Privacy-Preserving Machine Learning : Federated Learning, Differential Privacy et Synthetic Data

Lien : https://innov-systems.com/formation/privacy-preserving-machine-learning-federated-learning-differential-privacy-et-synthetic-data

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI158

CATÉGORIE
Sécurité de l'Intelligence Artificielle

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes du machine learning respectueux de la vie privée
- Maîtriser Federated Learning, Differential Privacy et Synthetic Data
- Concevoir des systèmes IA sécurisés et distribués
- Réduire les risques de fuite de données sensibles
- Implémenter des architectures ML respectueuses de la confidentialité
- Utiliser les frameworks spécialisés de privacy-preserving ML
- Évaluer les compromis entre utilité et confidentialité
- Déployer des modèles IA conformes aux exigences réglementaires
- Protéger les données personnelles dans les pipelines ML
- Résister aux attaques d’inférence sur modèles
- Développer des solutions IA sécurisées en production
- Étudier des cas concrets de protection des données

POUR QUI ?

- Data scientists
- Machine learning engineers
- Ingénieurs IA
- Data engineers
- Architectes data
- Cybersecurity engineers
- Consultants en IA et sécurité
- Responsables conformité et DPO
- Chercheurs en intelligence artificielle
- Product managers techniques
- Développeurs logiciels
- Toute personne impliquée dans le développement de modèles IA sécurisés

Innov Systems

Programme détaillé

1 / Introduction au Privacy-Preserving Machine Learning

- Enjeux de la confidentialité des données en IA
- Équilibre entre performance et protection des données
- Cas d’usage en santé, finance et industrie

2 / Fondements de la protection des données en ML

- Types de données sensibles
- Risques de fuite et d’inférence
- Principes de minimisation des données

3 / Federated Learning

- Concept d’apprentissage distribué
- Entraînement sans centralisation des données
- Architecture client–serveur et agrégation des modèles

4 / Differential Privacy

- Définition et principes mathématiques
- Ajout de bruit et budget de confidentialité (epsilon)
- Compromis entre utilité et protection

5 / Synthetic Data

- Génération de données artificielles
- Méthodes statistiques et génératives
- Utilisation pour l’entraînement et les tests

Innov Systems

6 / Architectures hybrides de protection de la vie privée

- Combinaison Federated Learning + Differential Privacy
- Pipelines sécurisés de machine learning
- Modèles distribués sécurisés

7 / Outils et frameworks spécialisés

- TensorFlow Federated et PySyft
- Librairies de Differential Privacy
- Générateurs de données synthétiques

8 / Sécurité et attaques contre les modèles ML

- Membership inference attacks
- Model inversion attacks
- Stratégies de défense

9 / Déploiement en environnement réel

- Intégration dans les systèmes cloud et edge
- Contraintes de performance et scalabilité
- Gouvernance des données sensibles

10 / Études de cas et applications pratiques

- Cas d’usage en santé et finance
- Implémentation d’un pipeline privacy-preserving
- Bonnes pratiques industrielles

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 2027	Présentiel - Casablanca
13 au 17 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés