A propos du centre ou de la direction fonctionnelle

Inria Lille - Nord Europe Research Centre was founded in 2008 and employs a staff of 360, including 300 researchers working in sixteen research teams. Recognised for its outstanding contribution to the socio-economic development of the Nord - Pas-de-Calais Region, 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

Inria Lille is seeking collaborators (engineers, PhD student and/or postdoctoral researcher) for a new collaborative project on privacy-preserving (semi-)decentralized learning in an IoT setting. The successful candidate will be part of the Magnet team, which gathers 15 researchers (Faculty, postdocs, PhD students) in the field of machine learning, with focus on learning from graph-structured data as well as decentralized and privacy-friendly algorithms. The team is very international and English is the working language.

Driven by awareness raised by the recently introduced GDPR and by privacy concerns of their customers, many companies have expressed an interest in more human-friendly and in particular privacy-friendly technology, but have also expressed concerns about the difficulty of applying existing theory in their industrial environment. The proposed project aims at bridging this gap to a large extent. It will feature both research and contributions to open source software in a broader collaborative context.

Collaborators will work in the Magnet team but also collaborate with industrial and academic partners.

Mission confiée

The research topic has several components. First, we will investigate more generally applicable methods to assess privacy. While differential privacy is a popular paradigm, both classic differential privacy and extensions such as pufferfish differential privacy consider a single run of an algorithm and don't allow for continuous querying of data nor for modeling systems of many communicating parties where it makes sense to quantify privacy from the point of view of the party who tries to infer information. This part of the project will involve probability theory and AI algorithms. Second, we will investigate the integration of privacy-preserving AI in real-world applications. Most current approaches consider privacy of algorithms solving small, isolated problems. Making a full process or platform privacy-preserving means that all steps/modules should be (together) privacy-preserving. To realize this, we will combine and build on three elements: (1) the generalized privacy notion of the first PhD research component, (2) formal ways to describe processes and the information they transfer, and (3) techniques from areas of cryptography. Therefore, this part of the project will involve cryptography, process modeling, and further probability theory.

The objectives are:

- to develop an integrated, transparent and verifiable framework for analyzing privacy and guaranteeing privacy over a continuous process involving elementary actions (such as machine learning tasks) of which we can describe the privacy implications, and
- to develop the missing but non-trivial building blocks needed to realize such integration.

The main expected results are:

- to make AI (and machine learning) more human-friendly,
- to bring currently emerging privacy-friendly technology closer to real-world applications of industrial and societal relevance.

The work will be conducted at INRIA Lille in the Magnet group, in tight collaboration with several international partners.

Principales activités

A possible approach to the project is the following:

1. Privacy measures (8 months)
   - Develop privacy measures for repeated querying
   - Develop models of information flow to assess the consequences of knowledge distributed over many parties, especially for what concerns privacy

2. Process modeling (8 months)
   - Develop a language for modeling distributed processes able to express information flow and privacy aspects
   - Integrate in this language metrics and notions compatible with legal and human-interpretable concepts, allowing for verification and transparency
   - Develop algorithms to perform verification of privacy claims for a process and for explaining a process and its privacy properties to non-expert humans

3. Integrated framework (6 months)
   - Develop a generic framework to integrate the results of the previous two WP (privacy measures and process models) with existing privacy-preserving...
technology.
- adapt existing privacy-preserving algorithms to fit the framework
- develop missing building blocks needed for applications
4. Validation (10 months)
- Interface the developed techniques with applications on which other team members work
- evaluate the performance (e.g., functionality, efficiency) on these application domains.
5. Publication (articles, thesis) and exploitation (4 months)

**Compétences**
A good candidate will have the following skills:
- A good command of English
- A strong background in mathematics
- A good knowledge of machine learning, statistics and algorithms
- Preferably some knowledge on distributed systems and cryptography
- Some experience with implementation and experimentation

Please follow the instructions given in https://team.inria.fr/magnet/how-to-apply/ to set up your application file.

**Avantages**
- Partially-reimbursed public transport
- Sports facilities
- Social security

**Rémunération**
Gross monthly salary 1982€ for the 1st and 2nd year.
2085€ gross monthly salary for the 3rd year.