Federated and decentralized Learning: security and privacy in edge-to-cloud infrastructures

Cédric GOUY-PAILLER
CEA

13/06/2025, session 6, orateur 2

Résumé

Within the REDEEM project (PEPR IA, https://redeem-pepria.github.io/en/), federated and decentralized learning are investigated as key enablers for trustworthy AI across distributed, edge-to-cloud infrastructures. These approaches support data minimization by design, enabling model training without centralizing sensitive data. REDEEM addresses critical challenges related to security, privacy preservation, and robustness. This presentation aims at introducing important challenges of decentralized artificial intelligence across heterogenous infrastructures.