Principal activities

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.
- Design and development of the TRUMPET platform and its supporting algorithms.
- Contribute to the research of the TRUMPET project.
- Collaborate with other MAGNET and TRUMPET team members.
- Disseminate research results.

Mission assigned

The recruited PhD student will collaborate with colleagues in the MAGNET team and the TRUMPET project consortium in general. Part of the work may involve travel to other partners.

If the research features a prototype, it will contribute to the project's open source library and may be supported by engineers in the team.

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.
- Design and development of the TRUMPET platform and its supporting algorithms.

Context and advantages of the position

This PhD position will be supported by the HE Trumpet project.

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 overall goal of the TRUMPET project is to research and develop novel privacy enhancement methods for Federated Learning, and to deliver a highly scalable Federated AI service platform for researchers, that will enable AI-powered studies of siloed, multi-site, cross-domain, cross-border European datasets with privacy guarantees that exceed the requirements of GDPR.

INRIA's MAGNET team will contribute among others to tasks involving AI algorithms and architectures, federated Learning, privacy platforms, privacy measurement and metrics, privacy-enhancing technologies and applied cryptography.

Informations générales

- Thème/Domaine :
  Représentation et traitement des données et des connaissances Statistiques (Big data) (BAP E)
- Ville : Villeneuve d'Ascq
- Centre Inria : Centre Inria de l'Université de Lille
- Date de prise de fonction souhaitée : 2023-09-01
- Durée de contrat : 3 ans
- Date limite pour postuler : 2023-09-30

Contacts

- Equipe Inria : MAGNET
- Directeur de thèse : 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 research (including the mathematics needed to realize privacy) who welcomes the broad range of challenges leading to a successful result.

Candidates should provide sufficient information to support their application, the page
https://team.inria.fr/magnet/how
Compétences
The ideal candidate will have the following skills:

- Good mastery of English
- A strong background in computer science and mathematics.
- Subject matters which will be needed during the research include (but are not limited to) machine learning, statistics, cryptography, distributed systems, constraint programming.
- Good programming skills (e.g., C/C++ or python) and supporting tools.
- Relational skills, e.g., working in a team, effective reporting and communication with all involved stakeholders.

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

1st and 2nd year : 2051 € gross monthly salary (before taxes)
3rd year : 2158 € gross monthly salary (before taxes)