Contribution ID: **5** Type: **not specified**

Federated Learning with CAFEIN for Decentralized, Privacy preserving and Secure AI development

Monday 24 March 2025 09:15 (1 hour)

Federated Learning represents a paradigm shift in artificial intelligence by allowing the training of machine learning algorithms without the need to transfer data or rely on centralized resources. FL's decentralized computing and data storage nature ensures privacy and regulatory compliance while enhancing scalability and robustness compared to traditional systems.

This talk will provide an introduction to the fundamentals of federated learning, the federated process across vertical and horizontal federations, and aggregation algorithms. We will then delve into key security challenges, including network security for secure communication and model security to prevent adversarial attacks and leakage of sensitive information.

The discussion will also feature CAFEIN, CERN's federated learning platform, showcasing real-world projects both at CERN and their application in society through industry and academic collaborations.

Number of lecture hours

1

Number of exercise hours

0 (no exercises)

Attended school

tCSC 2023 (Split)

Author: REIS SANTOS, Diogo (CERN)

Presenter: REIS SANTOS, Diogo (CERN)