). *International Journal of Information Security and Privacy* (pp. 1-13).

www.irma-international.org/article/memory-based-antiforensic-tools-techniques/2478

Blockchain With the Internet of Things: Solutions and Security Issues in the Manufacturing Industry

Kamalendu Pal (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 498-524).

www.irma-international.org/chapter/blockchain-with-the-internet-of-things/310466

Automated Formal Methods for Security Protocol Engineering

Alfredo Pironti, Davide Pozzaand Riccardo Sisto (2012). *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies* (pp. 138-166).

www.irma-international.org/chapter/automated-formal-methods-security-protocol/56300