Contribution ID: **459** Type: **Sectional talk**

PATE-FL: A Privacy-Preserving Federated Learning Framework with RAFT-Based Coordination

Thursday 10 July 2025 14:30 (15 minutes)

In federated synthetic data generation, model queries can expose statistical patterns, labeling behavior, and membership information—creating complex, layered privacy vulnerabilities. To this end, we propose PATE-FL: a federated learning framework that combines the PATE mechanism, Rényi Differential Privacy (RDP), and Paillier additive homomorphic encryption (HE), designed for the context of synthetic data generation under strict privacy requirements. In this study, we replace the gradient exchange in traditional federated learning with the voting result of the teacher model and implement secure aggregation through additive HE to effectively reduce the potential risk of information leakage during the query process. To support multi-node deployments, we introduce the Raft consensus mechanism to achieve state synchronization and fault tolerance. Considering the demand for query control and budget monitoring in practical scenarios, we design and implement a privacy management module to quantify the privacy cost of heterogeneous queries. To validate the effectiveness of these mechanisms under attack scenarios, we develop an internal testing pipeline to assess the system's resistance to membership inference attacks (MIA) and attribute inference attacks (AIA). The proposed system integrates privacy safeguards and query monitoring mechanisms, demonstrating practical potential for cross-institutional deployment in privacy-regulated environments.

Authors: Prof. BOGDANOV, Alexander (St. Petersburg University St. Petersburg, Russia); Dr KHVATOV, Valery (DGT Technologies AG., Toronto, Canada); Mr CHIANG, Yueh (St. Petersburg University St. Petersburg, Russia); Prof. SHCHEGOLEVA, Nadezhda (St. Petersburg University St. Petersburg, Russia)

Presenter: Mr CHIANG, Yueh (St. Petersburg University St. Petersburg, Russia)

Session Classification: Round Table on the Areas of Work of the SPbSU-JINR Joint Scientific and Educational Laboratory