Escuela AI HUB de verano
Sobre IA y Educación

BARCELONA, 3 AL 7 DE JULIO 2023
CaixaForum Macaya

APPLICATION OF FEDERATED LEARNING TO MEDICAL IMAGING SCENARIOS

Judith Sáinz-Pardo Díaz and Álvaro López García

Instituto de Física de Cantabria (IFCA), CSIC-UC

SUMMARY

The **privacy issues** arising from the application of machine/deep learning models in **medical environments** are clear, and in many cases, due to **legal, technical or security issues**, they prevent the sharing of data between different entities for training such models.

Federated learning is a **privacy-preserving data decentralization technique** used to perform secure machine/deep learning. In this poster a use case of medical image analysis of **chest X-ray images** obtained from an open data repository is presented. **Privacy-related advantages, improvements in predictions and reduction of execution times** are obtained compared to the centralized approach. Two approaches to be applied in case of **intermittent clients** are exposed.

FEDERATED LEARNING

- **Collaborative** and **decentralized** approach to machine and deep learning
- Client data are never uploaded to the server, **ensuring privacy.**
- Client-server communication must be **encrypted**.
- Additional privacy techniques may include: **homomorphic encryption** or **differential privacy**.
- In some cases clients can be **intermittent**.

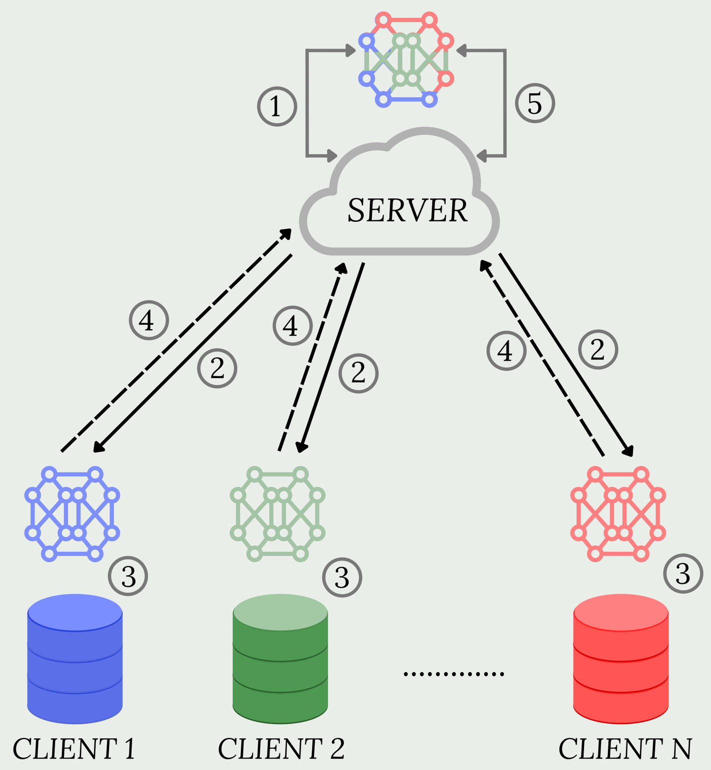

Figure 1. Federated Learning architecture.

Server-client architecture:

- **SERVER**: creates the model. (1)
- **SERVER**: transmits the model to the clients. (2)
- **CLIENT:** each client trains the model with its own data. (3)
- **CLIENT:** each of them sends the local parameters defining the model to the server. (4)
- **SERVER:** aggregates the weights of each client. (5)

Repet as many round as necessary.

USE CASE: CHEST X-RAY IMAGES

Objective: classify chest X-Ray images according to whether or not the patient has pneumonia.

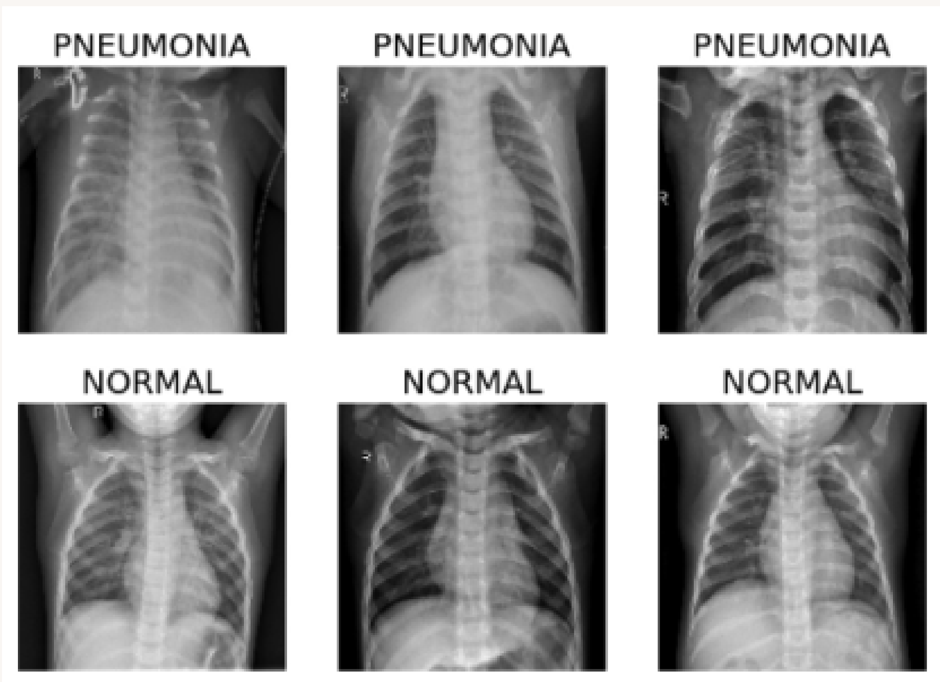

Figure 2. Example of the images used.

Simulating 3 clients (e.g. 3 hospitals).

Simulating 10 clients.

Model:

- **Conv2D layer**. Filters: 32. Kernel size: (3, 3). Activation: *ReLU*. Input shape: (150,150,1).
- **BatchNormalization layer.**
- **MaxPooling2D layer**. Pool size: (2,2). Strides: 2.
- **Conv2D layer**. Filters: 64. Kernel size: (3, 3). Activation: *ReLU*.
- **Dropout layer**. Rate: 0.1.
- **BatchNormalization layer.**
- **MaxPooling2D layer**. Pool size: (2,2). Strides: 2.
- **Conv2D layer**. Filters: 64. Kernel size: (3, 3). Activation: *ReLU*.
- **BatchNormalization layer.**
- **MaxPooling2D layer**. Pool size: (2,2). Strides: 2.
- **Conv2D layer**. Filters: 128. Kernel size: (3, 3). Activation: *ReLU*.
- **Dropout layer**. Rate: 0.2.
- **BatchNormalization layer.**
- **MaxPooling2D layer**. Pool size: (2,2). Strides: 2.
- **Conv2D layer**. Filters: 256. Kernel size: (3, 3). Activation: *ReLU*.
- **Dropout layer**. Rate: 0.2.
- **BatchNormalization layer.**
- **MaxPooling2D layer**. Pool size: (2,2).
- **Flatten layer**.
- **Dense layer**. Units: 128. Activation: *ReLU*.
- **Dropout layer**. Rate: 0.2.
- **Dense layer**. Units: 1. Activation: *sigmoid*.

	Average loss (client test set)	Average test accuracy (client test set)
3 clients	0.1246	0.9726
10 clients	0.1405	0.9786

Table 1. Summary of results for 3 and 10 clients, mean loss and accuracy for each test set.

Intermittent clients:

New clients can join the training process once started, while others may leave it

Approach 1: When a client leaves, the weights obtained for that client in previous repetitions **are not taken into account** for subsequent repetitions of the training.

Approach 2: When a client leaves, its last weights calculated **are kept** and are used in subsequent aggregations to update the model.

In both cases **the weights obtained for the new client are included in the aggregation.**

	Approach 1 (test)		Approach 2 (test)	
	Average loss	Average accuracy	Average loss	Average accuracy
3 clients	3.0453	0.7927	3.3200	0.7703
10 clients	3.6947	0.7552	4.7223	0.7093

Table 2. Summary of results in an scenario of intermittent clients (using approaches 1 and 2) for 3 and 10 clients, mean loss and accuracy for the same test set.

SUMMARY OF RESULTS

	Test Loss	Test Acc.	Test AUC	N_r	Exc. time (s)	Time reduction vs cent. apr. (%)
Centralized approach	3.0694	0.6619	0.9429	—	1386	—
Decentralized approach						
3 clients	**2.6034**	**0.8029**	0.9185	10	401	71.07
	4.3232	0.7308	**0.9313**	8	320.8	76.85
10 clients	4.7813	0.7212	0.9095	10	110	92.06
	3.8730	**0.7340**	**0.9130**	9	99	92.85

Table 3. Comparision of results for the same test set considering the centralized approach and the FL one with 3 and 10 clients.

Reference: Sáinz-Pardo Díaz, Judith, and Álvaro López García. "Study of the performance and scalability of federated learning for medical imaging with intermittent clients." Neurocomputing 518 (2023): 142-154.

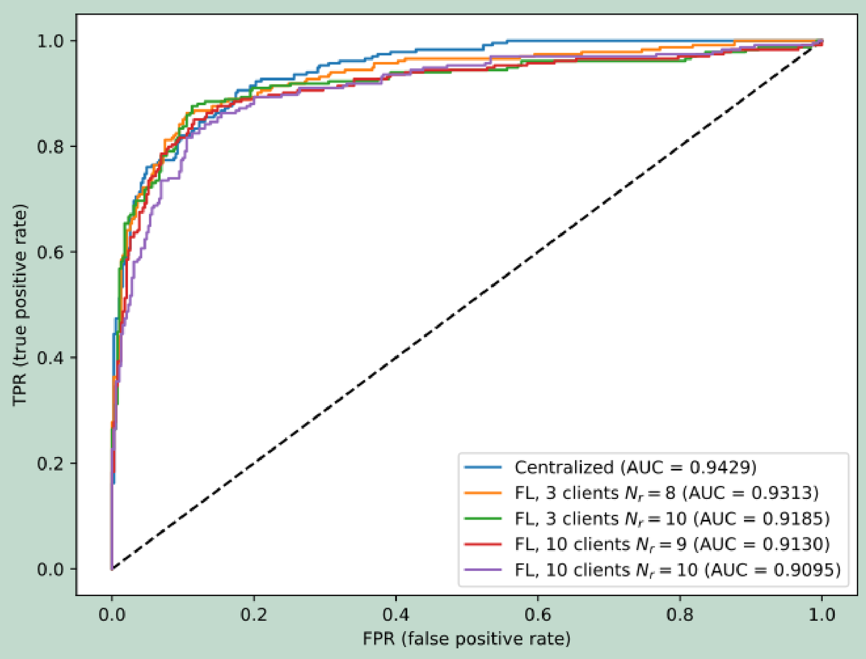

Figure 3. ROC curves and AUC for the centralized approach and the FL one with 3 and 10 clients and different number of rounds.

Acknowledgements: The authors thank the funding through the European Commission - NextGenerationEU (Regulation EU 2020/2094) through CSIC's Global Health Platform (PTI Salud Global) and the support from the project AI4EOSC "Artificial Intelligence for the European Open Science Cloud" that has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement number 101058593.

AI4 eosc

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA E INNOVACIÓN · PTI SALUD GLOBAL · CSIC

CSIC Consejo Superior de Investigaciones Científicas · CSIC HUB · AI HUB · Fundación "la Caixa"