Chapter 11
Secure Health Data Management via Federated Learning and Privacy-Aware Large Language Models

R. Felista Lizy
http://orcid.org/0000-0003-3648-0205
Department of Computer Science, A.P.C. Mahalaxmi College for Women, Thoothukudi, India

Amit Kumar Tyagi
http://orcid.org/0000-0003-2657-8700
School of Law, Forensic Justice and Policy Studies, National Forensic Sciences University, Gandhinagar, India

K. R. Pundareeka Vittala
http://orcid.org/0000-0002-5579-2813
ICFAI Foundation for Higher Education (Deemed to be University), Bengaluru, India

Smirty Prasad
http://orcid.org/0000-0002-8057-3612
Christ University, Bengaluru, India

ABSTRACT

Healthcare has moved today with rapid digital transformation, leading to the generation of vast volumes of sensitive patient data that are stored and analyzed on

DOI: 10.4018/979-8-3373-7426-0.ch011

heterogeneous platforms. Although improved machine learning and large language models (LLMs) can bring a radical change in clinical decision support, diagnostics, and operational efficiency, they also raise serious issues concerning data privacy, security, regulatory adherence, and ethical governance. Conventional centralized data analytics methods are becoming increasingly infeasible when it comes to serious health privacy regulations and the need to build trust among the population. This chapter presents an in-depth discussion of secure health data management systems that combine federated learning (FL) with privacy-conscious large language models. It explores architectural concepts, threat analysis, privacy preservation mechanisms and system design strategies that can facilitate collaborative intelligence without affecting patient privacy.

1. INTRODUCTION

The adoption of electronic health records (EHRs), wearable sensors, medical imaging systems, telemedicine platforms and AIs based clinical decision support systems is quickly transforming the global healthcare industry into a digital one. All those technologies generate high-dimensional, heterogeneous and longitudinal data that can be taken to a great potential in regard to improved patient outcomes and healthcare performance. However, health data is sensitive; it is composed of personal, genomic, behavioral and diagnostic data, this data must be accorded the highest level of confidentiality and integrity.

The classical machine learning procedures rely on one centralized data collection; that is, the movement of raw patient data of various sources towards a central server where models are inferred and trained. Despite the fact that this paradigm simplifies the models development, healthcare organizations become vulnerable to various risks, which include data breach, insider threats, regulatory breaches, and patients loss of confidence. Centralized data architecture weakness is also demonstrated by high-profile data breaches and ransomware attacks of hospitals.

Concurrently, the large language models have now become powerful technologies capable of perceiving and writing clinical descriptions, summarizing medical histories, helping to diagnose patients, and assist patients and doctors in communication. However, LLMs pose new threats to privacy such as the unintentional memorization of sensitive data, inference, and non-transparent decision-making.

It is against this backdrop that the idea of federated learning begins to appear like a desirable alternative because it allows one to train the model in a collaborative manner without necessarily sharing the data among themselves. Federated learning, along with privacy-conscious LLM architecture, is applicable to providing safe, compliant, and scalable healthcare intelligence in distributed healthcare