



Offre n°2024-07160

Post-Doctoral Research Visit F/M privacy preserving federated learning with applications in medical domains

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-Doctorant

Niveau d'expérience souhaité : Jusqu'à 3 ans

A propos du centre ou de la direction fonctionnelle

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region. For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

Contexte et atouts du poste

This post-doctoral position will be supported by the [HE Trumpet project](#), the [HE Flute project](#) and/or the [PEPR IA Redeem](#) project. While this position will be in the MAGNET team in Lille, we will collaborate with the several European project partners.

While AI techniques are becoming ever more powerful, there is a growing concern about potential risks and abuses. As a result, there has been an increasing interest in research directions such as privacy-preserving machine learning, explainable machine learning, fairness and data protection legislation. Privacy-preserving machine learning aims at learning (and publishing or applying) a model from data while the data is not revealed. Notions such as (local) differential privacy and its generalizations allow to bound the amount of information revealed.

The MAGNET team is involved in the related TRUMPET, FLUTE and REDEEM projects, and is looking for team members who can in close collaboration with other team members and national & international partners contribute to one or more of these projects. All of these projects aim at researching and prototyping algorithms for secure, privacy-preserving federated learning in settings with potentially malicious participants. The TRUMPET and FLUTE projects focus on applications in the field of oncology, while the REDEEM project has no a priori fixed application domain.

The start and end date of the offered post-doctoral positions can be negotiated, subject to the administrative constraints that they start at the earliest on 1/5/2024 and end before or around 30/04/2026 and that individual contracts last no longer than 2 years.

Mission confiée

The recruited post-doc will collaborate with colleagues in the MAGNET team and the TRUMPET, FLUTE and REDEEM project consortia.

If the research features a prototype, it will contribute to the project's open source library.

We hope the post-doc can bring new expertise to the group and/or can help intensifying collaboration in the project consortium. He will collaborate closely with the other group members on realizing the research objectives of the project. Engineers in the team can support the prototyping and validation.

Possible topics of research include (but are not limited to):

- Cryptography-based strategies to improve the security of privacy-preserving AI systems.
- Inference methods for privacy assessment and/or theory for statistical privacy in general

- Programming language strategies such as those relevant in compilers and interpreters
- Design and development of the TRUMPET/FLUTE platform and its supporting algorithms.

Principales activités

- Contribute to the research of the projects
- Collaborate with other MAGNET and project team members
- Collaborate with engineers to prototype proposed algorithms and validate them
- Disseminate research results

Compétences

The following skills are desired for this position:

- a strong research background in the domain of the project (or at least a specific area such as privacy, cryptography, statistics, distributed systems, ...)
- good communication and reporting skills, and an interest in collaborative work
- proficiency in English

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

Gross monthly salary (before taxes) : 2 788 €

Informations générales

- **Thème/Domaine** : Sécurité et confidentialité Statistiques (Big data) (BAP E)
- **Ville** : Villeneuve d'Ascq
- **Centre Inria** : [Centre Inria de l'Université de Lille](#)
- **Date de prise de fonction souhaitée** : 2024-05-01
- **Durée de contrat** : 12 mois
- **Date limite pour postuler** : 2024-12-31

Contacts

- **Équipe Inria** : [MAGNET](#)
- **Recruteur** :
Ramon Jan / jan.ramon@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

We are looking for a candidate with a strong background in computer science, with interest in the multiple challenges related to privacy and an approach involving several specializations (e.g., machine learning, security, cryptography, compilation,

Candidates should provide sufficient information to support their application, the page <https://team.inria.fr/magnet/how-to-apply/> lists the minimum information desired (which is more than

what is stricly required by the online submission platform

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

CV + application letter + recommendation letters + List of publications

Academic transcripts, thesis, project report

Sécurité défense :

Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.