# Federated Machine Learning

## L'idée principale

- prévenir les fuites de données
- créer des modèles d'apprentissage
  - basés sur des données réparties sur plusieurs appareils
- la résolution des défis statistiques
- l'amélioration de la sécurité dans l'apprentissage fédéré
- rendre l'apprentissage fédéré plus personnalisable
- Les améliorations concentrées

## APERÇU DE L'APPRENTISSAGE FÉDÉRÉ

### la méthode conventionnelle

- rassembler toutes les données
- utiliser $D = D_1 \cup ... \cup D_N$ pour former un modèle $M_{SUM}$

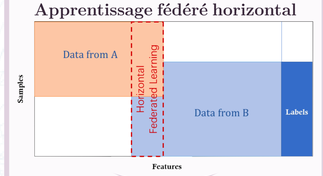
### Définition de l'apprentissage fédéré

- les propriétaires de données forment en collaboration un modèle $M_{FED}$
- aucun propriétaire de données $F_i$ n'expose ses données $D_i$ à d'autres
- un processus d'apprentissage

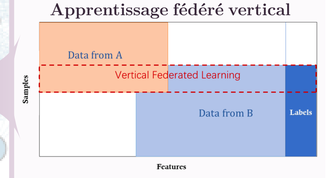
### Catégorisation de l'apprentissage fédéré

- matrice $D_i$ dénote les données de propriétaire i
  - chaque ligne représente un échantillon
  - chaque colonne représente une caractéristique

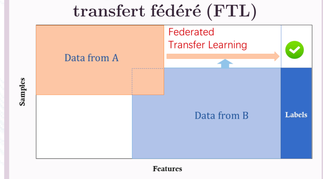
Apprentissage fédéré horizontal




Apprentissage fédéré vertical




Apprentissage par transfert fédéré (FTL)




### Confidentialité de l'apprentissage fédéré

- une des propriétés essentielles de l'apprentissage fédéré
- 1. calcul multiparties sécurisées (SMC)
- 2. confi-dentialité différentielle
- 3. cryptage homomorphe

### $|V_{FED} - V_{SUM}| < \delta$

- $V_{FED}$, la précision de $M_{FED}$
- $V_{SUM}$, la performances de $M_{SUM}$
- $\delta$, un nombre réel non négatif, perte de précision d'apprentissage fédéré