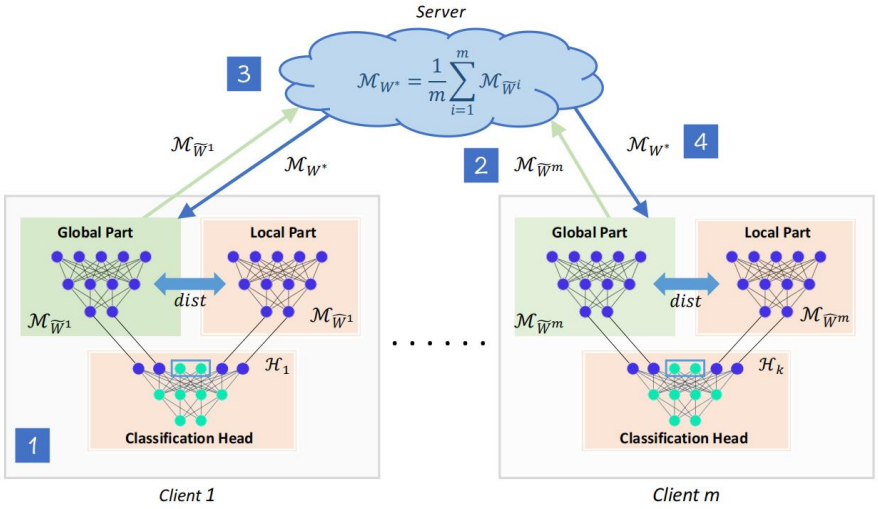
Federated Learning-Outcome Prediction with Multi-layer Privacy Protection

Yupei ZHANG, Yuxin LI, Yifei WANG, Shuangshuang WEI, Yunan XU, Xuequn SHANG

Frontiers of Computer Science, DOI: 10.1007/s11704-023-2791-8

Problems & Ideas

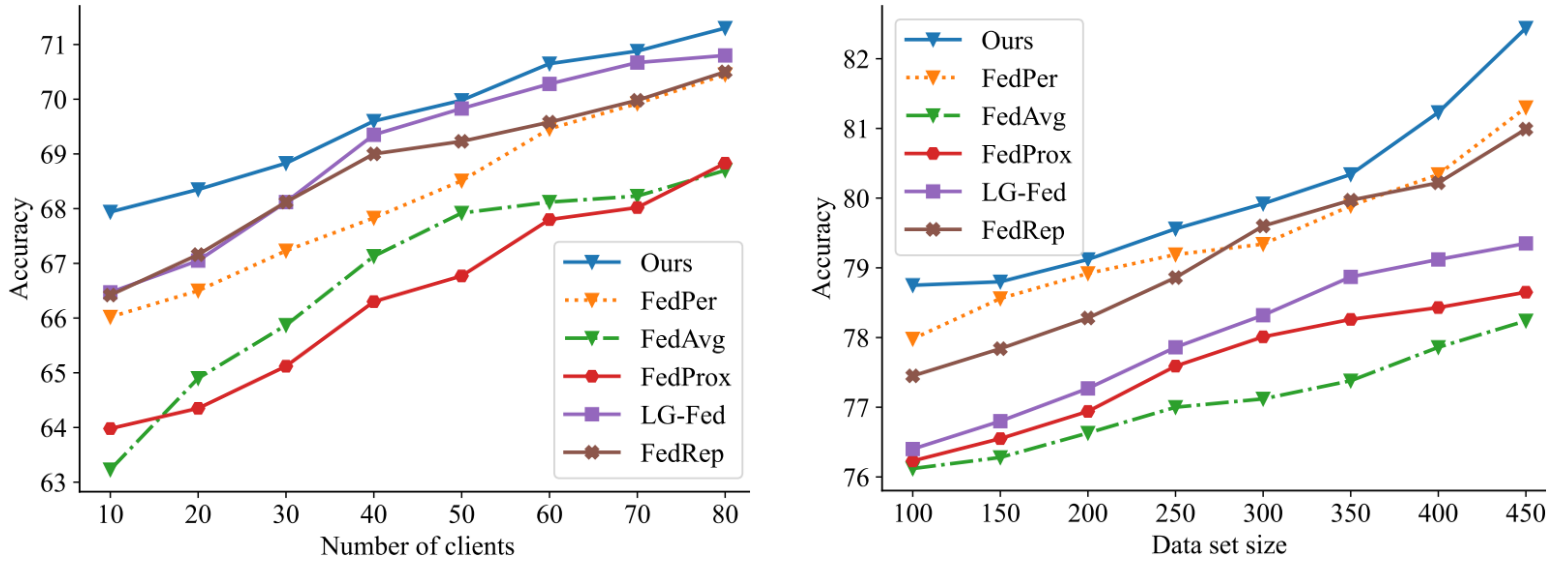
- Problems of conventional Learning-outcome prediction approaches:
  - Many studies have contributed to developing effective models while often suffering from data shortage and weak generalization to various institutions due to the privacy-protection issue.
- Ideas: A distributed grade prediction model using the federated learning (FL) framework that preserves the private data of clients and communicates with others through a global model.



The FecMap model trained in an iterative manner. An FL communication is completed by (1) training the local model, (2) uploading to the server, (3) computing the global model, and (4) updating the local model.

Main Contributions

- Contributions:
  - LSL divides the feature space of the local client into a local subspace and a global subspace by introducing the maximization subspace separation criterion.
  - MPP divides the local client's privacy features into a multi-level privacy hierarchy by partitioning the model parameters to learn model-shareable features and not-allowed features.
  - A FL framework, i.e., FecMap, is proposed for LOP, which is carried out online.



Parameter discussion on the number of clients n (left) and the data set size d (the number of samples per client, right) in the proposed model and other comparison methods.