Federated Learning

Read Advances and Open Problems in Federated Learning

▼ Resources

Dataset

LEAF

A Benchmark for Federated Settings LEAF is a benchmarking framework for learning in federated settings, with applications including federated learning, multi-task learning, meta-learning, and on-device learning. Future releases will include additional tasks and datasets. Please contact Sebastian Caldas with questions

https://leaf.cmu.edu/

Tutorials

Federated Learning: Collaborative Machine Learning without Centralized Training Data

Standard machine learning approaches require centralizing the training data on one machine or in a datacenter. And Google has built one of the most secure and robust cloud infrastructures for processing this data to make our services better. Now for models trained from user interaction with mobile devices, we're

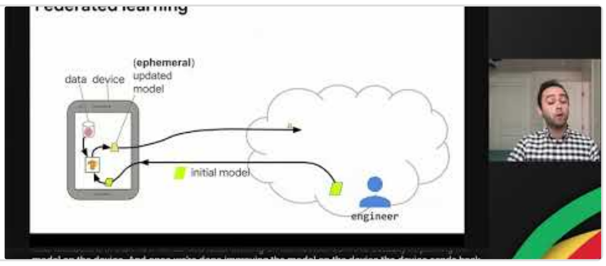
https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

TensorFlow Federated

TensorFlow Federated: Machine Learning on Decentralized Data TensorFlow Federated (TFF) is an open-source framework for machine learning and other computations on decentralized data. TFF has been developed to facilitate open research and experimentation with Federated Learning (FL), an approach to

https://www.tensorflow.org/federated

https://youtu.be/JBNas6Yd30A



2020 Google Workshop on Federated Learning and Analytics

Share your videos with friends, family, and the world

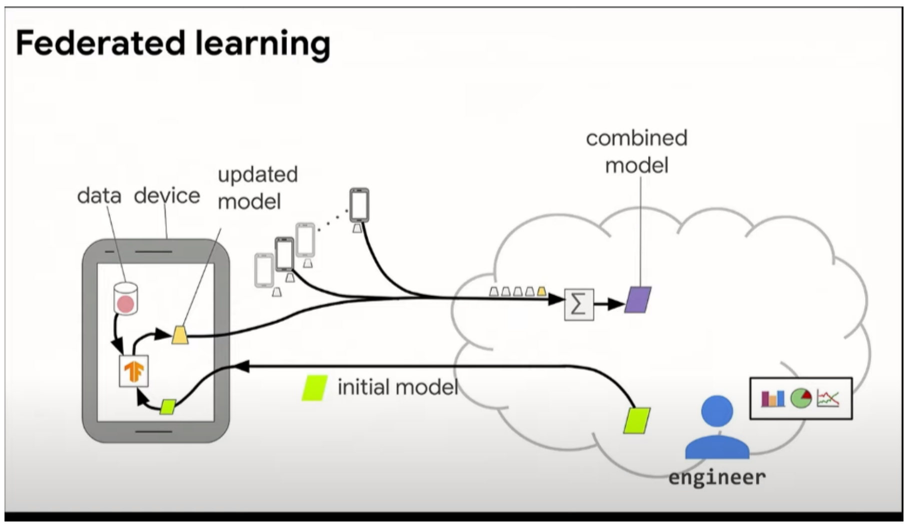
https://youtube.com/playlist?list=PLSIUOFhnxEiCJS8q6SYdc0944xlV_6Jbu

https://www.youtube.com/watch?v=nBGQQHPkyNY

Basics

- Normally when training a ML model we generally host model and the data on the same device. This is known as the **"Centralized Machine Learning" .** This also means less privacy as companies like google Upload our data onto the cloud storages they hold.
- In **Federated Learning** we try to flip the logic and instead of sending the data to the cloud we try to send the model to the device & train these models locally. This ensures the data never leaves the device. After this we send the updated model to the cloud which only includes the updated weights and biases. After this the models are combined using the avg. method or aggregate method.
- We also don't send these models to all the devices we have , instead we send these models to only few of the total devices and get their updated models. Build a new model with aggregate method and do this over multiple iterations , to get the final build of the model. This final build of the model is then shipped to all the devices .

Federated Learning Working



This is the updated version of the basic loss function we know. We first decide the number of clients we have (k) , then we find the loss of individual client on the device and then we multiply these losses with respective weights of the amount of data the device has with respect to the total data. After this we sum these losses to get Fed-Avg Loss.

Each client runs Stochastic Gradient Descent on the models.

We need to improve Fed-Avg as it is not the perfect.

> 🚨 We generally do 100-1000s of rounds of this , were we repeat the same process & 100-1000s of rounds to converge.
>
> Each round approx. takes 1-10 min

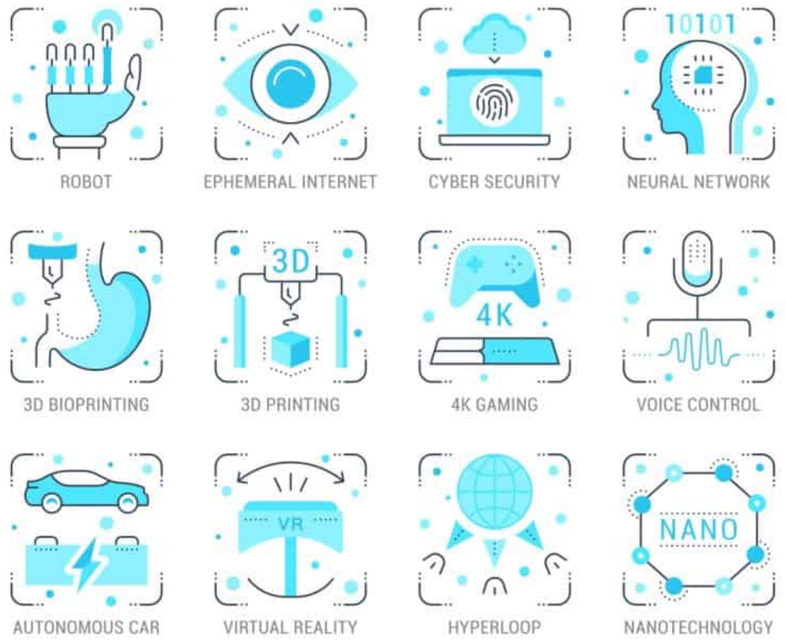
What is Federated Learning

Federated learning (also known as collaborative learning) is a machine learning technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples, without exchanging them.

Why do we need Federated Learning

Well, for starters, the most crucial reason for relying on Federated Learning is that it keeps things private on your part. This is because of how your machine or your mobile device continues to learn and adapt without the need to make use of the data sent over to it from the cloud. In that sense, your smartphone doesn't send over your personal data and information to a central server as only the updates on the phone are sent to it. That means that what is meant to stay on your mobile device will remain on your mobile device. This ability allows anyone to enjoy using their smartphone or other devices while minimizing the risk of their personal data and information being leaked online. Especially now that we live in an age where cyber-attacks are becoming more common as hackers and cyber-criminals are getting smarter and better at what they do.

Use of Federated Learning



Frameworks

- **TensorFlow Federated**
- Flower
- PyTorch Federated

Refer this page for further information about federated learning on TensorFlow.

Federated Learning