UNIVERSITÉ DE RENNES 1

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2023

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : MATISSE **POLE DE RECHERCHE : Mathématiques-Numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA (UMR 6074)

Equipe : WIDE (The World is Distribued)

Encadrement

Directeur de thèse : Davide Frey **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Inria

HDR : X oui ☐ non **Nb de thèses en cours** : 3

Mail : davide.frey@inria.fr **Tél.** : +33 (0) 2 99 84 75 65

Co-directeur de thèse : Romaric Gaudel **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes (ex UR1)

HDR : X(*) oui ☐ non **Nb de thèses en cours** : 0 (*) soutenance le 2 février 2023

Mail : romaric.gaudel@irisa.fr **Tél.** : +33 (0) 2 99 84 75 65

Sujet

Titre : Privacy-Preserving Decentralized Learning Through Model Fragmentation and Private Aggregation

Mots clés : Machine Learning, Decentralization, Privacy Protection, Middleware, Randomized Algorithms

Cotutelle internationale (oui/non) : non **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Machine learning consists in producing (learning) a computer-based function (usually referred to as a model) from examples (training data). The accuracy and quality of the resulting model are usually directly related to the size of the training data, but training from very large datasets raises at least two problems. First, very large training sets require substantial computing power to train the model in a reasonable time. Second, as machine learning is increasingly applied to sensitive and personal data (e.g. health records, personal messages, user preferences, browsing histories), exposing this data to the learning algorithm raises far-reaching privacy-protection concerns, and carries important risks of privacy violation.

These two problems have prompted the emergence of a range of distributed learning techniques, which seek to distribute the learning effort on many machines to scale the learning process and limit privacy leaks by keeping sensitive data on the learning devices. Two related strategies have in particular emerged to address these challenges: *Federated Learning*, initially promoted by Google, and *Decentralized Learning*, which forgoes entirely any centralized entity in the learning process. Unfortunately, recent works have shown that, in spite of their promises, both of these approaches can be subject to privacy attacks such as membership inference, data reconstruction, or attribute inference, that make it possible for malicious participants to access private and or sensitive information through the learning process.

This PhD aims to improve the privacy protection granted by decentralized learning by exploring how *model fragmentation*, a technique developed by the WIDE team within the ANR Pamela project (2016-2020), can be combined with *private aggregation* and *random peer sampling*, two of the strategies successfully applied to P2P networks.

More concretely the PhD will address the three following research questions:

1. How to fragment, distribute, and reconstruct decentralized models?
2. How to combine fragmentation and privacy-preserving averaging without disrupting learning?
3. How to characterize the gains of protection obtained from fragmentation and privacy- preserving averaging?

In terms of methodology the PhD will combine the design, implementation, and characterization of research prototypes to gain practical insights, coupled with algorithmic and statistical models on which we will carry systematical analysis and reasoning.

➢ **Ce document est à renvoyer par la direction de l'unité de Recherche aux animateurs du Pole Recherche et à l'école Doctorale pour le 6 février 2023 au plus tard**