

Medical Disease Prediction Using Federated Learning and Secure AI

Abstract

Medical disease prediction is a critical field in healthcare, enabling early diagnosis, personalized treatment, and efficient resource allocation. Traditional AI-based medical models often rely on centralized datasets, raising concerns about data privacy and security. To address this, our project introduces a **Federated Learning-based Secure AI model** that enhances privacy while maintaining prediction accuracy for disease detection.

Federated Learning (FL) enables multiple hospitals and research centers to collaborate on training AI models without sharing raw patient data, ensuring compliance with **HIPAA and GDPR regulations**. The proposed system utilizes **Transformer-based deep learning models (BERT for medical text analysis, Vision Transformers for medical imaging)** to analyze patient symptoms, lab reports, and medical histories.

The model integrates **Homomorphic Encryption and Differential Privacy** to ensure secure AI processing while maintaining high prediction accuracy. AI-driven radiology analysis is powered by **NVIDIA Clara and Google Health AI**, which process **CT scans, X-rays, and MRI images** to detect diseases such as pneumonia, cancer, and neurological disorders.

A **cloud-based AI deployment framework** ensures that real-time disease predictions are accessible through **secure medical applications**. Future improvements include integrating **Wearable IoT devices** for continuous health monitoring and using **Quantum AI for drug discovery**.