2018-00400 - [Campagne Doctorant 2018/CRI LILLE] - PhD
Thesis: Privacy-preserving decentralized machine learning (M/F)

Type de contrat: CDD de la fonction publique
Niveau de diplôme exigé: Bac + 5 ou équivalent
Fonction: Doctorant
Niveau d'expérience souhaité: Jeune diplômé

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 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

Job environnements

This project will be carried out in the MAGNET Team at INRIA Lille and will be co-supervised by Jan Ramon and Aurélien Bellet. In particular, Jan Ramon did research in several areas of graph-based machine learning including learning theory, supervised learning algorithms, communicating learning agents and information optimization, while Aurélien Bellet is a machine learning specialist with some prior publications on distributed learning and decentralized gossip protocols.

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. In particular, MAGNET has collaborations with the ASAP Team at INRIA Rennes (working on distributed systems) and the CIDRE Team (working on security and privacy) through the ANR Pamela. MAGNET has also developed contacts with international partners in Europe and USA which can serve as possible student exchange during this PhD.

Mission confiée

Assignments

The research work in the context of this Ph.D. project consists in developing a theoretical and algorithmic framework for privacy-friendly distributed machine learning, so that prediction tasks can be performed securely using the data of many users without storing personal data on a central server or disclosing them to other users. The candidate will work with Jan Ramon and Aurélien Bellet.

Principales activités

Main activities

- Analyze the problems related to privacy-friendly machine learning
- Propose algorithms for decentralized privacy-preserving machine learning
- Propose metrics and analysis methods for estimating privacy risks in a machine learning process
- Propose techniques for making the algorithms more robust against failures and attacks.
- Validate the proposed solutions

Additional activities

- Reporting, disseminating and presenting results
- Coordinating with related efforts in the team / community
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

Avantages sociaux
Benefits

- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Sports facilities
- Flexible working hours

More information about Lille:
http://www.lille3000.eu/portail/
http://www.lillemetropole.fr/mel.html

Rémunération
Remunerating

The gross monthly salary is 1982€ for the 1st and the 2nd year, 2085€ for the 3rd year.