Research Grants for PhD students from the China Scholarship Council

Information Form (please read the guidelines carefully on the website www-csc.utt.fr)

Supervisor's name : NGUYEN Given names : BENJAMIN

Status (prof., assistant prof., …) : Professor

Laboratory :	Laboratoire d'Informatique Fondamentale d'Orléans (LIFO, EA 4022)	Website address : http://www.univ-orleans.fr/lifo/?lang=en
Institution :	INSA Centre Val de Loire	Website address : http://www.insa-centrevaldeloire.fr/en

Scientific competence of the supervisor:

Anonymization techniques. Models to represent, quantify and enforce limited data collection. Methods to enforce existing privacy models using secure hardware devices or cryptographic techniques. Design and implementation of large scale privacy-by-design personal information management applications.

Two major publications in the field proposed for the PhD :

1. Quoc-Cuong To, Benjamin Nguyen, Philippe Pucheral: Private and Scalable Execution of SQL Aggregates on a Secure Decentralized Architecture. ACM Trans. Database Syst. 41(3), 2016.
2. Quoc-Cuong To, Benjamin Nguyen, Philippe Pucheral: TrustedMR: A Trusted MapReduce System Based on Tamper Resistance Hardware. OTM Conferences 2015: 38-56, 2015.

Website address of the personal page : https://www.benjamin-nguyen.fr/

Supervisor's email : benjamin.nguyen@insa-cvl.fr

Description of the research work proposed for a PhD ***Topic # (see list) :*** I-13

Title : Privacy-Preserving Multi-Armed Bandits

Subject :

The multi-armed bandit is a decision making model, where an agent repeatedly chooses an action (pull a bandit arm) and the environment responds with a stochastic outcome (reward) coming from an unknown distribution associated with the chosen action. Popular objectives are those of maximizing the sum of observed rewards or to identify the best arm. The main applications of the multi-armed bandit setting are recommendation services and clinical trials. It can happen that data and computations used as input for bandit algorithms are outsourced to a public cloud. The outsourced data may be communicated over an untrustworthy network, where malicious users may have access and learn private data. There is a recent line of research on adding privacy to existing bandit algorithms, which follow two privacy-preserving approaches: differential privacy and cryptography. The goal of this PhD thesis is to push forward the state of the art on adding privacy guarantees to bandit algorithms, using both approaches. Before starting the actual algorithm design and implementation, the student will do a bibliographical study on the techniques currently used in the literature. Then, the student will tackle some of the main current open problems e.g., how to add differential privacy guarantees to the problem of best arm identification, and how to use cryptographic techniques to secure cumulative reward maximization for new classes of bandit problems.

Keywords :

Security in machine learning, Honest-but-curious cloud, Secure multi-party computations, AES-CBC symmetric encryption scheme, Paillier's additive homomorphic asymmetric encryption scheme, Differential privacy.

Expected collaborations :

Radu Ciucanu (LIFO / INSA CVL)
Pascal Lafourcade (LIMOS / University of Clermont Auvergne)
Marta Soare (LIFO / University of Orléans)

Background required from the applicant :

The ideal candidate is close to obtaining a Bac+5 (e.g., Engineering or Master) degree in Computer Science and has very good academic results. Both theoretical and programming skills are needed to handle the foundational and implementation aspects of the PhD thesis.

Existence of a PDF file detailing the proposal ("yes" or "no") : no

(see guidelines on the website www-csc.utt.fr)