USEES3 - Distributed and Federated Learning

Mis à jour le 03-07-2024

Code : USEES3

Unité spécifique de type cours

5 crédits

Responsabilité nationale : EPN05 - Informatique / Stefano SECCI

Présentation

Prérequis

- Students are required to have taken an introductory machine-learning course
- Good knowledge on supervised learning.
- Some knowledge on Gradient descent
- Bases on unsupervised learning is recommended, but this is not a prerequisite.

Objectifs pédagogiques

This course provides an overview of federated and distributed learning in terms of performance and sécurité. Both theoretical and practical aspects will be extensively explored in this course in order to acquire solid expertise on both aspects. By the end of the course, students should

- Understand the major difference between centralized and decentralized learning
- Understand the methods most commonly used in federated learning
- Understand the performance of federated learning when data is heterogeneous (Non-IID data).
- Be able to build and scale a simple federated system
- Have acquired competence in implementing federated learning in the fields of networks, security, health or others.

Programme

Contenu

This course is designed to extend students' knowledge of learning in a decentralized setting. Decentralized learning techniques, such as federated learning, are set to deliver a new generation of machine learning applications by enabling efficient and reliable learning between multiple parties and from diverse data sources. This course will cover different aspects of federated learning, focusing on recent research developments and exploring important applications in different fields such as security, networks and healthcare.

Lectures

- Course Overview. Introduction to machine learning and Federated Learning.
- Decentralized Optimization and Gradient descent
- Federated learning: FedSGD and FedAvg
- Variations of Federated Aggregation.
- Federated Averaging with Heterogeneous Data
- Communication-Efficient Learning of deep networks in Federated Learning
- Federated Multi-Task learning

Lab sessions

- Build and scale a simple federated learning with MNIST, Cifar-10, Fashion-MNIST, MedMNIST, Shakespeare, and BCN Open Data. Open-source Federated Learning tools (Pytorch, Flower, etc.).
- Federated learning with Non-IID data.

Complementary content:

- Threats, attacks, and defenses to federated learning
- Designing an attack and setting up a defense for federated learning.
- Applications to Images, Networks, health, and vehicle-to-vehicle communications

Labs

- Applications of federated learning to network anomaly detection: use of 5G and LoRaWAN

testbeds and datasets, with lab [by CNAM].
- Applications of federation learning to medical equipment: use of aggregated and anonymized field data [by NTUU].
- Applications of federation learning to vehicle-to-vehicle communications: routing and content offloading [by UPC].

Modalités de validation

- Contrôle continu
- Projet(s)
- Mémoire
- Examen final

Description des modalités de validation

- The evaluation will be based on a final exam, lab reports and/or project activity.
- For the project, students may also conduct research in the field of federated learning and write a short paper.

Bibliographie

Titre	Auteur(s)
Federated Learning with Python, O'Reilly, October 2022	Kiyoshi Nakayama, George Jeno
Federated Learning.Theory and Practice. Elsevier 2024. ISBN: 9780443190384	Lam M. Nguyen, Trong Nghia Hoang, Pin-Yu Chen