Contribution ID: **42** Type: **Paper presentation**

Benchmarking privacy in text classification

Friday 5 November 2021 16:40 (20 minutes)

In most Machine Learning models, the data used for training or testing is public, available to anyone who wishes to see it. New research has improved these models, by adding privacy and distributing the processing load on multiple workers in the cloud. The aim of the paper is to perform an analysis between a classical approach (in which we have access to all the data) and one in which the privacy is preserved (Federated Learning) to explore the cases when a private model can be suitable in real-life scenarios.

Authors: FLOREA, Iulia (Politehnica University of Bucharest); CIOCIRLAN, Stefan-Dan (Politehnica University of Bucharest); CONSTANTIN, Mihai (Politehnica University of Bucharest)

Presenter: FLOREA, Iulia (Politehnica University of Bucharest)

Session Classification: Technologies for Future Internet

Track Classification: Technologies for Future Internet