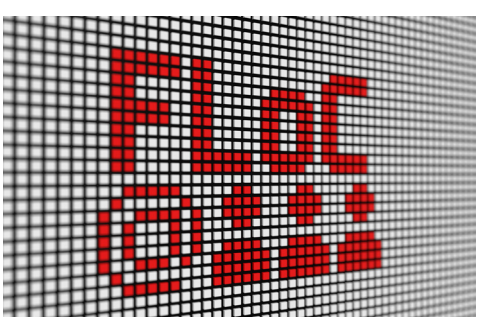
Leçon inaugurale

Systèmes d'apprentissage collaboratif dignes de confiance

L'apprentissage fédéré (« federated learning ») est un paradigme d'apprentissage collaboratif émergent permettant aux propriétaires de données d'extraire des connaissances et d'apprendre des modèles conjointement. L'apprentissage fédéré renforce la démocratie en invitant publiquement les utilisateurs à participer à l'apprentissage des modèles et protège la confidentialité des données en conservant les données sur place auprès de leur propriétaire. Dans cet exposé, je parlerai tout d'abord de l'intérêt et des défis techniques liés à la construction de modèles d'apprentissage diversifiés, allant de la classification et des graphes jusqu'aux modèles génératifs. À l'aide d'exemples concrets, j'illustrerai ensuite les problèmes de vulnérabilité liés aux utilisateurs malveillants et j'évoquerai finalement quelques pistes de recherche pour améliorer la confiance dans l'apprentissage fédéré.



Lydia Chen

Chaire d'apprentissage automatique

La leçon inaugurale aura lieu
le **mercredi 30 octobre 2024** à 18h15
UniMail, rue Emile-Argand 11

unine
Université de Neuchâtel
Faculté des sciences