Offer #2022-05007

PhD Position F/M Transparent privacy preserving AI

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Up to 3 years

About the research centre or Inria department

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.

Context

This PhD student position will be supported by the TIP project on Transparent artificial Intellgence preserving Privacy (a project jointly funded by I-Site, INRIA, U-Lille and MEL) and the EU-project Trumpet. 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 athttp://researchers.lille.inria.fr/jramon/projects/tip.html

Assignment

The recruited PhD student 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.

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

Main activities

- 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

Skills

The following skills are desired for this position:

- a strong background in computer science (including basic course material on mathematics and algorithms)
- good communication and reporting skills
- 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

1st and 2nd year : 1 982€ gross monthly salary (before taxes)

3rd year : 2085€ gross monthly salary (before taxes)

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 :** 2022-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2022-07-15

Contacts

- **Inria Team :** MAGNET
- **PhD Supervisor :**
  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 (or statistics), with interest in the multiple challenges related to privacy (e.g., machine learning, probability theory, cryptography, logic, ...)

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

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.