PRIVACY-PRESERVING MODEL TRAINING FOR BREAST CANCER PREDICTION

Machine Learning Memorization

It has been shown that machine learning techniques memorize patient data and can be reverse-engineered to identify patients. This makes medical institutions wary of distributing data for researchers to train machine learning models.

Need

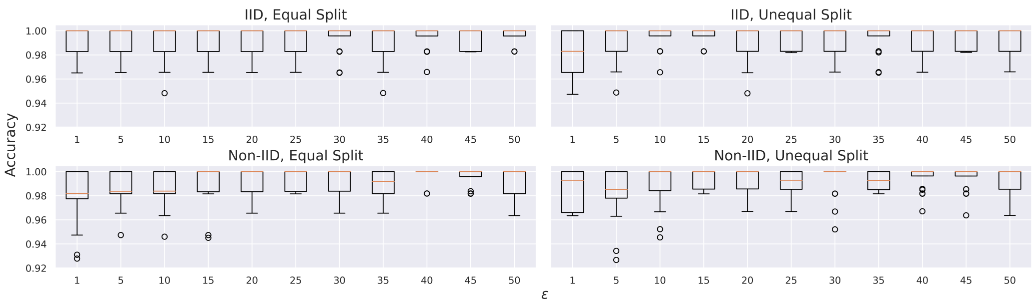
Data scientists require a way to build medical machine learning models while maintaining patient privacy.

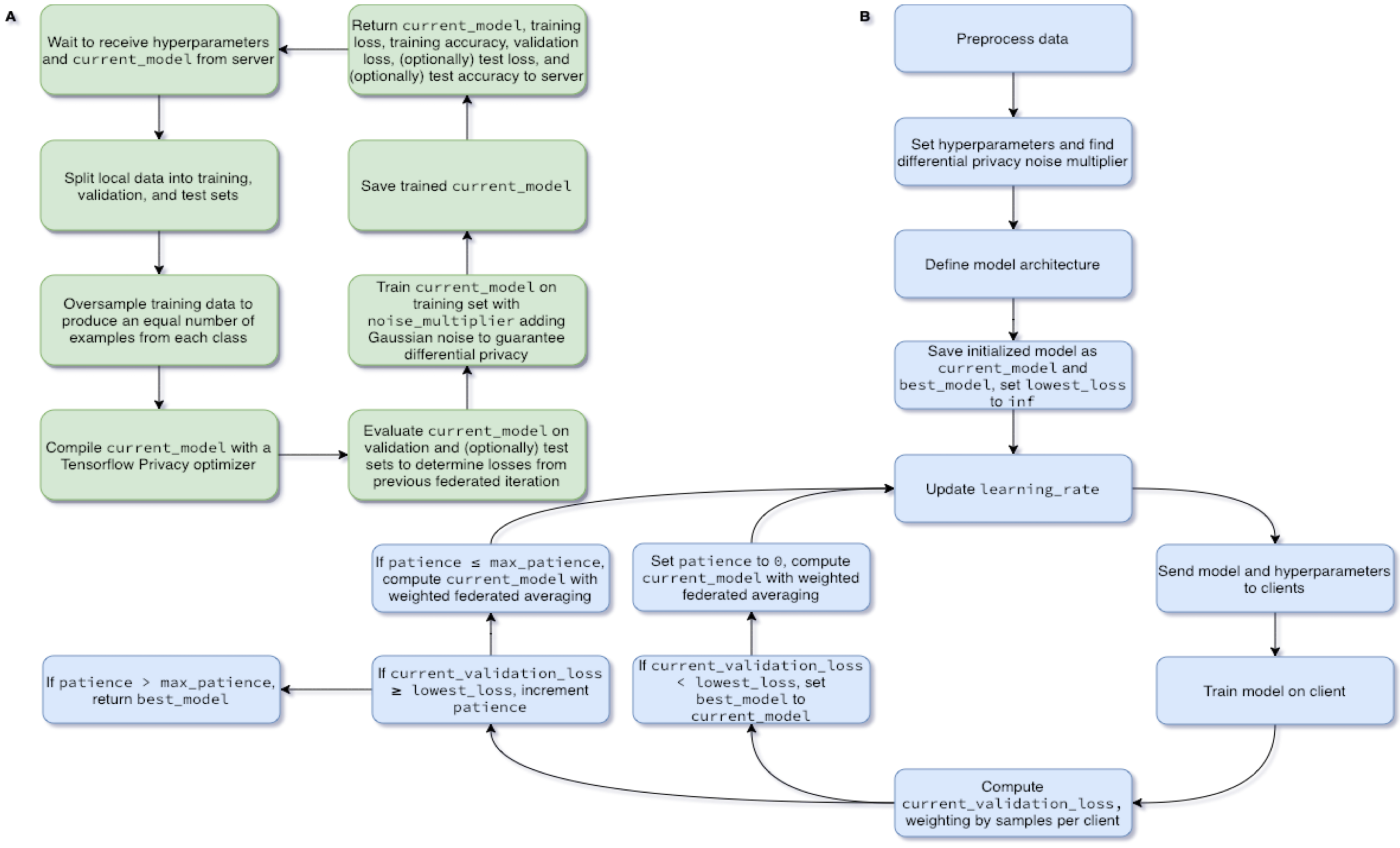
Solution

The flowchart below highlights our solution to this solution to this problem. It allows hospitals to keep their data entirely on-site and prevents machine learning algorithms from memorizing information.

Testing

We created a model to predict breast cancer under varying privacy requirements. We then compared the accuracies in the figure shown below. Note that smaller ε values correspond to higher levels of privacy.





Wait to receive hyperparameters and `current_model` from server

Split local data into training, validation, and test sets

Oversample training data to produce an equal number of examples from each class

Compile `current_model` with a Tensorflow Privacy optimizer

Evaluate `current_model` on validation and (optionally) test sets to determine losses from previous federated iteration

Train `current_model` on training set with `noise_multiplier` adding Gaussian noise to guarantee differential privacy

Save trained `current_model`

Return `current_model`, training loss, training accuracy, validation loss, (optionally) test loss, and (optionally) test accuracy to server

Preprocess data

Set hyperparameters and find differential privacy noise multiplier

Define model architecture

Save initialized model as `current_model` and `best_model`, set `lowest_loss` to `inf`

Update `learning_rate`

Send model and hyperparameters to clients

Train model on client

Compute `current_validation_loss`, weighting by samples per client

If `current_validation_loss < lowest_loss`, set `best_model` to `current_model`

Set `patience` to `0`, compute `current_model` with weighted federated averaging

If `current_validation_loss ≥ lowest_loss`, increment `patience`

If `patience ≤ max_patience`, compute `current_model` with weighted federated averaging

If `patience > max_patience`, return `best_model`

Data Reference: Xie, H, et al. (2017, December 21). *Gene Expression Profiles of Breast Cancer.* Mendeley Data.

Authors: 1. Amol Khanna, 2. Vincent Schaffer, 3. Gamze Gürsoy, 4. Mark Gerstein

1. <akhann13@jhu.edu> Department of Biomedical Engineering, Department of Applied Mathematics and Statistics, Johns Hopkins University. 2. Department of Computer Science, Yale University. 3. Department of Biomedical Informatics, Columbia University; Core Faculty, New York Genome Center. 4. Department of Molecular Biophysics and Biochemistry, Department of Computer Science, Department of Statistics and Data Science, Yale University.

JOHNS HOPKINS
BIOMEDICAL ENGINEERING