Project Title: Cyber-Attack Detection System for Internet of Health Things (IoHT) Devices Using Federated Learning

Project Description:

With the growing volume of sensitive data transmitted through IT infrastructures, healthcare organizations and companies that generate user wearable data have become prime targets for cyber-attacks. To safeguard electronic healthcare data, Internet of Health Things (IoHT) devices must be protected by robust Intrusion Detection Systems (IDS) to ensure a secure environment. However, due to regulations and policies, hospitals and organizations are restricted from sharing patient data for running IDSs to detect cyber-attacks in IoHT traffic. As a result, it is not feasible to collect patient data and develop IDSs using machine learning (ML) directly. In this context, federated learning (FL) offers a solution to enhance privacy without significantly compromising detection accuracy. Unlike the centralized paradigm of traditional ML models, FL is a privacy-aware ML framework designed to analyze data without sharing it.

This project aims to address the data privacy challenge and provide a more secure environment for patients' private data. Students will investigate the design of an ML-based FL architecture to detect anomalies in IoHT traffic without compromising patient data. They will also explore the development of a decentralized ML model in federated learning (ML-FL model), including (i) Support Vector Machines (SVM), (ii) Feedforward Neural Networks (FNN), (iii) Convolutional Neural Networks (CNN), and (iv) Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) units. Specifically, the ML-FL model will act as a classifier for each client and will analyze network traffic to detect various cyber-attacks, such as spoofing attacks, data alteration, ARP spoofing, DoS attacks, NMAP port scans, and smurf attacks. Additionally, students will investigate the effectiveness of ML-FL models and compare their performance with centralized ML models in terms of prediction accuracy. This project will not only enhance students' understanding of ML/FL and cybersecurity but also contribute to the development of more robust IDSs for e-healthcare.

References:

1. Mosaiyebzadeh, Fatemeh, et al. "Intrusion Detection System for IoHT Devices using Federated Learning." IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2023.
2. https://github.com/fatemehm/Federated-Learning-IDS
3. Vijayakumar, Kedalu Poornachary, et al. "Enhanced cyber attack detection process for Internet of health things (IoHT) devices using deep neural network." Processes 11.4 (2023): 1072.
4. Ahmed, Mohiuddin, et al. "ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things." Ad Hoc Networks 122 (2021): 102621.
5. https://ro.ecu.edu.au/datasets/48/