

Methods and Algorithms of Ensuring Data Privacy in AI-Based Healthcare Systems and Technologies

Authors : Omar Farshad Jeelani, Makaire Njie, Viktoriia M. Korzhuk

Abstract : Recently, the application of AI-powered algorithms in healthcare continues to flourish. Particularly, access to healthcare information, including patient health history, diagnostic data, and PII (Personally Identifiable Information) is paramount in the delivery of efficient patient outcomes. However, as the exchange of healthcare information between patients and healthcare providers through AI-powered solutions increases, protecting a person's information and their privacy has become even more important. Arguably, the increased adoption of healthcare AI has resulted in a significant concentration on the security risks and protection measures to the security and privacy of healthcare data, leading to escalated analyses and enforcement. Since these challenges are brought by the use of AI-based healthcare solutions to manage healthcare data, AI-based data protection measures are used to resolve the underlying problems. Consequently, this project proposes AI-powered safeguards and policies/laws to protect the privacy of healthcare data. The project presents the best-in-school techniques used to preserve the data privacy of AI-powered healthcare applications. Popular privacy-protecting methods like Federated learning, cryptographic techniques, differential privacy methods, and hybrid methods are discussed together with potential cyber threats, data security concerns, and prospects. Also, the project discusses some of the relevant data security acts/laws that govern the collection, storage, and processing of healthcare data to guarantee owners' privacy is preserved. This inquiry discusses various gaps and uncertainties associated with healthcare AI data collection procedures and identifies potential correction/mitigation measures.

Keywords : data privacy, artificial intelligence (AI), healthcare AI, data sharing, healthcare organizations (HCOs)

Conference Title : ICPHI 2024 : International Conference on Public Health Informatics

Conference Location : Paris, France

Conference Dates : April 11-12, 2024