FEDERATED LEARNING

Tensorflow

Sommaire

C’EST QUOI LE FEDERATED LEARNING

Le **"federated learning"** est une technique d'apprentissage automatique qui permet à plusieurs appareils ou clients de former collaborativement un modèle sans partager leurs données avec un serveur centra**l.**

Le flux de travail de l'apprentissage collaboratif

Les avantages du Federated Learning

confidentialité | Une meilleure protection de la vie privée en conservant les données sur les appareils

01

02

Réduction des communications réseau et des charges computationnelles | **Latences minimales**

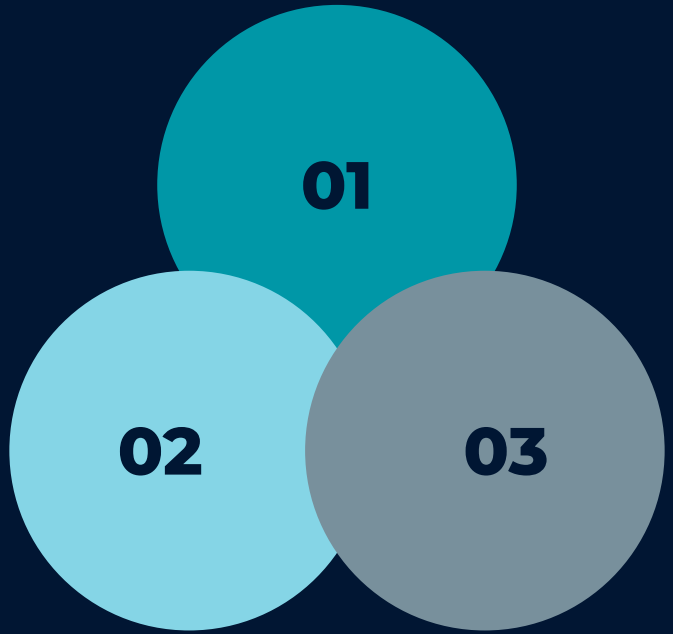
Diversité | Amélioration de la généralisation du modèle due à la diversité des sources de données locales

03

Défis et orientations futures

Assurer la confidentialité et la sécurité des données

Gestion des données non-indépendantes et non-identiquement distribuées

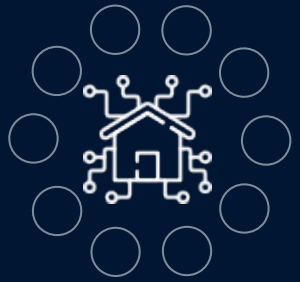


Développement de meilleurs algorithmes et techniques d'optimisation

Applications du Federated Learning

Healthcare

Entraînement d'un modèle de diagnostic médical sur les données de patients provenant de différents hôpitaux



Smart Homes

Entraînement d'un modèle de reconnaissance vocale sur des données audio collectées à partir de différents appareils

Automotive

Entraînement d'un modèle de conduite autonome sur des données collectées à partir de différents véhicules

Libraries et Frameworks du FL

Il existe plusieurs bibliothèques et frameworks disponibles pour implémenter l'apprentissage collaboratif, certains d'entre eux sont:

- **TensorFlow Federated (TFF):** C'est un framework open-source développé par Google pour implémenter des algorithmes d'apprentissage collaboratif en utilisant la bibliothèque **TensorFlow**
- **PySyft:** C'est une bibliothèque Python qui fournit des outils pour l'apprentissage collaboratif et l'apprentissage automatique préservant la confidentialité en utilisant le framework **PyTorch**
- **Flower:** C'est un framework Python open-source pour construire des systèmes d'apprentissage collaboratif

Étapes pour fédérer avec TensorFlow

01 Définir votre modèle : Définissez votre modèle d'apprentissage automatique en utilisant **TensorFlow**. Il peut s'agir de n'importe quel modèle que **TensorFlow** prend en charge

02 Définir vos données : Définissez vos données d'entraînement comme une collection d'ensembles de données. Chaque ensemble de données représente les données d'un client différent

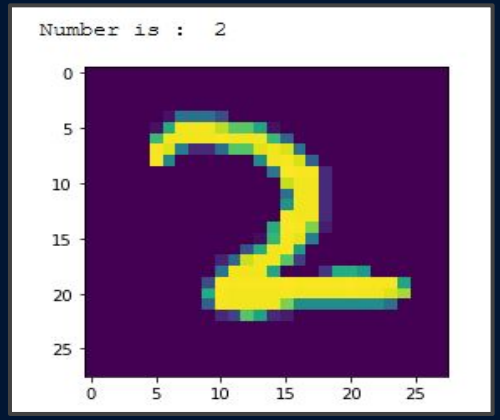
03 Définir votre calcul fédéré : Définissez votre calcul fédéré en utilisant **TFF**

04 Compiler votre calcul fédéré : Utilisez **TFF** pour compiler votre calcul fédéré en un graphe **TensorFlow** qui peut être exécuté sur des périphériques ou des clients distants

05 Entraîner votre modèle : Exécutez votre calcul fédéré sur les périphériques ou les clients distants pour entraîner votre modèle

Exemple d’usage: The MNIST Dataset

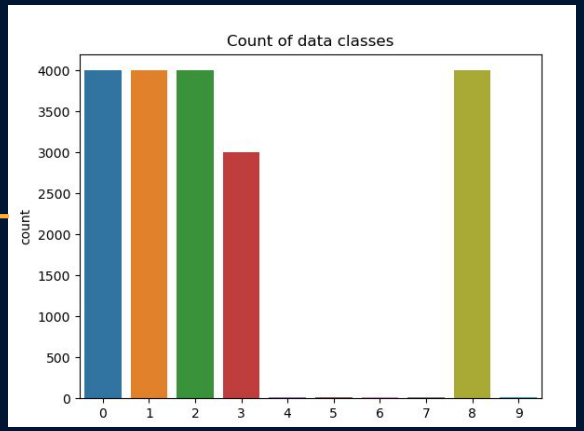
Le jeu de données **MNIST** est un jeu de données largement utilisé en apprentissage automatique et en vision par ordinateur. Il se compose d'un ensemble de 70 000 images en niveaux de gris de chiffres écrits à la main, chacune étant de taille 28 pixels par 28 pixels.

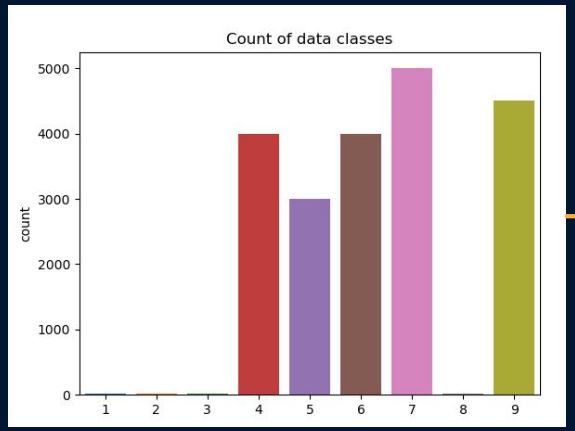


Exemple d’usage: The MNIST Dataset

Dans notre projet, les données seraient réparties sur plusieurs appareils, tels que des smartphones que nous appelons "**clients**", et chaque appareil entraînerait un modèle local sur son propre sous-ensemble de données. Ces modèles locaux seraient ensuite agrégés par un serveur central pour créer un modèle global qui a appris à partir des données de tous les appareils.

Client 1





Client 2