Confidentialité et Sécurité dans le FL en Santé

Objectif : Comprendre les mécanismes clés de protection des données dans l'apprentissage fédéré.

🎯 Objectif

- Se familiariser avec les concepts de confidentialité différentielle et d'agrégation sécurisée dans un contexte de federated learning (FL) appliqué à la santé.

🔐 Confidentialité différentielle (DP) - Concept

- • Mécanisme mathématique garantissant la protection des données personnelles.
- • Empêche l'inférence de la présence ou absence d’un individu dans un jeu de données.
- • Repose sur l'ajout de bruit statistique aux données ou gradients.
- • Permet des analyses ou entraînements tout en préservant la vie privée.

🔐 Confidentialité différentielle - Exemple concret

- Imaginez un hôpital entraînant un modèle prédictif à partir des données de patients.
- ➡️ Grâce à la confidentialité différentielle, un attaquant ne peut pas déterminer si les données d’un patient spécifique ont été utilisées.
- ➡️ Du bruit est ajouté aux gradients pendant l'entraînement pour masquer les contributions individuelles.

🔐 Agrégation sécurisée - Concept

- • Protocole cryptographique combinant les contributions de plusieurs clients.
- • Le serveur central ne peut pas voir les poids individuels des modèles locaux.
- • Garantit la confidentialité même si le serveur est compromis.
- • Très utile dans les environnements où la sécurité est cruciale (ex: santé).

🔐 Agrégation sécurisée - Exemple concret

- Chaque hôpital chiffre ses poids de modèle localement.
- ➡️ Le serveur central ne reçoit que la somme agrégée des poids.
- ➡️ Impossible pour lui de retracer les poids individuels.
- ➡️ Permet de collaborer sans sacrifier la confidentialité des données locales.

✅ Résumé de la session

- • La confidentialité différentielle protège les données au niveau mathématique.
- • L'agrégation sécurisée protège contre les attaques lors de la transmission des poids.
- • Ces deux techniques sont complémentaires et essentielles en FL pour la santé.