SIG workshop series presents you

Federated Learning Workshop

By Aswarth Narayana and Jaideep Reddy

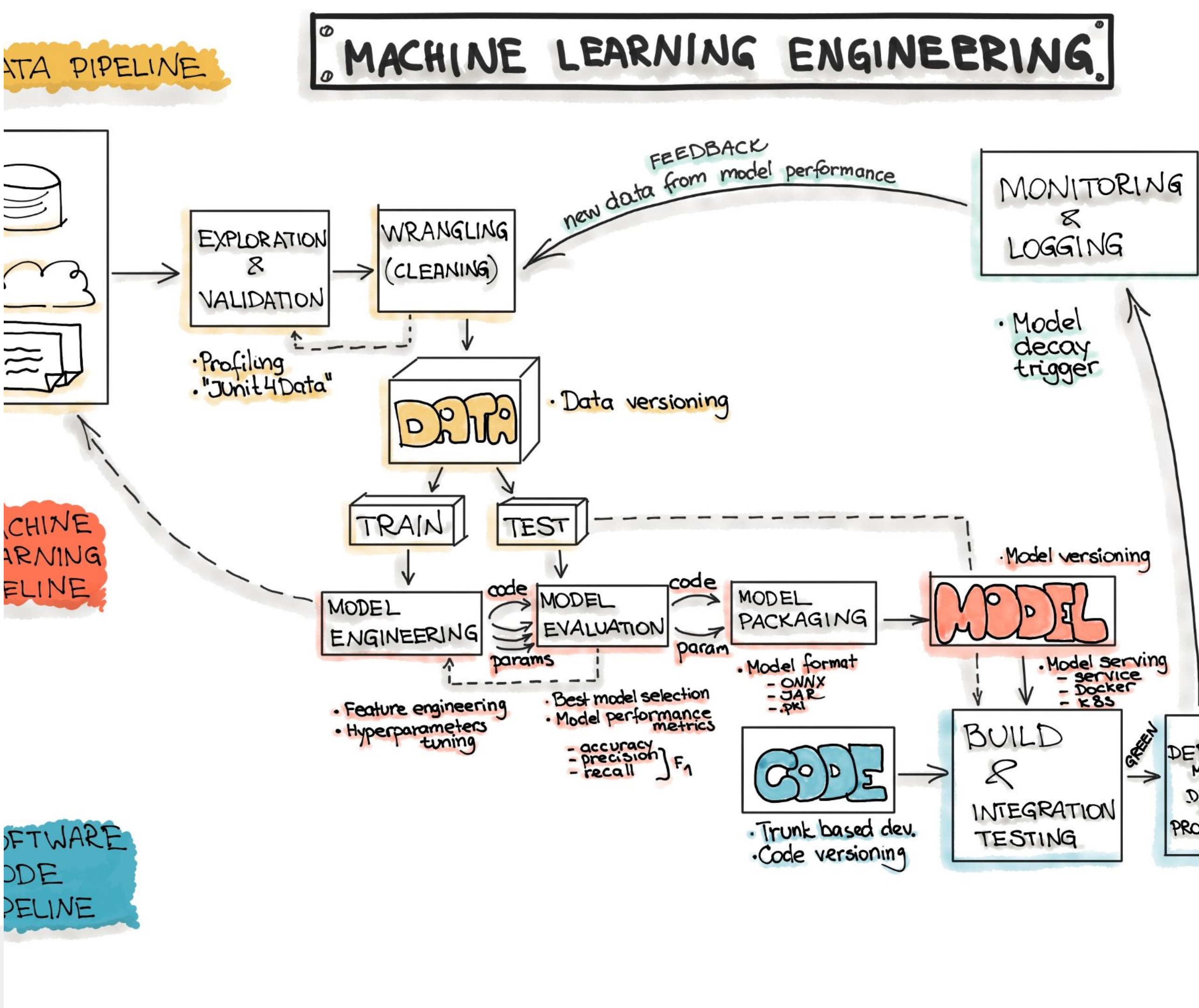
Agenda

- Brief insight into Traditional ML WorkFlow
- Idea behind Distributed ML
  - Advantages and Disadvantages of Distributed ML
- Idea behind Federated Learning
  - Applications
  - Advantages & Disadvantages of FL
- FL architecture Implementation using TensorFlow model
- References

A brief insight into Traditional Machine Learning WorkFlow

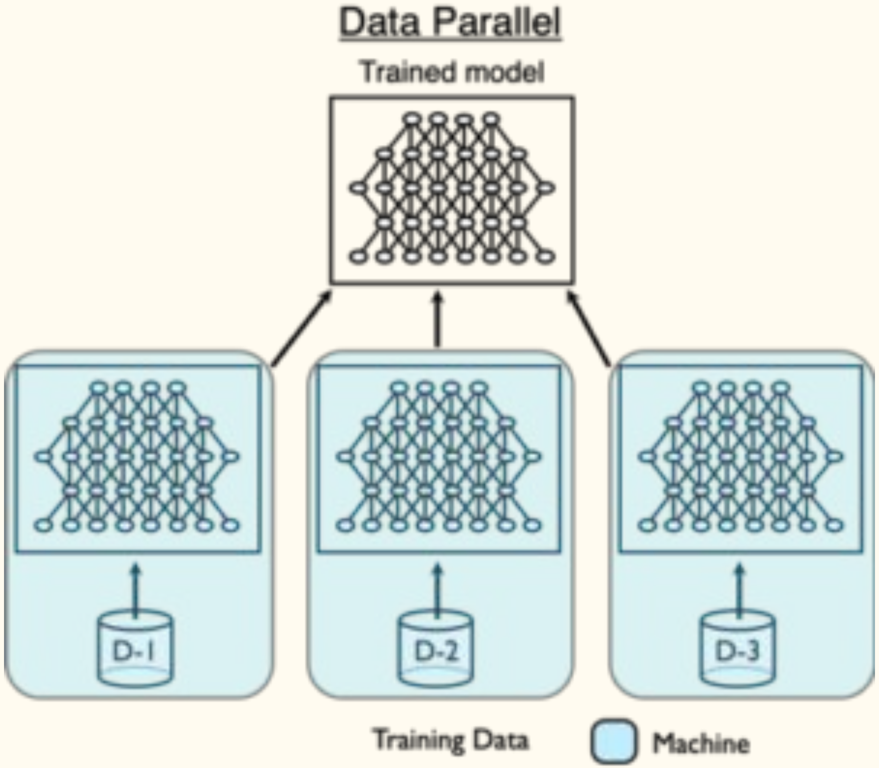
Traditional ML WorkFlow

- Data
  - Acquisition
  - Exploration
  - Preparation
- Feature Engineering
- Model
  - Selection
  - Training
- Hyperparameter Tuning
- Predictions



Distributed Machine Learning idea

“ Distributed machine learning refers to multinode machine learning algorithms and systems that are designed to improve performance, increase accuracy, and scale to larger input data sizes. ”



Core Idea of Distributed ML - **Parallelism**

- Data Parallelism
  - Data is partitioned as per number of worker nodes
  - All workers apply the same algorithm to different partitions of data
  - The same model is available to all worker nodes (either through centralization, or through replication) so that a single coherent output emerges naturally

Advantages and Disadvantages of Distributed ML

Advantages

- Can handle very large data sets (Scalability)
- develop efficient and scalable algorithms (with regards to accuracy and computational power)

Disadvantages

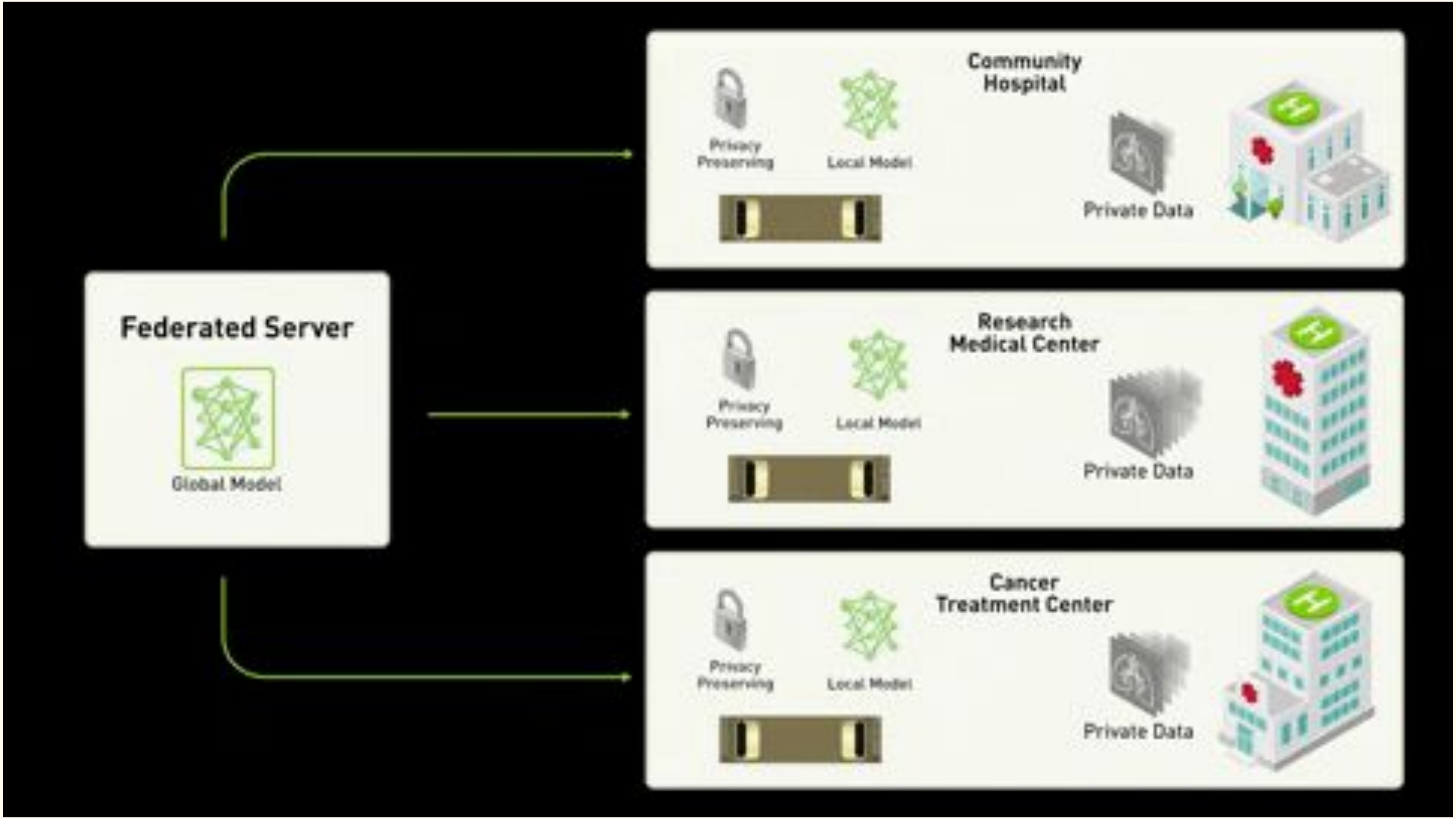
- Writing and running a distributed ML algorithm is highly complicated and developing distributed ML packages
- There are no standardised measures to evaluate distributed algorithms

Federated learning idea

> “ Federated learning is a machine learning technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples, without exchanging them.”

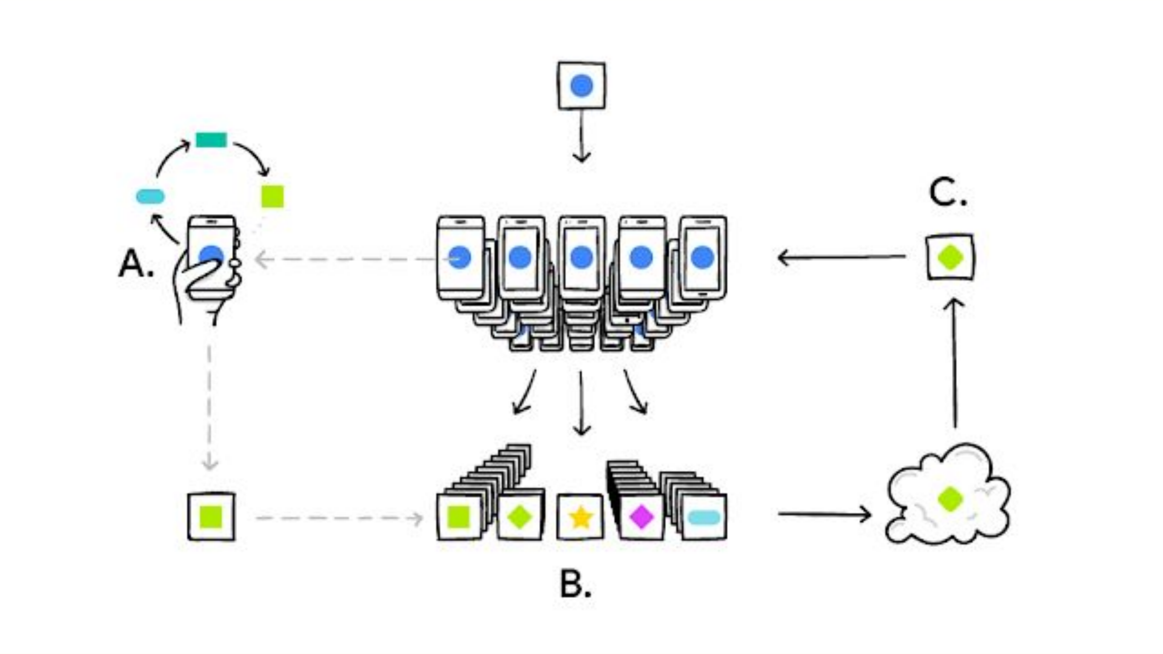
**Federated - (of a country or organization) set up as a single centralized unit within which each state or division keeps some internal autonomy.

Federated Learning in Action


Federated Server
Global Model
Community Hospital
Privacy Preserving
Local Model
Private Data
Research Medical Center
Privacy Preserving
Local Model
Private Data
Cancer Treatment Center
Privacy Preserving
Local Model
Private Data

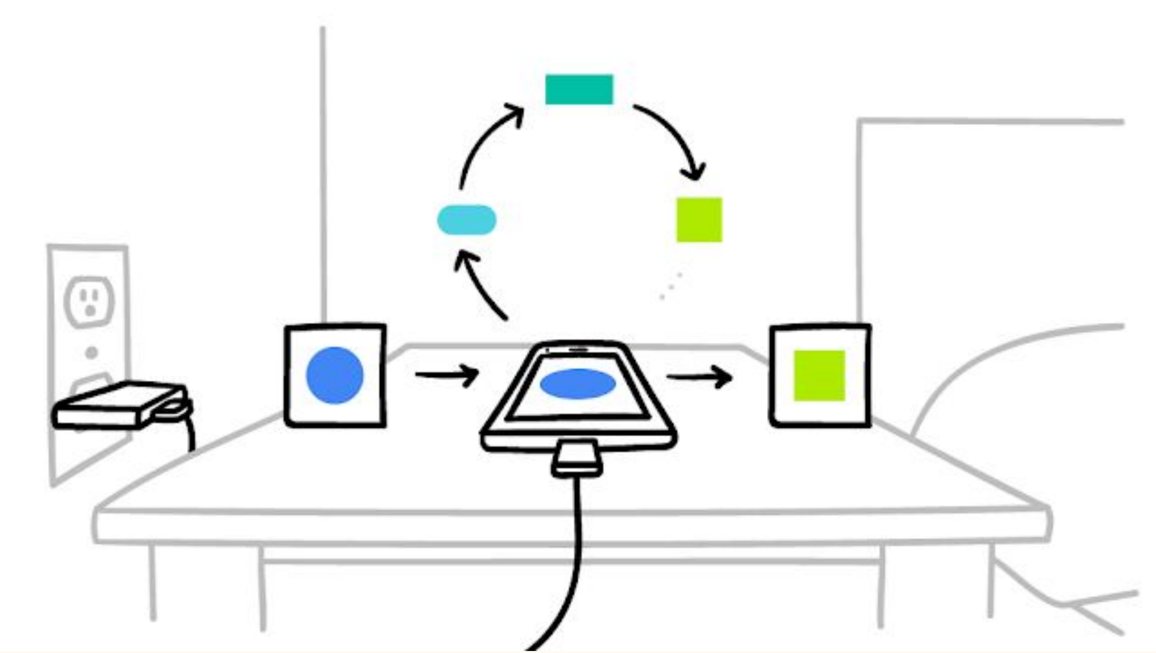
Understanding FL Through Application - Gboard

- The device downloads the **current model**
- Improves it by **learning from data on your phone**, and then summarizes the changes as a **small focused update.**
- Only this update to the model is sent to the cloud, **using encrypted** communication, where it is immediately **averaged with other user updates** to improve the shared model
- All the training data remains on your device, and **no individual updates are stored in the cloud**



Your phone personalizes the model locally, based on your usage (A). Many users' updates are aggregated (B) to form a consensus change (C) to the shared model, after which the procedure is repeated.

- Federated Learning allows for **smarter models**, **lower latency**, and **less power consumption**, all while **ensuring privacy**
- The **improved model on your phone can also be used immediately**, powering **experiences personalized** by the way you use your phone
- **Secure Aggregation protocol** that uses cryptographic techniques so a coordinating server can only **decrypt the average update if 100s or 1000s of users have participated** — no individual phone's update can be inspected before averaging.



Your phone participates in Federated Learning only when it won't negatively impact your experience.

Federated Learning Advantages & Disadvantages

Advantages

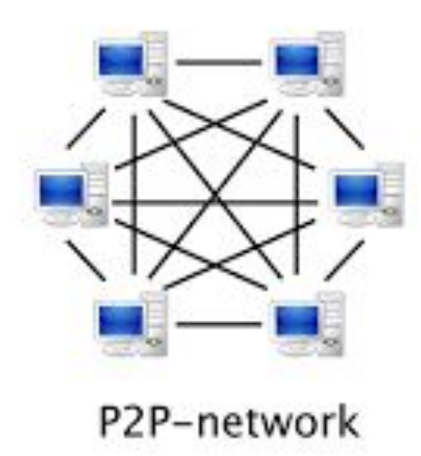
- ***Wide range of Use Cases:*** Mobile applications, Healthcare, Autonomous Vehicles, Manufacturing – predictive maintenance and counting ...
- ***Data security:*** Keeping training dataset on the devices.
- ***Data diversity:*** FL facilitates access to heterogeneous data.
- ***Real time continual learning:*** Models are constantly improved using client data.
- ***Hardware efficiency:*** FL uses less computational power on the end devices.

Disadvantages

- ***Expensive Communication:*** Federated networks are potentially comprised of a **massive number of devices** and **communication in the network can be slower** than local computation by many orders of magnitude.
- ***Systems Heterogeneity:*** The storage, computational, and communication capabilities of each device in federated networks may differ due to **variability in hardware**
- ***Statistical Heterogeneity:*** Devices **frequently generate and collect data** in a non-identically distributed manner across the network.

Gossip Learning

This approach is fully decentralized and there is no server for merging outputs from different locations. Local nodes directly exchange and aggregate models. This approach requires even less infrastructure since there is no centralization requirements compared to FL.



References

- https://ml-ops.org/content/end-to-end-ml-workflow
- https://ai.googleblog.com/2017/04/federated-learning-collaborative.html
- https://docs.microsoft.com/en-us/azure/machine-learning/concept-distributed-training#model-parallelism
- https://analyticsindiamag.com/distributed-machine-learning-vs-federated-learning-which-is-better/
- https://www.analyticsvidhya.com/blog/2021/05/federated-learning-a-beginners-guide/
- https://www.guavus.com/technical-blog/distributed-machine-learning-for-big-data-and-streaming/
- https://research.aimultiple.com/federated-learning/

THANK YOU