2019-01372 - PhD Position F/M [Sub - 2019] - integration of privacy-preserving AI in real-world applications

Type de contrat : CDD de la fonction publique
Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

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 360, including 300 scientists 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

The research topic has several components. First, we will investigate more generally applicable methods to assess privacy. While differential privacy [1] is a popular paradigm, both classic differential privacy and extensions such as pufferfish dierential privacy consider a single run of an algorithm and don’t allow for continuous querying of data nor for modeling systems of many competing parties where it makes sense to quantify privacy from the point of view 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 realise this, we will combine and build on three elements: (1) the generalized privacy notion of the rst 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.

Industrial context

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 diculty of applying existing theory in their industrial environment. The proposed project aims at bridging this gap to a large extent.

We have contacts with companies in the domain of transportation (ranging from SMEs based in Lille such as Xee to large car OEMs such as BMW and collective organizations such as r-trans), medicine (hospitals (e.g., Lille hospitals) and other organizations working with patient data, and researchers using human data (e.g., Johnson&Johnson)), user behavior (e.g., Mediego, Snips.ai, CityGuide, Samsung).

References


Mission confiée

This project will be carried out in the MAGNET Team at Inria Lille, in which all required competences are present, such as experience in domains as machine learning, dierential privacy, algorithms, basic privacy-related cryptography and applications in transportation and medicine.

Existing collaborations such as in the projects ANR-Pamela, H2D2D-Comprisa, ANR-DeepPrivacy are further enriching this basic expertise. We also collaborate with associated teams providing advanced cryptographic expertise in the context of the PAD-ML associated team project.

This project will also stimulate existing and emerging collaborations with other research groups on themes at the intersection between machine learning, privacy, complex systems and cryptography. E.g., the IPI-HyAI project will allow us to collaborate with other teams who are interested (https://team.inria.fr/magnet/) in variability and transparency of algorithms (TAU, LACODAM) and real-world applications of privacy-preserving techniques (Multispeech).

The PhD student will interact with partners of the PAD-ML associated team, especially where there is a need to optimize cryptographic solutions (international collaboration). The PAD-ML team is a north European team between Magnet and the Alan Turing institute in London. The PhD student will interdisciplinarily interact with Juliette Senéchal (Department of Law, ULeuL) where the work concerns guaranteeing transparency of descriptions of processes and their privacy implications (regional collaboration).

The PhD student will interact with potential users (in industry and academia) to better understand requirements in real-world applications.

Principales activités
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 project has the following work packages and tasks:

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 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)

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)
- Access to vocational training
- Social security coverage

Rémunération

1st and 2nd year: 1593.50€ Net monthly salary (after taxes)
3rd year: 1676.31€ Net monthly salary (after taxes)