Federated Learning (FL)

EE6350: Artificial Intelligence

Mr. M.W.G.C.K Moremada
Lecturer, Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna

Lecture Outline

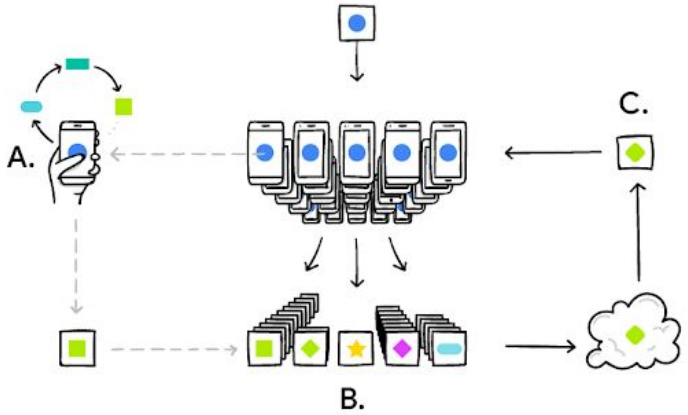
1. What is FL?
    a. Example: Gboard Query Suggestion
2. Classical ML
    a. Challenges
3. FL Working
    a. FL
    b. The Original Process as Proposed by Google (Federated Average)
    c. Advantages
4. Characteristics of FL
    a. Traditional Distributed Systems Vs FL
    b. FL Characteristics
5. Categorization of FL
    a. Horizontal FL
    b. Vertical FL
    c. Federated Transfer Learning
6. Applications of FL
7. FL Frameworks

What is FL?


Text generate image with Bing Image creator powered by DALLE-3

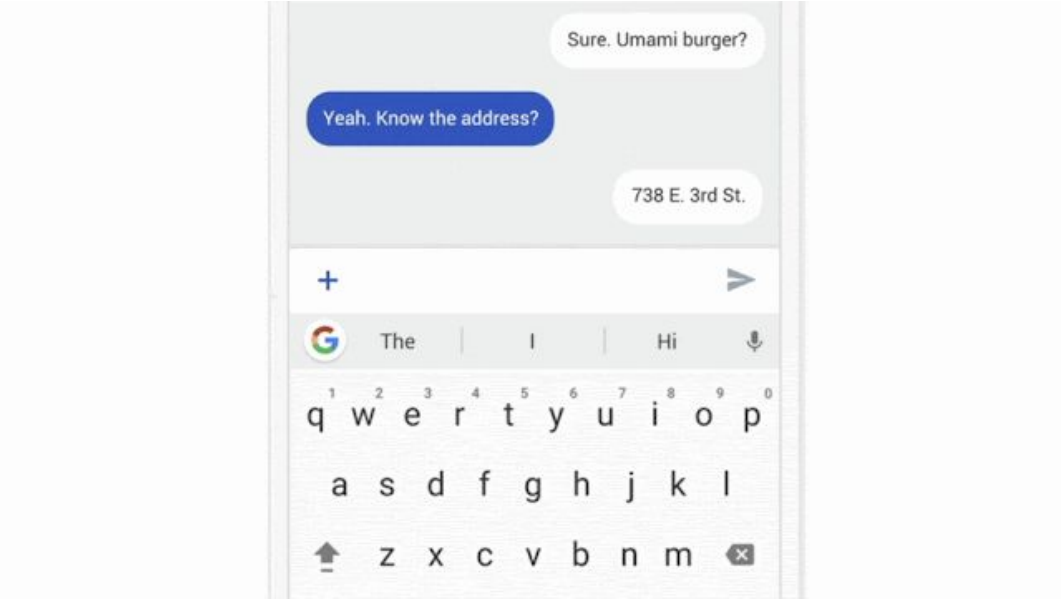
What is Federated Learning

- Federated learning allows local/distributed devices such as mobile phones to **collaboratively learn a shared prediction model while keeping all the training data in device**, while removing the requirement of storing the data for ML model training in a centralized server/storage.
- **Proposed by Google in 2016** to predict user's text input.



Ref: https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/

Example: Gboard Query Suggestion

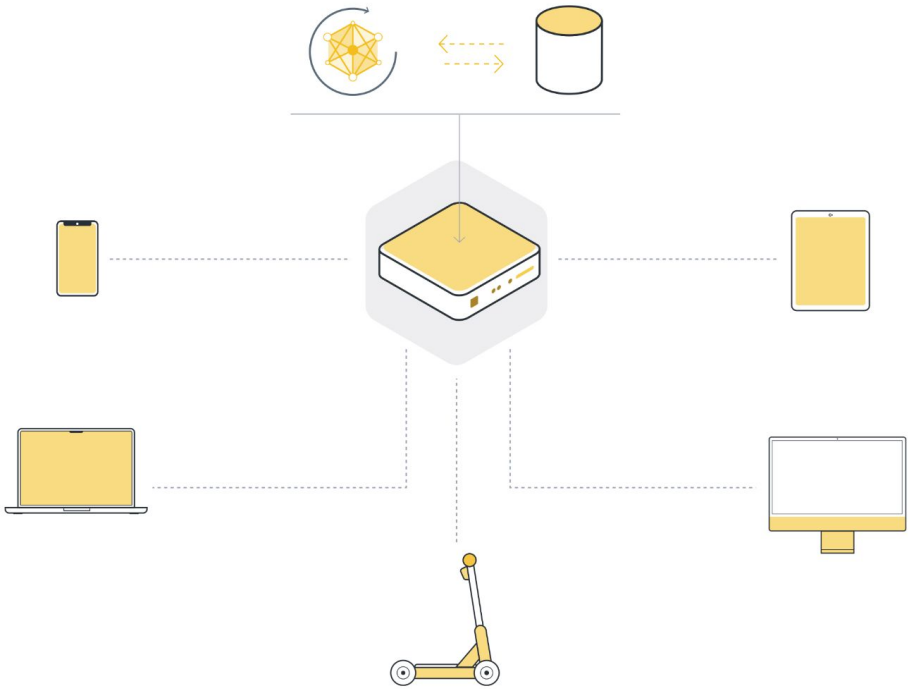


- When Gboard shows a suggested query, your **phone locally stores information about the current context** and **whether you clicked the suggestion.**
- FL processes that history on-device to suggest improvements to the next iteration of Gboard's query suggestion model.

Ref: https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/

Classical ML

Classical ML



https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

Classical ML: Challenges

- **Regulations** to protect sensitive data from being moved (E.g. GDPR - Europe, CCPA - California, PIPEDA - Canada etc.)
- **User preferences** that not to leave their data from their devices.
- Difficulty in collecting **large data volumes** generating from sensors (e.g., cameras).
- **Centralized ML might not work with:**

Health Records | Financial Information

Location Data | End-to-End Encrypted Messages

FL Working

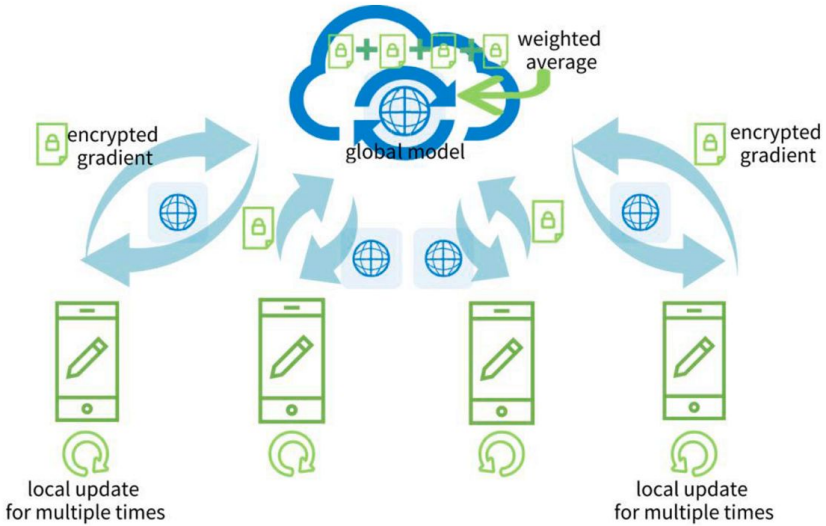

Text generate image with Bing Image creator powered by DALLE-3

FL

- FL refers to multiple clients that can be mobile devices, institutions, organizations etc. **coordinated with one or more central servers for decentralized ML settings**.
- FL become an appropriate technique especially for **privacy-sensitive applications.**
  - E.g., Health care.

FL: The Original Process as Proposed by Google (Federated Average)

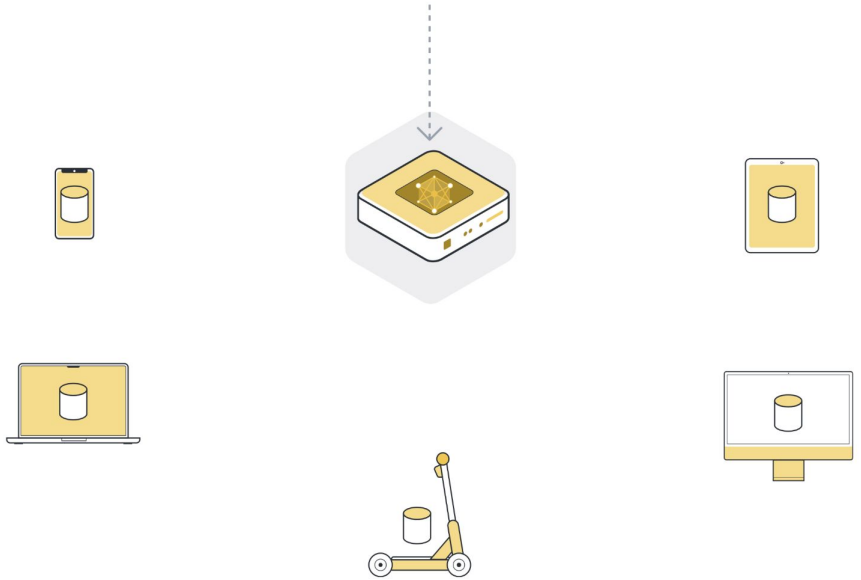
- **Federate Average (FedAvg)** is the baseline of FL in many other research.
- The steps of the process can be broken down into six stages.



L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," Computers & Industrial Engineering, vol. 149, p. 106854, Nov. 2020, doi: https://doi.org/10.1016/j.cie.2020.106854.

FL Steps

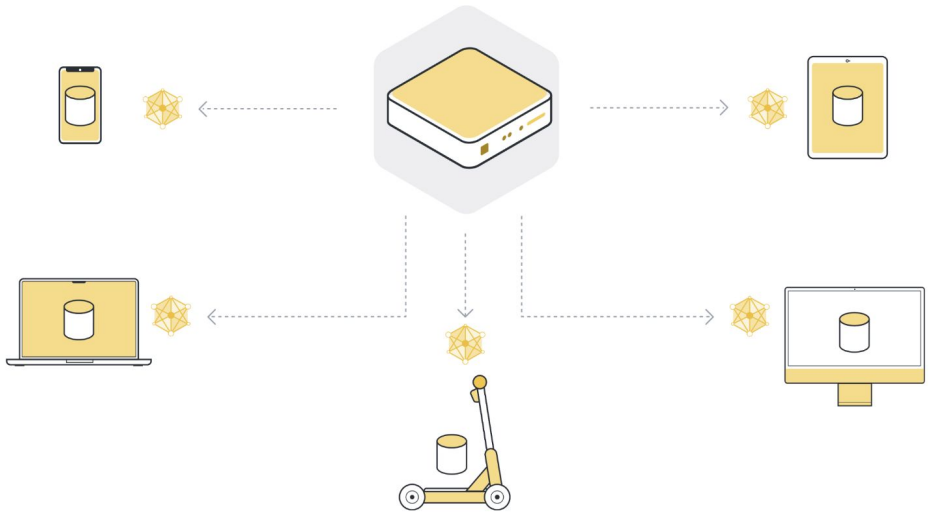
Step 01: Initialize global model



https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

FL Steps

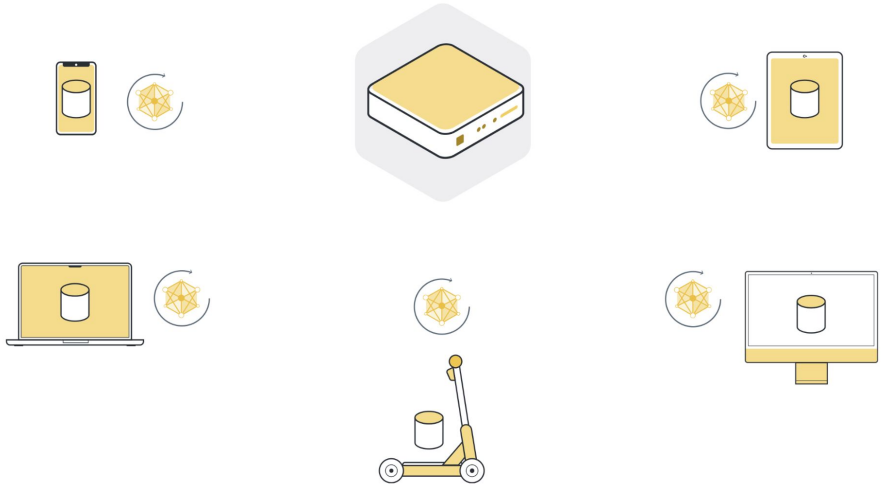
Step 02: Send model to a number of connected organizations/devices (client nodes)



https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

FL Steps

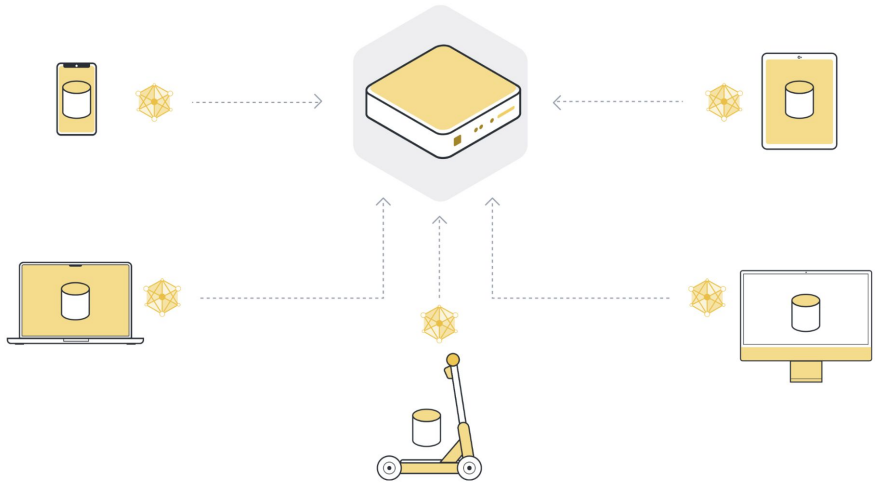
Step 03: Train model locally on the data of each organization/device (client node).



https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

FL Steps

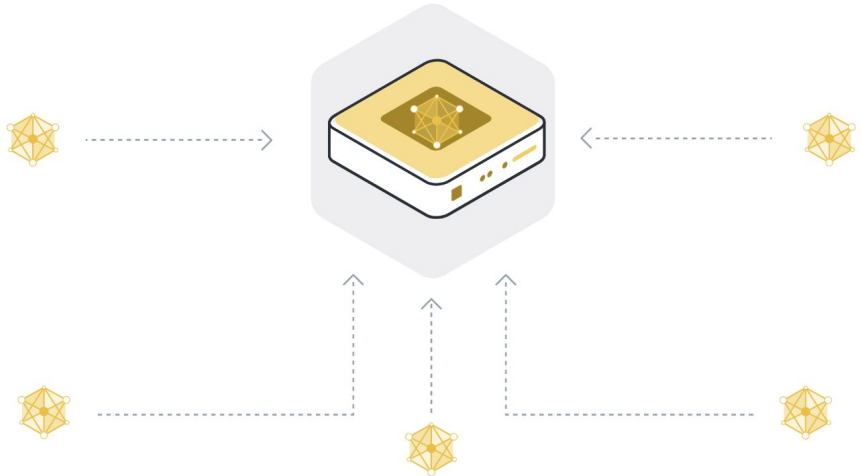
Step 04: Return model updates back to the server - either full model parameters (wights) or just the gradients.



https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

FL Steps

Step 05: Aggregate model updates into a new global model. Among many different ways Federated Averaging (FedAvg) is the most basic way to do it.



What are the other methods available for aggregation in FL systems?

https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

FL Steps

Step 06: Repeat steps 2 to 5 until the model converges.

1. The global model parameters get sent to the participating client nodes.
2. The client nodes train on their local data.
3. They send their updated models to the server.
4. The server then aggregates the model updates to get a new version of the global model

https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html

FL: Advantages

- FL solves the contradiction between **data privacy and data sharing** for disperse devices since data will not be exposed to third party central server.
- FL allows for smarter models, **lower latency, and less power consumption, all while ensuring privacy.**
- The **improved model on your device (e.g., smartphone) can also be used immediately,** powering experiences personalized by the way you use your device.

Characteristics of FL

Info Slide

Traditional Distributed Systems Vs FL

Traditional Distributed Systems	Federated Learning

• Made up of,
  ○ Distributed computation.
  ○ Distributed storage.
• Mainly targeted at accelerating the processing stage.
	• Focus on building a collaborative model without data leakages.
	More characteristics to be introduced...

Traditional distributed processing, connect multiple computers in different locations via communication network under the control of center server, so that each computer undertakes different parts of the same task to complete it

FL Characteristics

1. **Universality for cross-organizational scenarios:**
   - FL could be extended to bring cross-organizational enterprise into federal framework.
   - E.g., **Bank that possess data of clients' purchasing power could cooperate with electronic business platform which possess data of product features, to recommend products.**
   - Thus, intelligently construct joint model for **multiple entities, multiple data sources, different feature dimensions**.

FL Characteristics

2. Massively non-identically independent distribution (Non-IID):
    - FL is concentrated on **unbalanced and non-IID data because of the heterogeneity among device resources.**
    - Traditional distributed systems primarily works on balanced and IID data distributions.

Info Slide

Independent and Identically Distributed (IID)

- **Independent:** occurrence or value of one data point does not provide any information about the occurrence or value of another data point. It assumes that the data points are not influenced by each other and that there is no hidden structure or correlation among them.
- **Identical Distribution:** Data points are drawn from the same underlying distribution. It implies that the statistical properties, such as mean, variance, and other distributional characteristics, remain consistent across the entire dataset.

https://medium.com/@evertongomede/independent-and-identically-distributed-iid-in-machine-learning-assumptions-and-implications-930ee9821e14

FL Characteristics

3. Decentralized technology:
    - In a technical sense, **decentralization does not means complete decentralization,** but there is no definitive center and it dilutes the awareness of the central node.
    - In FL,
        i. Each client is completely autonomous.
        ii. Data is not allocated by a central server.
        iii. Training process is not governed by a central server.

FL Characteristics

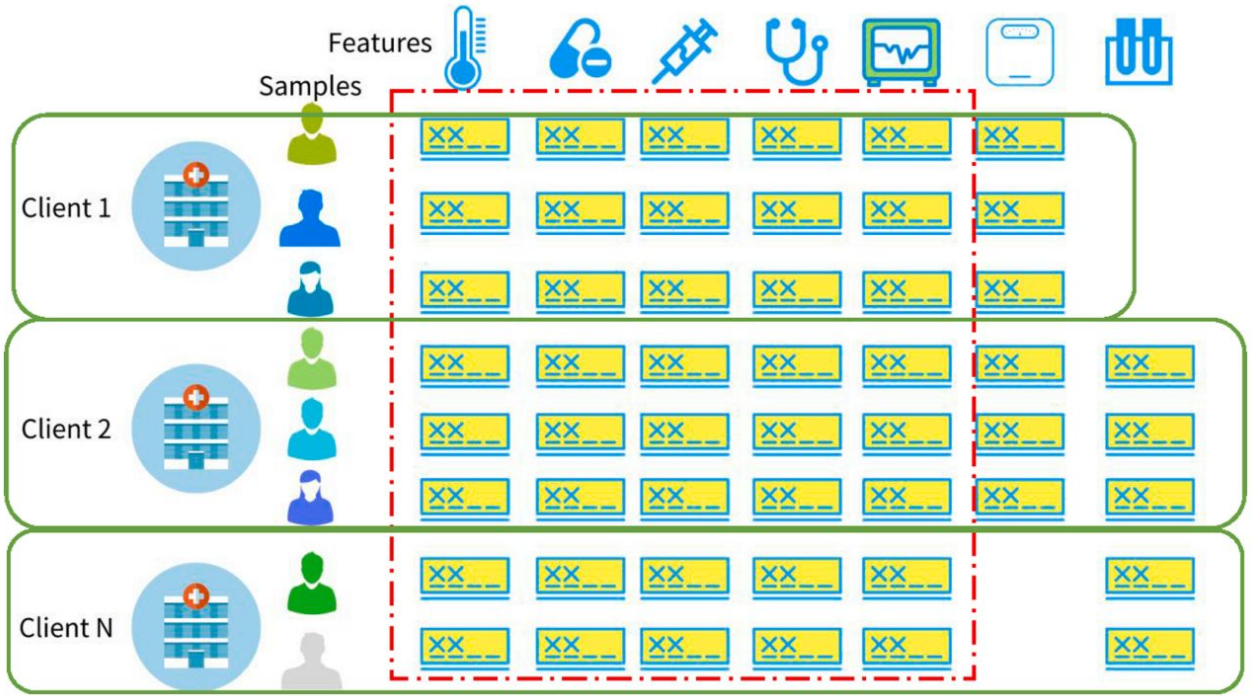
4. Equality of status for each node
    - All parties **enjoy equal status** and certain dominion to achieve common prospective,
    - In traditional distributed collaborative training **whoever possesses a great mass of data has the dominant position.**
    - However in FL, **position of clients with small amount of data would also be promoted due to equality.**

Categorization of FL

FL Categorization: Horizontal FL

- There is a **certain amount of overlap between the feature of data spread across various nodes**, while the data are quite different in sample space.
- E.g.,
  - A FL framework for cross-regional hospitals with similar medical information.

FL Categorization: Horizontal FL

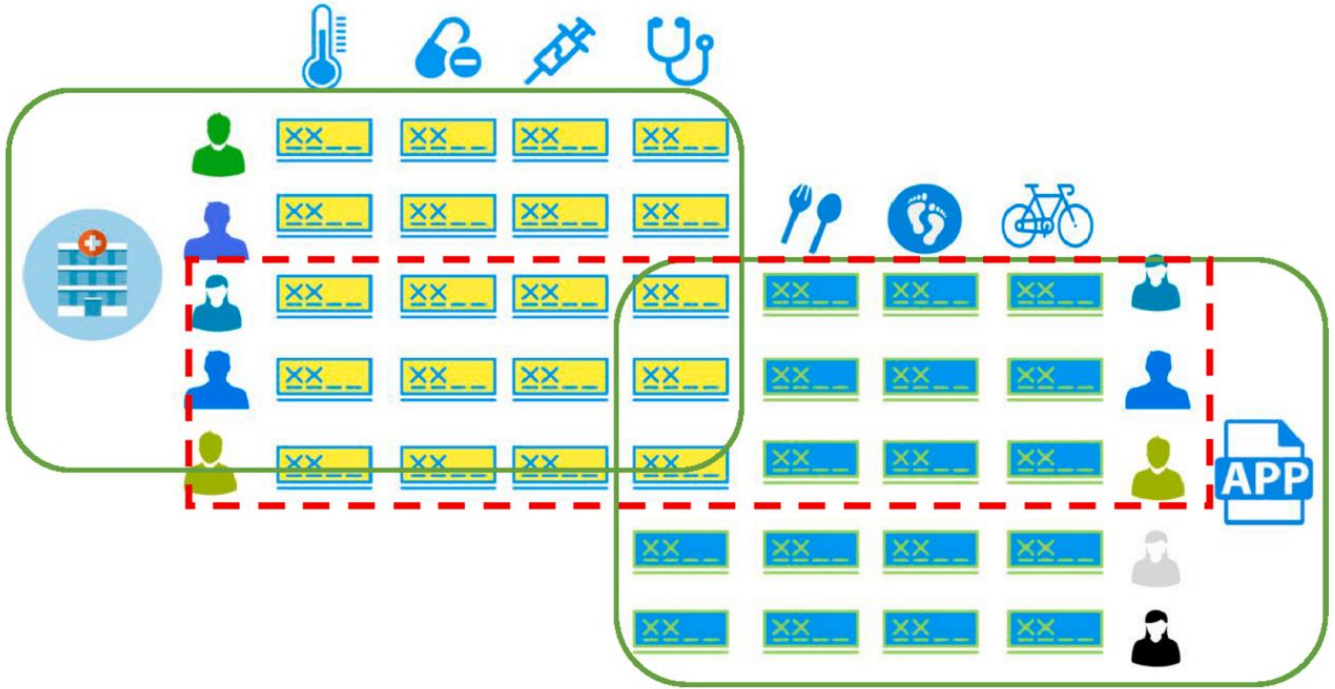


L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," Computers & Industrial Engineering, vol. 149, p. 106854, Nov. 2020, doi: https://doi.org/10.1016/j.cie.2020.106854.

FL Categorization: Vertical FL

- All the parties involved in FL system have partial **overlap on sample ID whereas differ in feature space** (i.e., applicable for the cases where the **datasets share the same ID space but differ in feature space**) .
  - E.g., Incorporation of hospital with a smartphone company for diabetes prediction.
    - Features from hospital's dataset: **Age, Weight, Medical History.**
    - Features from smartphone company's dataset: **Step Counter, Dietary Structure.**

FL Categorization: Vertical FL

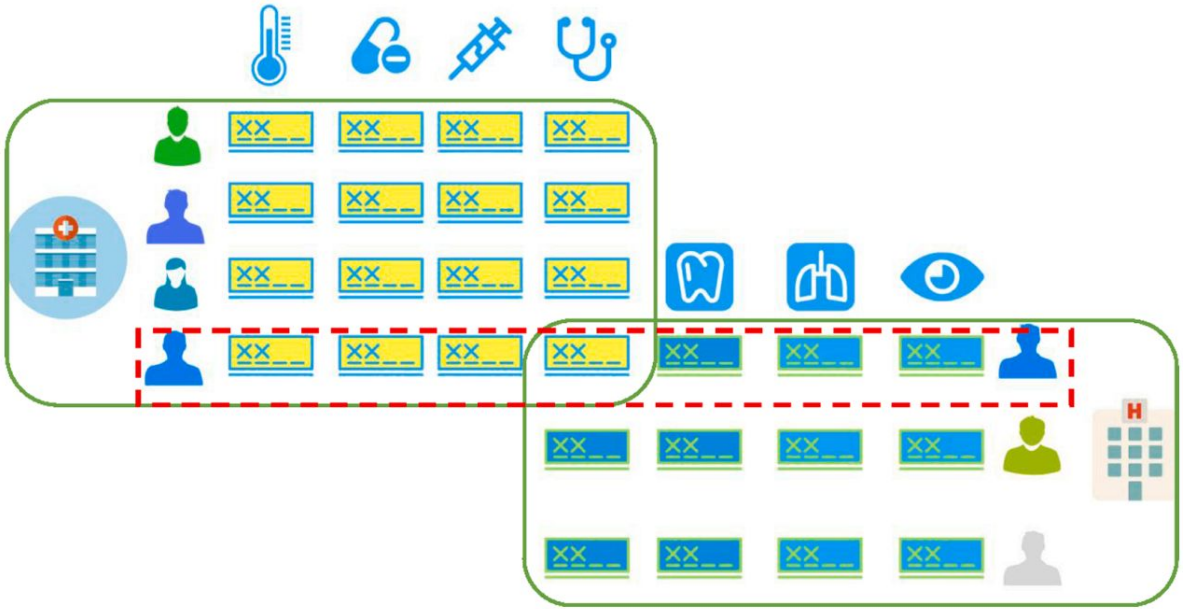


L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," Computers & Industrial Engineering, vol. 149, p. 106854, Nov. 2020, doi: https://doi.org/10.1016/j.cie.2020.106854.

FL Categorization: Federated Transfer Learning

- Transfer learning enables to move the knowledge of **source domain to target domain** to achieve better learning results.
- Under the scenarios where the datasets **differs from not only in samples but also in features** Federated Transfer Learning applies.
- Federated Transfer Learning **generalizes** the Federate Learning to have broader application when it comes to common parties with **small interactions.**
- E.g.,
  - Some disease diagnostic and treatment information from one hospital could be transferred to another hospital to help other disease diagnosis.

FL Categorization: Federated Transfer Learning



L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," Computers & Industrial Engineering, vol. 149, p. 106854, Nov. 2020, doi: https://doi.org/10.1016/j.cie.2020.106854.

Applications of FL

FL Applications: Smartphones

- FL applications in smartphones:
  - Word prediction.
  - Face recognition for logging.
  - Voice recognition (e.g., Siri or Google Assistant).

https://www.xfinity.com/hub/mobile/facial-recognition-on-phone

FL Applications: Transportation

- FL applications in transportation:
  - Self-driving cars: To continuously adapt to the environment.

https://www.fau.edu/newsdesk/articles/self-driving-cars-behavior.php

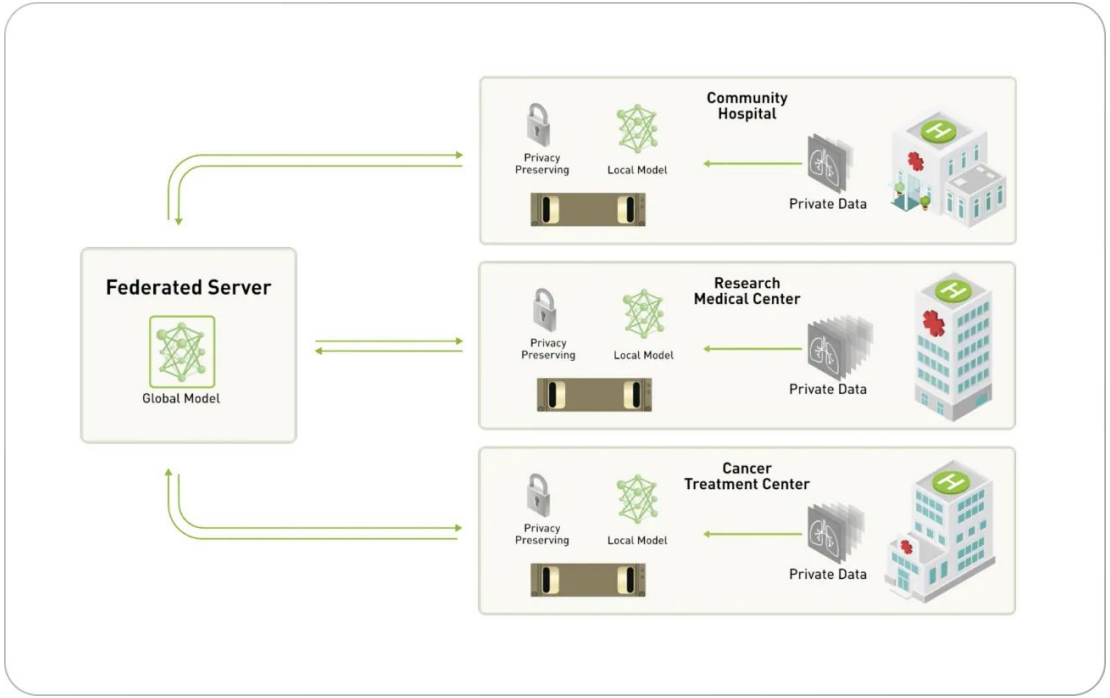
FL Applications: Manufacturing

- FL examples in manufacturing:
  - **Product recommendation systems:** Understand the depend for a product based on personal sales.
  - **Object detection, remote operation and virtual assembly:** AR/VR based techniques.
  - **Industrial environment monitoring:** FL makes it easier to perform time-series analysis using data from multiple sensors.

https://www.eflexsystems.com/lean-manufacturing-blog/scenarios-of-common-assembly-line-issues

FL Applications: Healthcare

- FL helps to train models by providing **secure access to data while protecting patient's privacy.**
- Data will never have to leave the original premises.



https://www.v7labs.com/blog/federated-learning-guide

FL Frameworks

FL Frameworks

TensorFlow Federated

Federated AI Technology Enabler

Flower

References

1. “Federated Learning: Collaborative Machine Learning without Centralized Training,” research.google. https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/ (accessed Apr. 11, 2024).
2. L. Li, Y. Fan, M. Tse, and K.-Y. Lin, “A review of applications in federated learning,” Computers & Industrial Engineering, vol. 149, p. 106854, Nov. 2020, doi: https://doi.org/10.1016/j.cie.2020.106854.
3. Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated Machine Learning,” ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, Feb. 2019, doi: https://doi.org/10.1145/3298981..
4. Y. Shastri, “A Step-by-Step Guide to Federated Learning in Computer Vision,” www.v7labs.com, Feb. 03, 2023. https://www.v7labs.com/blog/federated-learning-guide
5. “Flower Framework main,” flower.ai. https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html (accessed Apr. 11, 2024).

Thank You