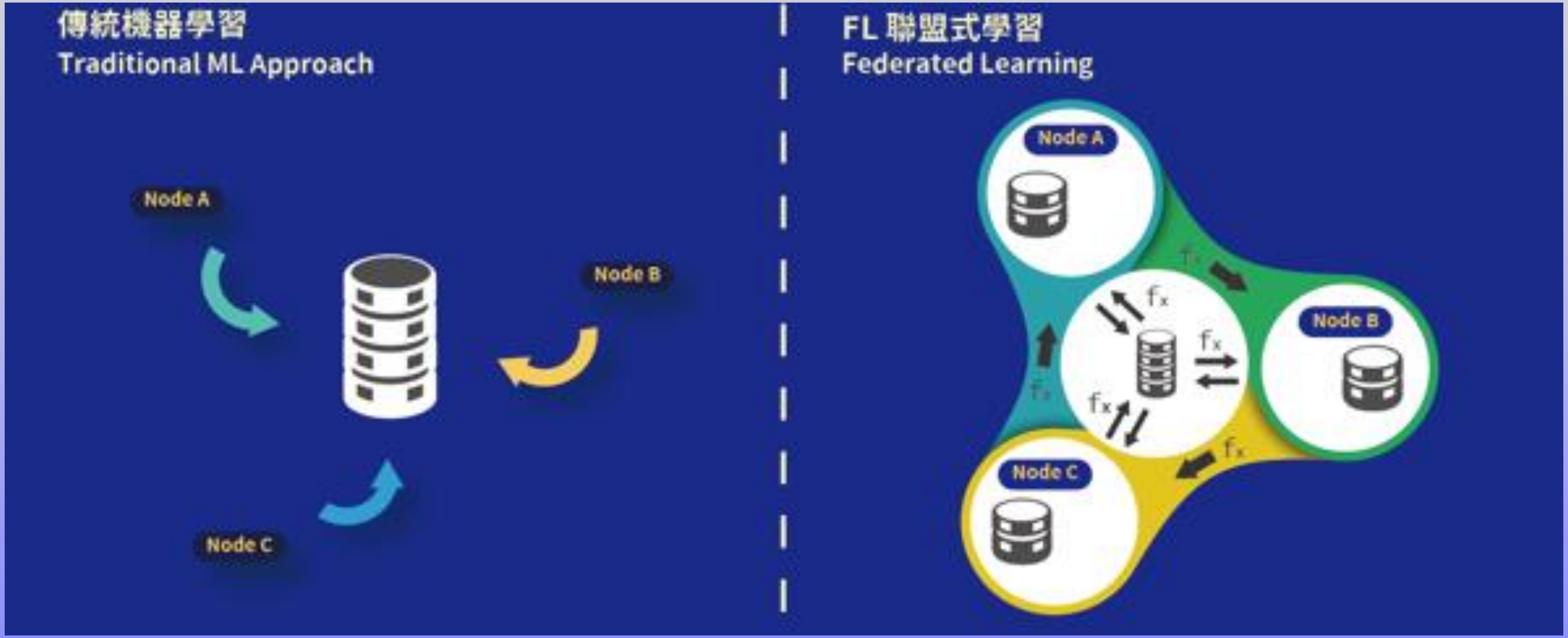
Federated Learning

https://medium.com/sherry-ai/聯盟式學習-federated-learning-b4cc5af7a9c0

https://www.tensorflow.org/federated/tutorials/federated_learning_for_image_classification?hl=zh-tw

What is Federated Learning?



Why Federated?

- Privacy Problem
- Large Datasets

PDJ #3, Spring 2012
cc by Personal Data Journal
http://pde.cc/journal

Privacy Problem

- Attackers might learn by inspecting the model parameters
  - Aggregate of updates from many individual users
  - Rather than adding noise to the final model, we noise the individual updates
  - Encryption

Large Datasets

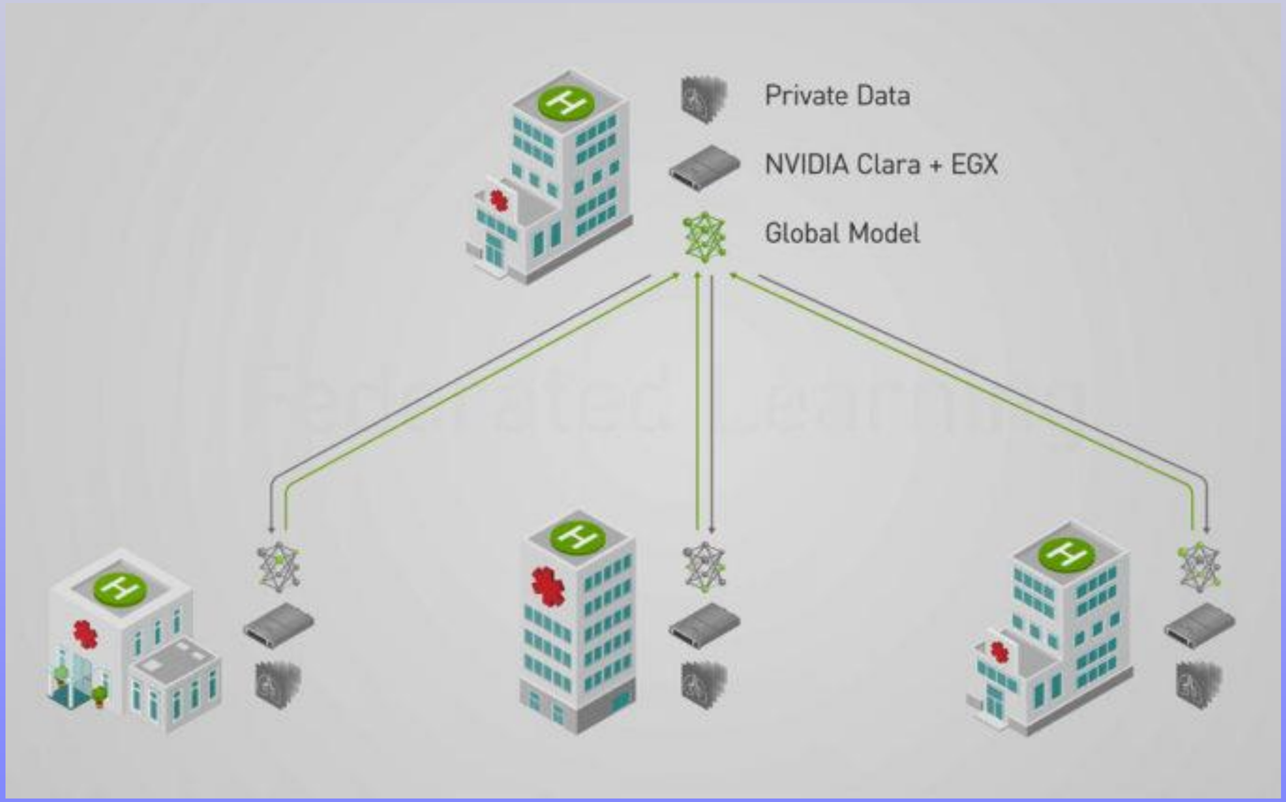
- (#-Communication rounds) x (update size)
- The update size is the O(#-model parameters)

Types of Federated

- According to data type, separated into three types:
  - Horizontal federated learning
  - Vertical federated learning
  - Federated transfer learning

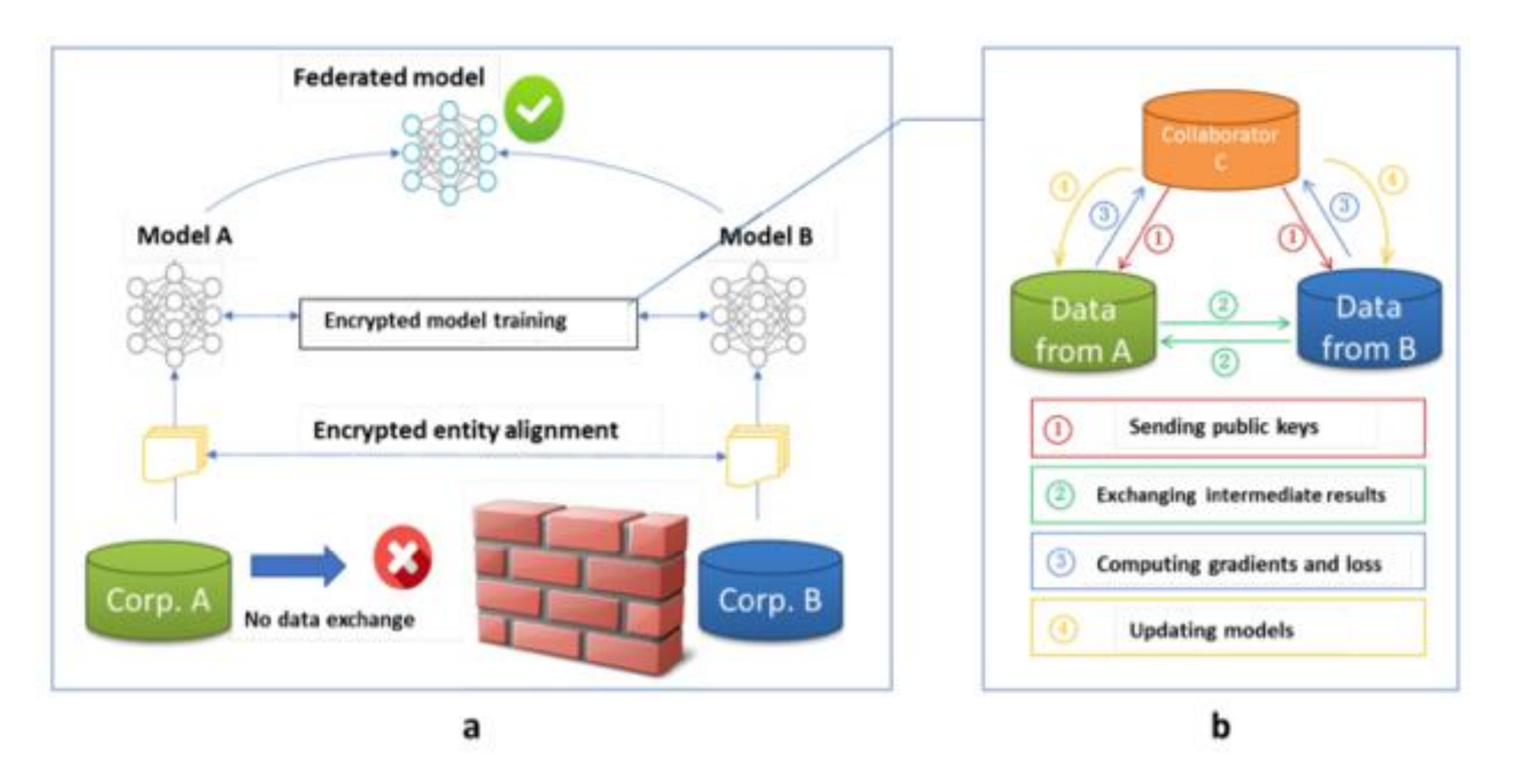
Horizontal Federated Learning

- Hight overlap feature
- Low overlap sample



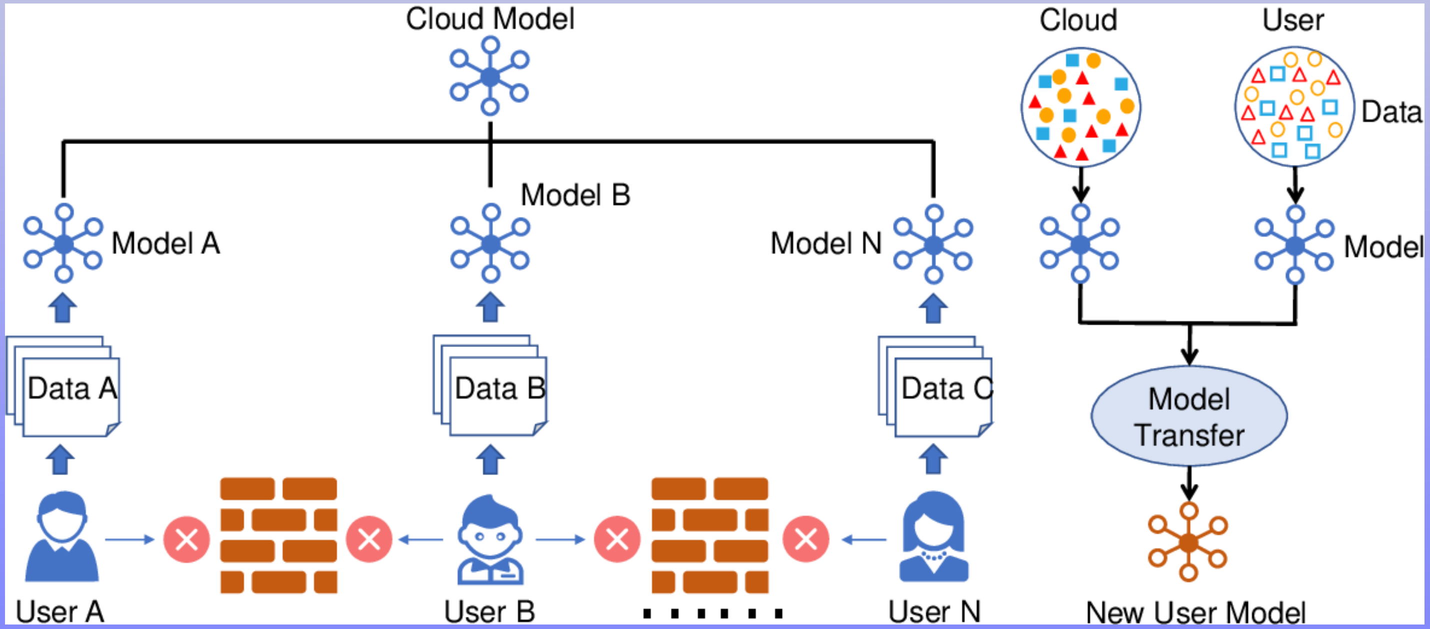
Vertical Federated Learning

- High overlap sample
- Low overlap feature



Federated Transfer Learning

- Low overlap in both sample and feature

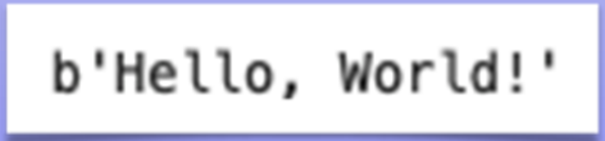


環境設置

```
!pip install --quiet --upgrade tensorflow-federated
%load_ext tensorboard


import collections
import numpy as np
import tensorflow as tf
import tensorflow_federated as tff
from matplotlib import pyplot as plt


np.random.seed(0)
tff.federated_computation(lambda: 'Hello, World!')()
```



```
b'Hello, World!'
```

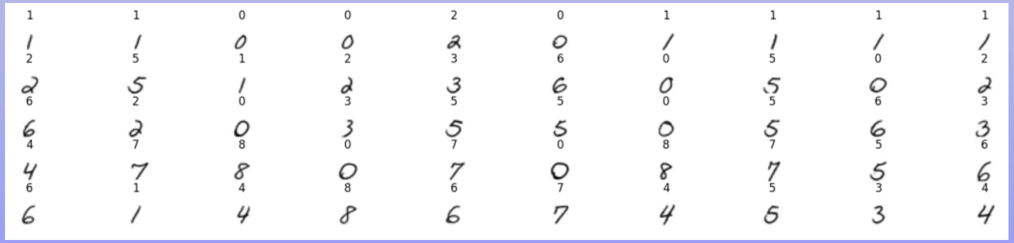
1. Prepare the input Data

a. 印出前50組第X位用戶的資料

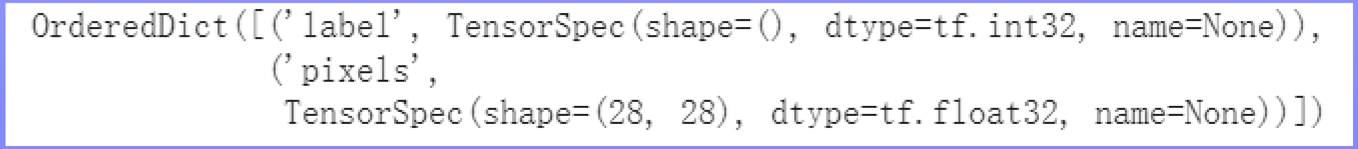
要求: X為學號後三碼

資料標籤用tittle顯示

範例:



b. 當執行emnist_train.element_type_structure指令時，會產生出下圖的輸出，請解釋這行輸出的意義



```
OrderedDict([('label', TensorSpec(shape=(), dtype=tf.int32, name=None)),
             ('pixels',
              TensorSpec(shape=(28, 28), dtype=tf.float32, name=None))])
```

2. Explore Heterogeneity in FL

a. 印出第X-1, X, X+1位用戶的資料分布

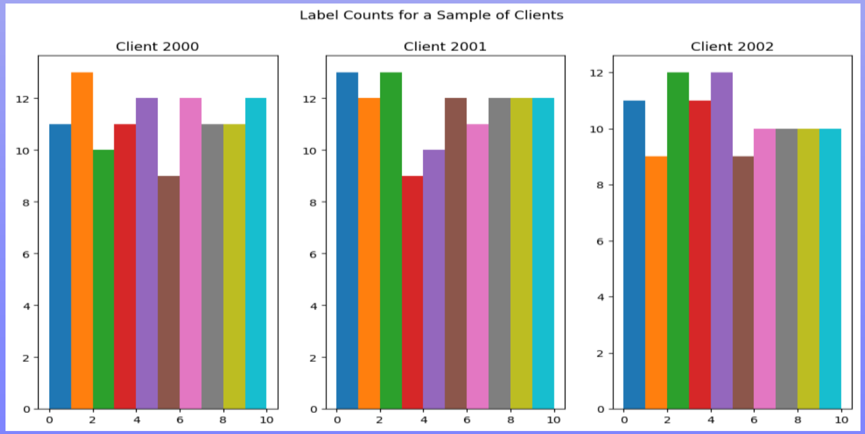
要求: X為學號後三碼

Ex: 001要印出第0,1,2位，999要印出第998,999,1000位

b. 印出第X-1,X,X+1位用戶的Mean Image

c. 根據結果推論本次實驗是執行何種類型的FL，並說明原因

範例:

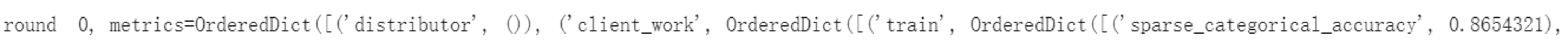


Client #2002's Mean Image Per Label

3. Train the Model on Federated Data

a. 印出訓練30輪的結果(至少顯示出accurency以及loss的數值)

範例:



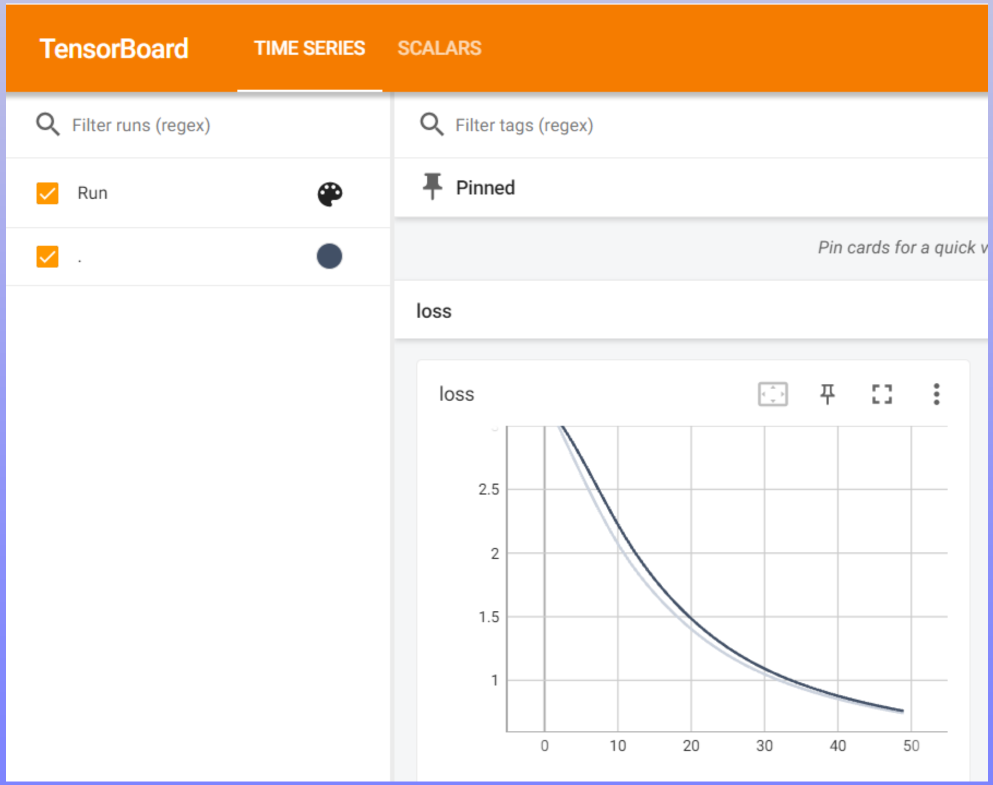
```
round  0, metrics=OrderedDict([('distributor', ()), ('client_work', OrderedDict([('train', OrderedDict([('sparse_categorical_accuracy', 0.8654321),
```

b. 解釋client_optimizer_fn以及server_optimizer_fn當中learning_rate各自所代表的意義

4. Display Model Metrics in TensorBoard

a. 將上個步驟所訓練30輪的結果顯示在TensorBoard上(請至少貼出accurency以及loss的結果)

範例:



作業繳交方式

1.程式碼(.ipynb , EX : 610430000_姓名.ipynb ）

2.報告書：

1) 封面（學號、姓名）
2) 程式題要將新增上去的程式碼以及執行結果貼上來，並且每題前面請標清楚題號
3) 檔案格式為.pdf(EX : 610430000_姓名_HW2.pdf)

3.將兩個檔案放進一個資料夾，壓縮後上傳(EX : 610430000_姓名_HW2.zip)

上述所有繳交格式若有錯誤一律0分!!!