

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PhD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Course announcement

Title: Ensuring Trustworthiness in Federated Learning

Lecturer: Dr. Marco Fisichella

L3S Research Center, Leibniz University, Hannover, Germany
Email: mfisichella@L3S.de

Credits: 2 ECTS

Overview

Ensuring the trustworthiness of AI models can be challenging due to their brittleness, limited ability to adapt to new domains, and difficulty in generalizing to data drawn from different distributions. These limitations may lead to inaccurate predictions, unfair treatment of specific groups, and difficulties in interpreting model decisions, thereby reducing human trust.

Improving the trustworthiness of AI models requires greater transparency, interpretability, robustness, and generalizability. Federated learning (FL) offers a way to pursue these goals while preserving data privacy and security. FL enables AI models to be trained on decentralized data without requiring sensitive information to be transferred to a central location.

By leveraging data from multiple sources, federated learning can support the development of more accurate, robust, and generalizable models for real-world applications, while reducing the risks associated with the centralized collection and processing of sensitive data.

There will be a final assessment.

Schedule

Lecture	Date	Time	Topics	Lecturer
1	26/10/2026	16:00-18:00	Introduction to course	Marco Fisichella
2	02/11/2026	16:00-18:00	Fundamentals of FL (Part 1)	Marco Fisichella
3	09/11/2026	16:00-18:00	Fundamentals of FL (Part 2)	Marco Fisichella
4	10/11/2026	10:00-12:00	Introductory code for FL	Marco Fisichella
5	16/11/2026	16:00-18:00	Deep dive into one advanced topic in FL (e.g., Federated Fine Tuning of LLMs, Federated Passenger Flow Prediction, etc.)	Marco Fisichella
	31/01/2027		Assessment test	

Content details

Lesson 1 – Introduction to course

Overview of the course objectives, structure, and expected learning outcomes. The lesson introduces trustworthy AI, the motivation for federated learning, and the main challenges addressed throughout the course.

Lesson 2 – Fundamentals of FL (Part 1):

Introduction to the foundations of deep learning and federated learning. The lesson covers neural network training, distributed data settings, the FedAvg algorithm, and the differences between centralized and federated learning.

Lesson 3 – Fundamentals of FL (Part 2):

Introduction to differential privacy in federated learning. The lesson explains privacy budgets, noise mechanisms, clipping, privacy-utility trade-offs, and how differential privacy protects client data during training.

Lesson 4 – Introductory code for FL:

Hands-on introduction to federated learning through code.

Lesson 5 – Deep dive into one advanced topic in FL:

In-depth analysis of an advanced federated learning topic, such as federated fine-tuning of large language models or federated passenger-flow prediction, focusing on methods, challenges, and real-world applications.

Participants are requested to send an e-mail to mfisichella@L3S.de by date, with the following information:

Student name and surname, name of the PhD course, PhD cycle.

For information: Dr. Franca Rocco di Torrepadula (DIETI, UniNA) –
franca.roccoditorrepadula@unina.it (organizer)