HR EXCELLENCE IN RESEARCH

2021-04084 - Post-Doctoral Research Visit F/M Transparent privacy-preserving AI

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 Lille - Nord Europe Research Centre was founded in 2008 and employs a staff of 320, including 280 scientists working in fourteen research teams. Recognised for its outstanding contribution to the socio-economic development of the Hauts-De-France région, the Inria Lille - Nord Europe Research Centre undertakes research in the field of computer science in collaboration with a range of academic, institutional and industrial partners.

The strategy of the Centre is to develop an internationally renowned centre of excellence with a significant impact on the City of Lille and its surrounding area. It works to achieve this by pursuing a range of ambitious research projects in such fields of computer science as the intelligence of data and adaptive software systems. Building on the synergies between research and industry, Inria is a major contributor to skills and technology transfer in the field of computer science.

Contexte et atouts du poste

This post-doctoral position will be supported by the TIP project on Transparent artificial Intellgence preserving Privacy. This project will be jointly funded by I-Site, INRIA, U-Lille and MEL. This is a project in the MAGNET team (INRIA-Lille, https://team.inria.fr/magnet/).

While this position will be in the MAGNET team in Lille, we will collaborate with users (e.g. medical research groups in CHU-Lille) for the validation and exploitation of the work.

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. Explainable machine learning aims at learning models which are not only accurate but also can be explained to humans.
The overall goal of the TIP project is to develop, exploit and explain a sound understanding of privacy-preserving strategies in larger AI-based processes involving massive numbers of agents among whom a part may be malicious.
Key challenges are related to the fact that we study applications from a holistic point of view (rather than individual operations in isolation), the need for transparency and explainability, and the need to consider more realistic assumptions than the popular honest-but-curious model.

To realize this project, a team of PhD students, post-docs, senior researchers and engineers will collaborate to perform the necessary research and develop a prototype. The successful candidate will be a member of this team. The TIP project team will collaborate with other members of the MAGNET group, e.g., on decentralized algorithms, interpretable privacy requirements and cryptographic components for federated ML algorithms.

More project information will be posted at http://researchers.lille.inria.fr/jramon/projects/tip.html

Mission confiée

The recruited post-doc will collaborate with the TIP project researchers and the MAGNET team engineers.

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 in the group. He will collaborate closely with the other group members on realizing the research objectives of the TIP 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
- Modeling of information flows and privacy properties

Principales activités

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

Compétences

The following skills are desired for this position:

Informations générales

- **Thème/Domaine :** Sécurité et confidentialité Statistiques (Big data) (BAP E)
- **Ville :** Villeneuve d'Ascq
- **Centre Inria :** CRI Lille - Nord Europe
- **Date de prise de fonction souhaitée :** 2022-01-01
- **Durée de contrat :** 1 an, 1 mois
- **Date limite pour postuler :** 2022-02-15

Contacts

- **Equipe 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 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3500 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 180 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,

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

The postdoc ideally should have a background in one of the specializations relevant to the TIP project, e.g., differential privacy, multi-party computing, explainable AI, ...

Consignes pour postuler

CV + application letter + recommendation letters + List of publications

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.

- a strong research background in the domain of the project (or at least a specific area relevant to the project, e.g., see "assignments").
- good communication and reporting skills
- proficiency in Englis

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 (after 6 months of employment) 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) : 2 653 €