15th JLESC Workshop

Joint Laboratory for Extreme-Scale Computing

Contribution ID: **30** Type: **Short talk**

# Malicious Peers Detection in Federated Learning

*Wednesday 22 March 2023 16:40 (10 minutes)*

Federated Learning (FL) is proposed as a solution to collaboratively learn a shared model in massively distributed environments without sharing private data of the participating parties.
While taking advantage of edge resources to compute model updates from a massive number of clients, it may lead to security risks.
Selected clients for a training round get access to the global model in order to update it with their local data. However, such access to the global model is an entry for potential poisoning attacks.
Malicious clients that are sampled in a given round can manipulate the weights of the model before sending them back to the server.
In this work, an approach for discarding malicious updates in Federated Learning is proposed.
This approach is leveraging auto-encoders to generate synthetic data that are used to evaluate client updates.

## JLESC topic

**Primary author:** PRIGENT, Cedric (INRIA)

**Presenter:** PRIGENT, Cedric (INRIA)

**Session Classification:** Short Talks on AI/MD/DL

**Track Classification:** AI and ML/DL