Evaluation of Privacy-Preserving Logistic Regression and Naive Bayes Classifiers in Healthcare*

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

Machine Learning (ML) has had a substantial influence on the healthcare system during the last decade or so. Breast cancer and diabetes, two of the most prevalent and deadly diseases, are only two examples of a vast number of healthcare issues that have benefited significantly from machine learning. Early identification of malignant tumors and the reduction of the risk of maltreatment are now a reality thanks to ML. Similarly, several machine learning approaches for early diabetes prediction have been suggested and published in recent years. Although ML-based solutions appear to be rather appealing, the vulnerabilities associated with their design have yet to be completely explored. The ML model responsible for classification is regarded as a very valuable intellectual property in prediction-based healthcare applications that is subject to membership inference attacks, model inversion attacks, and training data leaks via the model's prediction. When this data leakage is combined with information regarding query distribution, a full reconstruction attack may be conducted. In this work, we show how to use differential privacy versions of two widely used and very effective machine learning algorithms, Logistic Regression and Naive Bayes, to classify breast cancer and predict diabetes. The privacy need and model accuracy trade-off are depicted using the prominent Wisconsin Diagnostic Breast Cancer (WDBC) dataset and the Pima Indians Diabetes dataset.