PRIVACY-PRESERVING FEDERATED LEARNING SYSTEM FOR HOSPITAL MANAGEMENT

DONE BY

K DHANUSH VARDDHAN
SAI KRISHNAN
NARAYAN KRISHNA R

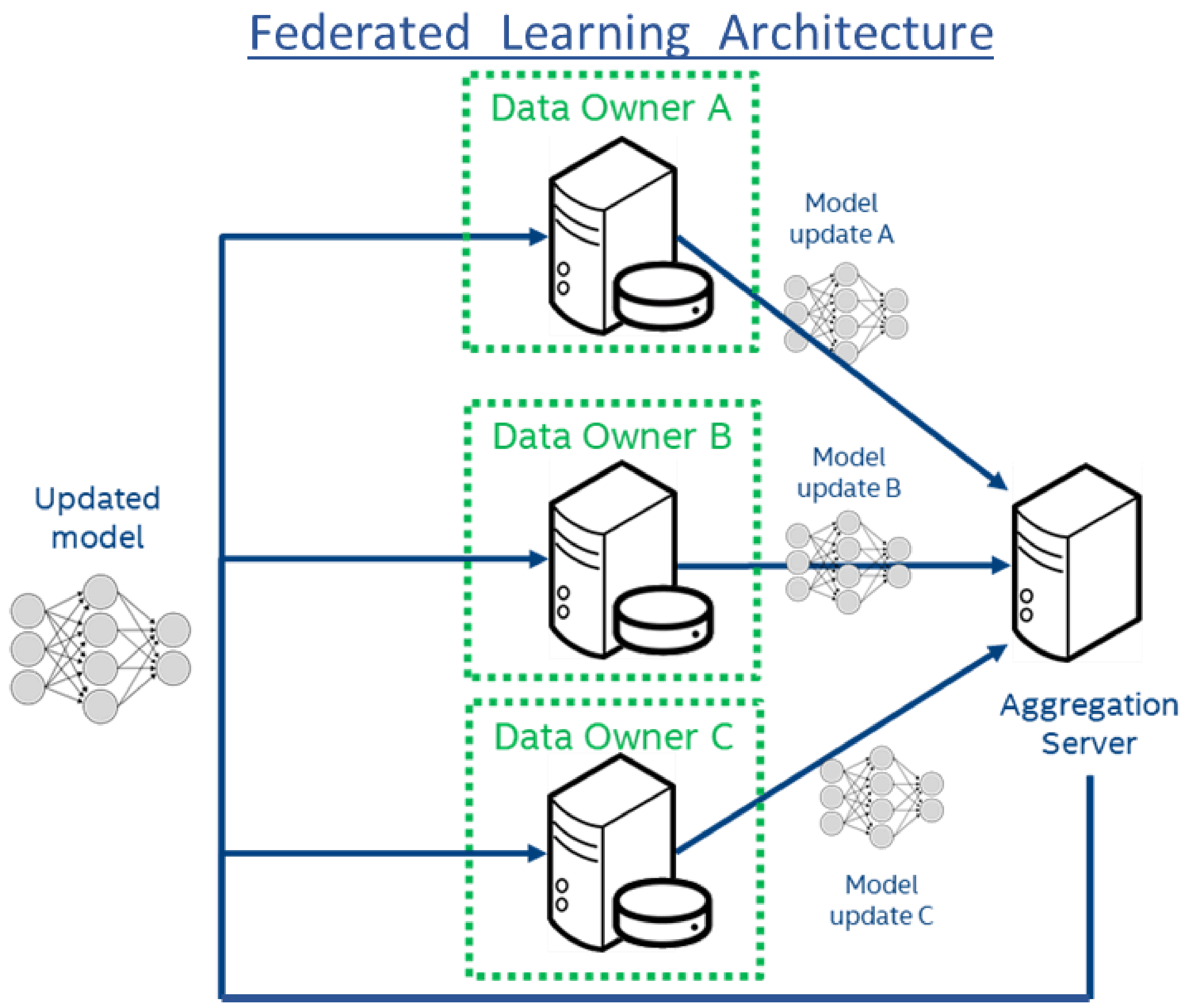
TABLE OF CONTENT

01.

INTRODUCTION

INTRODUCTION

- Federated learning is a machine learning approach that enables the training of models across decentralized devices or servers holding local data samples, without exchanging them.
- Instead of sending data to a central server for training, federated learning allows model training to be carried out locally on each device or server, with only model updates being shared.



02.

PROBLEM STATEMENT

PROBLEM

- Healthcare institutions face challenges in effectively leveraging patient data for improving medical research, diagnosis, and treatment recommendations while ensuring patient privacy and data security.

- Traditional centralized approaches to data analysis and model training pose risks to patient privacy and may not fully utilize the diverse and distributed nature of healthcare data across different hospital systems.

Algorithm 1 `FederatedAveraging`. The K clients are indexed by k; B is the local minibatch size, E is the number of local epochs, and η is the learning rate.

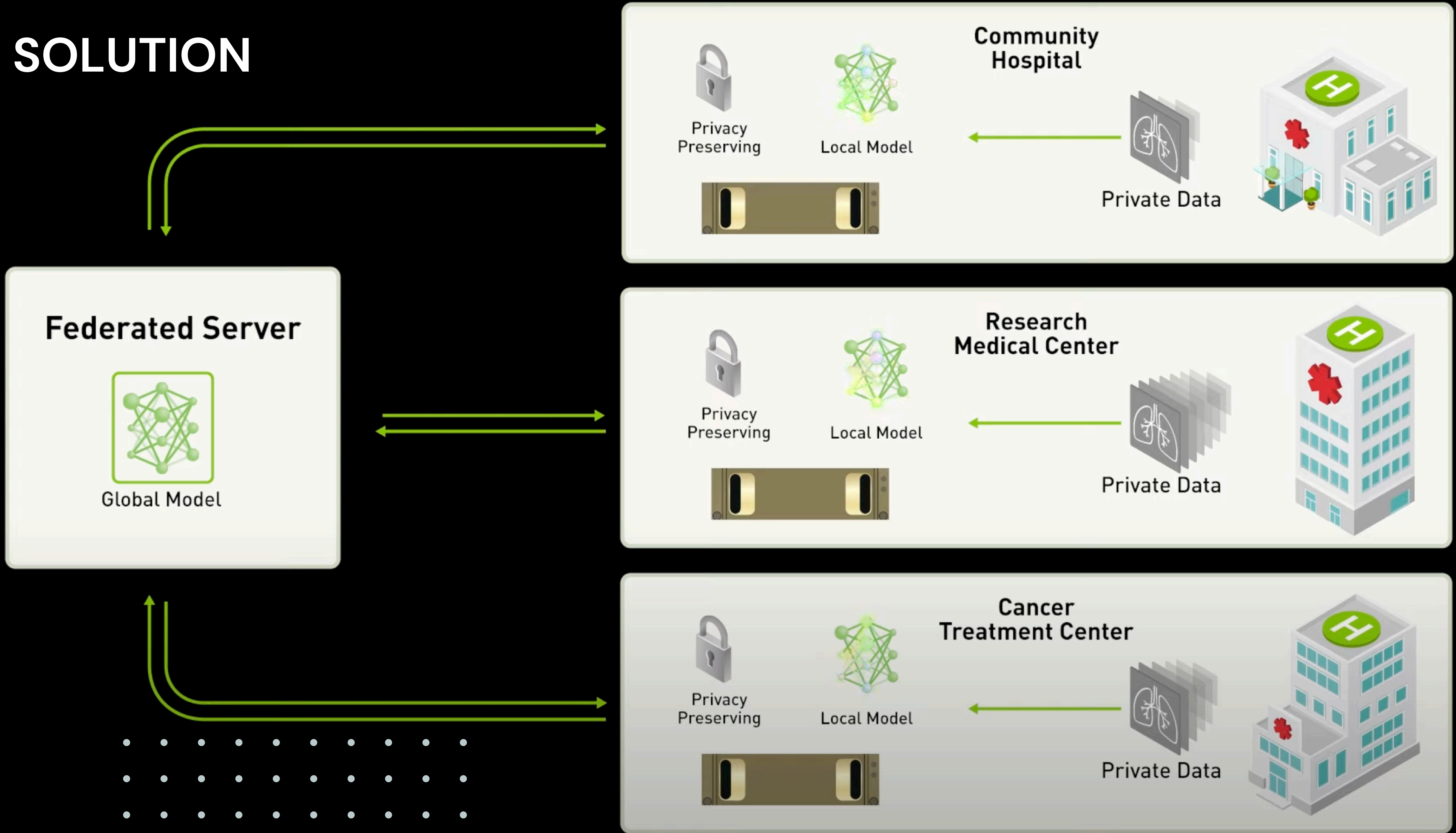
Server executes:
  initialize w_0
  for each round $t = 1, 2, \ldots$ **do**
    $m \leftarrow \max(C \cdot K, 1)$
    $S_t \leftarrow$ (random set of m clients)
    for each client $k \in S_t$ **in parallel do**
      $w_{t+1}^k \leftarrow \text{ClientUpdate}(k, w_t)$
    $m_t \leftarrow \sum_{k \in S_t} n_k$
    $w_{t+1} \leftarrow \sum_{k \in S_t} \frac{n_k}{m_t} w_{t+1}^k$ *// Erratum*[4]

ClientUpdate(k, w)**:** *// Run on client k*
  $\mathcal{B} \leftarrow$ (split $\mathcal{P}_k$ into batches of size B)
  for each local epoch i from 1 to E **do**
    for batch $b \in \mathcal{B}$ **do**
      $w \leftarrow w - \eta \nabla \ell(w; b)$
  return w to server

03.

SOLUTION

SOLUTION


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

SOLUTION

1. Federated learning ensures privacy by allowing hospitals to collaborate on training without sharing patient data.
2. The machine learning model accurately diagnoses bladder inflammations, improving human error rates.
3. Hospitals retain control over their data, preventing disclosure of sensitive patient information.
4. Improved patient care outcomes are expected with a more accurate diagnosis tool.
5. Resource usage is optimized as model training is distributed across hospitals' dataset

04.

OUR APPROACH

APPROACH PART 1

- Data Preprocessing:
- Load dataset from CSV file.
- Preprocess data: split into features and labels, replace 'no' with 0 and 'yes' with 1, convert temperature values to correct format.
- Split dataset into training and testing sets.
- Normalize features using StandardScaler.
- Defining the Model:
- Define a simple neural network model (SimpleNN) with four fully connected layers and ReLU activation functions, followed by a sigmoid activation for binary classification.
- Training the Model:
- Train the model using the training dataset.
- Iterate over epochs, calculate loss, and update model parameters using backpropagation.

APPROACH PART 1

- Evaluating the Model:
- Evaluate the model using the testing dataset.
- Calculate accuracy for each disease based on predicted and actual labels.
- Federated Learning Simulation:
- Simulate clients by splitting training data and labels.
- Train the model on each client's dataset for a specified number of epochs.
- Aggregate model updates by averaging the weights.
- Simulate federated learning rounds by iterating over clients, training on each client's dataset, and aggregating model updates to form a new global model.
- Model Evaluation (Federated Learning):
- Evaluate the final global model using the testing dataset to assess performance.