N° d'ordre : D -

THESE

présentée

devant l'Institut National des Sciences Appliquées de Rennes

en vue de l'obtention du

DOCTORAT

spécialité : Informatique

par M PRIGENT Cédric

Intitulé : Towards Efficient and Trustworthy Federated Learning on the Computing Continuum

Directeur de Thèse : COSTAN Alexandru et ANTONIU Gabriel

Date, heure et lieu de soutenance : 26/05/2025, 13h30, INSA Rennes, Amphi Bonnin

Membres du jury (nom, prénom, titre et établissement de rattachement, fonction)

- BEN MOKHTAR Sonia, Directrice de recherche, HDR, LIRIS - Lyon, France
- SENS Pierre, Professeur des universités, HDR, Sorbonne Université, France
- CIORBA Florina, Associate professor, University of Basel, Switzerland
- COSTAN Alexandru, Maître de conférences, HDR, INSA Rennes, France
- ANTONIU Gabriel, Directeur de recherche, HDR, Inria - Rennes, France
- CUDENNEC Loïc, Responsable recherche et innovation IA, HDR, DGA MI - Bruz, France

RESUME DE LA THESE

The emergence of new data privacy concerns and regulations advocates for decentralization by moving the computation at the Edge of the network, where the data is produced. Federated Learning (FL) is such a solution, running decentralized training, rather than consolidating large amounts of sensitive data on a single server, for running Machine Learning workflows. While this strategy proves effective in preserving data privacy, it also faces significant challenges in terms of practicality when deploying such FL systems at large scale on the Computing Continuum. The combination of heterogeneous, volatile, possibly defective or malicious devices greatly impacts training efficiency across decentralized environments.

This thesis makes a first step towards addressing these challenges for FL on the Computing Continuum. We propose new approaches to efficiently improve the resilience of FL systems to adversarial scenarios, and enable personalized training based on client local objectives. We further investigate how different infrastructures could be used for reproducing performance of real-world FL systems, as a first step towards understanding performance of FL systems across complex environments of the Computing Continuum.