AI Course Project Presentation: End-Sem

Demonstration and Implementation of Federated Learning

Group Members

Sr. No	Name	Roll No	PRN
1	Sarthak Pithe	9	12210166
2	Hrishikesh Potnis	10	12211239
3	Soham Nimale	53	12210227
4	Madhur Vaidya	70	12211223

Division: CS-TY-D

Batch: 3

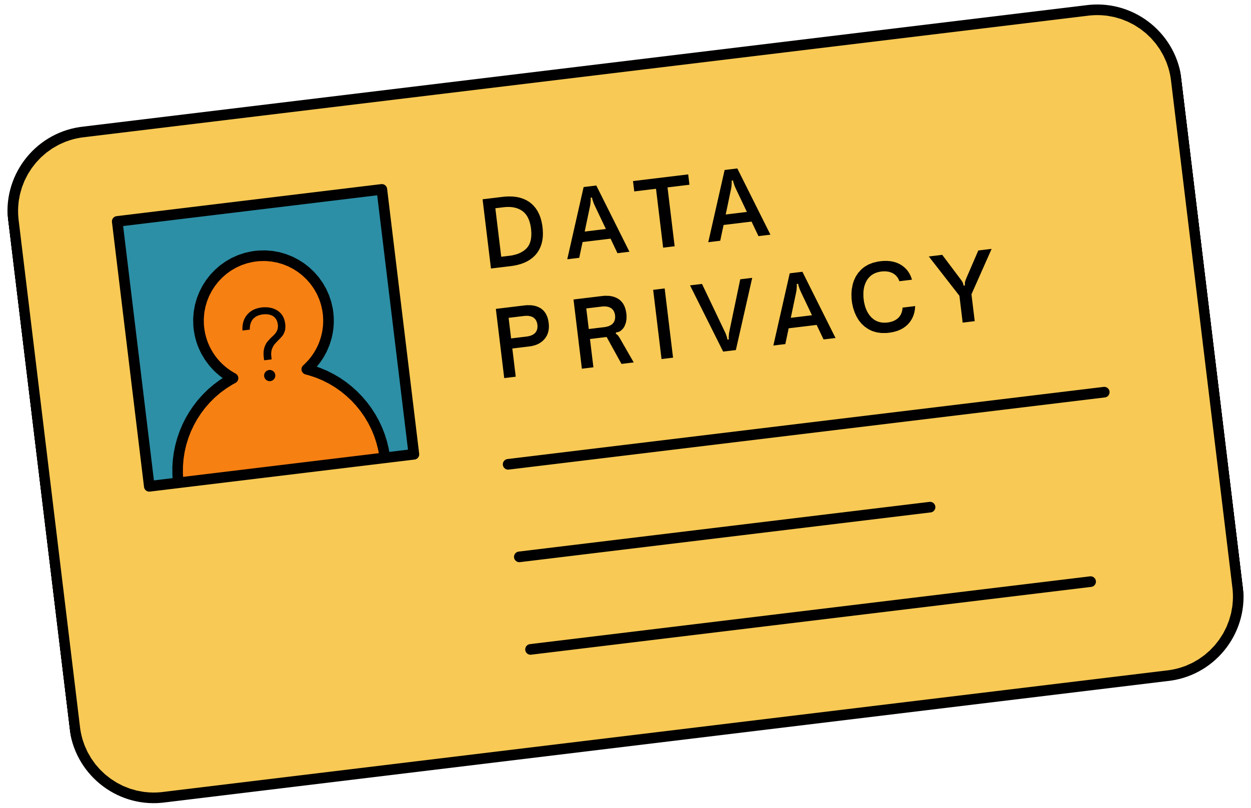
Group: TY-83

Project Guide:
Prof. Dr. Deepak Mane

Department of Computer Engineering
Vishwakarma Institute of Technology, Pune

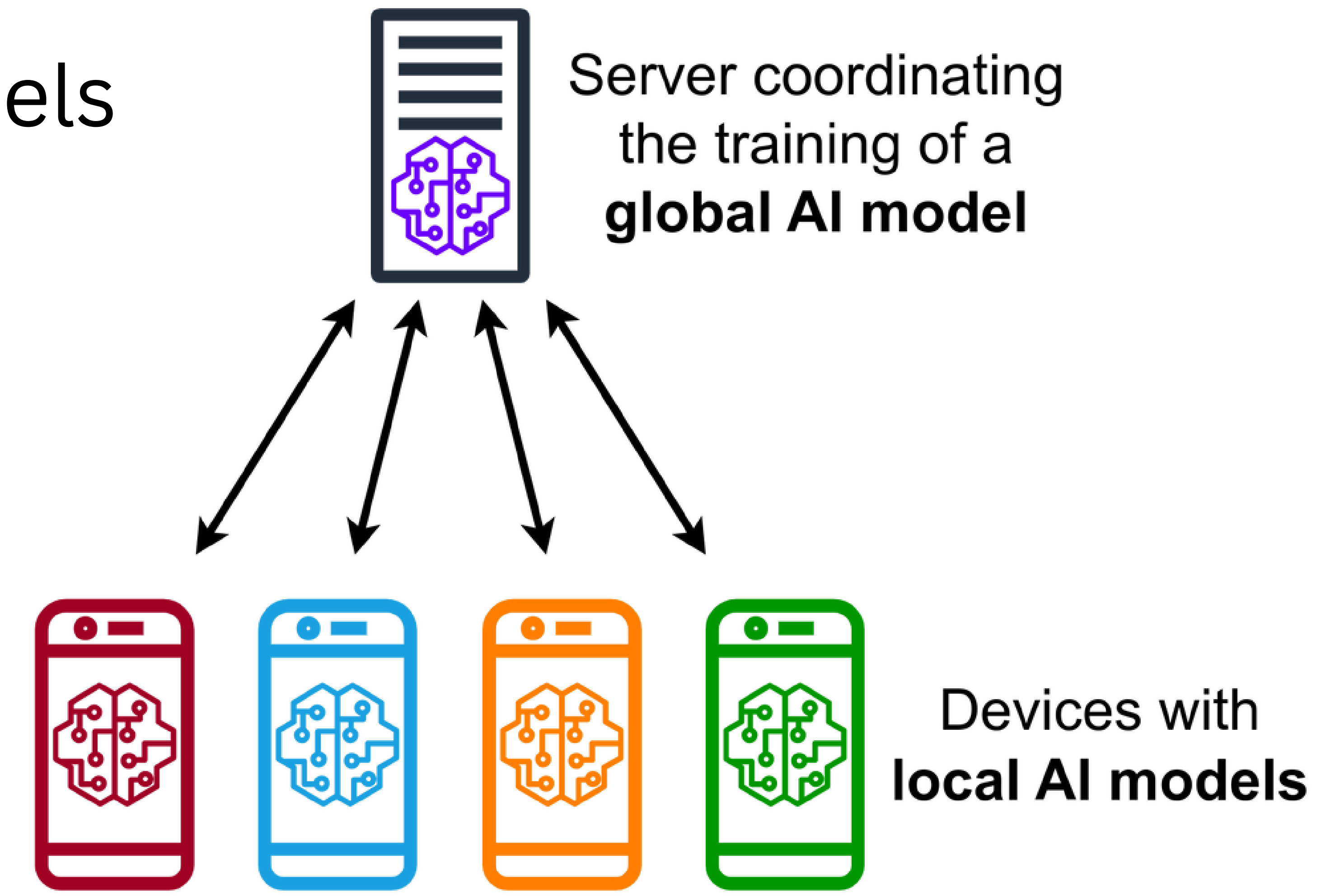
Introduction

- Importance of Data
- Some data needs privacy
- ML - All about data!
- Data Privacy using ML

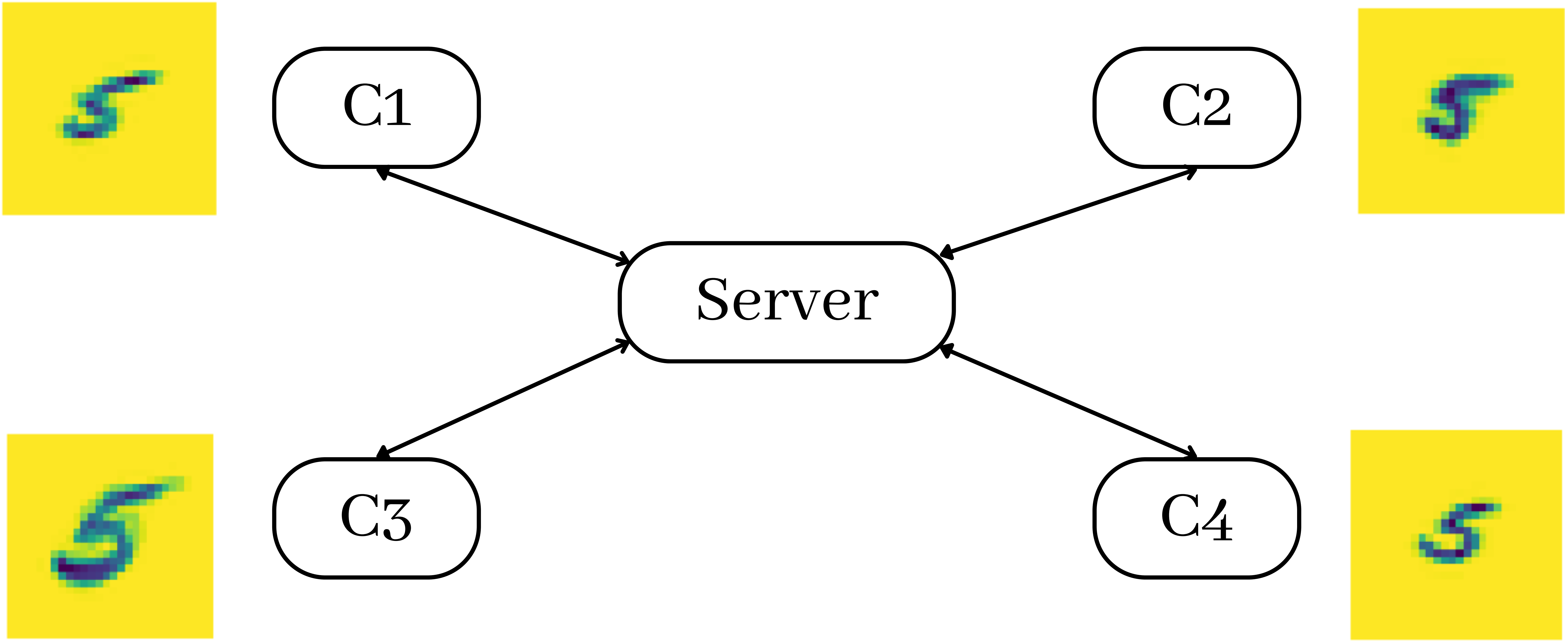


Federated Learning

- Decentralized approach to training ML Models
- Data does not leave client
- Data privacy is maintained
- Uses - Healthcare, Automotive, Security



Federated Learning

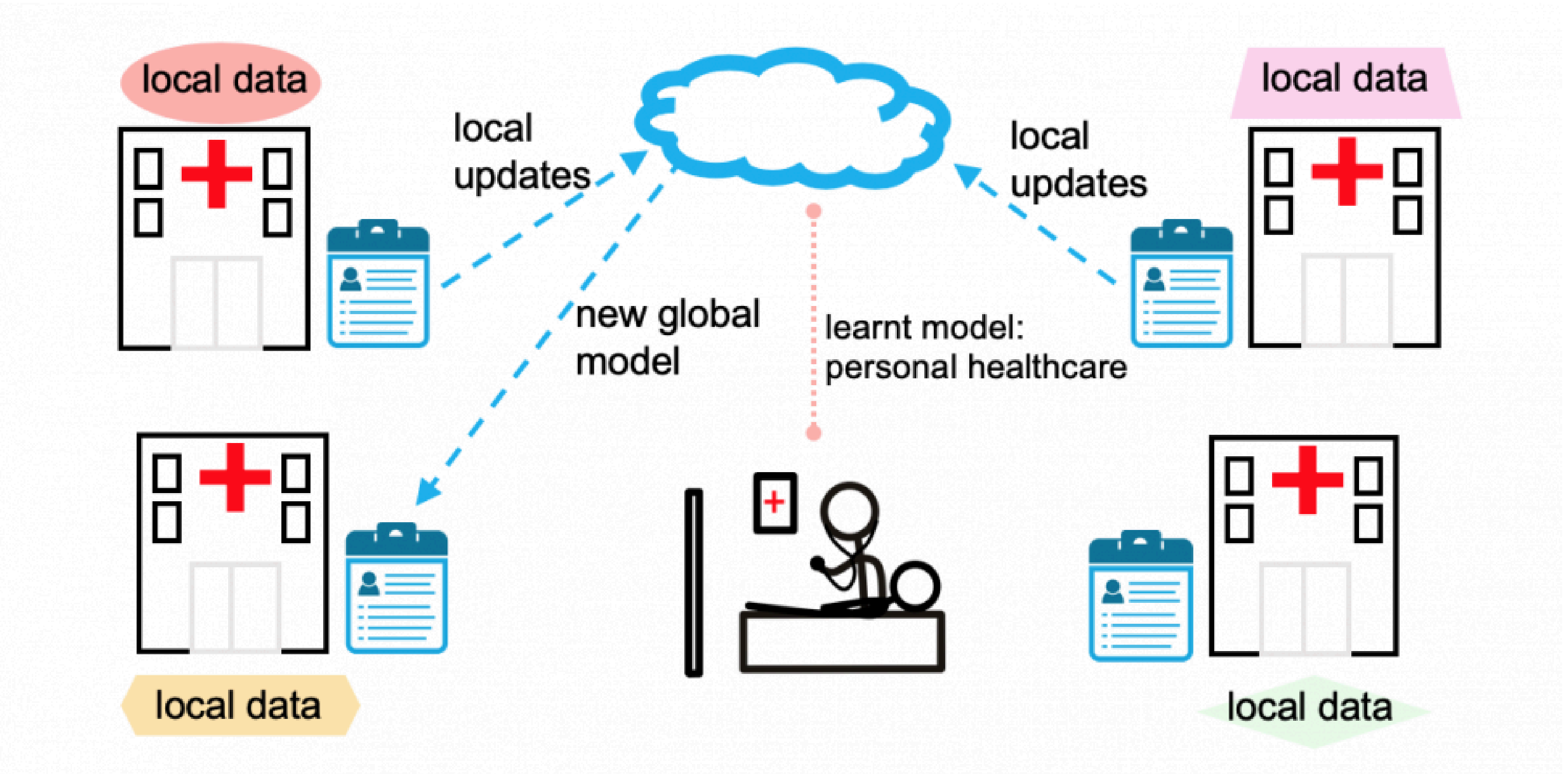


Challenges of Federated Learning

- High Communication requirement
- Impact on accuracy
- Homogenous data needed
- Aggregation challenges
- Slow model convergence

Applications

- Mobile Applications
- Health Care and Medical Research
- Personalized Recommendations



In general Federated Learning can be used in applications requiring data security and privacy

Problem Statement

To develop a federated learning based solution for Glaucoma detection using hospital networks without the need to share patient data.

Literature Review

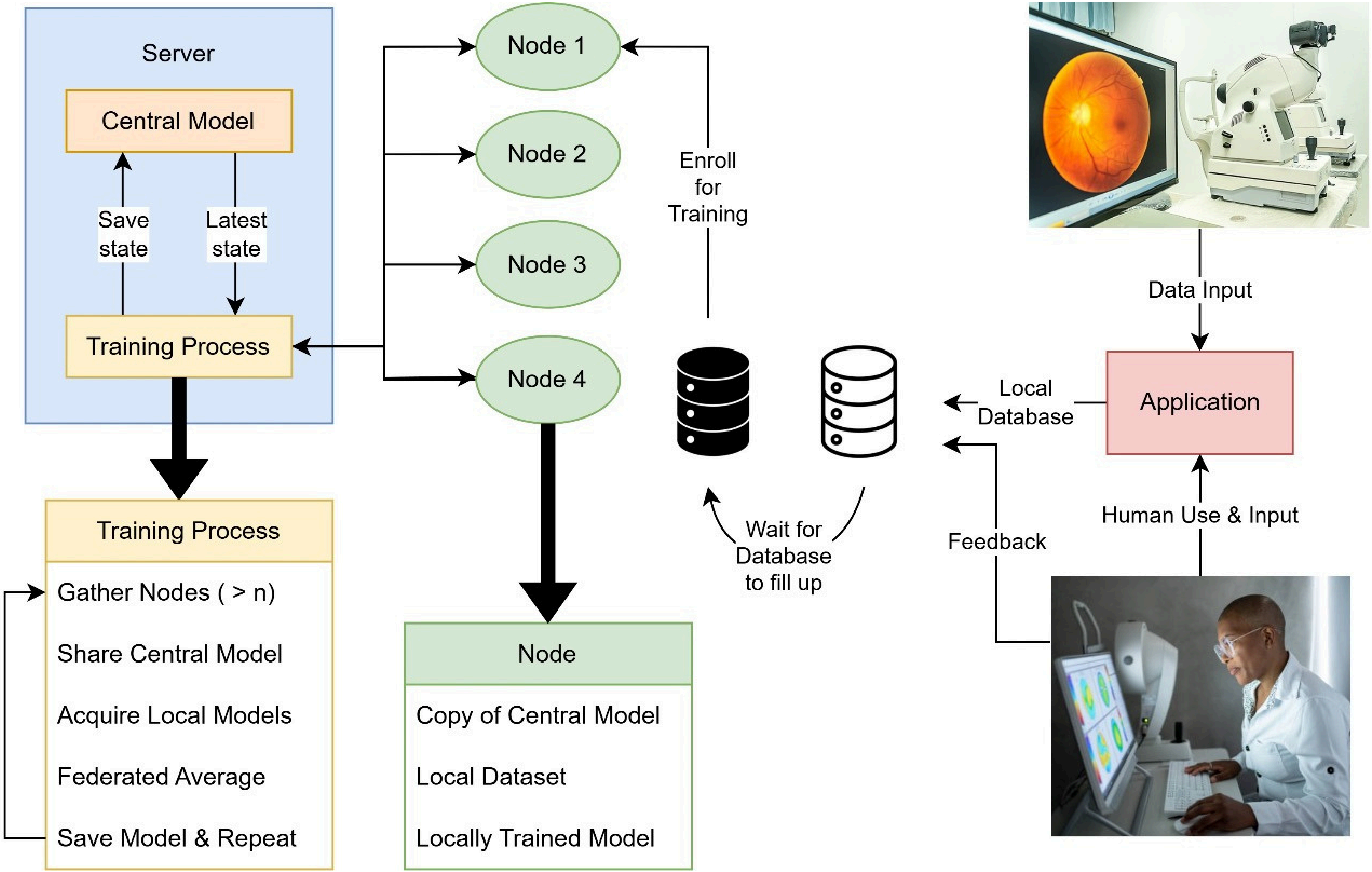
Name	Author	Summary
Collaborative Federated Learning for Healthcare: Multi-Modal COVID-19 Diagnosis at the Edge	Adnan Qayyum, Kashif Ahmad, Muhammad Ahtazaz Ahsan, Ala Al-Fuqaha, Junaid Qadir	Use of edge computing with clustered federated learning for privacy-focused, real-time COVID-19 diagnosis, achieving notable accuracy improvements over centralized models.
Federated Learning for Healthcare Informatics	Jie Xu, Benjamin S. Glicksberg, Chang Su, Peter Walker, Jiang Bian & Fei Wang	This survey reviews federated learning in healthcare, highlighting its potential to securely unify fragmented, private data from diverse sources for more robust, generalizable insights.

Name	Author	Summary
Federated Learning for Computer-Aided Diagnosis of Glaucoma Using Retinal Fundus Images	Telmo Baptista, Carlos Soares, Tiago Oliveira, Filipe Soares	Evaluates federated learning strategies for glaucoma diagnosis on diverse retinal fundus image datasets, finding that FedProx effectively handles data heterogeneity with 82% accuracy while preserving privacy.
Federated Transfer Learning For Diabetic Retinopathy Detection Using CNN Architectures	Mohammad Nasajpour; Mahmut Karakaya; Seyedamin Pouriyeh; Reza M. Parizi	This study uses Federated Learning to accurately detect Diabetic Retinopathy in fundus images while preserving patient data privacy.

Our Solution

- Glaucoma is a leading cause of irreversible blindness
- Early treatment helps fast recovery
- Eye data being sensitive must not leave hospitals
- What is the suitable machine learning approach in this scenario?

Federated Learning



Server
Central Model
Save state
Latest state
Training Process
Node 1
Node 2
Node 3
Node 4
Enroll for Training
Data Input
Application
Local Database
Feedback
Human Use & Input
Wait for Database to fill up
Training Process
Gather Nodes (> n)
Share Central Model
Acquire Local Models
Federated Average
Save Model & Repeat
Node
Copy of Central Model
Local Dataset
Locally Trained Model

Methodology

- Data Processing
- Model definition
- Federated Learning setup
- Training Loop
- Centralized Evaluation

Preprocessing

- Resized to (128, 128, 3)
- Normalized pixel value between [0,1]
- 80-20 split

Dataset

- 2081 samples
- Two labels

```
Dataset size: (2081, 128, 128, 3)
Training set size: (1664, 128, 128, 3)
Test set size: (417, 128, 128, 3)
```

Model Definition

- Convolutional layers
- Flatten Layers
- Dense Layers
- Output Layer with Softmax actv.

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 128, 128, 32)	896
max_pooling2d (MaxPooling2D)	(None, 64, 64, 32)	0
conv2d_1 (Conv2D)	(None, 64, 64, 64)	18496
max_pooling2d_1 (MaxPooling2D)	(None, 32, 32, 64)	0
conv2d_2 (Conv2D)	(None, 32, 32, 128)	73856
max_pooling2d_2 (MaxPooling2D)	(None, 16, 16, 128)	0
flatten (Flatten)	(None, 32768)	0
dense (Dense)	(None, 128)	4194432
dense_1 (Dense)	(None, 2)	258

Total params: 4287938 (16.36 MB)
Trainable params: 4287938 (16.36 MB)
Non-trainable params: 0 (0.00 Byte)

Federated Learning Setup

- TensorFlow Federated (TFF)
- Federated model wrapper
- 4 clients

```
Adding data from 0 to 416 for client : client_1
Adding data from 416 to 832 for client : client_2
Adding data from 832 to 1248 for client : client_3
Adding data from 1248 to 1664 for client : client_4
```

```
global_model_weights=<
  trainable=<
    float32[3,3,3,32],
    float32[32],
    float32[3,3,32,64],
    float32[64],
    float32[3,3,64,128],
    float32[128],
    float32[32768,128],
    float32[128],
    float32[128,2],
    float32[2]
  >,
  non_trainable=<>
>,
distributor=<>,
client_work=<
  learning_rate=float32
>,
aggregator=<
  value_sum_process=<>,
  weight_sum_process=<>
>,
finalizer=<
  learning_rate=float32
>
```

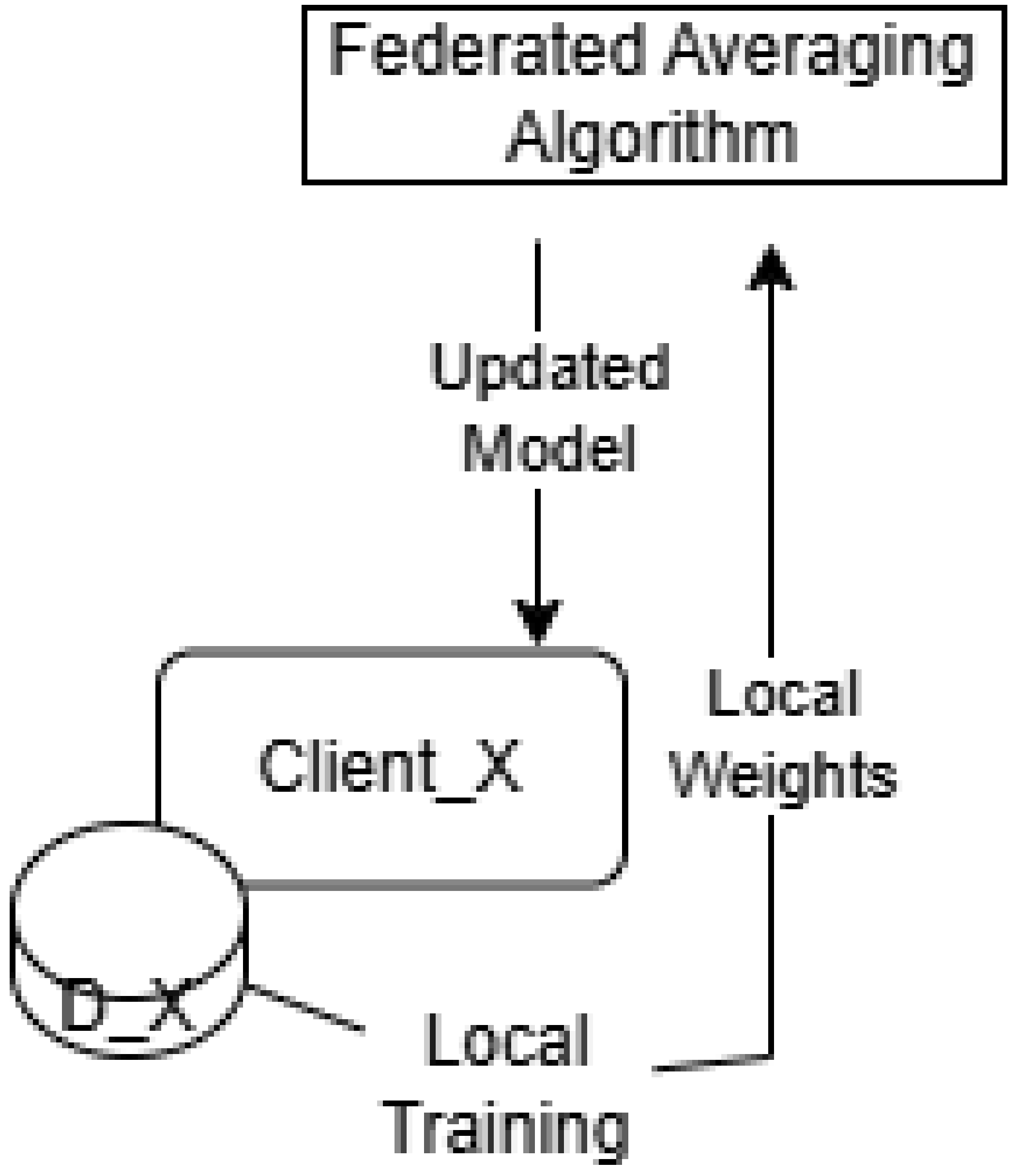
Type Signature

Training Loop

Each Client -

1. Trains model on local data
2. Sends model weights
3. Receives updated model

Server aggregates all the client model weights into an updated model



Centralized Evaluation

- Model evaluated after each round on
- Final tested model distributed to all clients

Optimization

- Local Optimization
    - log-loss
    - sgd and sgdm

$$F_k(w) = \frac{1}{n_k} \sum_{i \in \mathcal{P}_k} f_i(w)$$

- Global Optimization

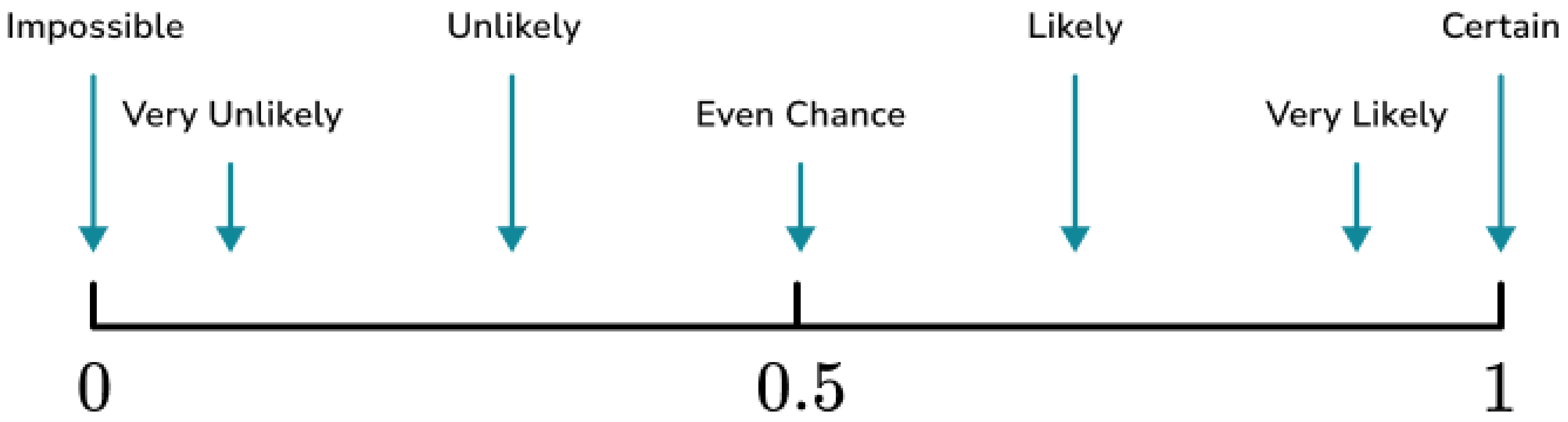
Aggregation

Simple Average
Weighted Average
Drift + Penalty Method

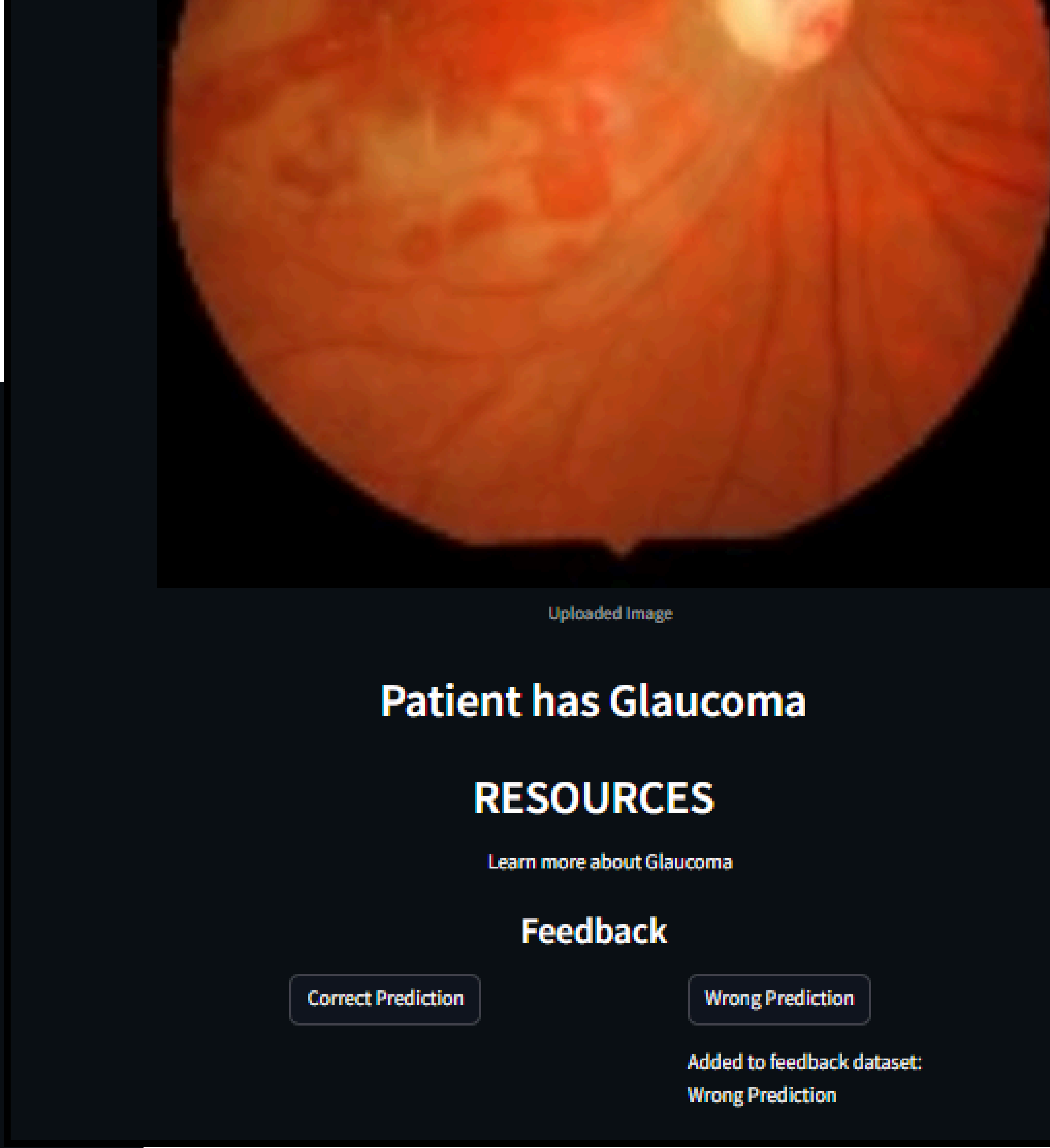
$$Weighted\ Average = \frac{\sum wx}{\sum w}$$

Participation

Bernoulli Constant (p)



Demonstration



Results

- Achieved global accuracy of **85.7%**
  - Clients - 4
  - Number rounds - 20

Conclusion

- Demonstrated effectivnes of Federated Learning for image classification
- Maintained data privacy

References

[1] https://en.wikipedia.org/wiki/Federated_learning

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

[3] https://federated.withgoogle.com/

[4] https://www.tensorflow.org/federated

[5] https://www.tensorflow.org/federated/federated_learning

[6]https://blog.ml.cmu.edu/2019/11/12/federated-learning-challenges-methods-and-future-directions/

Thank You!