UNIVERSITÉ CÔTE D'AZUR

Post-doctorat Research Visit F/M Privacy-preserving and Robust Federated Learning

> Entité/Service : INRIA

- **Type de recrutement : Contractuel (CDD renouvelable)**
- **Catégorie : Post doctorat**
- **Temps de travail : Temps Complet**
- **Localisation : INRIA - 2004, route des Lucioles, Sophia Antipolis**
- **Référence de l'annonce: 2024-INRIA01**

Le défi à relever

Nous recherchons notre futur/future post doctorant/post doctorante ! L'apprentissage fédéré (FL) permet à une multitude d'appareils, y compris les téléphones mobiles et les capteurs, de former collaborativement un modèle global d'apprentissage automatique tout en conservant leurs données localement. Un exemple marquant de FL en action est le Gboard de Google, qui utilise un modèle formé par FL pour prédire les saisies suivantes des utilisateurs sur les smartphones.
Deux défis principaux se posent pendant la phase d'entraînement de FL :

1. Confidentialité des données : Comment garantir que les données des utilisateurs restent confidentielles ? Même si les données sont conservées localement par les appareils, il a été démontré qu'un serveur honnête mais curieux peut toujours reconstruire des échantillons de données, des attributs sensibles et le modèle local d'un appareil ciblé. De plus, le serveur peut effectuer des attaques par inférence d'appartenance pour identifier si un échantillon de données a été utilisé lors de l'entraînement ou des attaques d'inférence de source pour déterminer quel appareil stocke un échantillon de données donné
2. Sécurité contre les participants malveillants : Comment garantir que le processus d'apprentissage n'est pas perturbé par des acteurs malveillants ? Des recherches récentes ont démontré que, en l'absence de mesures de protection, un agent malveillant peut détériorer les performances du modèle en inversant simplement les étiquettes et/ou le signe du gradient, et même injecter des portes dérobées dans le modèle (les portes dérobées sont des vulnérabilités cachées qui peuvent être exploitées sous certaines conditions prédéfinies par l'attaquant, telles que des entrées spécifiques).

Rejoignez-nous au sein d'Université Côte d'Azur, reconnue depuis 2016 pour son excellence scientifique et pédagogique, pour créer ensemble le modèle de l'université du 21ème siècle responsable et innovante.

Vos missions

Dans ce projet, nous visons à proposer de nouveaux algorithmes FL pour relever efficacement ces deux défis interdépendants. En particulier, nous voulons explorer les potentialités de la compression dans l'entraînement FL, car ces techniques peuvent réduire considérablement la dimension du modèle, ce qui peut offrir une solution pour un système FL efficace en termes de calcul, privé et sécurisé. Les techniques de compression ont été initialement introduites pour alléger les coûts de communication dans les processus d'entraînement distribués, où seule une proportion des paramètres du modèle est envoyée de l'appareil au serveur à chaque cycle de communication. L'objectif principal de la conception de la compression est d'assurer un système d'apprentissage automatique/FL efficace en termes de communication, en fournissant des règles de sélection des paramètres du modèle côté appareil qui optimisent les performances du modèle formé sous un budget de communication donné. Dans ce projet, notre objectif est différent : nous visons une meilleure stratégie de compression pour un système FL privé et sécurisé efficace en termes de calcul. Plus précisément, l'objectif de ce projet est d'étudier une stratégie de compression qui offre le meilleur compromis entre confidentialité, robustesse (contre les menaces adversariales), complexité computationnelle et performance du modèle. C'est encore une question ouverte, sans recherche antérieure explorant cette direction spécifique.
Ce projet sera co-supervisé par Giovanni Neglia (Inria, France) et Gupta Nirupam (EPFL, Suisse).

UNIVERSITÉ CÔTE D'AZUR

Votre parcours professionnel

Diplôme attendu : Doctorat
La personne retenue doit avoir une formation solide en mathématiques, de bonnes compétences en programmation et de l'expérience avec Pytorch ou Tensorflow. Elle devra avoir des connaissances en apprentissage automatique notamment l'apprentissage fédéré et avoir de bonnes capacités d'analyses.
Anglais courant exigé.

Rémunération et avantages sociaux

- Rémunération contractuels (hors variables) : selon profil
- Congés : 45 jours de congés annuels
- Prise en charge partielle des frais de transport domicile-travail
- Prise en charge partielle des frais de mutuelle
- Accès aux restaurants et cafétérias du CROUS avec tarif privilégié
- Billetterie loisirs et sorties à tarifs préférentiels

L'environnement de travail

Inria est l'institut national de recherche en sciences et technologies du numérique et a la responsabilité depuis janvier 2024 de l'Agence de programmes dans le numérique pour renforcer les dynamiques collectives de l'enseignement supérieur et de la recherche. La recherche de rang mondial, l'innovation technologique et le risque entrepreneurial constituent son ADN. Au sein de 220 équipes projets, pour la plupart communes avec les grandes universités de recherche, plus de 3 800 scientifiques y explorent des voies nouvelles, souvent dans l'interdisciplinarité et en collaboration avec des partenaires industriels pour répondre à des défis ambitieux. Institut technologique, Inria soutient la diversité des voies de l'innovation : de l'édition open source de logiciels à la création de startups technologiques (Deeptech).

Pour candidater

Intéressé/Intéressée par cette annonce ? N'hésitez plus ! Et postulez par mail à l'adresse suivante : chuan.xu@inria.fr
La candidature idéale comporte un CV et une lettre de motivation que nous lirons avec attention.

Calendrier de recrutement :

Date limite de réception des candidatures : 28/07/2024

A partir du 28/07/2024 : Réponses candidatures, présélection et organisation des entretiens

Date de prise de fonction souhaitée : 1er Octobre 2024

UNIVERSITÉ CÔTE D'AZUR

UNIVERSITÉ CÔTE D'AZUR

Ouverte sur l'Europe et le monde, Université Côte d'Azur coordonne les acteurs de l'enseignement supérieur et de la recherche de la Côte d'Azur, pour offrir un environnement de formation, de recherche et d'innovation de très haut niveau. Inscrite dans une trajectoire de profonde transformation de son rôle et de son organisation, c'est aussi un établissement acteur de la dynamique de son environnement territorial, connu pour la qualité de vie exceptionnelle qu'il offre à ses habitants, entre mer et montagne. Dans ce cadre, Université Côte d'Azur se présente comme une université d'excellence, aux valeurs humanistes, socialement engagée, et éthiquement responsable.

> En chiffres

36 116 étudiants

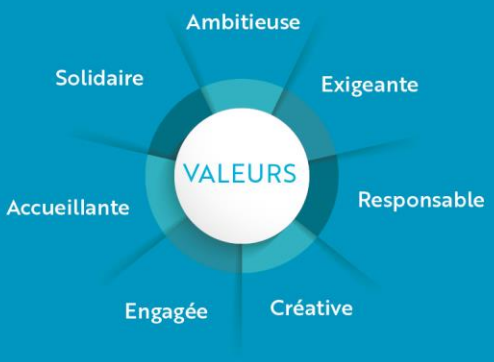
21 composantes de formation dont **8** Ecoles Universitaires de Recherche et **6** composantes dérogatoires

60 Laboratoires et unités de recherche

5432 personnels permanents

dont **1809** enseignants/chercheurs, **1347** administratifs auxquels se rajoutent environ **2276** intervenants en formation et les collègues chercheurs CNRS , INSERM, OCA, INRIA , INRAE . . .

> Les valeurs



univ-cotedazur.fr

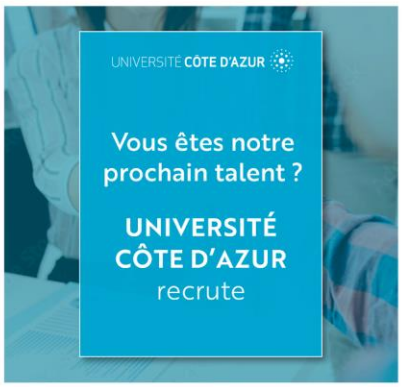
POURQUOI NOUS REJOINDRE ?

> Une Université engagée sociétalement

- Mission Handicap
- Égalité Femmes-Hommes
- Qualité de Vie au Travail
- Éthique et Intégrité Scientifique
- Prévention des Discriminations
- Campus Eco-Responsables

> Nos avantages

- De nombreux dispositifs de développement des compétences : formation, conseil en mobilité et carrière
- 2 jours de Télétravail par semaine, possible selon la nécessité de service
- 45 jours de congés / an (pour un temps plein)
- Forfait mobilité durable (vélo, covoiturage)
- Prise en charge partielle des frais de transport en commun
- Prise en charge partielle de la mutuelle
- Activités sportives, offres culturelles et clubs de loisirs
- Restauration collective
- Aides et prestations sociales
- Soutien à la parentalité



10 bonnes raisons de nous rejoindre

> Toutes nos offres en cours de recrutement

- Disponible sur notre portail web « Travailler à l'Université Côte d'Azur »
- Ouvertes aux personnes en situation de handicap

#DareToCreate Oser créer