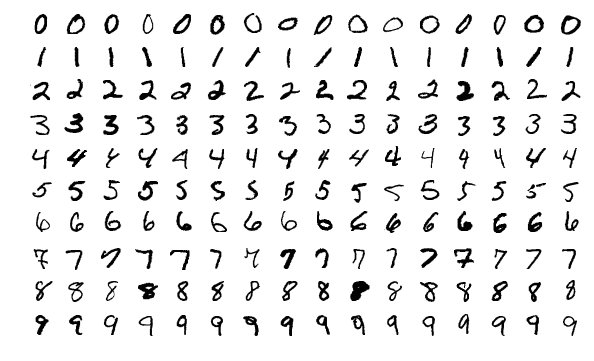
Distributed Differential Privacy

Applied in Federated Learning

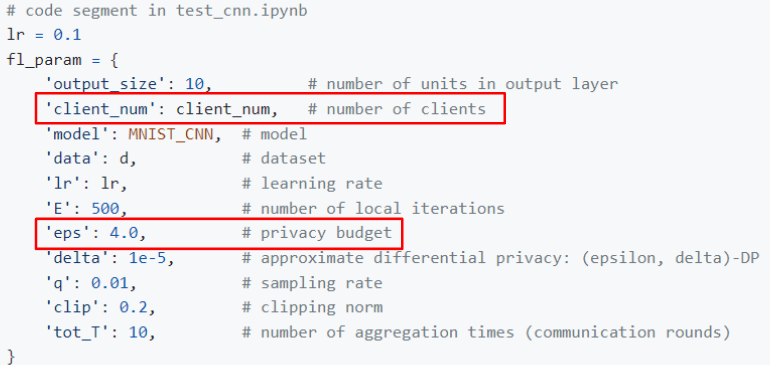
最後一組

M11215032 葉品和 M11215052 陳奕帆 M11215066 鄭宜珊

**Dataset : Mnist**

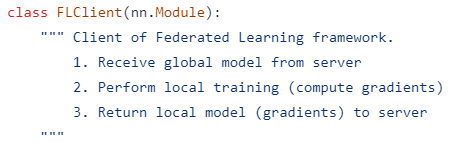


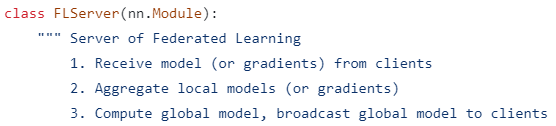
1**.How do you perturb the data?**

****

1. ‘client\_num’ sets the number of clients: n.
2. ‘eps’ sets the privacy level ε.

Divided into FLClient and FLServer, each client will get the same model from the Server and unify the initialization parameters of the model. Repeat the following steps to train the model：

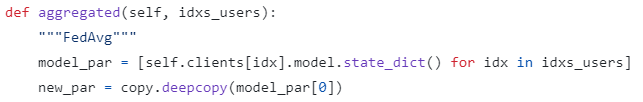




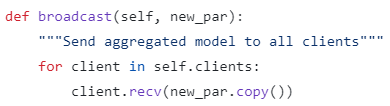
a. Each Client uses its own data to train the model, calculates its own gradient, and then uploads it to the Server.



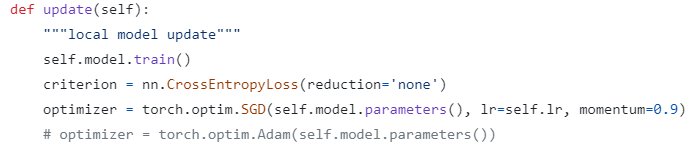
b. The Server integrates the gradients of each Client and updates the model.



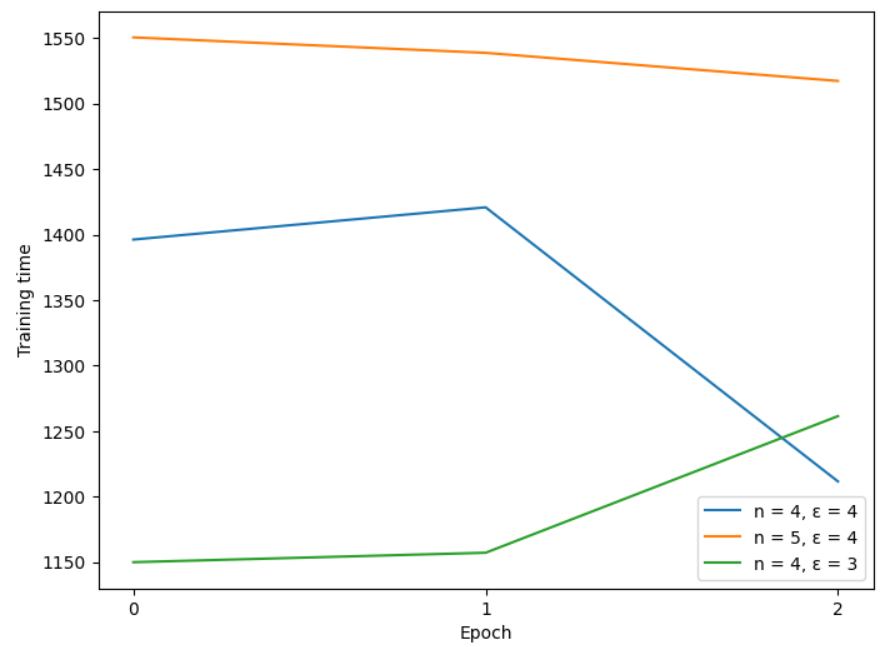
c. Server returns the updated gradient of the model to each Client.



d. Clients update their respective models.

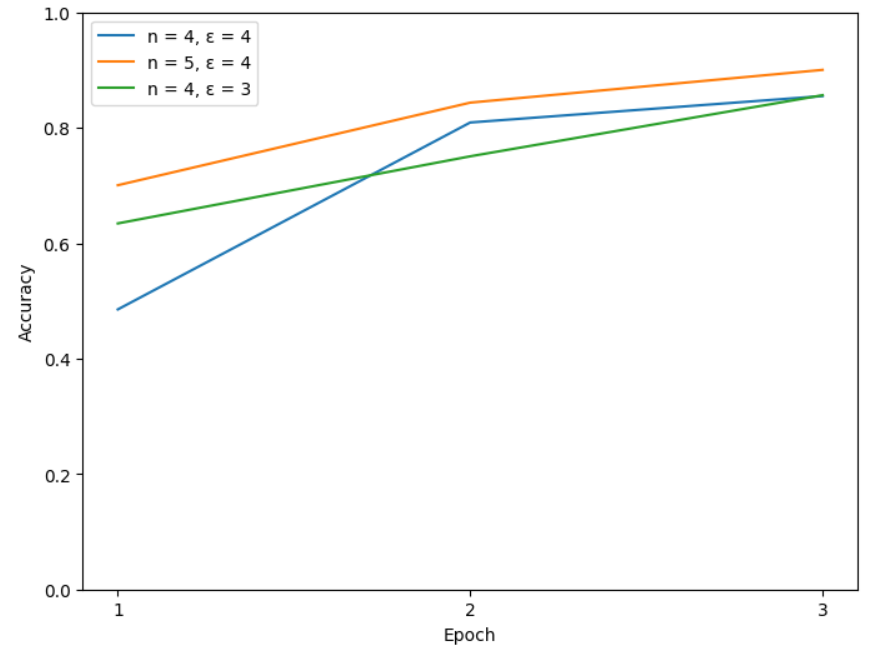


Since the training time of each epoch is very long, we do not train too many epochs. The following figure shows the training time of each epoch.



**2.Effectiveness measure: Accuracy**

* learning rate = 0.15
* epoch = 3
* delta = 1e-5
* sampling rate = 0.01



**3.Privacy level: the value of ε & Number of clients: n**

* learning rate = 0.15
* epoch = 3
* delta = 1e-5
* sampling rate = 0.01

| ε = 4 | n = 4 |
| --- | --- |