Model-Centric Federated Machine Learning

AUTHORS, Institute xx, Country

Tranditional Federated Machine Learning follows a server-domincated training paradigm which narrows the application scenarios of federated learning and decreases the enthusiasm of data holders to participate.

CCS Concepts: • **Computer systems organization → Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: datasets, neural networks, gaze detection, text tagging

ACM Reference Format:
Authors. 2018. Model-Centric Federated Machine Learning. *Proc. ACM Meas. Anal. Comput. Syst.* 37, 4, Article 111 (August 2018), 2 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Introduction: Federated Learning [3].

1.1 Related Surveys

In recent years, federated learning has become a buzzword in various fields, leading to the emergence of numerous FL studies. These works can be classified into two primary categories: FL system design and FL appllications. The initial architectures and concepts for FL systems were summaried by Yang *et al.* [9]. They categorize FL into horizontal FL, vertical FL and federated transfer learning based on the distribution characteristics of data, which are written in IEEE Standard 3652.1-2020 [6, 8]. Following this, an increasing number of surveys have emerged focusing on enhancing FL system design. From the algorithmic perspective, personlized FL [2, 7] aims to learn personlized models for each client to address the challenge of statistical heterogeneity. Besides, the privacy-perserving model aggregation protocols of FL systems also been widely studied and sumaried by [1, 4, 5, 10] Furthermore, Many advance FL architectures had been proposed and summaried, such as Decent Some surveys

1.2 Distinction of Our Survey

However,

Federated leanring is promising

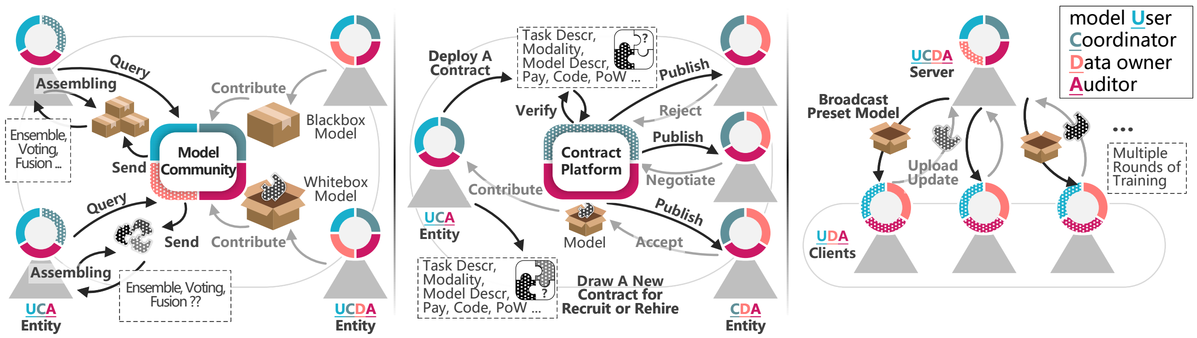
Three cooperation frameworks: query-based FL, contract-based FL, writ-based FL

ACKNOWLEDGMENTS

ACK.

Author's address: Authors, Institute xx, City, Country, @mail.com.

2476-1249/2018/8-ART111 $15.00
https://doi.org/XXXXXXX.XXXXXXX



(a) Query-based FML (b) Contract-based FML (c) Traditional FML

Fig. 1. Cooperation frameworks of FML.

REFERENCES

[1] Ahmed El Ouadrhiri and Ahmed Abdelhadi. 2022. Differential privacy for deep and federated learning: A survey. *IEEE Access* 10 (2022), 22359–22380. https://doi.org/10.1109/ACCESS.2022.3151670

[2] Viraj Kulkarni, Milind Kulkarni, and Aniruddha Pant. 2020. Survey of personalization techniques for federated learning. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 794–797. https://doi.org/10.1109/WorldS450073.2020.9210355

[3] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine* 37, 3 (2020), 50–60.

[4] Ziyao Liu, Jiale Guo, Wenzhuo Yang, Jiani Fan, Kwok-Yan Lam, and Jun Zhao. 2022. Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data (TBD)* (2022), 1–20. https://doi.org/10.1109/TBDATA.2022.3190835

[5] Lingjuan Lyu, Han Yu, and Qiang Yang. 2020. Threats to federated learning: A survey. *arXiv preprint arXiv:2003.02133* (2020).

[6] IEEE Computer Society. 2021. IEEE Guide for Architectural Framework and Application of Federated Machine Learning. *IEEE Std 3652.1-2020* (2021), 1–69. https://doi.org/10.1109/IEEESTD.2021.9382202

[7] Alysa Ziying Tan, Han Yu, Lizhen Cui, and Qiang Yang. 2022. Towards personalized federated learning. *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)* (2022), 1–17. https://doi.org/10.1109/TNNLS.2022.3160699

[8] Qiang Yang, Lixin Fan, Richard Tong, and Angelica Lv. 2021. IEEE Federated Machine Learning. *IEEE Federated Machine Learning - White Paper* (2021), 1–18.

[9] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)* 10, 2 (2019), 1–19. https://doi.org/10.1145/3298981

[10] Xuefei Yin, Yanming Zhu, and Jiankun Hu. 2021. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR)* 54, 6 (2021), 1–36. https://doi.org/10.1145/3460427

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009