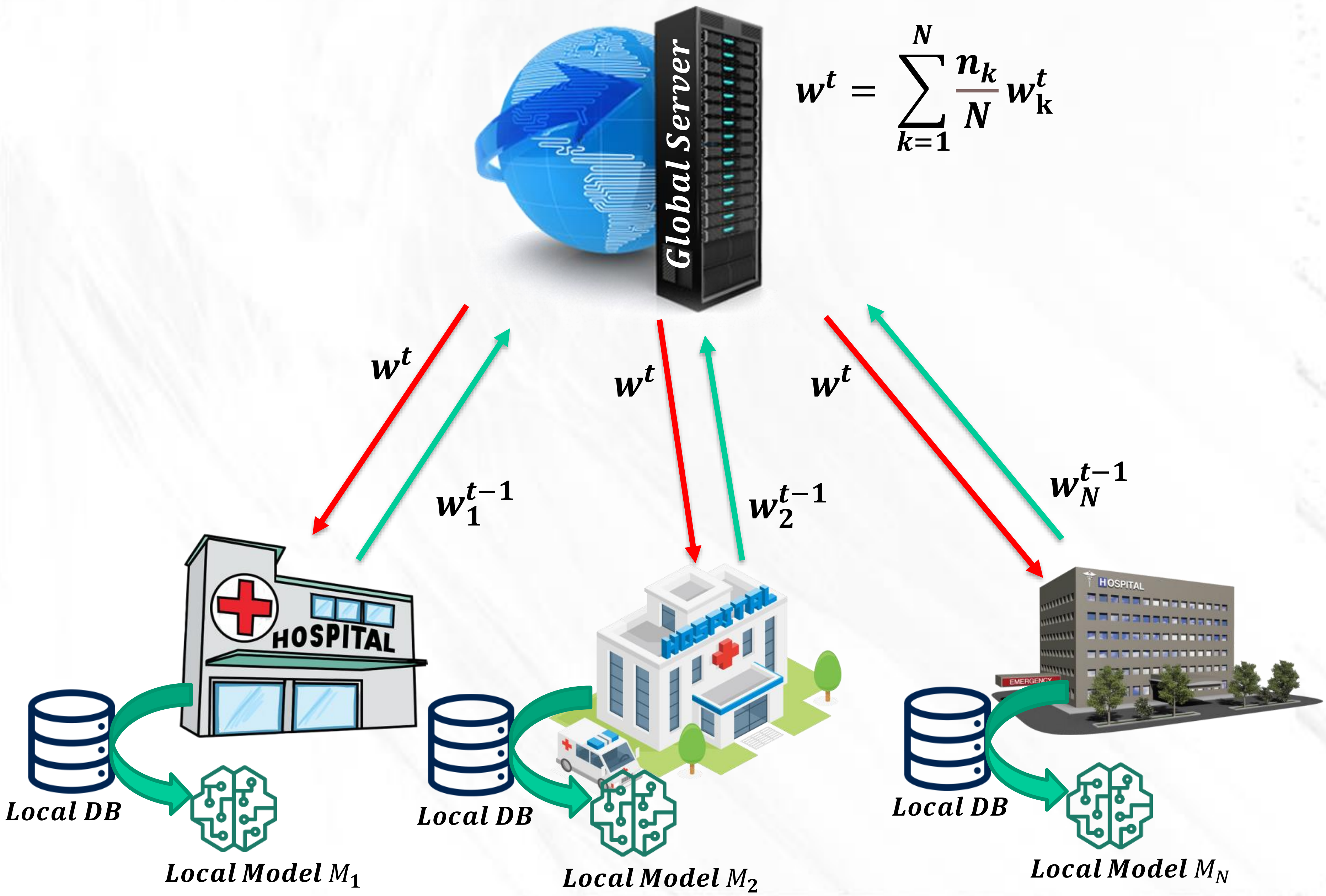
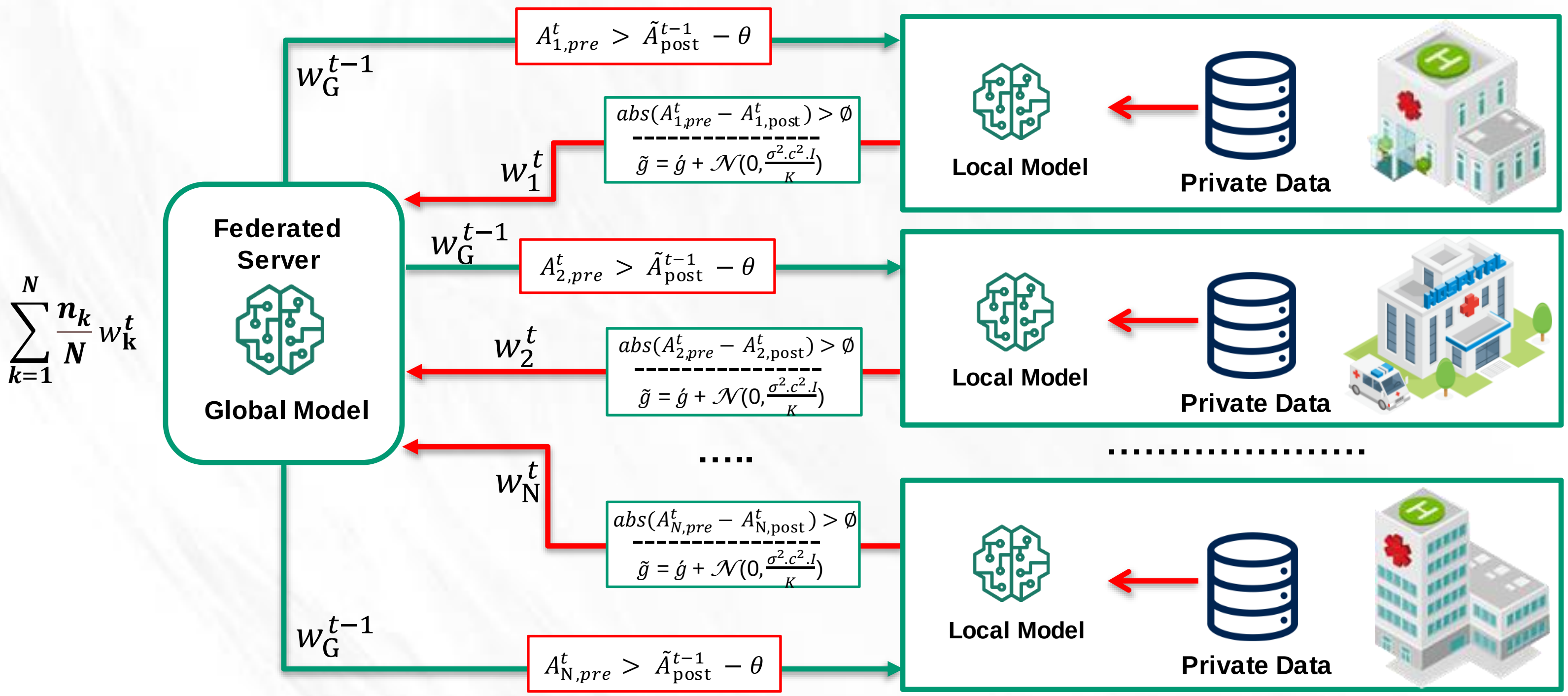
Differentially Private Federated Learning in Medical Context: Phenomenal Classification of Diabetic Retinopathy

Saiprasanna Cheedepudi
Ismail Hossain

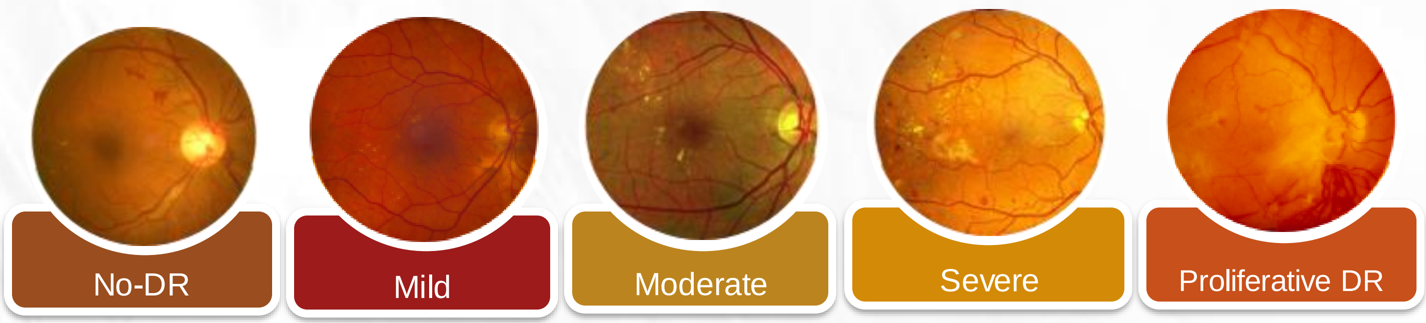
Introduction

- Diabetic retinopathy (DR) is a complication of diabetes mellitus, the most common cause of vision loss among people with diabetic
- Federated learning is a response to the question: *can a model be trained without the need to move and store the training data to a central location*?
- Differential privacy (DP) is a strong, mathematical definition of privacy in the context of statistical and machine learning analysis.
- The effective outcome is to predict the test image that can be classified into class of diabetic retinopathy problem.


Global Server
$w^t = \sum_{k=1}^{N} \frac{n_k}{N} w_k^t$
w^t
w^t
w^t
w_1^{t-1}
w_2^{t-1}
w_N^{t-1}
HOSPITAL
HOSPITAL
HOSPITAL
EMERGENCY
Local DB
Local DB
Local DB
Local Model M_1
Local Model M_2
Local Model M_N



Federated Server
Global Model
Local Model
Private Data
Local Model
Private Data
Local Model
Private Data
$\sum_{k=1}^{N} \frac{n_k}{N} w_k^t$
w_G^{t-1}
$A_{1,pre}^t > \tilde{A}_{post}^{t-1} - \theta$
$abs(A_{1,pre}^t - A_{1,post}^t) > \emptyset$
$\tilde{g} = \acute{g} + \mathcal{N}(0, \frac{\sigma^2.c^2.I}{K})$
w_1^t
w_G^{t-1}
$A_{2,pre}^t > \tilde{A}_{post}^{t-1} - \theta$
$abs(A_{2,pre}^t - A_{2,post}^t) > \emptyset$
$\tilde{g} = \acute{g} + \mathcal{N}(0, \frac{\sigma^2.c^2.I}{K})$
w_2^t
w_N^t
$abs(A_{N,pre}^t - A_{N,post}^t) > \emptyset$
$\tilde{g} = \acute{g} + \mathcal{N}(0, \frac{\sigma^2.c^2.I}{K})$
w_G^{t-1}
$A_{N,pre}^t > \tilde{A}_{post}^{t-1} - \theta$


No-DR
Mild
Moderate
Severe
Proliferative DR

Data set

- It is image dataset and is classified into 5 classes as No Diabetic Retinopathy, Mild, Moderate, Severe, and Proliferative Diabetic Retinopathy (PDR).
- The data set consists of 35120 and 5590 retina images collected from the two different datasets respectively, links of Kaggle repository are given below:

Dataset-1: https://www.kaggle.com/datasets/tanlikesmath/diabetic-retinopathy-resized

Dataset-2: https://www.kaggle.com/competitions/aptos2019-blindness-detection/data

Data preparation

Dataset-2 (5590 images)

Homogeneous: K = 5

Client	Number of Images	Category
1	1805	No DR
2	370	Mild
3	999	Moderate
4	193	Severe
5	295	Proliferative DR

Heterogeneous: K = 5

Client	Number of Images
1	1118
2	1118
3	1118
4	1118
5	1118

Dataset-1 (35120 images of 17560 persons)

Homogeneous: K = 5

Client	Number of Images	Category
1	25810	No DR
2	2440	Mild
3	5292	Moderate
4	870	Severe
5	708	Proliferative DR

Heterogeneous: K = 5

Client	Number of Images
1	3512
2	3512
3	3512
4	3512
5	3512

Process

- **Solution for how Heterogeneous and Malicious Data can be handled:**

  Federated Learning with Self-Regulating Clients (FedSRC) [1]

  Checkpoint-1: the client determines whether to proceed with local training or remove itself from the model update of the current round.

  Checkpoint-2: the client determines if the model update should be sent to the central server or not

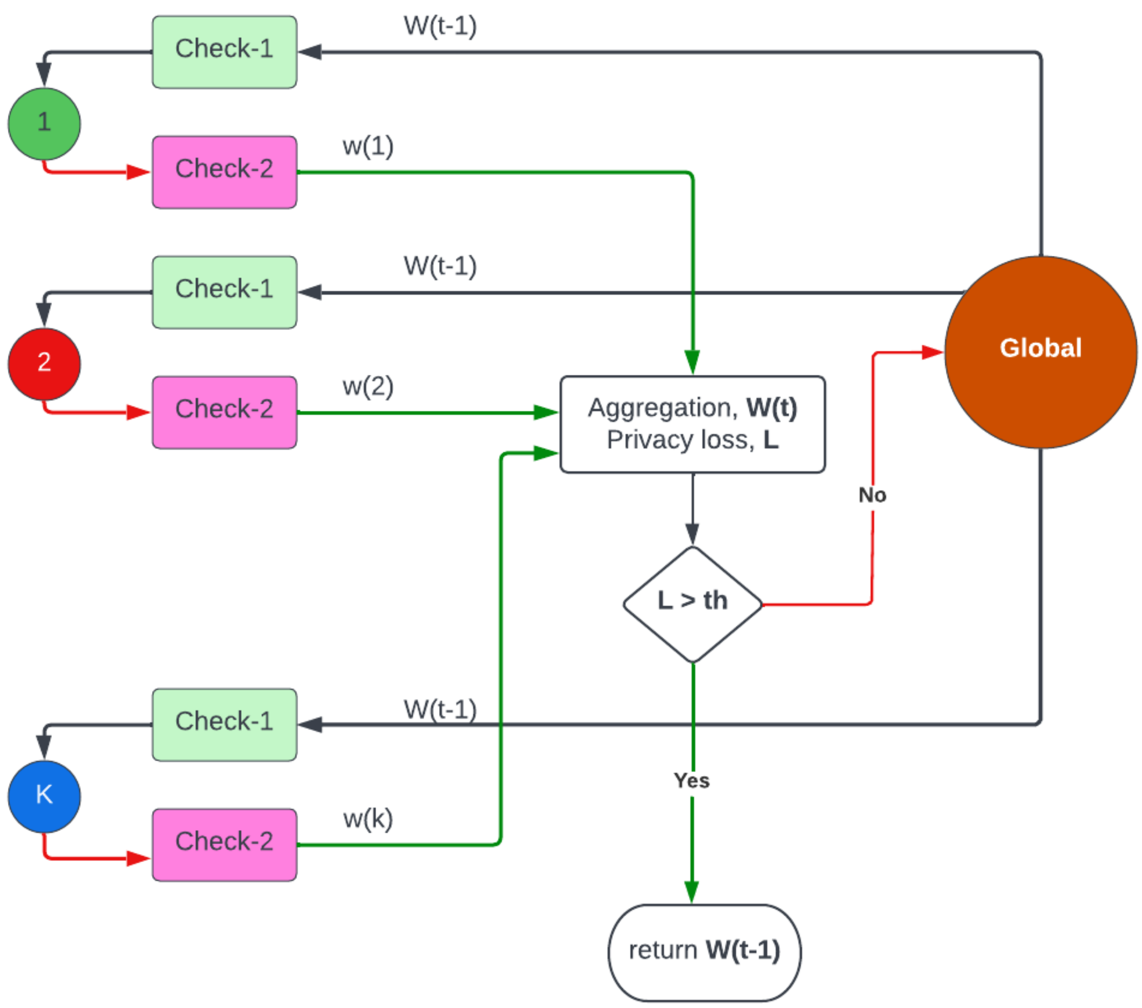
- **Solution how Data Privacy can be Preserved:**

  DPSDG – Differentially Private Stochastic gradient decent [2]

  Added Gaussian Noise with aggregated gradient [2]

  Laplace Noise can be added as it’s better for getting good accuracy than Gaussian Noise

Process


Check-1
W(t-1)
1
Check-2
w(1)
Check-1
W(t-1)
2
Check-2
w(2)
Global
Aggregation, **W(t)**
Privacy loss, **L**
No
L > th
Check-1
W(t-1)
K
Yes
Check-2
w(k)
return **W(t-1)**

Progress

1. **Models selection**
   - SqueezeNet1.1, VGG-16, & ResNet50
2. **Dataset**
   - Two labeled datasets collected from Kaggle
3. **Architecture**
   - Initial architecture is drawn might be modified later.
4. **Implementation**
   - SqueezeNet1.1 are experimented at google colab
   - Will try to train other two models
5. **Paper writing**
   - Created project at overleaf
   - Following IEEE paper format
   - Abstract part is added

Required Tools and Timeline

Software & Libraries:
Jupyter notebook, pytorch, tensorflow
Hardware:
GPU

Implementation and paper writing completion tentative time:
20-Nov-2022

Reference

[1] https://www.researchgate.net/publication/361939981
[2] https://arxiv.org/abs/2101.11693
[3] https://github.com/ipc-lab/private-ml-for-health