AutoML in Federated Learning

1. General Info

Project Title: AutoML in Federated Learning

Contact Person: Azade Farshad, Yousef Yeganeh

Contact Email: azade.farshad@tum.de, y.yeganeh@tum.de

2. Project Abstract

The goal of this project is to investigate AutoML techniques[1] to improve performance of Federated Learning[3]. AutoML techniques are methods such as meta-learning (learning to learn) and hyperparameter optimization which aim to automate the learning process using meta-features. We use either PyTorch or Tensorflow Federated as our platform, and we work on benchmark datasets like mnist, fashion-mnist or cifar-10 and medical imaging datasets like HAM10k or any dataset of choice.

3. Background and Motivation

In the last few years, Federated Learning (FL) emerged as the state-of-the-art in privacy oriented machine learning. It is designed to train models over remote data on distributed clients without having access to the data. The models are trained privately and updates are sent to a server for aggregation. Its applications range from Gboard (Google Keyboard App) on mobile devices to hospitals that want to share their knowledge while keeping patients' privacy.
FL has faced many challenges[2], and we want to use AutoML to increase its performance. AutoML includes many techniques in ML that have been well adopted for different tasks, but it is a fairly new approach to use AutoML techniques in FL. Tackling these approaches requires well-trained students who have a good understanding of standard ML approaches, and are already comfortable with implementing them.

4. Technical Prerequisites

- Good background in statistics
- Good background in machine learning, deep learning
- Good skills in Python
- Good skills in PyTorch

5. Benefits:

- Possible novelty of the research
- Possible publication

6. Students' Tasks Description

Students' tasks would be the following:

Groups 1 & 2:

- Understanding the underlying methods
- Choosing the baseline federated learning framework

- Implementing and adapting the FL framework to AutoML
- Choosing the appropriate AutoML techniques and performance measures
- Running the evaluation metrics on a toy dataset
- Running the evaluation metrics on a medical imaging dataset
- Testing and documentation.

7. Work-packages and Time-plan:

	Description	#Students	From	To
WP1	Familiarize with the literature.	4	01.11	08.11
WP2	Familiarize with the required frameworks. Come up with a detailed time-plan (gantt)	4	08.11	15.11
WP3	Implementing and adapting the FL framework to AutoML	4	15.11	29.11
WP4	Choosing the appropriate AutoML techniques and performance measures	4	29.11	03.12
WP5	Evaluation of the implemented method	4	03.12	17.12
M1	Intermediate Presentation II	4	17.12.2020	
WP6	Implementing the chosen AutoML techniques and performance measures	2 / 2	17.12	15.01
WP7	Familiarize with clinical data, data pre-processing	4	15.01	29.01
WP8	Implement and Evaluate WP3 & WP6 on medical data	4	29.01	12.02
WP9	Testing and Documentation	4	12.02	26.02
M2	Final Presentation	4	26.02.2021	

References

1. Hutter, F., Kotthoff, L. and Vanschoren, J., 2019. *Automated machine learning: methods, systems, challenges* (p. 219). Springer Nature.
2. Li, T., Sahu, A.K., Talwalkar, A. and Smith, V., 2020. Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), pp.50-60.
3. Sattler, F., Wiedemann, S., Müller, K.R. and Samek, W., 2019. Robust and communication-efficient federated learning from non-iid data. *IEEE transactions on neural networks and learning systems*.
4. He, C., Li, S., So, J., Zhang, M., Wang, H., Wang, X., Vepakomma, P., Singh, A., Qiu, H., Shen, L. and Zhao, P., 2020. Fedml: A research library and benchmark for federated machine learning. *arXiv preprint arXiv:2007.13518*.
5. Khodak, M., Balcan, M.F.F. and Talwalkar, A.S., 2019. Adaptive gradient-based meta-learning methods. In *Advances in Neural Information Processing Systems* (pp. 5917-5928).

6. Jiang, Y., Konečný, J., Rush, K. and Kannan, S., 2019. Improving federated learning personalization via model agnostic meta learning. *arXiv preprint arXiv:1909.12488*.