Computer Science and Application 计算机科学与应用, 2025, 15(3), 102-107
Published Online March 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.153062

Hans汉斯

联邦学习综述

温泽诚，陈　磊

广东工业大学数学与统计学院，广东 广州

收稿日期：2025年2月13日；录用日期：2025年3月12日；发布日期：2025年3月19日

摘　要

随着隐私保护和机器学习数据量需求的攀升，传统机器学习面临诸多挑战。联邦学习作为一种去中心化的分布式机器学习策略受到了广泛的关注。联邦学习通常由中央服务器发起，诸多形态、性能各异的边缘客户端设备共同参与。在联邦学习过程中，客户端设备不需要将私有数据共享给任何一方，从而起到隐私保护以及防止数据泄露的作用。不仅如此，联邦学习具备分布式机器学习的特点，可以有效发挥边缘设备的存储资源和计算资源。本文系统性地回顾了联邦学习的基本概念，并对联邦学习的实际应用和发展作了凝结性介绍，总结了联邦学习当前面临的数据异质性、掉队者效应、隐私保护等挑战，以促进联邦学习的发展和应用。

关键词

隐私保护，去中心化，分布式机器学习，联邦学习

A Review of Federated Learning

Zecheng Wen, Lei Chen

School of Mathematics and Statistics, Guangdong University of Technology, Guangzhou Guangdong

Received: Feb. 13th, 2025; accepted: Mar. 12th, 2025; published: Mar. 19th, 2025

Abstract

With the increasing demand for privacy protection and large-scale machine learning datasets, traditional machine learning faces numerous challenges. As a decentralized and distributed machine learning paradigm, Federated Learning (FL) has garnered widespread attention. FL is typically initiated by a central server, with various different edge client devices participating collaboratively. During the FL process, client devices do not need to share their private data with any party, thereby ensuring privacy protection and preventing data leakage. Moreover, FL leverages the characteristics of distributed machine learning, effectively utilizing the storage and computational resources of edge devices. This paper systematically reviews the fundamental concepts of FL and provides a

文章引用: 温泽诚, 陈磊. 联邦学习综述[J]. 计算机科学与应用, 2025, 15(3): 102-107.
DOI: 10.12677/csa.2025.153062

concise overview of its practical applications and developments. Additionally, it summarizes key challenges in FL, including data heterogeneity, straggler effects, and privacy protection, to promote further advancements and applications of FL.

Keywords

Privacy Protection, Decentralized, Distributed Machine Learning, Federated Learning

1. 引言

自 FedAvg [1]被提出以来，联邦学习便受到了广泛的关注和应用。传统的机器学习策略在当下数据量爆炸式增长以及隐私保护备受呼吁的背景下面临诸多挑战。一方面，传统机器学习往往需要庞大的数据量支撑才能获取性能稳定乃至出众的模型，这一点恰恰受到各地区隐私保护条例的限制；另一方面，传统机器学习依赖集中存储的方式统一管理数据，大批量的数据对中央服务器带来严重的存储开销，同时，集中存储面临数据泄露、数据损坏或丢失、数据备份以及数据完整性等一系列问题。为了应对上述挑战，联邦学习应运而生。联邦学习是一种分布式机器学习策略，通过多方协作训练的方式，联合多方的计算资源和数据资源完成建模及模型训练，在多方协作训练的过程中，中央服务器作为联邦学习的发起方，并不会收集、存储多方的原始数据资源。联邦学习在保证充足数据量支撑的条件下，避开了数据集中存储带来的风险，有效保护多方数据隐私，是极为高效的开源节流的机器学习策略。当前联邦学习广泛应用于金融[2]、医疗[3]、推荐系统[4]、物联网[5]、智能驾驶[6]等领域，比如在医疗领域，各医院通过联邦学习可以获得有效的医学成像分析模型与此同时不需要将患者数据共享给他方医院或第三方机构；在推荐系统领域，诸如各大电商、短视频平台，在不存储用户数据的前提下，通过联邦学习可以获取更具有个性化的推荐系统，为用户推荐可能喜欢的产品或短视频。本文将深入探讨联邦学习的核心思想、发展、当前的挑战以及未来展望，为研究者提供一个新视角，帮助其理解联邦学习的基本概念。

2. 联邦学习概述

联邦学习的核心思想是由中央服务器发起联邦学习，中央服务器下发初始模型给多方客户端，客户端接收初始模型，使用本地计算资源和私有数据完成本地数据信息提取，将完成本地数据信息提取的模型上传给中央服务器进行模型整合，以此在不接触多方私有数据的前提下，完成多方数据信息的汇集。中央服务器将聚合后的全局模型再次下发给参与联邦学习的多方客户端作为新一轮联邦学习的初始模型，重复上述过程直至完成预期目标，如图 1 所示。

联邦学习保证了数据的本地化管理，有效规避了数据传输带来的数据泄露、数据完整性等问题，降低了集中存储数据、管理数据的风险，并且发挥了分布式训练的优势，充分利用了多方设备的计算资源。联邦学习作为一种分布式机器学习策略，与传统的分布式学习有显著区别：

1) 联邦学习关注隐私保护。联邦学习中客户端设备对私有数据有绝对的控制权和管理权，中央服务器并不能收集、存储客户端私有数据；传统分布式机器学习中，中央结点统一管理全局结点以及数据划分，对全局数据享有绝对管理权。

2) 联邦学习对客户端设备有更高的包容度。参与联邦学习的客户端设备可以是手机、平板、智能家

居、网关又或者是交通电子眼、新能源电车车机等，这些设备呈现出算力不一、资源不一、类型不一的特点；传统分布式机器学习通常布局在机房中，除中央节点外，参与分布式机器学习的全局工作结点在算力、资源和类型上都相对一致。

3) 应对的挑战不同。联邦学习是在分布式的基础框架上的进一步扩展，关注隐私保护以及模型的信息提取能力和信息整合能力；分布式机器学习重点是提升大数据背景下的计算效率，通过分配任务、数据到全局结点进行并行训练，加速模型收敛，降低时间成本。

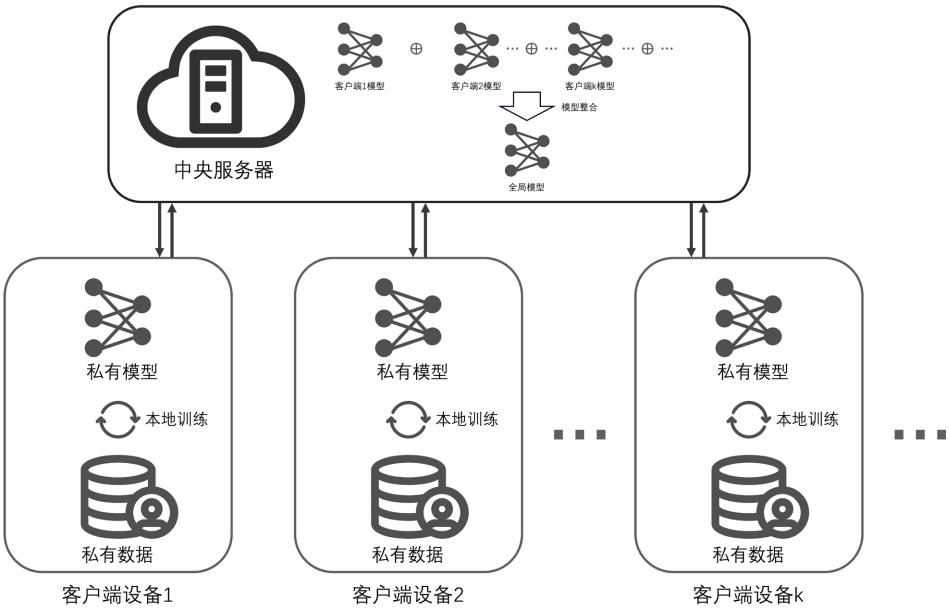

Figure 1. Federal learning framework
图 1. 联邦学习框架

3. 联邦学习的发展

联邦学习概念最早由 Google 研究团队在 2016 年提出[1]，中央服务器不收集客户端设备数据的前提下，在参与联邦学习的客户端设备上完成模型训练，从而保护客户端设备隐私。FedAvg 是使用最广的联邦学习方法，中央服务器只需要完成对客户端设备上传的参数求均值，而不需要参与到模型训练和数据管理过程中。然而，现实场景的非独立同分布数据导致模型无法稳定收敛，因此研究者引入了正则项来控制非独立同分布数据造成的模型偏差，如 FedProx [7]在模型更新过程中通过正则化项不断调整全局模型和客户端设备私有模型之间的偏差；SCAFFOLD [8]侧重于避免本地模型偏离全局模型，FedDyn [9]则将历史更新作为校准偏差的指标，而不是仅考虑当前的模型更新方向。

个性化联邦学习[10]是联邦学习的又一里程碑，个性化联邦学习旨在为每个客户端设备定制个性化模型以适应本地数据分布，如 LG-FedAvg [11]将模型的顶层参数作为共享参数，将模型的底层参数作为个性化参数，FedRod [12]的客户端设备除了将整个私有模型共享之外还会维护一个私有的个性化分类器，FedBABU [13]的客户端设备前期持续对私有模型的底层参数进行更新及共享，在后期通过微调获取个性化模型顶层。个性化联邦学习不仅能够训练适应自身数据分布的个性化模型，而且不影响全局联邦优化。

随着深度学习的持续推进和大模型时代的到来，大模型联邦学习[14]成为时下的研究热点，相关研究尝试在联邦学习的框架下完成大模型训练，在理想场景下该设想可以充分利用边缘客户端设备的数据。此外，联邦学习配合区块链[15]可以进一步加强隐私保护，同时使联邦学习具备区块链的可溯源性。

4. 联邦学习当前的挑战

4.1. 数据异质性

理想的联邦学习场景中，数据是独立同分布的，经典的联邦学习方法在此类场景中可以训练出性能优越的模型。但是在实际场景中，多方客户端设备的数据往往是非独立同分布的，这对模型收敛产生严峻的挑战[16]。非独立同分布数据使多方客户端设备训练的模型性能不一，进而导致中央服务器聚合的全局模型难以稳定、高效收敛。定制个性化参数和知识蒸馏是两个常用的应对数据异质性问题的策略。定制个性化参数可以有效适应本地数据分布，知识蒸馏则可以高效利用全局共享信息，但两种策略都会造成额外的计算开销。

4.2. 掉队者效应

当前的联邦学习研究主要基于全局参与这一假设。在现实的联邦学习场景中，由于多方客户端的硬件、网络带宽、数据量等因素存在差异。具体来讲，硬件差异会造成算力的差异，进而造成不同客户端设备训练效率的差异；网络带宽差异会造成客户端设备从中央服务器下载模型、上传模型到中央服务器的效率差异；数据量差异表现为数据量大的客户端设备相比数据量小的客户端设备需要更多的计算资源，进而导致不同客户端设备的私有模型收敛程度不一。这些效率低的客户端设备便是联邦学习中的“掉队者”，掉队者会为中央服务器聚合模型从过程、结果层面都造成严重的破坏[17]。异步更新策略通过对异常客户端的模型作丢弃或降低权重的处理可以有效应对掉队者问题，但是异步更新策略并不能使收益最大化且在过程中容易造成过多的时间开销。

4.3. 隐私保护及安全

联邦学习的隐私保护主要通过以下几种方式实现：第一，联邦学习框架自身得天独厚的设计优势，也就是中央服务器不需要收集、存储客户端设备数据；第二，通过差分隐私引入噪声[18]，使攻击者无法辨别攻击对象的差异；第三，通过同态加密运算实现对共享参数、数据的加密[19]。差分隐私和同态加密是联邦学习中使用较为广泛的隐私保护策略，但是会产生额外的计算开销和通信开销，在客户端设备计算、存储资源受限的条件下，亟需更高效、轻量化的隐私保护策略。

5. 联邦学习的未来展望

5.1. 个性化联邦学习

个性化联邦学习的有效性已经得到广泛的验证。当前的个性化联邦学习研究主要基于全局客户端设备拥有相同的模型结构这一假设，未来可以进一步推进个性化策略，根据客户端设备的自身条件，自适应匹配合适的模型结构，此方向的关键难点之一是中央服务器如何有效整合异构模型。此外，可以设计主动调整策略，客户端设备根据历史更新过程自主调整更适合本地模型更新的超参数。

5.2. 联邦学习与大模型

大模型在近几年的研究中热度极高，尽管大模型本身和联邦学习理念截然不同，联邦学习主张轻量化模型以减轻边缘设备的计算、存储和通信开销，显然，大模型并不能保证这一点，因为大模型主要依靠庞大的模型结构和参数量解析更多维度的数据信息。未来，可以通过联邦学习进行信息整合，由中央服务器中的大模型进行信息提炼和学习，进而通过知识蒸馏生成效率更高的轻量化模型，发挥联邦学习和大模型的各家所长；此外，可以通过模型压缩，对大模型进行剪枝、蒸馏，使大模型能在资源受限的客户端设备上训练，再通过联邦学习进行信息的整合。

6. 总结

联邦学习自2016年提出以来，在隐私保护、分布式机器学习、多方协作方面备受关注并已取得了巨大突破。在医疗、金融、推荐系统、物联网、智能驾驶等领域也受到了广泛应用。然而，当前的联邦学习仍然面临数据异构性、掉队者效应、隐私保护等挑战。异构数据和掉队者效应都会对模型的整合、收敛造成破坏，隐私保护亟需更高效的策略来防止数据泄露、隐私攻击等问题，我们仍需要进一步降低计算开销、存储开销、通信开销等损耗，未来的研究方向需要围绕这几个方面作进一步扩展。联邦学习的发展将推动更安全、高效的机器学习、深度学习时代。

参考文献

[1] McMahan, B., Moore, E., Ramage, D., *et al.* (2017) Communication-Efficient Learning of Deep Networks from Decentralized Data. arXiv: 1602.05629.

[2] Byrd, D. and Polychroniadou, A. (2020) Differentially Private Secure Multi-Party Computation for Federated Learning in Financial Applications. *Proceedings of the First ACM International Conference on AI in Finance*, New York, 15-16 October 2020, 1-9. https://doi.org/10.1145/3383455.3422562

[3] Xu, J., Glicksberg, B.S., Su, C., Walker, P., Bian, J. and Wang, F. (2020) Federated Learning for Healthcare Informatics. *Journal of Healthcare Informatics Research*, **5**, 1-19. https://doi.org/10.1007/s41666-020-00082-4

[4] Muhammad, K., Wang, Q., O'Reilly-Morgan, D., Tragos, E., Smyth, B., Hurley, N., *et al*. (2020) FedFast: Going Beyond Average for Faster Training of Federated Recommender Systems. *Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 6-10 July 2020, 1234-1242. https://doi.org/10.1145/3394486.3403176

[5] Nguyen, D.C., Ding, M., Pathirana, P.N., Seneviratne, A., Li, J. and Vincent Poor, H. (2021) Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, **23**, 1622-1658. https://doi.org/10.1109/comst.2021.3075439

[6] Zeng, T., Semiari, O., Chen, M., Saad, W. and Bennis, M. (2022) Federated Learning on the Road Autonomous Controller Design for Connected and Autonomous Vehicles. *IEEE Transactions on Wireless Communications*, **21**, 10407-10423. https://doi.org/10.1109/twc.2022.3183996

[7] Li, T., Sahu, A.K., Zaheer, M., *et al*. (2020) Federated Optimization in Heterogeneous Networks. *Machine Learning and Systems* (*MLSys*), **2**, 429-450.

[8] Karimi Reddy, S.P., Kale, S., Mohri, M., *et al*. (2020) SCAFFOLD: Stochastic Controlled Averaging for Federated Learning. arXiv: 1910.06378.

[9] Acar D A E, Zhao Y, Navarro R M, *et al*. (2021) Federated Learning Based on Dynamic Regularization. arXiv: 2111.04263.

[10] Tan, A.Z., Yu, H., Cui, L. and Yang, Q. (2023) Towards Personalized Federated Learning. *IEEE Transactions on Neural Networks and Learning Systems*, **34**, 9587-9603. https://doi.org/10.1109/tnnls.2022.3160699

[11] Liang, P.P., Liu, T., Ziyin, L., *et al*. (2019) Think Locally, Act Globally: Federated Learning with Local and Global Representations. https://arxiv.org/abs/2001.01523

[12] Chen, H.Y. and Chao, W.L. (2022) On Bridging Generic and Personalized Federated Learning for Image Classification. arXiv: 2107.00778.

[13] Oh, J., Kim, S. and Yun, S.Y. (2022) FedBABU: Towards Enhanced Representation for Federated Image Classification. arXiv: 2106.06042.

[14] Chen, C., Feng, X., Zhou, J., Yin, J. and Zheng, X. (2023) Federated Large Language Model: A Position Paper. arXiv: 2307.08925.

[15] Wang, Z. and Hu, Q. (2021) Blockchain-Based Federated Learning: A Comprehensive Survey. arXiv: 2110.02182.

[16] Li, Q., Diao, Y., Chen, Q. and He, B. (2022) Federated Learning on Non-IID Data Silos: An Experimental Study. 2022 *IEEE 38th International Conference on Data Engineering* (*ICDE*), Kuala Lumpur, 9-12 May 2022, 965-978. https://doi.org/10.1109/icde53745.2022.00077

[17] Chai, Z., Chen, Y., Zhao, L., Cheng, Y. and Rangwala, H. (2020) FedAT: A Communication-Efficient Federated Learning Method with Asynchronous Tiers under Non-IID Data.

[18] Wei, K., Li, J., Ding, M., Ma, C., Yang, H.H., Farokhi, F., *et al*. (2020) Federated Learning with Differential Privacy: Algorithms and Performance Analysis. *IEEE Transactions on Information Forensics and Security*, **15**, 3454-3469.

https://doi.org/10.1109/tifs.2020.2988575

[19] Wibawa, F., Catak, F.O., Kuzlu, M., Sarp, S. and Cali, U. (2022) Homomorphic Encryption and Federated Learning Based Privacy-Preserving CNN Training: COVID-19 Detection Use-Case. *EICC* 2022: *Proccedings of the European Interdisciplinary Cybersecurity Conference*, Barcelona, 15-16 June 2022, 85-90. https://doi.org/10.1145/3528580.3532845