Privacy-Preserving Personal Model Training

Hamed Haddadi
Imperial College London

Joint work with: Sandra Servia-Rodriguez, Liang Wang, Jianxin R. Zhao, Richard Mortier
Machine Learning today

- Get Users, collect loads of labelled data, train model, at a Data centre
- Privacy, cost, personalization challenges
- Think about sensitive images on FB, and voices on Echo, accountability, responsibility, GDPR, …
Privacy during Usage of ML models

Training Data

Prediction

Input data
Classification

Training

Do model's predictions leak information about training data?

Query Input

Model

Prediction API

Input data
Classification

Training API

DATA

Google Cloud Platform

Amazon Web Services
Distributed Learning

Service Provider

Parameters' Container

Global Machine Learning model

Local Machine Learning model

Local Data

User 1

Local Machine Learning model

User 2

Local Machine Learning model

User n

Local Machine Learning model
Federated Learning

Federated Learning: Collaborative Machine Learning without Centralized Training Data (Google 2017)
Databox

- See the details on  www.databoxproject.uk  &  github.com/me-box
Dataset 1

• Motion-based activity classifier on smartphone without revealing their data to others.

• WISDM Human Activity Recognition dataset, accelerometer data on an Android phone by 35 subjects performing 6 activities (walking, jogging, walking upstairs, walking downstairs, sitting and standing).

• Statistical measures obtained for every 10 seconds of accelerometer samples as the \( d = 43 \) dimensional features in our models.

Final sample: 5,418 accelerometer traces from 35 users, with on average 150.50 traces per user and standard deviation of 44.73.
privacy-preserving activity recognition

• Multilayer Perceptron with 2 layers for activity recognition, 1 hidden layer with 128 nodes, 1 logistic regression layer.
• 6,406 parameters to be determined during training.
• All on Raspberry Pi 3 Model B
More samples, good samples!
Topic modelling from Wikipedia using LDA

Using OWL Library: https://github.com/owlbarn
Training time

Graphs showing training time vs. number of samples, and histograms for different variables such as training document amount, vocabulary amount, and percentage of data included in g0.
Thank You!

Privacy-Preserving Personal Model Training

We are looking for postdocs and PhD students!

Hamed Haddadi
Imperial College London

https://haddadi.github.io/
h.haddadi@imperial.ac.uk
@realhamed