Is Federated Learning *Still* Alive in the Foundation Model Era?

Nathalie Baracaldo

IBM Research
baracald@us.ibm.com

Introduction

Federated learning (FL) has arisen as an alternative to collecting large amounts of data in a central place to train a machine learning (ML) model. FL is privacy-friendly, allowing multiple parties to collaboratively train an ML model without exchanging or transmitting their training data (Baracaldo and Xu 2022). For this purpose, an *aggregator* iteratively coordinates the training process among parties, and parties simply share with the aggregator *model updates*, which contain information pertinent to the model such as neural network weights. Besides privacy, generalization has been another key driver for FL: parties who do not have enough data to train a good performing model by themselves can now engage in FL to obtain an ML model suitable for their tasks. Products and real applications in the industry and consumer space have demonstrated the power of this learning paradigm.

Recently, foundation models have taken the AI community by storm, promising to solve the shortage of labeled data. A foundation model is a powerful model that can be recycled for a variety of use cases by applying techniques such as *zero-shot* learning and full or parameter-efficient fine tuning. The premise is that the amount of data required to fine tune a foundation model for a new task is much smaller than fully training a traditional model from scratch. The reason why this is the case is that a *good* foundation model has already learned relevant general representations, and thus, adapting it to a new task only requires a minimal number of additional samples. This raises the question: *Is FL still alive in the era of foundation models?*

In this talk, I will address this question. I will present some use cases where FL is very much alive (Castiglia et al. 2023; Kadhe et al. 2023). In these use cases, finding a foundation model with a desired representation is difficult if not impossible. With this pragmatic point of view, I hope to shed some light into a real use case where disparate private data is available in isolation at different parties and where labels may be located at a single party that doesn't have any other information, making it impossible for a single party to train a model on its own. Furthermore, in some *vertically-partitioned* scenarios, cleaning data is not an option due to privacy-related reasons and it is not clear how to apply foundation models. Finally, I will also go over a few other requirements that are often overlooked, such as unlearning of data (Halimi et al. 2022) and its implications for the lifecycle management of FL and systems based on foundation models.

Nathalie Baracaldo leads the AI Security and Privacy Solutions team and is a Research Staff Member at IBM's Almaden Research Center in San Jose, CA. Nathalie is passionate about delivering machine learning solutions that are highly accurate, withstand adversarial attacks and protect data privacy. She focuses on multiple areas including federated learning, where models are trained without directly accessing training data, and adversarial machine learning, where defenses are designed to withstand potential attacks to the machine learning pipeline and most recently unlearning. Nathalie is the Principal Investigator for the DARPA program "Guaranteeing AI Robustness Against Deception" (GARD). In 2022, Nathalie co-edited the book "*Federated Learning: A Comprehensive Overview of Methods and Applications*". In 2020, Nathalie received the *IBM Master Inventor* distinction for her contributions to the IBM intellectual property and innovation. Nathalie received her Ph.D. degree from the University of Pittsburgh, USA in 2016.

References

Baracaldo, N.; and Xu, R. 2022. Protecting Against Data Leakage in Federated Learning: What Approach Should You Choose? In *Federated Learning: A Comprehensive Overview of Methods and Applications*, 281–312. Springer.

Castiglia, T.; Zhou, Y.; Wang, S.; Kadhe, S.; Baracaldo, N.; and Patterson, S. 2023. LESS-VFL: Communication-Efficient Feature Selection for Vertical Federated Learning. *ICML 2023*.

Halimi, A.; Kadhe, S.; Rawat, A.; and Baracaldo, N. 2022. Federated unlearning: How to efficiently erase a client in fl? *arXiv preprint arXiv:2207.05521*.

Kadhe, S. R.; Ludwig, H.; Baracaldo, N.; King, A.; Zhou, Y.; Houck, K.; Rawat, A.; Purcell, M.; Holohan, N.; Takeuchi, M.; et al. 2023. Privacy-Preserving Federated Learning over Vertically and Horizontally Partitioned Data for Financial Anomaly Detection. *arXiv preprint arXiv:2310.19304*.