BATCH NO: 5

PROJECT TITLE: FEDERATED ARTIFICIAL INTELLIGENCE EDGE ANALYSIS FOR SECURING HEALTH CARE DATA IN INSDUSTRIAL CYBER PHYSICAL SYSTEMS

ABSTRACT:

The advent of machine learning techniques has significantly advanced disease prediction and diagnosis in healthcare. However, the utilization of sensitive medical data for training models poses substantial privacy concerns. Federated learning offers a promising solution by allowing collaborative model training across multiple institutions without sharing raw data. This study proposes a novel framework for multi-disease prediction, focusing initially on heart disease and diabetes, leveraging Support Vector Machine (SVM) algorithm. Federated learning is employed to train disease prediction models on decentralized datasets from the data provided. Homomorphic encryption is integrated to ensure privacy preservation during model aggregation. Initially, the patient health information is collected from Fog Nodes and stored on a Blockchain followed by processing using a Support Vector Machine algorithm. SVM models are trained locally on encrypted data using homomorphic encryption techniques. The encrypted model updates are then aggregated securely using homomorphic encryption without revealing sensitive information. Finally, the aggregated model is decrypted to obtain the global model, which is then deployed for disease prediction. Experimental evaluation is conducted using real-world healthcare datasets to assess the effectiveness and privacy preservation capabilities of the proposed framework. Results demonstrate that the federated learning with homomorphic encryption approach achieves comparable prediction accuracy to centralized models while preserving data privacy. Moreover, the framework exhibits scalability and robustness in handling multiple diseases and accommodating additional healthcare institutions.

Keywords: Blockchain technology, Healthcare, Predictive disease analysis, Federated learning, Data security, Homomorphic encryption, Privacy- preserving.