Chapter 6
Privacy-Preserving AI for Medical Applications: A Scalable and Secure Approach

Usharani Bhimavarapu
https://orcid.org/0000-0002-0246-1420
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, India

ABSTRACT

The sudden infusion of artificial intelligence (AI) into the medical sector requires strong frameworks that address regulatory requirements, ethical issues, privacy issues, and concerns related to interoperability. The current research conceptualizes a dynamic system of AI governance that changes dynamically along with advancements in AI, avoiding the constraints of fixed models of governance. In contrast to conventional methods, the model incorporates adaptive compliance processes, explainable AI models, and user-managed data-sharing systems to enable transparency and trustworthiness. It also uses federated learning methods to enable secure and scalable AI adoption in healthcare and avoid data heterogeneity challenges. The model includes enhanced privacy protection with less homomorphic encryption and optimally utilized blockchain, reducing

DOI: 10.4018/979-8-3373-1205-7.ch006

computation overhead and allowing practical application.

INTRODUCTION

MedTech has transformed the healthcare sector by incorporating digital technologies for diagnostics, treatment, and patient monitoring. With the growing use of electronic health records (EHRs), wearables, and artificial intelligence (AI)-driven diagnostics, vast amounts of sensitive patient data are created every day. Clever handling of data guarantees that such data is stored, accessed, and processed securely without loss of integrity. However, ineffective management of data can contribute to breaches, loss of patient trust, and fines. Data collection, storage, and data transfer need to become efficient in MedTech businesses with the formation of strong data governance processes. Regulation of laws relating to patient confidentiality, i.e., HIPAA and GDPR, needs to be followed diligently. Encryption, access controls, and anonymization strategies also have to be used for security tightening in organizations. Ethical concerns must take precedence in data usage to avoid misuse or bias. Data processing transparency must be maintained to generate trust among healthcare providers and patients.

MedTech necessitates compliance with data privacy since health information is sensitive by its nature. Medical records harbor personally identifiable information (PII) that, once revealed, may result in identity theft or insurance fraud. Global regulatory institutions have established tough data protection statutes to mitigate such exposures. The U.S., for instance,. Health Insurance Portability and Accountability Act (HIPAA) requires patient data to be protected by administrative, physical, and technical controls in healthcare organizations. The General Data Protection Regulation of Europe provides greater control of the individuals over their data and enforces transparency and accountability of data processing. Violation of such regulations can result in huge penalties and destroy the image of MedTech firms. Healthcare professionals need to incorporate privacy by design into their systems, with data protection built into every step. Firms need to perform regular audits and risk assessments to determine areas of weakness. Training employees in data privacy best practices will help