Offer #2024-07160

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

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Fonction : Post-Doctoral Research Visit

Level of experience : Up to 3 years

About the research centre or Inria department

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).

Context

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 inthe 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 algoirhtms 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.

Assignment

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.

Main activities

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

Skills

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

Benefits package

- 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

Remuneration

Gross monthly salary (before taxes) : 2 788 €

General Information

- **Theme/Domain :** Security and Confidentiality
  Statistics (Big data) (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2024-05-01
- **Duration of contract :** 12 months
- **Deadline to apply :** 2024-12-31

Contacts

- **Inria Team :** MAGNET
- **Recruiter :**
  Ramon Jan / jan.ramon@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

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

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

CV + application letter + recommendation letters + List of publications

Academic transcripts, thesis, project report

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.