Privacy-Preserving Activity Recognition from Sensor Data*

Faculty Poster Abstract

Abdur R. Shahid[1] and Sajedul Talukder[2]
[1] Robert Morris University
Moon Township, PA 15108
shahid@rmu.edu
[2]Southern Illinois University
Carbondale, IL 62901
sajedul.talukder@siu.edu

Abstract

Wearable sensor-based Human Activity Recognition (HAR) has applications in a variety of fields, including healthcare, remote monitoring, behavior analysis, social networks, sports, and surveillance. The data for HAR is generated by a variety of sensors, including accelerometers, gyroscopes, and GPS. The sensor data characteristics are used to build a machine learning model to identify distinct actions. Recently, there has been a rise in research efforts aimed at developing an effective and robust HAR classifier. Despite this, a practical HAR system is still a long way off because of its inability to safeguard the privacy of human data needed to train the classifier against various machine learning model attacks. In this paper, we present our study on developing privacy-preserving machine learning models for HAR. We train two differentially private machine learning models, Logistic Regression and Naive Bayes, to classify different activities. We use data from the smartphone's accelerometer and gyroscope to create data on six actions (walking, walking upstairs, going downstairs, sitting, standing, and laying). To investigate the trade-off between the amount of privacy and the efficacy of the two classifiers, we train various privacy-preserving models of the two classifiers. We utilize accuracy, recall, and F1 score to compare the two models to conventional and commonly used benchmarking classifiers, Logistic Regression and Naive Bayes.