Chapter 6
Privacy-Aware Federated Learning Architectures for Cross-Institutional Healthcare Collaboration

S. Aarthi
http://orcid.org/0009-0006-9064-2091
Marwadi University, Rajkot, India

Jaypalsinh A. Gohil
http://orcid.org/0000-0003-0925-6646
Marwadi University, Rajkot, India

ABSTRACT

The chapter explores Privacy-Aware Federated Learning (FL) architectures that enable secure, collaborative healthcare model training without sharing raw patient data. It highlights how Differential Privacy, Secure Multi-Party Computation, and Homomorphic Encryption protect sensitive information during federated aggregation while maintaining model accuracy. The integration of Generative AI enhances data diversity and fairness across institutions. Case studies demonstrate real-world applications in diagnostic imaging and chronic disease prediction. The discussion emphasizes scalability, compliance with HIPAA and GDPR, and the role of blockchain and explainable AI in shaping future digital health ecosystems. The chapter concludes with insights into ethical governance and cross-domain interoperability for transparent and trustworthy healthcare collaboration.

DOI: 10.4018/979-8-3373-7426-0.ch006

1. INTRODUCTION

The healthcare digitalization into an information ecosystem has transformed the ways of patient data collection, processing, and analysis in medical institutions. With the growing use of wearable devices, Electronic Health Records (EHRs), and IoT-connected medical systems, there was an enormous amount of sensitive data with massive predictive analytics and individual treatment potential. But the decentralised character of the data sources, combined with strict privacy laws, including HIPAA and GDPR, can be a hindrance to centralised model training. Therefore, there is an urgent requirement in the healthcare industry in both collaborative but privacy-minded models that allow securely developing models (Xu et al., 2021). Federated Learning (FL) and Generative AI become the most important solutions that enable a number of organizations to collectively train intelligent models without having to expose raw data. The chapter gives a background of the novel Privacy-Aware FL architectures and its contribution to the creation of secure, interoperable, and ethically acceptable collaboration in various healthcare settings.

1.1 Digital Transformation in Healthcare Data Management

Rather than the manual management data, the healthcare system has been redesigned into digital and intelligent cloud-based data ecosystems. Wearable biosensors, imaging systems and telemedicine platforms, plus EHRs have led to the development of heterogeneous data (text, image and signal). The development made it possible to decide in real-time, enhance the accuracy of the diagnosis, and engage patients more (Senbekov et al., 2020). However, the nature of interconnection of the systems also makes data privacy quite vulnerable. Traditional centralized data sharing approaches increase the risks of data breach, unauthorized access by users and losing patient trust. On the other hand, FL supported distributed models promote the sovereignty of the data, keeping it in local institutions yet providing global intelligence through exchanging the models. These developments demonstrate the importance of hard encryption, secure data communications systems, and regulatory systems. Integrating AI, blockchain, and privacy-aware calculation, the sphere of healthcare data is redefining the ideals of its management and is becoming clearer, safer, and careful regarding the needs of the organization and the rights of patients (Sadilek et al., 2021). Figure 1 is used to explain how FL assists in secure healthcare data management by combining the use of strong encryption, custom compliance frameworks, and distributed models. It emphasizes the fact of data upkeep in local establishments and allows sharing global models in a secure environment with transparent governance.

K-Means Cluster-Based Interference Alignment With Adam Optimizer in Convolutional Neural Networks

Tirupathaiah Kanaparthi, Ramesh S.and Ravi Sekhar Yarrabothu (2022). *International Journal of Information Security and Privacy (pp. 1-18).*
www.irma-international.org/article/k-means-cluster-based-interference-alignment-with-adam-optimizer-in-convolutional-neural-networks/308307