横向联邦学习:研究现状、系统应用与挑战

吴文泰[1] 吴应良[2] 林伟伟[3] 左文明[2),4)]

[1)](暨南大学信息科学技术学院 广州 510632)

[2)](华南理工大学电子商务系 广州 510006)

[3)](华南理工大学计算机科学与工程学院 广州 510006)

[4)](人工智能与数字经济广东省实验室(广州) 广州 510335)

摘 要 随着数据和算力向网络边缘下沉,人工智能应用的研发愈加依赖隐私敏感的用户数据。在这一趋势的推动下,联邦学习因其强调隐私保护的特性而逐渐成为一个广泛应用的分布式机器学习框架。作为联邦学习的原始范式,横向联邦学习(Horizontal Federated Learning,HFL)具有扩展能力强和使用场景广泛等特点,因此是近年来该领域的研究重心,同时在产业界相关需求的驱动下有着十分广泛的应用前景。横向联邦学习的研究涉及机器学习、分布式系统、无线通信和信息安全等多个学术领域,从研究动机到技术方法都呈现多样化,但现有文献未能展现相关研究现状的全貌。此外,横向联邦学习相关技术的发展催化出了一系列开源系统框架、公开数据集以及多种场景下的应用,对进一步研究与实践都具有参考价值。为此,本文对横向联邦学习的研究现状和系统应用进行综合性调研:首先,对相关文献按照研究目标和技术角度进行全面地分类梳理,从多领域视角分析了各分支的研究现状;其次,从应用实践的视角,对比分析了面向横向联邦学习的主流系统框架与代码库、描述了数据准备方法以及典型的应用场景。在此基础上,阐明了横向联邦学习算法研究和系统应用面临的 6 个关键挑战,为如何缩小相关研究与系统实践之间的鸿沟提供了新的参考。

关键词 横向联邦学习;数据隐私;分布式系统;机器学习;人工神经网络

中图法分类号 TP181 **DOI 号** 10.11897/SP.J.1016.2025.00035

Horizontal Federated Learning: Research Status, System Applications and Open Challenges

WU Wen-Tai[1] WU Ying-Liang[2] LIN Wei-Wei[3] ZUO Wen-Ming[2),4)]

[1)](College of Information Science and Technology, Jinan University, Guangzhou 510632)

[2)](Department of Electronic Business, South China University of Technology, Guangzhou 510006)

[3)](School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006)

[4)](Pazhou Laboratory, Guangzhou 510335)

Abstract With the decentralization of data and computing power, a growing number of AI-powered applications are now built on privacy-sensitive user data. Driven by this trend, Federated Learning (FL) has emerged as one of the most prevailing distributed learning frameworks that feature strong privacy protection. As the canonical FL paradigm, Horizontal Federated Learning (HFL) has been the focus of research in the academia and also attracted broad attention from the industry due to its strong scalability and compatibility to a diversity of application scenarios. The spectrum of HFL spans across several fields of research including machine learning, distributed systems,

收稿日期:2022-08-25;在线发布日期:2024-01-04。本课题得到国家自然科学基金(61872150,62072187,62402198)、国家社会科学研究基金后期资助项目(20FGLB034)、广东省基础与应用基础研究重大项目(2021B0101420002)、广东省自然科学基金面上项目(2020A1515010830)、人工智能与数字经济广东省实验室(广州)青年学者项目(PZL2021KF0027)资助。**吴文泰**,博士,副教授,主要研究领域为协同机器学习、分布式系统、可持续计算。E-mail:wentai.wu@foxmail.com。**吴应良**(通信作者),博士,教授,博士生导师,主要研究领域为信息系统、数据驱动的决策、数字生态系统。E-mail:bmylwu@scut.edu.cn。**林伟伟**,博士,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为云计算、大数据、人工智能应用技术等。**左文明**,博士,教授,博士生导师,主要研究领域为电子商务、数据挖掘与商务智能、数字经济等。

wireless communication and information security, which results in diversified research motivation and methodologies. However, an exhaustive view of the domain is still missing. In addition, the advance of technologies in these fields catalyzes rapid development of libraries, open platforms and practical systems, which in turn facilitates further research and practice. In view of this, we present a comprehensive review of the horizontal HFL paradigm. We first review recent studies on HFL following five different branches. Then, we shift the focuses to practice-related perspectives, where we introduce popular libraries, frameworks and platforms that facilitate HFL research, applications and systems, and public datasets for evaluating HFL algorithms. By analyzing the advance in the literature and the demands in practice, we describe several open challenges in the research and development of HFL, which can provide insights for bridging the gap between the research outcome and system practice.

Keywords horizontal federated learning; data privacy; distributed systems; machine learning; artificial neural networks

1 引 言

大数据时代背景下,在人工智能(Artificial Intelligence,AI)应用不断涌现的潮流背后,是"数据驱动模型"的思想演变和机器学习(Machine Learning,ML)技术的日新月异。近年来,机器学习的主流范式已经发生了转变(paradigm shift)[1],深度学习模型在计算机视觉、自然语言处理、自动语音识别和图处理等现实任务中都表现出了优异的性能[2-5]。这一方面得益于深度学习模型的复杂性带来的强大表征抽象能力,另一方面则高度依赖大规模的训练数据集和训练样本的丰富度。

在数据和计算需求剧增的趋势下,集中式的模型训练方法面临时间成本过高和明显的资源瓶颈等问题[6]。为此,基于梯度的机器学习算法(或称训练算法)的并行化和分布式优化成为了研究的焦点。虽然传统的分布式训练算法能够有效实现数据并行[7-9],但是通常存在训练数据共享或交换,而且高频率的梯度上传和模型下载操作造成高昂的通信开销,同时增加了源数据信息泄露的风险[10-11]。随着欧盟地区从 2018 年 5 月开始推行的《通用数据保护条例》(General Data Protection Regulation,GDPR①),各国家和地区纷纷加强或计划加强对区域内用户数据的管制②,这使得要求集中式访问数据的传统模型训练方法在自动驾驶、数字医疗和物联网等用户隐私敏感的场景下难以实现。随着 5G 技术的成熟和端侧设备性能的不断提升,AI 应用已经普及到了网络边缘,越来越多的终端设备已经具备执行机器学习任务的能力[12]。与此同时,它们又是业务相关数据(如用户数据和生产数据)的载体——据 Gartner 预测,到 2025 年 75% 的全球数据将由散布在数据中心以外的物联网设备产生[13]。

如何组织分布的设备、受保护的数据源以开展高效的分布式机器学习是当前的研究热点。谷歌(Google)提出了联邦优化(federated optimization)的概念[14],并进一步提出了称为联邦学习(Federated Learning,FL)的分布式模型训练框架[15]和相应的系统设计[16]。同样基于参数服务器(Parameter Server,PS)为中心的架构,联邦学习与传统分布式机器学习的主要区别在于:

(1)无数据共享。数据完全分散在各客户端节点且只允许本地访问,系统中各实体(包括参数服务器和客户端)间不允许交换源数据;

(2)加密模型交换。参数服务器和客户端之间信息交换的内容是模型(或其更新量),并且一般会经过加密或掩码等技术处理以避免信息泄露;

(3)低通信开销。每一轮中,客户端对本地模型进行多次更新后才与参数服务器进行一次模型交换,通信频率远低于基于梯度交换的传统方法。

由于上述特性,联邦学习非常适合隐私敏感的计算场景,其最初的设计理念是联合特征空间相同的数据来协同优化模型,因此严格遵照这一设定的联邦学习范式在相关文献和标准中被定义为横向联邦学习(Horizontal Federated Learning,HFL),其典型系统组织形式如图 1 所示。

① General Data Protection Regulation. https://gdpr-info.eu/

② 中国于 2021 年 9 月开始施行《中华人民共和国数据安全法》、2021 年 11 月开始施行《中华人民共和国个人信息保护法》

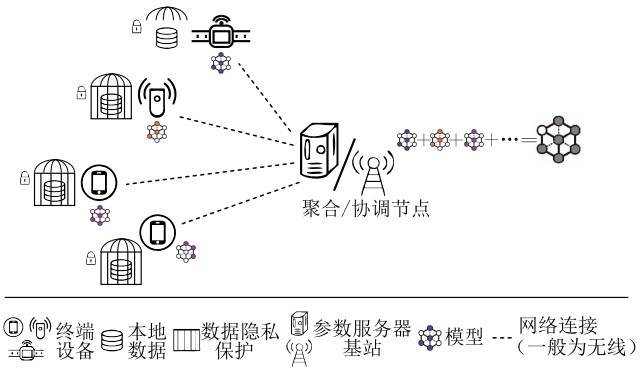


图 1　横向联邦学习的系统架构示意图

1.1　横向联邦学习的发展

横向联邦学习主要解决的是“数据孤岛”(data islands)问题，其最初的设计主要针对的是跨设备(cross-device)的协同训练场景[17]。因此，标准的横向联邦学习系统采用客户机-服务器(Client-Server，C-S)架构和星状拓扑，这种架构中服务器作为协调者需要与所有客户端交互，控制全局的协同过程。横向联邦学习中最基础且最常用的算法Federated-Averaging(FedAvg[15])是基于同步通信机制的训练算法；该算法十分简洁，能够兼容各类基于梯度的优化方法。这些特性使得横向联邦学习成为研究和应用最为广泛的联邦学习范式，同时也推动了联邦学习的快速发展。

联邦学习在学术界和工业界均受到广泛关注——Gartner 将联邦(机器)学习列为处在“创新触发”阶段的潜力技术之一[18]。作为联邦学习的标准范式，横向联邦学习的流行和迅速发展很大程度上归功于它的跨领域性质——相关研究涵盖了从分布式系统到机器学习、从信息安全到无线通信等多个研究领域。以机器学习领域的视角为例，横向联邦学习已经发展为当下热门的研究方向之一。

横向联邦学习面向的是相同特征空间内不同样本子集的联合学习问题，这一点是与纵向联邦学习(Vertical Federated Learning，VFL)和联邦迁移学习(Federated Transfer Learning，FTL)的关键区别[19]。IEEE发布了标准文档IEEE Standard 3652.1-2020：IEEE Guide for Architectural Framework and Application of Federated Machine Learning)[20]，对横向联邦学习、纵向联邦学习和联邦迁移学习给出了标准化的定义和描述，表 1 中对比了三者在数据关联和标签可用性上的区别。

表 1　横向联邦学习、纵向联邦学习和联邦迁移学习的对比

范式	特征重合度	样本重合度	可用标签
HFL	**高**	**低**	**全部**
VFL	低	高	部分
FTL	低	低	部分

注：粗体表示 HFL 是本文综述的对象。

根据上述标准，横向联邦学习遵循联邦学习最初的框架设定，面向的是样本联合的数据场景，即各客户端设备上的本地数据的特征空间一致，各数据子集与全体样本是“横向划分”的关系，如图 2 所示。

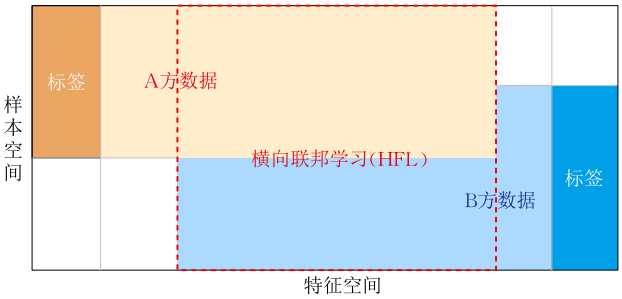


图 2　横向联邦学习中的数据关联(IEEE 标准 3652.1-2020)

横向联邦学习具有算法设计灵活和可扩展性强的特点，近年来联邦学习领域内的大多数研究和应用开发都集中在横向联邦学习这一范式上。因此，本文将横向联邦学习作为分析研究的重点。

1.2　横向联邦学习算法

横向联邦学习算法的执行实体一般包括参数服务器(下文亦简称服务器)和客户端，其中服务器负责协调整个训练流程、完成模型的聚合与分发，客户端则负责本地模型训练和模型上传。标准的横向联邦学习算法以通信轮(简称轮)为逻辑时间单位进行迭代，要求参与训练的客户端和服务器保持同步。

基本的横向联邦学习算法每一轮的步骤为：(1)客户端选择。随机(或按某规则)选择一定比例的客户端参与本轮的训练；(2)模型同步。向上一步中选中的客户端发送最新的全局模型；(3)本地训练。被选中的客户端以最新的全局模型为基模型，在本地数据上对模型进行多次更新；(4)模型上传。完成本地训练的客户端将模型①上传至服务器；(5)模型聚合。服务器将收到的本地模型以加权平均的方式将它们聚合成一个全局模型；(6)模型评估。服务器按某种基准(如准确率)对全局模型进行性能评估；如果性能达标，则结束流程，否则继续下一轮迭代。横向联邦学习的标准流程如图 3。

虽然横向联邦学习算法的基本流程较为简洁，但是由于数据异构性、设备异构性、数据隐私与系统安全等问题的存在，算法优化和系统优化都具有挑战性，该方向的研究仍在深入且呈现多样化。

① 有些算法上传的是累积梯度或模型的更新量，即更新前后模型参数的差值。

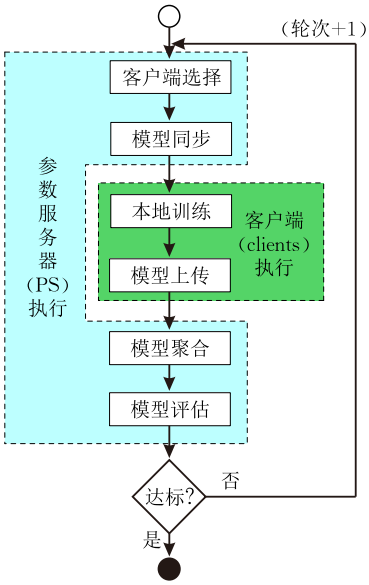


图 3 横向联邦学习算法的基本流程

1.3 相关综述对比

近年来联邦学习相关的研究工作呈现出多场景、多角度、多样化的趋势[17]。例如杨强等人[21]从群体智能的视角分类介绍了联邦学习算法框架、算法优化与算法模型。在原理方面,联邦学习与群体智能中的"探索-融合-反馈"宏观循环不谋而合。联邦学习算法的设计是决定系统效率和模型精度的关键。Yang 等人[22]从系统架构的视角详细介绍了三种联邦学习范式中系统各方的交互流程和各方之间交换的信息,基于线性回归等模型给出了算法案例。王健宗等人[23]对联邦学习算法层面的研究进行了总结对比,但仅涵盖了通信成本、客户端选择和聚合方法这三个优化角度。

目前,相关综述的研究视角较为单一且对横向联邦学习这一范式关注不足。孙兵等人[24]在综述中总结了面向移动计算和边缘计算系统的联邦优化方法,探讨的优化技术主要分为通信、训练及隐私安全三个层面。孙爽等人[25]关注的是隐私保护和系统安全,总结了针对联邦学习系统所面临的典型攻击手段和防御措施。Kairouz 等人[17]和 Li 等人[26]的工作涵盖了领域内较为前沿的理论研究、算法设计和隐私保护方法,但是对应用实践涉及较少,未能反映横向联邦学习应用现状。林伟伟等人[27]汇总了应用较为广泛的联邦学习开源框架并从架构和功能层面展开对比分析,但是缺少对 FedJAX 和 FedLab 等新框架的介绍,对算法研究与系统实践之间的结合问题关注不足。Li 等人[28]围绕联邦学习系统的研究和实践展开分析,从有效性、效率、隐私和自治四个主要视角探讨了系统设计的关键要素。该综述的文献分类方法主要围绕系统构成与布局,未体现相关研究的领域视角和技术共同点,且对开源框架和应用实践的描述不够全面。

因此,本文旨在全面地展现横向联邦学习的研究现状并提供应用实践方面的参考。首先,对横向联邦学习相关研究工作进行了全面分类,详细梳理分析了各方向的研究现状;其次,介绍了横向联邦学习在应用实践方面的情况,包括多个开源系统框架和应用场景,同时汇总了丰富的公开数据集并介绍了常用的数据准备方法。结合调研结果,分析指出了相关研究和实践所面临的挑战。表 2 对比了本文工作和现有相关综述。

表 2 本文工作与相关综述的对比

文献	视角	涵盖研究分支	系统框架	应用	数据集
[17]	理论研究、算法设计	效率与精度的优化、隐私保护、鲁棒性与安全、公平性、范式的拓展	√		√
[21]	系统架构、算法设计(群体智能视角)	系统组织框架、效率与精度的优化、适用模型、隐私保护	√	√	
[26]	理论研究、算法设计	通信效率优化、解决系统异构性方法、解决数据异构性方法、隐私保护			
[22]	系统架构、算法设计	HFL、VFL 和 FTL 的协同算法、模型更新和隐私保护		√	
[23]	算法设计	适用的模型、联邦学习算法优化			
[24]	理论研究、算法设计(移动边缘网络视角)	通信优化、训练优化、安全与隐私保护		√	
[25]	理论研究、算法设计(隐私保护与安全视角)	针对联邦学习的攻击手段、安全防御措施、隐私保护措施			
[27]	联邦学习开源框架	系统架构设计	√	√	
[28]	系统架构、应用实践	算法有效性优化、系统实用性增强、应用优化、基准测试	√	√	
本文	理论研究、算法设计、应用实践	协同算法优化、模型更新优化、通信协议优化、隐私保护与安全、范式的拓展	√	√	√

1.4 章节概要

本文围绕横向联邦学习的学术研究现状和应用实践展开,余下章节内容组织如下:第 2 节按研究分支分类概述横向联邦学习方向的研究现状;第 3 节介绍面向横向联邦学习的主流系统框架和开源代码库,分析对比它们的特性;第 4 节阐述横向联邦学习的代

表性应用；第 5 节简要描述横向联邦学习实验数据的处理方法，同时汇总了一系列公开数据集；在第 6 节，论述相关学术研究和工程实践中存在的关键问题，探讨了未来研究方向；第 7 节对全文内容进行总结。

2　研究现状

横向联邦学习相关研究工作涵盖机器学习、分布式系统、无线通信和信息安全等多个领域，在优化目标和技术方法等方面呈现出多样化和相互交叉的特点，如图 4 所示。本节将从协同算法优化、模型更新优化、通信协议优化、隐私保护与安全以及范式的拓展这五个角度回顾横向联邦学习的研究进展，并根据研究的侧重点对相关文献进行细分。相关文献的分类汇总见表 3。

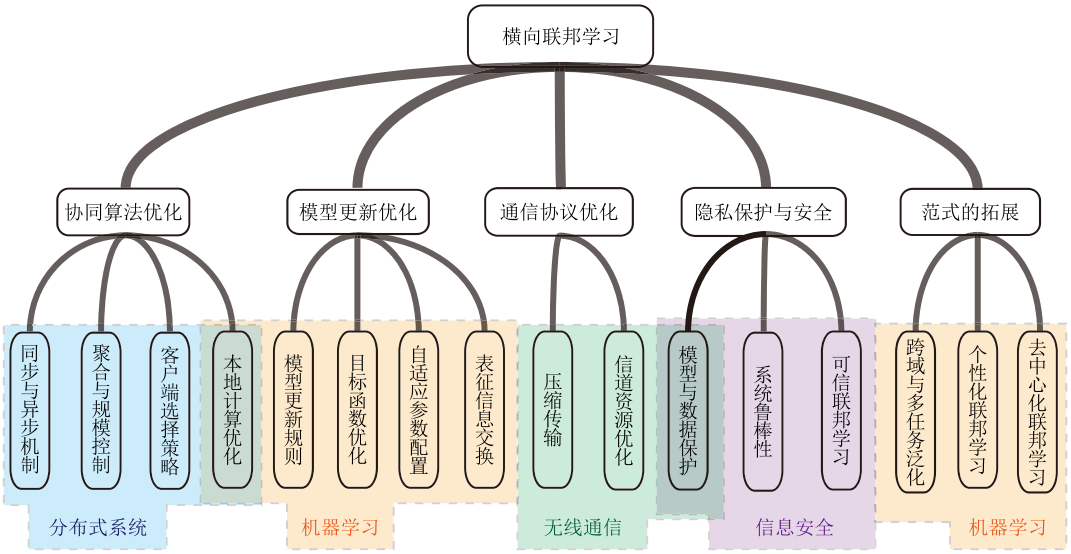


图 4　本文涉及的横向联邦学习研究分类、技术分支与领域视角关系图

表 3　横向联邦学习相关文献分类汇总表

研究分类	核心问题	技术分支	基本原理	文献
协同算法优化	设备异构性、数据异构性、掉队者效应、模型陈旧性问题	本地计算优化	在设备算力受限的情况下优化本地训练的计算过程	[29-36]
		同步与异步机制	提升客户端协作效率，加快全局迭代	[29,37-42,44-49,51-57]
		聚合与规模控制	优化模型聚合，控制训练规模	[15,17,38,47,58-62]
		客户端选择策略	差异化客户端选取，优化全局收敛	[15,38,40,46,55,59,63-65,70-75]
模型更新优化	数据异构性、本地最优不一致	模型更新规则	利用动量等信息校正模型的更新方向	[52,60,78-87]
		目标函数优化	校正全局的优化目标	[52,59,62-63,75,81,87-88,91-93]
		自适应参数配置	调整本地更新配置以优化全局收敛	[55,60,88,94-96]
		表征信息交换	利用表征信息优化模型的更新方向	[98-104]
通信协议优化	通信开销大、信道资源和质量受限	压缩传输	降低每次通信的载荷	[31-32,108-114,116]
		信道资源优化	寻求收敛速率和通信开销之间的权衡	[107,113,117-129]
隐私保护与安全	“拜占庭”设备、模型泄露、数据泄露	模型与数据保护	保证本地模型和本地数据无法被解读或不可见	[11,57,133-141,144,148-150,156]
		系统鲁棒性	规避或抵御恶意模型	[62,64,130,131,133,157-165]
		可信联邦学习	构建对所有用户都公平、安全、可信的协同训练环境	[132,166-177]
范式的拓展	特征空间不同、多任务适应、本地模型性能问题	跨域与多任务泛化	域适应，多范式交叉融合	[86,115,180-182,184-188]
		个性化联邦学习	以最大化本地模型性能为目标构建多个模型	[54,61,189-200]
		去中心化联邦学习	点对点网络中的信息交换与设备协同	[176,201-208]

2.1　协同算法优化

协同算法设计是提升横向联邦学习训练效率、优化模型质量的关键，本节主要分析本地计算优化、客户端协作机制、聚合与规模控制以及客户端选择策略方面的研究。

2.1.1　本地计算优化

横向联邦学习的本地计算开销主要来自本地模型训练时的参数优化过程，包括前馈计算、误差反向传播和参数更新等。虽然横向联邦学习与传统的分布式优化算法都以随机梯度下降（Stochastic Gradient

Descent,SGD)为共同基础,但横向联邦学习算法一般在本地执行多次模型更新后才对模型(或模型更新量)进行交换,本质上是以更大的梯度偏差为代价降低通信开销[29]。由于跨设备场景下设备算力受限,本地训练的计算过程可能成为整个算法的效率瓶颈[30]。

在模型层面,随着深度学习方法逐渐流行,模型训练对硬件资源要求越来越高,这对本地训练过程的计算效率提出了挑战。模型裁剪和低精度训练等通用的深度神经网络加速方法同样适用于横向联邦学习中的本地计算优化[31-32],这类方法通过对模型进行轻量化以降低参数优化过程的计算开销,但在实际应用中如何考虑全局的情况来设定合理的算法超参数(如模型裁剪比例)是一个难点。针对这一问题,Liu 等人[33]提出根据设备算力分配不同大小的模型以提高系统整体的计算效率;他们的方法中各尺寸的模型共享基层结构,对应的参数通过分层异构聚合来更新。

在算法层面,可以利用横向联邦学习的架构将部分本地计算的负担转移到本地设备之外,具体又可分为两种研究思路。第一种思路是数据卸载(data offloading),即放松数据约束,允许将部分数据在本地之外处理[34]。例如,在 Ji 等人[35]提出的 EAFL 算法中,训练过程被分为数据迁移和模型更新两个阶段,各设备先将部分本地数据卸载到服务器,由服务器承担这部分数据上的模型更新计算。本地计算负载转移的第二种思路是将部分模型卸载到本地之外,利用更强的算力加快训练。Ye 等人[36]基于拆分学习提出了 EdgeFed 算法,将模型的主要部分放置在资源充沛的边缘服务器上,本地设备仅保留一个卷积层和池化层。边缘服务器基于设备上传的中间结果和标签完成推理与参数更新,承担训练过程的大部分计算量。考虑到边缘服务器等辅助计算节点的可信问题,数据卸载和模型卸载均增加了隐私泄露的风险。

2.1.2 同步与异步机制

横向联邦学习中,一群客户端协同训练的基本模式有两种:同步和异步。二者的主要区别在于服务器是否直接或间接设置同步屏障(synchronization barrier)以保持所有(参与训练的)客户端始终工作在同一个逻辑轮次。如图 5 所示,同步方法保证所有本地更新都是以同一个全局模型(即参数空间中的同一个点)为起点[37];而异步方法不限制客户端的迭代进度,服务器每收到一个本地模型就更新一次全局模型。

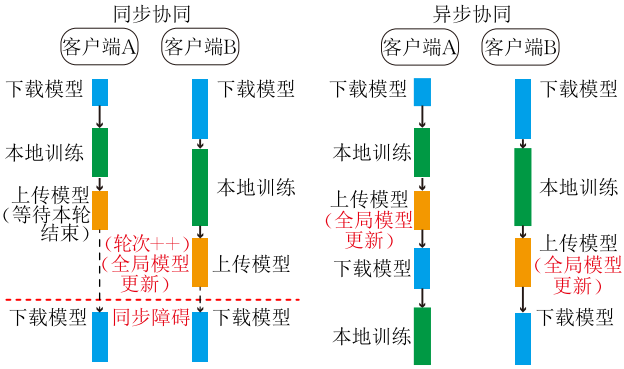


图 5 同步与异步横向联邦学习算法流程对比

在算法设计层面,当前大多数的研究更倾向于采用同步的客户端协同方法[38-39]。在服务器的协调下,同步协作最大的优势在于客户端的行为更加受控,能避免模型陈旧性(model staleness)问题[40]——即设备基于陈旧的全局模型进行本地训练[41-42],导致本地模型的更新出现较大偏差。在跨设备场景下,同步算法的实际效率对设备异构性非常敏感,而设备异构性包括设备性能异构和可用性异构两个方面。Abdelmoniem 等人[43]利用上千种超参数组合开展实验探索,发现设备异构性对同步算法的效率和模型准确率的影响显著高于各种超参数。同步算法的主要问题是掉队者效应(straggler effect)[44-45]——即全局迭代的整体效率取决于速度最慢的客户端[46]。对此,现有研究采用了各种机制来提高训练效率。例如,Li 等人[47]提出了一种分层同步的训练算法 FedHiSyn,将客户端按算力聚类成多个组,组内客户端形成环形拓扑并有序地训练和传递本地模型,该过程迭代一定步数后所有本地模型被上传到服务器进行聚合。

异步协同机制在灵活性、系统鲁棒性和模型迭代效率等方面具有天然优势,能直接避免掉队者效应,将服务器从由慢速客户端造成的漫长等待中解放出来[48-51]。一种代表性的实现是 FedAsync[52]算法,它引入了即时的全局更新方法[53],在服务端对全局模型进行增量更新,同时引入了模型陈旧度惩罚。Kall 等人[54]采用 FedAsync 算法在多个代码库上协同训练了一种敏感口令扫描器。他们在本地训练中引入了额外的个性化机制,包括模型插值法和数据插值法,用于优化模型在本地数据上的性能。通常异步方法在实际运行中会比同步方法需要更多次数的本地更新才能实现全局模型的收敛[55]。异步算法一般对全局模型进行增量更新而且不对客户端的

参与模式进行控制，因而与差分隐私等常用的隐私保护技术很难兼容[46,56-57]。为解决该问题，Meta AI 的研究人员实现了一种融合了缓存机制的异步横向联邦学习算法 FedBuff，该算法中客户端异步训练，服务器则将收到的本地模型缓存下来，从而可以利用 SecAgg 和 DP-FTRL[49]等隐私保护协议完成模型的安全聚合[41]。

综上，表 4 比较了横向联邦学习中的同步和异步协同方法的优缺点。

表 4　同步与异步协同的优缺点对比

	优点	缺点
同步	·模型收敛稳定 ·通信次数较少	·掉队者效应与掉线问题 ·全局模型更新频率低
异步	·无同步障碍，容错 ·全局模型更新频率高	·通信次数较多 ·模型陈旧性问题

2.1.3　聚合与规模控制

本小节阐述横向联邦学习中控制训练规模（即并发参与训练的客户端数量）的方法以及全局模型聚合规则。

横向联邦学习的实际规模可以很灵活，通常用参数 C 来控制参与一轮训练的客户端的（最大）比例[15]。当 $C=1$ 时，服务端不限制训练规模，对应的客户端参与模式称为全量参与（full participation），否则（$C<1$）称为部分参与（partial participation）。Kairouz 等人[17]建议将 C 设置为一个较小的值，可以从两个角度解释其必要性。首先，发动所有设备参与训练并不一定能保证全局模型更快或更好地收敛。有实验表明：在批大小（batch size）较大的情况下，全局模型无法在 $C=1$ 的设定下达到目标精度，但在适当减小 C 值的情况下能有效收敛[15]。限制训练规模的第二个原因是成本。较大的 C 值对应较高的客户端平均参与频率，会增加设备资源消耗、网络流量以及服务器的负担。为此，Wu 等人[58]根据设备在不同边缘区域中的可靠性差异设计了一种动态控制策略，通过分区域自适应地调整选择比例来逼近预期训练规模，提升整体迭代效率。

横向联邦学习的系统规模可以从几个到几百万个设备不等。Kairouz 等人[17]的研究综述描述了两种典型场景：跨设备（cross-device）联邦学习和跨筒仓（cross-silo）联邦学习。前者面向的是相对大规模的、异构的客户端群，全量参与不现实；后者面向的场景由为数不多、但资源充沛的几个节点组成（对应诸如电商企业、银行之类的大型组织），每个节点包含相对大量的本地数据，此时全量参与模式则是合理的。

模型聚合操作由服务器执行，也可以有两种不同的形式：全量聚合（full aggregation）和部分聚合（partial aggregation）。全量聚合包括两种不同的方式。第一种方式是保留本地模型，服务端直接对本地模型进行聚合；第二种是保留全局模型，将未更新的本地模型替换为当前的全局模型。部分聚合是另一种聚合规则，在合成全局模型时只考虑当前轮次更新的本地模型。例如，FedProx 算法[59]使用参与训练的客户端数量的倒数作为权重来对上传的本地模型进行加权合成。Li 等人[38]使用客户端的相对数据大小乘以常数 1/C 作为对应本地模型的权重。

在全量参与模式下，采用部分聚合在直觉上似乎不合理，但对于具有异步性质、选择性聚合规则和容错设计的算法，它实际上是合理的。例如，Dhakal 等人[60]提出了一种称为编码联邦学习（coded federated learning）的方法，预先估计梯度的聚合结果，以便服务器能够在只收到部分模型更新信息就执行聚合。全量参与下的部分聚合的一个特殊情况是基于客户端聚类的训练算法（例如文献[47,61-62]），这类算法可以允许所有客户端同时参与本地训练，但通过某些方法对客户端进行聚类，使它们仅对相应的聚类模型（而非全局模型）做出贡献。

2.1.4　客户端选择策略

客户端选择通常是算法（初始化之后）执行的第一个操作。客户端选择策略可以大致分为两种：静态采样和动态采样。静态采样策略对应的采样规模和规则是不变的（例如完全随机采样）。动态采样策略是指（实际）采样的规模或者采样的客户端对象是动态的，而非一次性确定的。例如 SAFA[40]算法根据本地模型的上传顺序对客户端的采样进行动态调整。目前绝大多数的横向联邦学习算法采用的是静态采样策略，主要因为全局目标函数和设备数据量等条件一般是确定的，使用固定不变的客户端选择概率分布就能从理论上满足全局模型收敛的相关条件[38]。动态采样策略能够更好地适应优化目标等方面的不确定性[63]，但是其有效性比较依赖场景和相关参数设定。

客户端选择策略是优化横向联邦学习效率的关键之一。均匀随机采样[15,55]隐含地赋予每个客户端同等的重要性，但是其合理性取决于全局优化目标和系统实际情况[64]。通过客户端选择可以解决或缓解掉队者效应，一种直接的解决方案是在客户端选择阶段预先排除可能存在的低速设备[65]，但这

种方法直接影响了训练的公平性。Chai 等人[46]则根据设备的性能高低将客户端集群分为多个层(tier),引入了一种新的客户端选择策略,对各层分别进行抽样,并结合了一种动态评估机制来更新各层在全局抽样时所占的比重。而针对数据异构性问题[66-69],研究者提出了多种基于客户端选择策略的解决方案,例如基于数据量的加权随机选择[59]、面向误差或损失的选择策略[70-71]和基于强化学习的选择策略[72-73]。由于客户端和本地数据集是一一对应的绑定关系,因此合理选择客户端可以优化整个训练过程。例如,Chen 等人[74]提出基于客户端提交的更新量的模长来动态调整客户端的参与概率,使得本地训练更有"针对性"。Nguyen 等人[75]通过引入一组额外的客户端来在模型聚合之前对本地更新量进行校正,缓解数据异构性导致的本地更新发散。

2.2 模型更新优化

相关研究中的模型更新优化方法主要包括更新规则优化、目标函数优化、自适应参数配置以及表征信息交换技术。我们对模型更新相关的数学符号作如下约定:θ 和 θ_k 分别代表全局模型和本地模型(的参数),$|D|$ 和 $|D_k|$ 分别表示全局数据量和客户端 k 上的本地数据量,F 和 F_k 分别代表全局目标函数和本地目标函数,上标 $*$ 代表最优解。

2.2.1 模型更新规则

在横向联邦学习中,本地模型更新本质上是基于梯度的参数优化,参数更新量取决于模型当前参数、目标函数、参数更新规则和学习率等。同时,近期的一些研究常利用动量(momentum)等信息来优化数据高度异构环境下的本地模型更新或全局模型更新。受方差缩减(variance-reduction)方法的启发[76-77],一些新的算法专注于改进全局模型更新规则,通过引入服务器端的增量更新[52,78]、本地动量和/或全局动量[79-84]以及模型更新相关的状态变量[85]来优化全局模型的更新方向。这些方法以随机梯度下降相关的最优化原理为理论基础,在给定条件下能保证全局模型的理论收敛率,但是主要问题是要求频繁地上传梯度相关信息。

一些横向联邦学习优化方面的研究采用特殊的更新规则。例如,为了补偿中途离线的客户端未(及时)提交的模型更新,Dhakal 等人[60]使用了一种新颖的梯度聚合公式,该公式包含两种类型的梯度,分别来自参与训练的本地设备上的数据和所有设备共享的复合对等数据(composite parity data)。一种称为 FedBoost 的算法[86]则将服务器上的传统全局模型替换为基于一组预训练学习器的集成模型,并设计了相应的更新规则以寻找最佳集成系数。Wang 等人[87]研究了神经网络的(神经元)置换不变性现象,并提出了一种模型分层聚合方法,在对参数进行聚合之前以神经元(针对全连接网络)、通道(针对卷积网络)或隐状态单元(针对循环神经网络)为对象执行"对齐"操作。

2.2.2 目标函数优化

在横向联邦学习中,全局目标函数通常被定义为本地目标函数的加权平均。每个参与训练的客户端根据本地目标函数的定义计算(随机)梯度,使用 SGD 或动量更新等方法对本地模型进行迭代更新,目标是最小化其本地目标函数[14-15,38]。

一些文献研究了全局目标函数 $F(\theta)$ 和本地目标 $F_k(\theta)$ 之间的关系[59,62,87-88],并分析了它们在异构数据上的不一致对全局模型的收敛速度和最终质量带来的影响[44]。本质上,目标函数的不一致性是本地数据分布和总体数据分布之间的差异造成的,不同的本地数据分布对应参数空间中不同的本地最优解(图 6),这种现象可以表述为

$$\underbrace{\arg\min_{\theta} F(\theta)}_{\theta^*} \neq \underbrace{\arg\min_{\theta_k} F_k(\theta_k)}_{\theta_k^*} \tag{1}$$

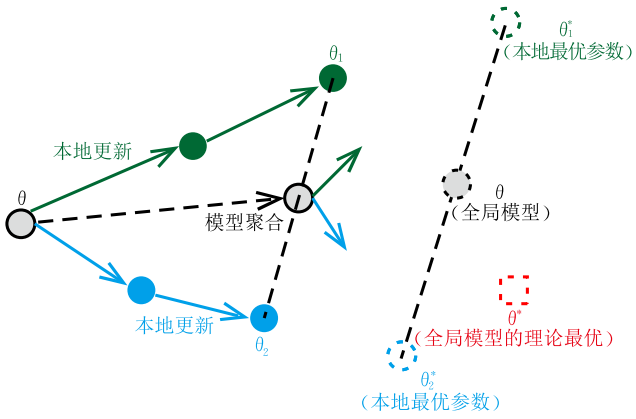


图 6 不同本地模型在参数空间中的最优解不一致导致模型聚合得到的全局模型参数并非最优解

另一方面,最优本地模型的加权组合(即模型聚合的结果)与全局模型在参数空间中的理论最优解往往是不一致的:

$$\theta^* \neq \sum_{k \in U} \frac{|D_k|}{|D|} \theta_k^* \tag{2}$$

上述原因导致聚合后的全局模型在异构数据条件下往往偏离最优。为了解决这个问题,需要调整本地目标函数和/或全局目标函数。一种常见的方法是改造本地目标函数[52,59,75,81],引入一个近端项(亦称作近端算子)。这个想法最初是在优化集中式 SGD

的方法（例如 SAGA[89]）中被使用的，其基本思想与方差缩减方法[90]异曲同工。在横向联邦学习的设定下，全局模型天然适合作为参数空间中本地模型的参照点，可以基于本地模型和全局模型的欧氏距离构造近端项，将近端项添加到原始的本地目标函数中：

$$F'_k(\theta_k;\theta)=F_k(\theta_k)+\underbrace{\frac{\mu}{2}\|\theta_k-\theta\|^2}_{\text{近端项}} \tag{3}$$

其中 μ 是可调参数。将近端项引入本地目标函数的本质是施加一种软约束，使本地模型在一定程度上向全局模型“靠拢”以缓解数据异构性带来的本地更新发散问题，FedProx[59]就是一种引入了近端项的代表性算法。此外，包括 FedDyn[81]和 FOLB[75]在内的一些算法则对本地目标函数做进一步的修改以加快模型的收敛，而另一些研究选择重新定义整个优化问题或重新定义本地更新和全局更新之间的关系[63,91-93]。

2.2.3　自适应参数配置

横向联邦学习算法本身的参数一般在算法执行前进行配置，考虑到算法迭代过程的成本远高于传统的机器学习，反复调试不太现实，因此如何合理地设置算法参数相当有挑战性。例如在跨设备场景中，客户端的可用性（即是否参与训练）和可靠性（即是否能完成训练）难以预测，需要充分考虑这些因素才能确定合适客户端选择比例。一些研究提出了灵活的客户端参与规则，通过允许客户端提交不完整的模型更新[94]或中途退出一轮训练[60]来加速每一轮训练过程，并且不妨碍全局模型聚合。Wang 等人[88]研究了由本地数据集的体量差异导致的客户端本地更新的步数不一致的问题，进一步提出通过使用归一化梯度和有效步数来缓解问题。其中，用归一化梯度替代梯度的线性累加能消除本地更新步数差异造成的全局模型更新方向偏差。

在大多数情况下，系统中的服务器负责协调和设置训练参数（作为训练算法自身的参数，亦称为超参数），包括批大小、学习率、本地遍历次数等。在现实环境中，在资源预算有限的系统（例如物联网和移动边缘计算系统）之上设计算法和设置参数需要考虑迭代效率和资源消耗之间的权衡。在这种情况下，本地更新的参数配置应当与终端设备的异构性和本地数据的异构性相适应，影响因素包括但不限于本地数据集的大小、设备计算能力和网络吞吐量等。引入自适应的参数配置方法可以缓解设备异构性、数据异构性等因素对全局迭代效率的影响，这方面的技术包括自适应聚合频率控制[55]和自适应（本地）批大小和学习率[95-96]。

2.2.4　表征信息交换

深度学习模型能够提取数据多个层次的特征，产生更具表达能力的数据表示（即表征），这一特性使模型能够很好地从复杂的数据中学习知识[97]。在横向联邦学习的设定下，数据表征作为可交换的信息在数据异构性较强的场景中很有用[98-99]。Li 等人[100]提出了 MOON——一个结合了模型对比学习（model contrastive learning）的横向联邦学习训练框架。该框架的核心思想是通过约束本地模型产生的表征之间的差异来纠正本地训练中模型的更新方向。具体而言，MOON 向本地损失函数引入了当前本地模型、旧版本地模型和全局模型三者之间的表征相似性度量。基于横向联邦学习的迭代特点，可以利用全局模型来提取本地数据的表征信息，感知本地数据的分布性差异，优化算法中的客户端选择等相关技术。考虑到表征信息量与数据体量有关（每一个样本经过相应模型结构的前向传播会产生一个表征向量，在某些任务下亦称嵌入向量），一种降低通信开销的代表性方法是基于先验分布假设对数据产生的表征进行统计学压缩，进而在通信协议中仅交换相应分布的参数[101]。在横向联邦学习中利用度量学习等方法训练嵌入模型（例如基于嵌入的分类器）时，往往需要交换样本的表征以满足各方都能正常计算对比损失的要求，因此一些研究通过对表征进行聚合[102]、编码[103]或替代[104]等方式来优化这一交换过程。

此外，表征信息常用于纵向联邦学习和联邦迁移学习算法，例如以中间运算结果的形式在这两类算法的实现中作为多方之间交换的信息[105]。这方面的研究工作超出了本文范畴，在此不展开讨论。

2.3　通信协议优化

通信是影响分布式系统性能的主要瓶颈，横向联邦学习系统也不例外，客户端和服务器的通信成本通常是决定算法效率的关键因素[106-107]。

2.3.1　压缩传输

降低通信成本最直接的方法是直接压缩有效载荷[108]，这里有效载荷可以是模型本身，也可以是模型更新量（例如累积梯度）。在无线网络环境中，最流行的两种压缩方法是稀疏化（sparsification）和量化（quantization）。稀疏化，或称为 top-k 稀疏化，是指一类通过仅保留绝对数值前 k 大的元素而将所有其余元素省略掉的压缩方法[109-110]。稀疏化一般通过掩码的方式实现，例如 Sun 等人[109]根据全局模

型的更新量生成掩码向量，将其同步给所有参与设备实现本地模型的 top-k 稀疏化，节省通信成本的同时配合空中计算技术实现模型的高效聚合。

与稀疏化相比，量化压缩不会改变载荷向量的长度，而是对向量中的每个分量进行从连续空间到离散空间的映射 $\phi: R \to F_q$，这里 F_q 是一个只有 q 个有效元素的有限域。Liu 等人[111]通过系统分层提高了量化的压缩效果，理论分析了量化操作的参数和横向联邦学习算法的参数对全局模型收敛率的影响。当涉及规模较大的设备集群时，对模型信息做量化压缩引起的误差通常是可控的，而节省的网络流量是十分可观的[112-114]。Sattler 等人[110]提出了一种混合压缩机制，通过将稀疏化和量化这两种方法组合在一起，进一步提高了模型压缩率，同时降低了上行和下行带宽需求。

减少通信开销的另一条途径是直接对模型本身作裁剪，这类方法已在深度学习中广泛应用。在横向联邦学习场景下，模型裁剪有助于降低计算和通信成本[31]。Jiang 等人[32]在本地模型裁剪基础上引入了一种分布式裁剪方法，由客户端根据训练情况反馈参数重要性向量，服务器则迭代地更新掩码以实现自适应的模型裁剪。对模型做拆分后再传输是减少通信开销更直接的方式，其基本思路是让每个客户端仅与服务器交换模型参数向量的限定部分来减少需要传输的参数量[115-116]，这类方法通常需要预先确定模型的拆分方式（例如以神经网络某一层为界）。

2.3.2 信道资源优化

在网络边缘这种资源受限环境下，通信资源的分配至关重要[117]。基于这一事实，一些研究试图找到客户端调度和网络资源分配这一联合优化问题的最优解[113,118-120]。Amiri 等人[121]考虑了一种通信资源十分受限的场景——客户端和服务器通信使用带宽受限、存在衰减的多址接入信道（Multiple Access Channel，MAC）。作者研究了如何在这种不理想的网络环境中优化横向联邦学习，并提出了两种不同的通信协议（基于单信道的 D-DSGD 协议和基于多信道的 CA-DSGD 协议）和一个发射功率分配方法，用于在信道资源限制下加速全局模型的收敛。类似的研究工作也表明了信道资源管理的重要性，其本质上可以归结为加快模型收敛和降低通信成本这两个目标之间的权衡[122-125]。从通信的角度来看，在资源有限的边缘环境中控制训练规模是非常有必要的——一些文献已经从理论上和实验上证明，排除一些“不太有用”的更新可以在基本不影响全局收敛的情况下节省流量[119,126]。

横向联邦学习的一个主要应用场景是在通过无线网络连接的移动设备集群上进行机器学习模型的协同训练[107,127-128]。智能应用和无线通信技术的进步促进了横向联邦学习在移动边缘网络中的发展[121-123]。5G 技术的快速落地为加速网络边缘的智能化提供了重要助力，仍处在研发和标准制定阶段的 6G 技术则为泛在智能（ubiquitous intelligence）的实现描绘了广阔的前景。作为以分布式系统为基础的机器学习框架，横向联邦学习在移动边缘计算、工业物联网和车联网等新兴领域和场景展现出无限潜力，同时也面临复杂多变的边缘网络环境带来的诸多挑战[129]。在 5G 和后 5G 时代，面向横向联邦学习的算法研究、通信协议设计和系统性优化仍然有大量探索的空间。

2.4 隐私保护与安全

隐私和安全是横向联邦学习中的两个突出问题[130]。在横向联邦学习的语境中，二者侧重点有所不同[131]。一般来说，系统涉及的隐私问题通常是指与用户相关的信息泄露，包括模型、梯度和最重要的原始数据。另一方面，系统中的安全问题通常是指协同训练过程遭到干扰或恶意破坏的可能性。在某些情况下，安全问题也可能导致用户隐私泄露[132]。

2.4.1 模型与数据保护

在横向联邦学习的设定下，模型保护与数据保护研究的目标分别是最小化模型和数据泄露的风险。

针对模型保护，现有的研究给出了多种解决方案，涉及同态加密[133-134]、差分隐私[135-137]、秘密共享[138-141]等。作为一种支持密文空间中执行特定运算的密码学技术，同态加密（Homomorphic Encryption，HE）是保障模型安全的密码学方案，然而最具通用价值的全同态加密[142]技术因计算开销等原因不太可能在现实中实现。对大多数横向联邦学习算法来说，满足加法同态的方案就能够支持模型聚合操作所需的运算[133-134]。即便如此，加解密操作以及在密文空间进行运算仍会带来比较大的计算开销 Paillier[143]。安全多方计算（secure Multi-Party Computation，MPC）则是一种广泛采用的计算框架，囊括了秘密共享、混淆电路和茫然传输等多种具体的技术或协议[144-147]。相关领域的研究人员基于 Shamir 秘密共享原理已经开发了一系列方法并将其应用于横向联邦学习中的本地模型保护[57]。为了达到所需的隐私和/或安全级别，可以在实践中结合多种技术[134,148-149]。但始终有必要考虑实现成本和模型性能损失[150]。此外，

无线通信中的空中计算(over-the-air computation)技术能够利用模拟信号在多址接入信道上的叠加特性，在传输模型的同时完成聚合，避免本地模型在服务器端被窃取[123]。

针对数据保护，有研究表明在计算机视觉和自然语言处理等任务中，可以利用梯度来重构深度模型的原始输入[11,151-152]，这说明尽管没有原始数据交换，不安全的信道也会带来数据泄露的风险。在计算层面，成员推理攻击(Membership Inference Attack，MIA)能在样本级别构成对本地数据安全的威胁，这种攻击可描述为：给定一个样本(x,y)和在数据集D上训练过的模型M，根据M的推理结果等信息判定该样本是否属于D。很多情况下，由于客户端和服务器能够分别获知本地模型和全局模型的结构与参数，因此针对横向联邦学习的成员推理攻击属于白盒攻击，相比仅知道模型输出的黑盒成员推理攻击更加危险。Gu 等人[153]进一步利用联邦学习多轮迭代过程产生的本地模型和全局模型序列，根据模型对给定样本的预测置信度的变化趋势提升成员推理的准确率。防御成员推理攻击的方式主要包括正则化、dropout 以及安全聚合技术[154]。正则化和 dropout 通过避免模型过拟合降低其对训练样本的敏感程度，安全聚合则使得本地模型无法被直接用于推理攻击。

差分隐私(Differential Privacy，DP)可用于保护本地计算的梯度(如 DP-SGD[155])，也可以保护被上传的本地模型。后者的原理是通过向模型参数(或其更新量)施加人工噪声来掩护其原始向量，并在服务器端通过模型聚合以抵消这些噪声。但是由于噪声的随机性和设备数量的变动等原因，模型聚合操作往往不能完全消除噪声以还原模型参数，某些条件下其负面影响可能很显著(例如精度损失超过 10%[144])。虽然在给定条件下，基于差分隐私的方法能为聚合后有效恢复全局模型提供概率性保证[134,156]，但是在实际应用中，仍需考虑隐私保护水平和模型精度损失之间的权衡。低成本是差分隐私的主要优势，其在计算上是轻量级的，并且对部分攻击和设备故障具有一定鲁棒性[144,148-149]。

2.4.2　系统鲁棒性

系统安全和鲁棒性方面的隐患主要是由(潜在的)拜占庭客户端设备(Byzantine devices)引起。根据相关文献给出的定义，拜占庭客户端包括因为客观原因而不可靠的设备和因为主观原因意图破坏或操控全局模型的恶意设备[62,133]，其中恶意设备通常是各种攻击的发起方。

本节重点讨论针对横向联邦学习有效性和公平性的攻击。从攻击实现的方式分析，以操纵或破坏全局模型为意图的最常见攻击有两种：数据投毒攻击(data poisoning attacks)和模型投毒攻击(model poisoning attacks)[130-131]。顾名思义，数据投毒攻击意指通过恶意添加、篡改和删除本地的训练数据样本(例如标签翻转)来误导本地模型的训练[64,157]，目标是让模型推理出现显著偏向，一般属于有针对性攻击。模型投毒攻击的主要手段是直接对本地模型的参数进行修改(例如放大某些权重)，从而在模型被聚合后对全局模型造成总体性能影响[158]，通常属于无针对性攻击。

由于直接针对的是模型参数本身，模型投毒攻击的检测和防御比较直观，基本思路是判定本地模型(或其更新量)向量的内容是否异常。根据模型(或模型更新量)在参数空间的分布来找出(潜在)异常模型的方法在相关研究中较为常见[159-160]，其中模型距离/相似性的度量方式非常重要。例如，Mao 等人[159]提出了一种称为 Romoa 的模型聚合方法，由服务器追踪本地参数更新和聚合后参数变化量，采用 lookahead 策略计算二者的余弦相似性，结合模型聚合过程中的参数加权，实现模型投毒攻击的防御。文献[161]则选择从客户端的视角，研究如何降低已发生的投毒攻击对后续训练的持续影响。

数据投毒攻击较为隐蔽，因为横向联邦学习对数据访问的限制，针对数据的恶意篡改难以被直接检测出来，因此现有研究主要还是通过检查模型参数来间接检测这类攻击。例如 Tolpegin 等人[162]首先对模型参数进行降维，然后根据降维后的空间中各模型的分布找出在异常数据对应的本地更新。Li 等人[163]采用了类似的思路，借助光谱异常检测(spectral anomaly detection)技术对模型更新做降维编码后再进行检测。另外，可以利用预先训练好的自编码器来对本地模型进行重构，然后通过分析模型参数的重构误差来判定异常。此外，数据噪音可能会和数据投毒攻击产生类似的负面影响，现有研究采用更具样本鲁棒性的损失函数和调整模型聚合权重来解决这一问题[164]。

在上述两种攻击的基础上，又衍生出了一些新的攻击方式，例如搭便车攻击(free-rider attack)和女巫攻击(sybil attack)等。搭便车攻击是通过构造虚假参数的方式欺骗服务器，在未实际参与训练的情况下获取全局模型；女巫攻击是通过伪造出多个

设备身份来干扰或攻击学习过程，例如增强模型投毒的效果。本质上，这两种攻击仍然可以通过分析参数来检测。Sun 等人[165]研究指出这些攻击的效果非常依赖恶意设备所占比例，而且通过实验表明基于范数裁剪和差分隐私能够实现有效防御。

2.4.3 可信联邦学习

可信联邦学习(Trustworthy Federated Learning，TFL)是可信人工智能的延伸，旨在联邦学习的基本框架下构建一个对所有用户都安全、可信的协同训练环境[166]。

如何保证模型聚合结果的正确性和可验证性是可信联邦学习的关键问题。VerifyNet[132]是实现可验证安全聚合的代表性方法，其核心是利用同态哈希函数和伪随机数机制由服务器生成一个证明，用户通过验证该证明是否满足一定条件来验证聚合结果。Guo 等人[167]则在线性同态哈希的基础上引入了承诺系统(commitment scheme)，提出了一种更高效的框架 VeriFL 以实现模型聚合结果的验证，同时利用批量验证方法进一步缩减计算成本。Jiang 等人[168]针对系统可能遭受的欺骗攻击，提出结合以太坊区块链和密码学累加器(cryptographic accumulator)技术生成成员证明供用户验证，同时在服务器端引入了基于 ElGamal 加密算法实现的模型聚合结果验证技术，保证协同训练过程对各方安全可信。该方法存在的问题是验证过程的复杂度较高，计算和通信开销比较大。相比之下，VerSA[169]则采用一种基于双重聚合的轻量级聚合验证技术，其本地训练后的掩码操作开销远低于 VerifyNet，而验证聚合结果的时间开销仅为数十毫秒。安全聚合引入的掩码对本地模型在服务器端的验证造成困难。为此，Chowdhury 等人[170]提出了一种带输入验证的安全聚合协议 SAVI 和相应的系统 EIFFeL，其核心思想是要求客户端生成本地模型的有效性证明，然后基于秘密共享技术实现互相验证，服务器根据反馈结果判别本地模型的有效性。相比密码学方法，基于可信硬件的可信执行环境能更高效地从底层确保模型机密性和完整性，但是因受限于内存和硬件环境等原因，在实际系统中应用尚不广泛[171]。

引入一个对所有参与方而言都可信的信用系统是实现可信联邦学习的一种途径。Rehman 等人[172]基于区块链实现了一种横向联邦学习协作框架 TrustFed。为解决设备可能提交低质量模型的问题，TrustFed 首先根据服务质量(Quality of Service，QoS)要求作初步的客户端选择，然后将参与设备分为两组实现相互验证，并根据反馈过滤掉部分模型，完成链上模型聚合并更新各设备的信用值。借助区块链能有效达成系统内共识，为参与方的信用评估提供了可靠的机制[173-176]。利用区块链建立的信用系统还能有效保障参与方的利益，保护经过训练的全局模型不被非法复制、滥用或二次分发。例如，Li 等人[177]提出了一种将全局模型视作知识产权权益(intellectual property rights)的系统框架 FedIPR。该框架由水印嵌入和所有权验证这两个独立的学习过程组成，前者允许每个客户端嵌入私有的基于特征或基于后门的水印，后者允许各方独立验证全局模型的所有权。值得一提的是，引入这类信用机制不代表将系统去中心化，基于区块链的信用系统完全可以与有服务器协调的算法相兼容[172]。

2.5 范式的拓展

有一些应用场景超出了横向联邦学习的适用范围或设定了与其截然不同的优化目标，为此需要对横向联邦学习的范式进行相应的拓展和泛化[178]。

2.5.1 跨域与多任务泛化

从机器学习的视角看，横向联邦学习的缺陷之一是无法泛化到多个特征空间，即异构域适应[179]。在这一点上，横向联邦学习的泛化研究可以借鉴纵向联邦学习和联邦迁移学习中的技术思想。大多数跨特征空间的协同算法研究主要局限于相对简单的机器学习模型(例如树模型)[180]。在横向联邦学习的典型规模(如千级节点)上实现跨特征空间的协同设计中存在的主要困难之一是样本对齐(在文献中也称为实体解析)，这在协同算法中是一项重要的预处理操作[180-181]。样本对齐中可能出现的错误(例如样本类别不匹配)会对构建出的模型造成很大影响[182]。

横向联邦学习的普适性和实用性促进了将新兴机器学习范式与其结合的交叉研究，即所谓的 Federated x Learning(FxL)[183]。这些基于范式的拓展很大程度上能解决横向联邦学习泛化到多任务的能力，实现更加通用的知识表示以服务于多样化的任务。例如，Liu 等人[184]探索了联邦学习与其它机器学习范式的内在关联，描述了联邦元学习(federated meta learning)和联邦多任务学习(federated multi-task learning)等新的学习形态。一些研究则将分割学习[115]、多视图学习[185]和集成学习[86,186]技术用在横向联邦学习的算法优化中。考虑到本地数据的后验分布可能不同，这种异构性造成学习任务的差异，因此横向联邦学习可视作实现多任务学习的一种方式[187-188]。Google Research 的研究人员针对每个设

备仅有一类样本的极端场景提出了 FedAwS 算法[104]，该算法的核心思想借鉴了对比学习中的损失函数设计，解决了类嵌入坍缩到单点的问题。针对同一问题，文献[102]则基于度量学习(metric learning)提供了一种更安全的协同算法 FedMetric，避免直接暴露样本的嵌入向量。虽然这类算法目前主要应用于用户验证类任务[103]，但是基于联邦度量学习得到的嵌入模型(embedding model)有泛化到多种下游任务的潜力。

2.5.2　个性化联邦学习

横向联邦学习的基本目标是构建一个全局通用的共识模型，但是在一些场景下，需要训练出个性化、差异化的模型来更好地支撑应用[189]。例如基于横向联邦学习联合用户的设备和数据训练推荐系统类的模型时，得到一个较为普适的全局模型可能意义不大，用户更多时候期望得到的是一个准确捕捉自己行为模式的模型，让模型输出个性化的推荐结果[190]。个性化联邦学习(Personalized Federated Learning，PFL)由横向联邦学习范式拓展而来，其目标是为客户端训练出本地性能优异的模型，同时利用其基本框架解决本地数据量不足和数据高度异构的问题[54,190]。PFL 的难点在于个性化模型的构建同样需要依赖来自其它客户端数据的知识。换言之，PFL 需要在横向联邦学习的基础上借助全局模型(或其它全局信息)来辅助本地模型的训练。主流的 PFL 算法大致可分类为基于数据的方法和基于模型的方法。大多数 PFL 算法都是采用基于模型的方法，例如设计特殊的本地目标函数和模型更新规则[191-194]、对模型结构进行拆分[195-196]以及将全局模型与局部模型进行混合[197]。

客户端聚类(或称用户分组)是实现 PFL 的另一种有效途径[198]，在相关文献中亦称为半中心化联邦学习[21]或聚类联邦学习[199]。这类算法相当于在统一的全局模型和完全个性化的本地模型之间寻求折中，通过某种规则将客户端动态归类到多个分组中，以组内信息交换为主要途径，为每个组构建一个“集群模型”以服务组内的用户。基于用户分组的算法的关键在于聚类规则，其设计一般是基于本地模型参数的距离[61,200]或者它们与集群模型的亲和力[199]。作为预期的训练结果，每个客户端与同组的客户端(如一组相似的用户)共享一个模型——这个集群模型具备一定的通用性，又能保证本地推理性能。

2.5.3　去中心化联邦学习

标准的横向联邦学习系统存在服务器单点故障、通信瓶颈等架构层面的问题。基于这些问题，点对点(Peer-to-Peer，P2P)网络中的完全去中心化联邦学习成为了受关注的研究课题[201-204]。将横向联邦学习范式拓展到去中心化的组织架构改变了各方的协作方式，例如模型交换方式从一对多变为多对多，维护一个全局一致的全局模型更加困难。因此，本节重点分析在相关研究中针对去中心化联邦学习系统的信息传播效率、模型聚合方法以及模型管理与验证问题的解决方法。

在信息传播效率方面，在 P2P 网络拓扑中传递信息的成本高于中心化的星状拓扑。标准横向联邦学习中的客户端与服务器逻辑通信距离为一跳，而 P2P 网络中非邻居节点通信距离为多跳，因此很多研究针对去中心化拓扑的通信方式进行优化。Hu 等人[201]利用 Gossip 协议在 P2P 网络中传播模型，同时采用模型分片的技术将模型的传输开销分散到多个链路上去，充分利用多链路带宽的同时利用冗余分片提供了容错能力。类似地，横向联邦学习系统 IPLS[205]也采用了模型分片技术，同时基于星际文件系统(Interplanetary File System，IPFS)技术支持节点自主启动训练和中途加入/退出训练。在聚合方法方面，基于 Gossip 的协作算法可以采用梯度聚合(aggregate)和模型合并(merge)这两种方式[203]。前者是指节点接收来自多个其它节点的梯度，将它们合并后用于更新自己的模型。后者则是直接将本地模型与任一收到的模型进行合并。值得一提的是，去中心化系统不能忽略设备在网络中的可达性，模型组播操作要考虑成本和效率的权衡。

去中心化架构天然缺少可信的中心节点，这就导致模型难以被可靠管理和验证。很多现有研究借助区块链等技术来解决相关问题[176,206]。Warnat-Herresthal 等人[207]提出了一种称为群体学习(Swarm Learning)的去中心化训练框架，用于跨多个医疗机构协同构建模型。该框架通过 Swarm 网络共享参数，引入区块链和智能合约实现节点注册和模型管理。区块链的一个突出问题是需要很高的验证成本才能在网络内达成共识。为此，Li 等人[208]提出了一种新的去中心化架构 BFLC，在区块链的基础上引入委员会机制，由共识委员会(consensus committee)验证各设备上传的模型更新，将验证通过的模型更新放置到区块链上，并基于智能合约触发模型聚合操作。

3 系统框架与代码库

联邦学习研究的热潮推动了系统框架/平台以及各类应用的发展。本节首先描述主流的横向联邦学习开源框架的关键特性(关于框架的详细介绍可参考文献[27]),然后对它们进行对比分析。

3.1 开源框架

3.1.1 TensorFlow Federated

TensorFlow Federated(简称 TFF)①是由谷歌主导的 TensorFlow② 社区下的项目,是联邦学习提出后最早出现的开源框架③之一。TFF 建立在开源机器学习库 TensorFlow(TF)之上,以 TF 中的计算图等核心模块为引擎,提供了两个级别的 API,即 Federated Learning API 和 Federated Core API,能够满足敏捷的开发需求和灵活的研究需求。

TFF 目前只提供 Python 的编程接口,官方文档推荐使用 Keras 库来编写模型。TFF 的开发和设计主要面向的是横向联邦学习范式,运行方式上支持单机模拟和基于移动设备的分布式训练。TFF 支持 Windows 和 Linux 等操作系统,但是目前除基于 DP-SGD 的差分隐私外,尚未提供丰富的多方安全计算的能力,而且无法直接扩展到去中心化的 HFL 训练架构。

3.1.2 PySyft

PySyft 是一个用于在协同机器学习中实现信息安全和隐私保护的开源 Python 代码库④,集成了非常丰富的安全多方技术接口,包括构建 HFL 系统常用的同态加密、差分隐私以及基于 SPDZ 的多方安全计算。其中同态加密的实现主要依赖 TenSEAL 代码库,使用 CKKS 技术;而差分隐私则支持 DP-SGD 中的 Moment、Laplace 多种噪音生成机制。PySyft 能够帮助开发者很方便地结合主流的机器学习框架,在现有的分布式系统中实现安全多方计算。

PySyft 代码库针对横向联邦学习的数据设定提供了一系列应用程序接口,既能用于安全地在多个节点的数据上执行协同训练,也能针对大数据集做逻辑分割和封装,为伪分布式和仿真环境下的实验提供便利。PySyft 仅提供 Python 接口,该代码库专注于安全和隐私保护相关协议的实现,本身不包含机器学习的核心逻辑(如模型定义和训练算法),并且不提供完整的建模流水线或模型部署方案。

3.1.3 FATE

FATE⑤ 是由微众银行主导开发和维护的一个工业级开源项目,内置一系列"开箱即用"的算法、数据以及多种内置的安全计算协议。同时,它还融合了可扩展的建模流水线工具链、清晰的可视化界面和灵活的调度系统。

在系统架构方面,FATE 依托云原生技术的 KubeFATE 模式,支持容器化任务部署和集群管理,而计算存储层的后端可以在 EggRoll 和 Spark 这两种分布式计算引擎中选择。FATE 的核心组件层是基于 FATE 项目下的 FederatedML 库⑥搭建,实现了一系列常用的联邦学习算法的标准实现以及算法的开发接口和基础模型。DHKE、Paillier、SPDZ 和 OT 等加密或安全多方计算协议的标准实现包含在该库的安全协议模块中。

FATE 项目下的 FATE-Serving⑦ 是一个高度集成的平台,提供模型部署流水线工具链,基本上覆盖了从输出后处理到模型 A/B 测试的所有工作流程。FATE-Serving 在底层实现了十分完善的模型存储和管理功能,同时引入了分布式缓存和预热调度等机制用于加速模型调用与推理。

3.1.4 PaddleFL

PaddleFL⑧ 是基于深度学习平台飞桨(PaddlePaddle)[209]开发的开源 FL 框架。作为百度研发和维护的飞桨生态系统下的项目,PaddleFL 可用于在大规模设备集群上部署横向联邦学习系统,同时也支持在数个数据仓储上构建纵向联邦学习系统。PaddleFL 为开发者提供了多种多样的数据预处理逻辑、标准模型、安全协议以及一系列内置的训练算法。在可扩展性方面,PaddleFL 基于云原生容器编排框架 Kubernetes⑨ 提供了在大规模设备集群上对训练任务进行弹性调度和灵活部署的能力。

在兼容性方面,PaddleFL 同时提供 Python 和 C++两种编程接口,支持 Windows、Linux 和 Mac 等操作系统上的单机模拟运行,同时基于 gRPC 通信后端支持分布式训练,但是目前没有提供专门针对移动设备的训练模式。

① https://www.tensorflow.org/federated/get_started
② https://www.tensorflow.org/
③ https://github.com/tensorflow/federated
④ https://openmined.github.io/PySyft/
⑤ https://fate.fedai.org/
⑥ https://fate.fedai.org/federatedml
⑦ https://fate.fedai.org/fate-serving/
⑧ https://github.com/PaddlePaddle/PaddleFL
⑨ https://kubernetes.io/

3.1.5　FedML

FedML[①] 是一个以同名代码库为核心的开源端到端机器学习平台，提供了边缘 AI 开发包 Edge AI SDK 和 MLOps Cloud 服务组件——前者为 IoT 等边缘环境下的算法开发和模型部署提供了良好的支持，后者则以云服务的形式为真实生产环境下的设备协作提供运行环境。

文献[210]中详细描述了 FedML 的设计理念、核心模块和关键技术。FedML 支持三种不同的运行模式：基于边缘设备的联邦学习、分布式计算和独立仿真。FedML 代码库还集成了最新的 FL 算法（包括 FedOpt、FedGKT、FedNova 等），将模型与数据以打包的形式提供给开发者直接使用，具体分为三类：(1) 线性模型：用于 MNIST、Synthetic 等数据集；(2) 浅层神经网络模型：用于 EMNIST、CIFAR-10、Shakespeare 等数据集；(3) 深度神经网络模型：用于 CINIC-10、StackOverflow 等数据集。

在架构方面，FedML 库以 PyTorch 作为其底层的训练引擎，并使用 MPI[②] 和 MQTT[③] 作为其主要后端网络通信模块。FedML 支持不同操作系统的移动设备（Android 和 iOS）和异构的物联网设备（如 NVIDIA Jetson Nano 和 RaspBerry Pi），在此基础上衍生出了两个扩展框架 FedIoT 和 FedMobile（详见文献[211]）。FedML 提供自定义拓扑的接口，这项功能对去中心化 FL 等拓展范式的研究十分有用。在隐私保护和系统安全方面，FedML 基于密码原语支持多种秘密共享和同态加密技术，同时还专门提供了对抗攻击、后门攻击等 API 接口，帮助使用者衡量系统的鲁棒性。

针对自然语言处理（Natural Language Processing，NLP）、图处理和计算机视觉（Computer Vision，CV）这三个典型应用领域，FedML 平台集成了专门用于领域任务建模的横向联邦学习代码库：FedNLP、FedGraphNN 以及 FedCV。

FedNLP[212] 适用于文本分类、序列实体标记、序列对序列任务和语言建模等，提供了超过 10 个专门用于对 NLP 任务进行实验评估的基准数据集（包括 Sentiment140、WikiNER 和 AGnews 等）。

FedGraphNN[213] 专门为关于图神经网络（Graph Neural Network，GNN）和图处理任务设计，提供了常用的模型，包括图卷积网络（Graph Convolutional Network，GCN）、GraphSage 和图注意力网络（Graph Attention Betwork，GAT）等，同时集成了 FedNAS[214]、FedGKT[215] 和 FedOPT[216] 等算法。

FedCV[217] 集成了四个流行的 CV 数据集（CIFAR-100、GLD-32、PASCAL VOC 和 COCO）和 6 种广泛应用的模型（EfficientNet、MobileNet、ViT、DeeplabV3$^+$、UNet 和 YOLOv5），涵盖了 CV 领域中的三类代表性任务：图像分类、图像分割和目标检测，可用于构建面向 CV 的横向联邦学习应用。在数据方面，提供了一个基于隐狄利克雷（Dirichlet）分布的数据预处理模块，能够将单个数据集逻辑分割成多个非独立同分布的子集。

3.1.6　Flower

Flower[④] 是由 Flower Labs 开发的开源联邦学习框架，支持在云基础设施上的安装部署，同时兼容安卓、iOS 移动设备以及 Raspberry Pi 和 Nvidia Jetson 系列的边缘设备。Flower 提供了良好的跨语言特性（Python、C++ 和 Java），同时在计算调度和内存管理等实现了多方面的优化，在移动和边缘计算等异构资源上有较高的运行效率。

Flower 集成了一系列常用的 HFL 算法，包括 FedAvg、FedProx、QFedAvg 和 FedOpt 等，同时提供抽象接口以方便开发者实现新的 HFL 策略。Flower 还提供了一套端到端的基准测试模块以及与系统部署和管理相关的工具包，可用于调整设备和服务器的性能、带宽设定以及网络状态。

在功能性方面，Flower 支持在虚拟设备上做集中式模拟，也支持在安卓等真实移动设备上开展横向联邦学习。当前版本的 Flower 在安全和隐私协议方面提供的功能比较有限，目前仅以包装类的形式提供了 DP 的实现，且仍处在试验性阶段。

3.1.7　FedJAX

FedJAX[⑤] 是由 Google AI 发布的联邦学习开源框架。FedJAX 基于 JAX 框架搭建，而 JAX 是专门针对机器学习程序的加速框架，针对 GPU 和 TPU 等 AI 加速硬件实现了高性能优化，其主要优势是训练和推理性能。

在架构方面，FedJAX 没有通信模块，因此仅支持单机仿真。功能特性方面，FedJAX 面向 EMNIST 和 Shakespeare 等常用数据集提供了相应的 CNN 和 LSTM 模型，同时提供了 FedAvg、AgnosticFedAvg

① https://fedml.ai
② https://www.open-mpi.org/
③ https://mqtt.org/
④ https://flower.dev/docs/
⑤ https://fedjax.readthedocs.io/en/latest/

和 Mime Lite 等 HFL 算法的标准实现。FedJAX 以简单原语(simple primitives)的方式为开发者提供实现联邦学习算法、预封装数据和模型构建的基本接口。

3.1.8 FederatedScope

FederatedScope[①] 是达摩院智能计算实验室主导开发的联邦学习开源框架,采用面向分布式系统的事件驱动架构,同时提供丰富的接口协助完成算法的自动调参。FederatedScope 对异步联邦学习有很好的支持,引入了一系列与学习范式拓展相关的基准测试组件,包括适用于联邦异构任务学习的 B-FHFL、适用于联邦超参数调优的 FedHPO-B、适用于 PFL 的 pFL-Bench 等。

FederatedScope 将联邦学习抽象为多方之间生产事件和处理事件的过程,通过丰富的事件类型和事件处理行为来描述系统中各方之间的交互行为。该框架目前支持单机仿真和分布式运行,其通信功能分别基于模拟和 gRPC 来实现。在安全和隐私保护方面,支持多种保护消息安全的技术实现,包括用于实现 DP、HE 和 MPC 的基本函数接口,例如噪音注入和秘密分片等。FederatedScope 还内置了各种主动攻击(包括成员推理攻击、属性推理攻击和标签推荐攻击等)和相应的防御模块。

3.1.9 FedLearner

FedLearner 是由字节跳动开源的联邦学习系统框架,但是目前关于该框架的官方文档相对不完善。FedLearner 的主要特点体现在产品化,其架构设计和功能特性与业务关系紧密。

在架构方面,FedLearner 采用基于云原生技术的部署方法,通过 Kubernetes 管理集群和编排训练任务,数据存储后端使用 Hadoop Distributed Filesystem(HDFS)、MySQL 和 Elasticsearch 的组合方案。在功能性方面,FedLearner 支持有两方参与的横向联邦学习和纵向联邦学习,在设计层面将两种范式抽象成一个统一的协作架构,即一对工作节点各自执行模型本地训练,基于 gRPC 通信协议交换中间结果。除了常见的神经网络模型的联合训练以外,FedLearner 针对通用业务需求中的数据求交操作提供了两种技术实现,包括基于时间窗的流式数据对齐以及基于 PSI(Private Set Intersection)的加密数据求交。

FedLearner 的典型应用案例是广告推荐业务。字节跳动凭借今日头条、抖音积累的数据优势,拥有超过 220 万用户标签,对用户行为的分析建模有充分的业务需求。字节跳动联合广告平台方的用户浏览点击数据和电商广告主的用户交易行为数据,基于 Fedlearner 平台进行数据对齐、中间结果的安全交换以及联合模型更新,据称实现了较显著的投放效率增长。FedLearner 的主要问题是集成的横向联邦学习算法、数据集和模型都非常有限,而且目前代码库中提供的样例和模块说明比较少。

3.1.10 FedLab

FedLab[②] 是由 SMILE Lab 开发的轻量级联邦学习开源框架,提供了灵活的 API 以及可靠的基准算法实现,有利于减轻实现和验证新算法的负担。FedLab 以 PyTorch 为基础,为联邦学习的单机仿真和分布式实验提供了通信、压缩、模型优化、数据切分及其他功能性模块。

在架构方面,FedLab 采用分层设计,将整体框架划分为通信层、协议层和算法层,层次之间模块化解耦。FedLab 的通信后端采用 gRPC 和 HTTP,支持丰富的网络拓扑结构,包括星型、环形和网状拓扑。用户可根据需求灵活组合数据处理、模型训练、评估等组件。FedLab 目前主要面向横向联邦学习,在客户端和服务器基本逻辑的基础上实现了 FedAvg、FedNova、SCAFFOLD 等经典算法,同时对拓展范式有良好的支持,提供了聚类联邦学习算法 CFL 和个性化联邦学习算法 Ditto 的标准实现。

在功能性方面,FedLab 支持容器化部署以提供较好的平台兼容性,同时以模块化的方式支持横向联邦学习算法中多个关键技术的优化和拓展,包括客户端协作策略、模型压缩传输和本地优化等。例如,FedLab 实现了同步、异步和半同步的客户端协作,用户可直接调用、改进默认实现或加入新的自定义算法。此外,提供了模型量化和稀疏化的标准方法接口。目前,FedLab 内置了十多个常用数据集和多种标准神经网络模型,但是 FebLab 的当前版本尚未提供加密或多方安全计算相关的模块。

3.2 对比分析

在系统架构方面,除 FedJAX 外大多数开源框架均支持单机仿真和分布式计算两种运行模式,其中 PySyft、FedML 和 Flower 等框架还能提供移动设备上的部署能力,有利于跨设备移动计算场景下

① https://federatedscope.io/
② https://fedlab.readthedocs.io/en/master/index.html

的算法与系统验证。分布式部署的 HFL 系统涉及大量的通信操作，这方面 TFF、FATE、PaddleFL、Flower、FedLearner 等框架都选择使用 gRPC 作为底层通信模块的实现；而 FedML 能够支持更丰富的通信后端选择（包括 gRPC、MPI 和 MQTT），同时支持自定义网络拓扑。有部分框架支持多范式联邦学习，其中 FedML 支持去中心化 HFL 的训练方式，FederatedScope 则为个性化 FL 提供了专门的接口和测试组件。

在功能特性方面，PySyft 提供的接口较为单一，集中在数据隐私与安全保护的功能实现。FedLearner 容器化的特性则有利于快速部署。FedJAX 依托底层的 JAX 加速框架，能够在单机仿真中有效提升 HFL 系统模拟的性能。开箱即用的数据集和模型已经成了大多数框架的标配，例如 TFF、FedML、FedJAX 都提供 EMNIST 和 Shakespeare 数据集接口，其中 FedML 框架还集成了面向 NLP、CV 和图处理任务的专门代码库，内置的 YOLOv5、GCN 等标准模型有利于面向相关领域的横向联邦学习应用的开发。

在兼容性和安全性方面，目前仅 PaddleFL 和 Flower 提供了 Python 以外的编程语言支持，其中 Flower 框架同时支持 Java 和 C++，且提供了优秀的跨平台兼容性，能够在 5 种操作系统上运行；FedML 则通过拓展的代码库 FedMobile 和 FedIoT 提供良好的 IoT 设备与移动设备兼容性。来自产业界的 FATE、PaddleFL 以及 FederatedScope 的共同点是内置了比较丰富的隐私保护与安全技术，例如常用的 DP-SGD 和基于 Paillier 的同态加密等。FedJAX 和 FedLab 目前没有提供内置的隐私计算或安全技术接口，模型加密和差分隐私等功能需要依靠第三方库或用户自己实现。

整体而言，FedML 是众多开源框架中功能特性最为全面的，具备良好的跨平台特性、多运行模式和多范式支持，针对多种领域建模任务提供了丰富的模型和数据集，适合作为算法验证环境。作为对比，FATE 的系统设计更接近工业级，例如其集成的 FATE-Serving 借助容器等云原生技术覆盖了从输出后处理到模型 A/B 测试的所有工作流程，高度服务化的部署能力和流水线设计非常适合应用的开发。

表 5 对比了各框架的主要特性。

表 5　系统框架特性对比

系统框架（提供商）	编程语言	跨平台	运行模式	协同和聚合算法	多范式	隐私与安全技术
TFF（Google）	Python	Windows/Linux/MacOS	单机仿真/分布式	FedAvg/FedSGD/FedKmeans/FedProx 等	仅支持 HFL	DP-SGD
PySyft（OpenMined）	Python	Windows/Linux/MacOS	单机仿真/分布式/移动设备	Fed-MPC/Fed-DP/Fed-HE 等	仅支持 HFL	DP-SGD/CKKS/SPDZ//Additive Secret Sharing
FATE（微众银行）	Python	Linux/MacOS	单机仿真/分布式	FedAvg/Fed-SMPC 等	HFL/VFL/FTL	DHKE/Paillier/OT/SPDZ/Feldman VSS
PaddleFL（百度）	Python/C++	Windows/Linux/MacOS	单机仿真/分布式	FedAvg/DPSGD/SECAGG/PFL 等	HFL/VFL	DP-SGD/ABY3/PrivC
FedML（FedML）	Python	Linux/MacOS/Android/iOS	单机仿真/分布式/移动设备	FedAvg/FedOpt/FedGKT/FedNAS 等	HFL/VFL/去中心化 FL	SecAgg/LightSecAgg/RSA/
Flower（Flower Labs）	Python/Java/C++	Windows/Linux/MacOS/Android/iOS	单机仿真/分布式/移动设备	FedAvg/FedProx/QFedAvg 等	仅支持 HFL	DP-SGD
FedJAX（Google AI）	Python	Windows/Linux/MacOS	单机仿真	FedAvg/Agnostic-FedAvg/Mime 等	仅支持 HFL	目前不支持
FederatedScope（阿里巴巴达摩院）	Python	Windows/Linux/MacOS	单机仿真/分布式	FedAvg/FedProx/FedOpt 等	HFL/VFL/PFL	DP-SGD/Paillier/Additive Secret Sharing/
FedLearner（字节跳动）	Python	Windows/Linux/MacOS	分布式	FedAvg/SecureBoost 等	HFL/VFL	Paillier/DPAUC/sumKL
FedLab（SMILE Lab）	Python	Windows/Linux/MacOS	单机仿真/分布式	FedAvg/FedDyn/Ditto/FedNova/CFL 等	HFL/PFL/聚类 FL	目前不支持

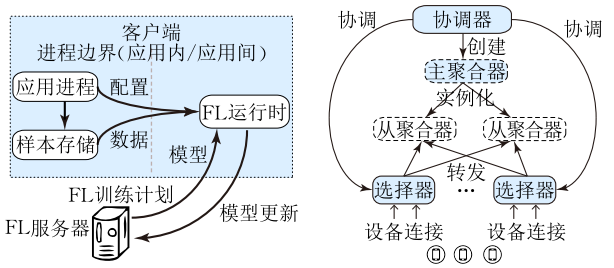
4　实际应用

横向联邦学习在很多 AI 驱动的应用场景下都拥有巨大的潜力，例如导航优化[218-220]、内容推荐[221-222]、医疗保健（例如 NVIDIA Clara Imaging 服务①）和服务推荐[223]等。本节介绍相关的 5 个典型应用或应用场景。

① https://developer.nvidia.com/clara-medical-imaging

4.1 GBoard

谷歌通过在大规模系统中部署横向联邦学习，研发或优化了相当多的商业应用，其中最广为人知的例子是 Google 虚拟键盘 GBoard——广泛用于移动端安卓(Android)系统的智能输入法。谷歌首先面向移动计算环境构建了一个可扩展的、生产级别的横向联邦学习系统。该系统基于 TensorFlow 开发，按照生产标准的高并发设计，能够在数千万真实环境中的用户设备上运行横向联邦学习。系统采用的训练算法基本遵循 FedAvg[15] 的流程设计，同时结合了多种优化技术和工程技巧来解决系统运行中的实际问题。如图 7 所示，系统在发布任务时需要为每个任务生成一个训练计划，以 TensorFlow 计算图的形式描述了模型、设备本地训练的参数配置以及服务端的模型聚合规则，由服务端生成后发送给客户端。系统的服务端架构包含静态型和动态型两种类型的功能模块。系统中扮演全局协调者的协调器和负责与用户设备直接交互的选择器均属于静态型模块。系统中的动态型模块在训练过程中根据设备规模而被动态实例化，例如聚合器负责接收本地模型并执行聚合，其数量是弹性变化的。



(a) 客户端逻辑　　(b) 服务端逻辑

图 7　谷歌研发的横向联邦学习系统[16]中的(a)客户端逻辑和(b)服务端逻辑

谷歌首先针对 GBoard 的三个基本功能开展建模，包括下一单词预测(next word prediction)、自动更正(auto correction)和单词补全(word completion)。为了在内存和数据受限的情况下提高预测质量，谷歌首先更换了模型架构，采用基于耦合输入-遗忘门(Coupled Input-Forget Gates，CIFG)的语言模型，进一步利用 GBoard 庞大的用户基础，在真实用户数据的基础上开展了大规模的横向联邦学习，训练过程涉及北美地区的 150 万用户，总计 3000 轮 HFL 迭代，历时超过 4 天[224]。

对于 GBoard，采用横向联邦学习来提升模型性能、优化用户体验的案例不仅限于基本的下一单词预测功能。谷歌的研究人员针对词汇表外(Out-Of-Vocabulary，OOV)单词处理和表情符号预测等功能对 GBoard 进行了专门的优化[225-226]。此外，谷歌基于横向联邦学习和大量用户行为数据训练了一系列的触发模型(trigger model)，然后以集成的方式将它们用于 GBorad 中的搜索查询建议功能[227](图 8)。GBoard 的这一功能会根据用户当前输入自动地给出查询建议(由基线模型生成，存储在本地 SQLite 数据库)，而触发模型充当过滤器以保留有价值的查询建议，在训练过程根据用户对 GBoard 查询建议的反应进行优化。

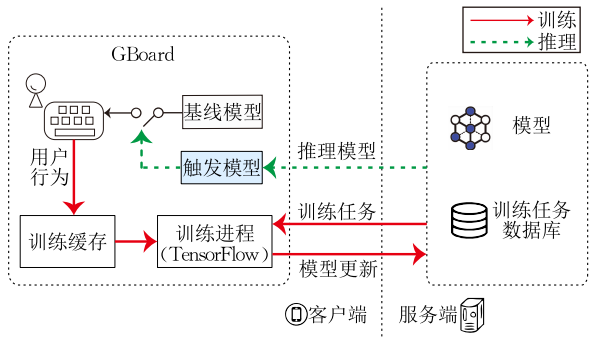


图 8　GBoard 搜索查询推荐功能的应用架构[227]

4.2 FloC

Web 应用中内容推荐和广告业务非常依赖与用户隐私高度相关的浏览数据。谷歌的研究与广告部(Google Research & Ads)针对这一问题做出了雄心勃勃的尝试，提出采用一种名为 FLoC(Federated Learning of Cohorts)[228]的基于用户分组的新技术来取代当下普遍用于存储用户浏览信息的(第三方)cookie。FLoC 旨在通过散列、聚类和联邦学习的方式更好地保护用户的浏览行为隐私，从而减少个人用户的属性过多暴露在互联网上。这种分组技术是根据用户的浏览历史来定义用户的(潜在)喜好。图 9 显示了 FLoC 如何依据属性将用户分组以保证“K 匿名性”(K-anonymity)。在这个案例中，无论采用群

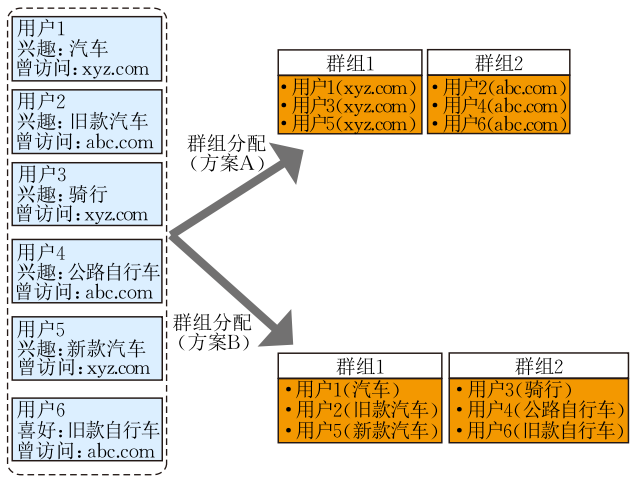


图 9　基于 FLoC 的用户属性匿名化方法[229]

组分配方案 A 或是群组分配方案 B，每个用户都处在一个基数至少为 3 的群组(cohort)中。换言之，通过用群组编号来标识用户，个体行为被隐藏在了群体的特征里。在 FLoC 的设计中，横向联邦学习相关技术用于搭配聚类算法使用，解决用户分组算法存在的隐私问题，技术细节详见文献[229]。

4.3　智慧医疗

在多样化的应用场景中，医疗卫生和医学信息学最受关注[230-231]——这主要是因为临床数据非常敏感，而以生物医学分析和 AI 辅助诊断等为代表的智能医疗应用长期以来严重依赖海量与患者相关的数据[202]。凭借隐私保护方面的特性，横向联邦学习使跨机构协作研发此类服务成为可能，因此被认为是生物医学研究的未来方向之一[232]。

Sheller 等人[233]分析了 HFL 在联合训练诊断模型方面的有效性，报告了一系列实验证据。作者在脑组织标记这一医学图像分析任务中评估了包括集中式训练、(跨机构)增量训练和(横向)联邦学习在内的多种模型训练方法。图 10 为基于横向联邦学习的跨机构协作训练架构。作者设计的实验使用来自 BraTS 2017 数据集(包含多个机构收集的神经胶质瘤数据)以及来自德克萨斯大学 MD 安德森癌症中心和圣路易斯华盛顿大学医学院的临床脑肿瘤 MRI 成像数据。他们的实证研究表明，横向联邦学习训练得到的模型质量(用 Dice Similarity 系数衡量)可以非常接近集中式训练的水平。

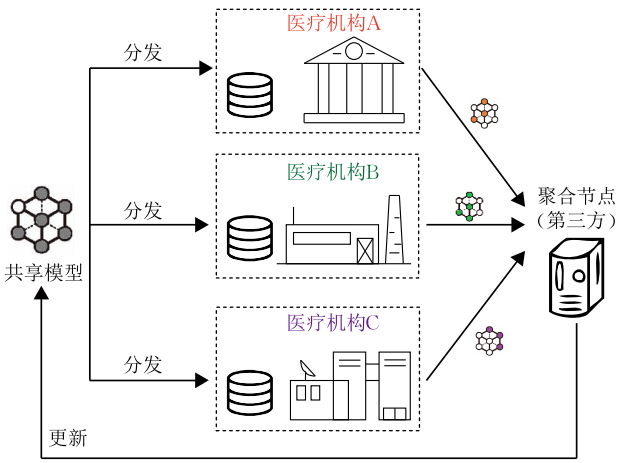


图 10　Sheller 等人[233]的工作中所评估的基于横向联邦学习的协作架构

4.4　网络安全

横向联邦学习能够催化多个企业组织之间的协作，在数据利用和业务建模上实现共赢。与基于大规模终端设备的跨设备场景不同，跨机构协作属于典型的跨筒仓式联邦学习场景，参与协作的机构数量不多，但各方持有的数据体量较大且计算资源较充足。适合在这类场景下开发的应用程序覆盖了很多新兴领域，包括网络安全[234]、智慧城市[235]、智能监控[236-237]和健康信息学[231]等。

安全风险是信息技术领域中相关研究的焦点，安全问题则在软件开发中尤为突出。为了实现自动化异常检测、风险评估这些关键能力，传统的方案一般依赖数据共享来丰富训练样本，提升模型泛化能力，但代价是业务数据的泄露。在这方面，联邦学习可能是最有前景的下一代解决方案。例如，很多网络安全公司使用其专有数据独立地开发自己的风险检测模型，但通过横向联邦学习，他们可以寻求通过多企业协作训练来增强自己的模型，同时无需透露自己的数据。SAP 公司开发了一个名为 Credential Digger[54]的代码扫描工具，它的核心是基于异步协同算法在私有代码仓库上训练出来的敏感代码口令检测模型。随着越来越多的风险感知、口令泄漏和异常检测工具成为模型驱动，并且建立在大量日志数据之上，横向联邦学习有望成为基于跨组织协作的下一代安全解决方案的基础框架。

4.5　智慧城市

从大数据中学习是实现智慧城市的关键路线，其中有许多日常应用都存在数据共享的现实困难，因此是可以预见的未来内会应用横向联邦学习的可能场景。例如，以 UberEats① 为代表的送餐、快递和打车服务每天都能从大量的用户订单中收集 TB 甚至 PB 级别的数据；考虑到数据的隐私属性，研究提出可以使用基于横向联邦学习的技术对这些应用进行优化[238-239]。交通管理是大都市发展中长期面临的难题，也是实现智慧城市过程中的主要课题。考虑到交通数据存在的不互通问题，Liu 等人[235]提出了以门控循环单元(Gated Recurrent Unit，GRU)网络作为预测模型、基于横向联邦学习的交通流预测(Traffic Flow Prediction，TFP)解决方案 FedGRU。为了解决 TFP 中的“数据孤岛”问题，他们使用了一种基于客户端聚类的横向联邦学习算法，围绕不同机构持有的交通数据构建了一个隐私保护训练框架(图 11)。在协调各机构的同时，FedGRU 根据协同规模进行参与方的下采样，采用一种称为联合公告协议(joint-announcement protocol)的技术来协调全局迭代过程。

① https://eng.uber.com/michelangelo-machine-learning-platform

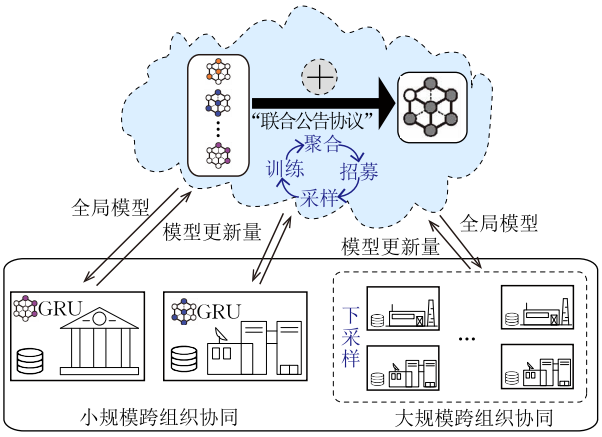


图 11 多规模跨组织场景下的 TFP 建模框架[235]

5 数据集与数据准备方法

5.1 公开数据集

横向联邦学习能够广泛地用于几乎所有领域的机器学习任务,目前已有十分丰富的横向联邦学习数据集可直接用于学术研究和应用验证。这类数据集的特点是带有天然的样本划分属性,例如用户名、设备编号和文本作者等。我们在表 6 中汇总了相关研究工作中提供或使用的横向联邦学习数据集,其中一些来自 LEAF 等公开的数据仓库。表 6 中的"子域数量"可以被理解为数据子集数量(每个子集对应一个本地数据集,即一个子域)。例如,这些子域可以对应书写体图片数据集 FEMNIST 中的书写者、推文数据集 Sentiment140 中的推特用户和剧本数据集 Shakespeare 中的角色。在表 6 中,最后一列注明的是数据集的发布者,而不是样本来源①。

数据集的数据体量、数据分布以及对应的任务难度等都是横向联邦学习算法验证过程中需要考虑的因素,例如 NLP 领域的 Sentiment140 和 Reddit 数据集包含数量众多的子域,每个子域中的词频分布可能存在较大差异。对于算法的性能评测,通用的评估指标大致可以分为三类:(1)算法有效性指标,包括模型的准确率(或误差)、全局目标函数值等;(2)算法效率指标,包括全局模型收敛所需的训练轮数、平均每轮时长、总训练时长等;(3)算法成本指标,包括训练和通信过程产生的资源开销、设备能耗等。

表 6 横向联邦学习公开数据集一览表

数据集	任务	样本数	子域数量	发布者/所属代码库
Street-5/20	目标识别	956	5/20	FedAI[9]
FEMNIST	图片分类	805263	3550	LEAF[240]
Shakespeare	台词预测	422615	1129	LEAF
Sentiment140	情感分析	1600498	660120	Kaggle LEAF
Celeba	图片分类	200288	9343	LEAF
Reddit	语言建模	56587343	1660820	LEAF
BigQuery	多目标预测	146404765	342477	StackOverflow
AGNews	文本分类	127600	1000	FedNLP[212]
20News	文本分类	18842	100	FedNLP
SST2	文本分类	8742	30	FedNLP
PLONER	序列标记	17501	50	FedNLP
W-NUT	序列标记	4681	30	FedNLP
WikiNER	序列标记	286495	1000	FedNLP
SQuAD	自动问答	122325	300	FedNLP
Movie-Dialogs	文本生成	221634	617	FedNLP
CNN/DM	文本生成	312085	100	FedNLP
hERG	回归(生物物理)	10572	4	FedGraphNN[213]
QM9	回归(量子力学)	133885	8	FedGraphNN
ESOL	回归(物理化学)	1128	4	FedGraphNN
FreeSolv	回归(物理化学)	642	4	FedGraphNN
Lipophilicity	回归(物理化学)	4200	8	FedGraphNN
BACE	分类(生物物理)	1513	4	FedGraphNN
BBBP	分类(生物物理)	2039	4	FedGraphNN
SIDER	分类(生理学)	1427	4	FedGraphNN
ClinTox	分类(生理学)	1478	4	FedGraphNN
Tox21	分类(生理学)	7831	8	FedGraphNN
GLD-23K	图片分类	23080	233	FedCV[217]
CIFAR-100-LDA	图片分类	60000	100	FedCV
PASCAL VOC	图片分类	11355	8/4	FedCV
COCO	图片分类	328000	10	FedCV

① 有些横向联邦学习数据集(如 FEMNIST)是依据附加属性对完整数据集的划分结果

5.2　数据准备方法

面向横向联邦学习的算法和协议设计都应该在相应的数据设定下进行评估。对于真实分布式场景，数据集天然与设备绑定，应保证：(1) 客户端之间不能共享本地数据集；(2) 服务器不能访问任何本地数据集。对于单机仿真实验环境，需要首先对一个完整的数据集进行划分，数据的统计学异构性应当在数据划分方法上有所体现：(1) 本地样本量通常呈非均匀分布；(2) 数据分布通常是统计学异构的。

在机器学习领域中，很多常用且优质的大数据集是开放下载的。因此，仿真实验中准备数据的一个简单方法是将一个源数据集手动划分为多个子集，将各子集分配给客户端作为本地数据。例如，MNIST[241]、CIFAR-10/100[242] 和 ImageNet[243] 等流行的图像分类数据集通过一些规则进行拆分后可用于 HFL 算法评估，很多现有研究都采用这种方式开展实验[40,100,192,244]。数据划分的规则决定了本地数据分布和异构程度。以分类任务为例，可以基于某种概率分布（例如 Dirichlet 分布）控制类别比例以制造类不平衡的本地数据集。基于人工划分的数据准备方法非常适合用于敏捷地实现算法验证。例如 Google Research 的研究人员在实验中将 CIFAR-10/100 和 AmazonCat 等数据集人工划分后作为客户端的本地数据集（例如 CIFAR-10 数据集按照样本标签被分为了 10 个不重叠的子集分给 10 个客户端），搭建出了数据极端分布的实验环境[104]。

以自然语言处理任务中常用的 Sentiment140 数据集为例，该数据集记录的是部分推特（Twitter）用户发布的推文（tweet）、推文的情感类别（消极或积极）以及时间戳等信息。图 12 展示了一种可以采取的数据准备方式。该数据集整体以 json 格式保存（为便于理解，图中以表的形式展现），包含各个推特用户的用户名和 tweet 文本等数据信息，因此每个推特用户的数据天然对应了一个客户端的本地数据集，这在原理上最符合用户数据和设备之间的对应关系。

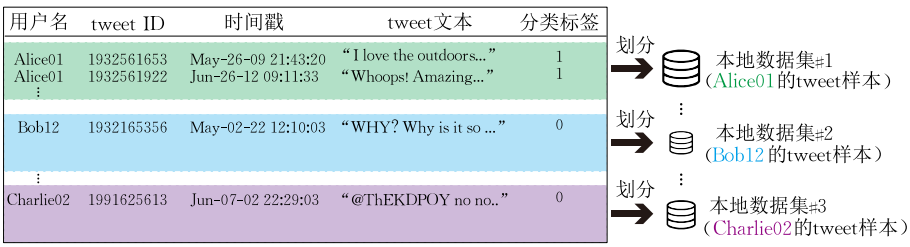


图 12　基于 Sentiment140 数据集的数据划分案例

6　研究与实践的挑战

横向联邦学习丰富的技术图谱为相关研究提供了宽阔的空间，但也造成了算法研究与系统应用实践之间的鸿沟。结合领域现状分析，本节将围绕横向联邦学习研究和系统实践面临的挑战展开讨论。

6.1　算法复现

FATE 和 FedML 等系统框架“开箱即用”的功能特性受到很多研究者和开发人员的青睐。它们提供的关键模块、预设配置、预定义模型和内置数据集很好地促进了基于通用联邦学习逻辑的原型系统和应用程序的敏捷开发。但在另一方面，通过不断增加新的模块和新的特性，这些平台使自己变得越来越庞大和复杂——这不可避免地带来了 bug、功能冗余、较差的向后兼容性和过度封装等问题。为了复现训练算法，用户必须处理系统相关、数据相关和模型相关的各种配置，并花费大量时间来学习哪些 API 是有用的以及它们是如何工作的。对于优先考虑算法研发效率和快速验证的研究人员来说，上述问题是这些平台的缺点。

代码库和开发框架的 API 设计的核心问题是灵活性和可用性之间的权衡。设计一个既涵盖高层抽象 API（满足需要低代码实现的应用程序开发人员），又提供丰富的底层基础操作 API（满足需要算法灵活性的研究人员）这样精细层次结构的横向联邦学习代码库和框架极具挑战性。同时，从使用的角度来看，开发者在选择相应的代码库和平台之前，应当首先充分明确自己的需求——是追求行业导向的敏捷开发，还是研究导向的算法试验。

6.2　算法有效性

横向联邦学习的核心价值在于数据的联合。考虑到面向横向联邦学习的应用研发是一个较庞大的系统工程，在技术选型的阶段首先应该回答两个核

心问题:(1)如何判定横向联邦学习适用性和必要性?(2)各种横向联邦学习算法是否能有效为目标任务带来实质性收益?

对于第一个问题,横向联邦学习相对于独立训练(即仅使用本地数据进行训练)的优势在大多数情况下是显而易见的,前提是每个本地数据集所能提供的知识都不足以完成学习任务——这是大多数横向联邦学习研究所依赖的基本假设(尽管可能没有明确提及)。然而不应忽视的是,理论上和实际上都存在协同训练(几乎)没有意义的情况。首先,学习任务的难度很重要。当每个本地数据集都足够大且信息量足以支持独立训练得到强大的模型时(尽管如果协作训练可能会更强大),那么横向联邦学习的必要性就要仔细考量了,因为性能增益可能无法弥补成本增加(除非每 0.01%的模型性能提高都是至关重要的)。

对于第二个问题,横向联邦学习算法的有效性与多种因素相关,算法对数据、设备等条件可能非常敏感。因此,在横向联邦学习系统的设计和研发阶段,在评估是否真的需要基于横向联邦学习来实现目标任务优化的基础上,还需要进一步结合应用需求、系统架构、数据条件等因素选择合适的横向联邦学习算法。各种算法具备的优势都是体现在特定的数据或系统设定下,而论文中给出的理论分析结果未必适用于实际场景。因此,在实践中需综合考量应用的优化目标(例如迭代次数最少、模型准确率最高),对各种算法进行综合调试比对后再进行应用部署。

6.3 复杂异构性

相较于学术研究,横向联邦学习系统研发中面临的一大挑战是设备和数据的异构性都可能比论文中假设的更加复杂。在设备异构性方面,除了性能之外,设备在可访问性和负载承受能力上也存在差异。在很多面向弱终端的场景(例如工业物联网)下,还需要确保本地训练不会使设备过载而影响时延等关键业务指标。设备异构性对系统的开发提出了巨大的挑战。从算法设计的角度来看,掉队者效应和拜占庭设备等问题很难通过算法彻底解决。从工程开发的角度来看,要兼容成百上千种设备型号、种类繁多的机器学习框架和不同的操作系统,无疑给用户端的程序开发和应用配置带来了巨大的挑战和沉重的负担,因此定制化的横向联邦学习系统可能更适合小规模应用。在数据异构性方面,除了相关研究通常做出的统计学分布方面和数据量方面的异构性假设,与实际生产关联的数据(例如工业数据)往往还存在标签缺失、样本质量混杂、概念漂移等问题,这使得联合多个数据集挖掘共性知识更加困难。因此,需要在隐私保护的基础上研究如何更好的衡量本地数据的训练价值,探索在这些复杂异构性条件下优化全局模型泛化能力的方法。

6.4 激励机制

横向联邦学习充分利用了分布式计算和分布式数据存储的优势,与众包(crowdsourcing)和群智感知(crowdsensing)[245-246]等新兴场景有很高的契合度。在这类系统中,作为客户端的用户设备往往是自治的、自由的、自利的,要求客户端无偿参与训练并不现实,尤其是当参与横向联邦学习的各方(比如营利性企业机构)都以提升自身利益为目标的情况下,需要研究相应的激励机制[247-248]。以招募大量用户设备为基础的系统必须要考虑设备可靠性、可信度等现实问题。

从任务发布者的角度来看,动态评估各参与设备在信用和在训练过程中的贡献非常重要[249-251]。完善的客户端信用评级方法可以使系统对恶意的、不可靠的客户端更具抵抗力,最小化拜占庭设备对联合训练的影响。区块链等技术能保证信用系统的可信度和可靠性[208,252],而奖励的发放可以基于智能合约实现,但这类技术会增加系统的计算、存储负担。如何衡量参与训练的客户端的贡献是另一个现实问题。很多研究采用有理论支撑的价值衡量方法,例如基于数据剔出和 Shapley 价值的方法[253-254]。从本质上分析,现有解决方案大多数是从边际效用的角度出发。这些方法的问题是计算成本极高(例如需要遍历幂集)。针对计算复杂度问题,已经有一些研究基于横向联邦学习的迭代特性,利用历史记录对 Shapley 价值等贡献评估算法进行了相应的改进[255]。考虑到现实系统中利益分配的重要性,易扩展的、轻量级的贡献衡量方案很可能将成为未来研究的重点。

6.5 系统拓扑

横向联邦学习的流行在很大程度上得益于客户机-服务器这种通信模式的普遍性。在大多数情况下,这种集中式拓扑结构是最自然的选择,然而现实应用中仍然存在该模式不(完全)适用的情况,例如多智能体机器人系统、基于车辆互联的智能交通和智慧医疗等[256-258]。一般来说,典型的跨筒仓联邦学习场景不适合使用中心化的网络拓扑,因为各方不完全信任其它参与方,也不希望引入第三方协调者。一些研究工作立足于对等网络、点对点通信方

式进行横向联邦学习算法和协议设计[202-203]。即便如此，去中心化网络最核心的问题依然是信息传播效率——没有了中心节点（hub 节点），模型信息的传播就要经过更多的平均跳数。因此，在流量受限的条件下，如何设计算法和通信协议以在这类网络中传播更多、更有用的模型信息，是需要深入研究的关键问题。

一种更加复杂的组网方式是自组织网络（self-organizing networks）。自组织网络的特点是拓扑结构的动态变化性。现有的探索性研究主要停留在全相连、固定拓扑结构的设定上，对去中心化网络拓扑中节点（即客户端）的动态加入和退出考虑不足。随着“万物互联”时代的到来，移动自组织网络（Mobile Ad hoc Network，MANET）和车联自组织网络（Vehicular Ad hoc Network，VANET）为特点的应用场景变得越来越普遍，面向这类网络环境的横向联邦学习算法设计和系统研发应当更多地围绕应用需求，充分考虑网络的动态因素。

6.6　前沿技术融合

横向联邦学习系统覆盖了十分宽泛的技术图谱，展现了跨学科、跨领域的系统工程特性。各领域的新兴技术与横向联邦学习的深度融合有望解决在系统规模化部署和自治能力方面的问题。

系统部署方面，相关研究开始将目光投向联邦学习在边缘计算中的应用，即基于联邦学习实现边缘智能（Edge Intelligence，EI）[55]。但是从研究现状来看，仍有多个亟需解决的关键问题，包括通信成本、无标签数据、移动设备互扰等[107]。此外，横向联邦学习在物联网（Internet of Things，IoT）相关场景中的应用亦受到了广泛关注。IoT 设备如同网络边缘的神经末梢，是最靠近数据的设备，因此基于 IoT 设备和边缘节点构建横向联邦学习系统逐渐成为现实需求[189]。横向联邦学习与 IoT 融合的焦点在于利用联邦学习的协同能力优化 IoT 系统的智能水平，主要包括两个层次：IoT 的基础功能以及 IoT 的上层应用[259]。在基础功能方面，借助横向联邦学习能优化 IoT 系统中的任务调度与缓存管理、攻击与异常检测、实时定位和移动群智感知等。在上层应用方面，横向联邦学习可用于各类涉及智能与数据隐私的 IoT 场景，例如基于数字孪生的工业物联网[260]。

在系统治理方面，区块链技术已经与横向联邦学习框架有机结合，能解决隐私保护、模型管理、信用管理等一系列问题[208,252,261]。作为代价，设备为了成为合法的训练节点，需要承担额外的计算和存储，某些情况下还需要通过竞争才能成功参与训练，这会影响诚实用户的积极性，需要配合激励机制等措施进一步完善。

7　结　论

在数据与算力向网络边缘下沉的背景下，横向联邦学习的提出为隐私敏感场景下的 AI 应用研发提供了一条新的路线。围绕横向联邦学习这一前沿方向，本文首先对相关领域内的文献按照五个研究分支进行了全面的分类梳理，更好展现了研究现状的全景。其次，介绍了广泛使用的开源系统框架以及典型应用案例，汇总了一系列可直接用于算法验证的公开数据集，描述了实验数据准备方法。从研究现状来看，横向联邦学习在机器学习领域中的受关注度最高，但在通信和分布式系统层面仍需深入探索。从应用实践来看，开源框架众多且呈现了云原生化的趋势，但是根据需求自行搭建平台或系统仍是较流行的选择。

基于现状分析，本文探讨了横向联邦学习算法研究和系统构建中的主要挑战。一方面，指出了该方向的研究与实践之间存在鸿沟，即实际应用中的算法复现、算法有效性和系统复杂异构性等问题在研究中未得到充分关注，我们认为在应用之前需要对算法的适用性做出衡量。另一方面，针对横向联邦学习的主要应用场景，本文论述了激励机制和动态系统拓扑等现有算法研究未能完全解决的难点，描述了横向联邦学习与区块链、物联网等前沿技术融合带来的新问题，讨论了在系统自治管理等方向上的研究机遇与挑战，以多视角的分析综合为相关领域的研究者和从业者提供了新的研究思路和实践参考。

参　考　文　献

[1] Tolstikhin I O, Houlsby N, Kolesnikov A, et al. MLP-mixer: An all-MLP architecture for vision//Proceedings of the 35th Conference on Neural Information Processing Systems. 2021: 1-12

[2] Liang W, Xue F, Liu Y, et al. Unknown sniffer for object detection: Don't turn a blind eye to unknown objects//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Vancouver, Canada, 2023: 3230-3239

[3] Xu Z, Zhang Y, Shperberg S S, et al. Model-based meta automatic curriculum learning//Proceedings of the Lifelong Learning Agents. Montreal, Canada, 2023: 846-860

[4] Baevski A, Hsu W N, Conneau A, et al. Unsupervised speech recognition//Proceedings of the 35th Conference on Neural Information Processing Systems. 2021: 1-14

[5] Jin D, Huo C, Liang C, et al. Heterogeneous graph neural network via attribute completion//Proceedings of the Web Conference 2021. 2021: 391-400

[6] Brown T B, Mann B, Ryder N, et al. Language models are few-shot learners//Proceedings of the Advances in Neural Information Processing Systems. 2020, 33: 1877-1901

[7] Xie C, Zheng S, Koyejo S, et al. CSER: Communication-efficient SGD with error reset//Proceedings of the Advances in Neural Information Processing Systems. 2020: 12593-12603

[8] Kumar M, Horn W P, Kepner J, et al. IBM POWER9 and cognitive computing. IBM Journal of Research and Development, 2018, 62(4/5): 10:1-10:12

[9] Luo J, Wu X, Luo Y, et al. Real-world image datasets for federated learning. arXiv preprint arXiv:1910.11089, 2019

[10] Zhu L, Liu Z, Han S. Deep leakage from gradients//Proceedings of the 33rd International Conference on Neural Information Processing Systems. Vancouver, Canada, 2019: 14774-14784

[11] Geiping J, Bauermeister H, Dröge H, et al. Inverting gradients-how easy is it to break privacy in federated learning?//Proceedings of the Advances in Neural Information Processing Systems. 2020: 16937-16947

[12] Zhou Z, Chen X, Li E, et al. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proceedings of the IEEE, 2019, 107(8): 1738-1762

[13] van der Meulen R. What edge computing means for infrastructure and operations leaders. https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders, 2018

[14] Konecný J, McMahan H B, Ramage D, et al. Federated optimization: Distributed machine learning for on-device intelligence. arXiv preprint arXiv:1610.02527, 2016

[15] McMahan H B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data//Proceedings of the Artificial Intelligence and Statistics(AIST-ATS). Ft. Lauderdale, USA, 2017: 1273-1282

[16] Bonawitz K, Eichner H, Grieskamp W, et al. Towards federated learning at scale: System design//Proceedings of the 2nd SysML Conference. Standford, USA, 2019

[17] Kairouz P, McMahan H B, Avent B, et al. Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 2021, 14(1-2): 1-210

[18] Gartner. Summary translation: Hype cycle for data science and machine learning. https://www.gartner.com/en/documents/4005710, 2021

[19] Wan S, Lu J, Fan P. How global observation works in federated learning: Integrating vertical training into horizontal federated learning. IEEE Internet of Things Journal, 2023, 10(11): 9482-9497

[20] IEEE Standard 3652.1-2020. IEEE guide for architectural framework and application of federated machine learning. https://standards.ieee.org/standard/3652_1-2020.html, 2020

[21] Yang Qiang, Tong Yong-Xin, Wang Yan-Sheng, et al. A survey on federated learning in crowd intelligence. Chinese Journal of Intelligent Science and Technology, 2022, 4(1): 29-44(in Chinese)
(杨强, 童咏昕, 王晏晟等. 群体智能中的联邦学习算法综述. 智能科学与技术学报, 2022, 4(1): 29-44)

[22] Yang Q, Liu Y, Chen T, et al. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology(TIST), 2019, 10(2): 1-19

[23] Wang Jian-Zong, Kong Ling-Wei, Huang Zhang-Cheng, et al. Research review of federated learning algorithms. Big Data Research, 2020, 6(6): 64-82(in Chinese)
(王健宗, 孔令炜, 黄章成等. 联邦学习算法综述. 大数据, 2020, 6(6): 64-82)

[24] Sun Bing, Liu Yan, Wang Tian, et al. Survey on optimization of federated learning efficiency in mobile edge network. Journal of Computer Research and Development, 2022, 59(7): 1439-1469(in Chinese)
(孙兵, 刘艳, 王田等. 移动边缘网络中联邦学习效率优化综述. 计算机研究与发展, 2022, 59(7): 1439-1469)

[25] Sun Shuang, Li Xiao-Hui, Liu Yan, et al. Survey on security and privacy protection in different scenarios of federated learning. Application Research of Computers, 2021, 38(12): 3527-3534(in Chinese)
(孙爽, 李晓会, 刘妍等. 不同场景的联邦学习安全与隐私保护研究综述. 计算机应用研究, 2021, 38(12): 3527-3534)

[26] Li T, Sahu A, Talwalkar A S, et al. Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 2020, 37: 50-60

[27] Lin Wei-Wei, Shi Fang, Zeng Lan, et al. A survey of federated learning open-source frameworks. Journal of Computer Research and Development, 2023, 60(7): 1551-1580(in Chinese)
(林伟伟, 石方, 曾岚等. 联邦学习开源框架综述. 计算机研究与发展, 2023, 60(7): 1551-1580)

[28] Li Q, Wen Z, Wu Z, et al. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. IEEE Transactions on Knowledge and Data Engineering, 2021, 35(4): 3347-3366

[29] Haddadpour F, Mahdavi M. On the convergence of local descent methods in federated learning. arXiv preprint arXiv: 1910.14425, 2019

[30] Niu C, Wu F, Tang S, et al. Billion-scale federated learning on mobile clients: A submodel design with tunable privacy//Proceedings of the 26th Annual International Conference on Mobile Computing and Networking. London, UK, 2020: 1-14

[31] Liu S, Yu G, Yin R, et al. Adaptive network pruning for wireless federated learning. IEEE Wireless Communications Letters, 2021, 10(7): 1572-1576

[32] Jiang Y, Wang S, Valls V, et al. Model pruning enables efficient federated learning on edge devices. IEEE Transactions on Neural Networks and Learning Systems, 2023, 34(12): 10374-10386

[33] Liu R, Wu F, Wu C, et al. No one left behind: Inclusive federated learning over heterogeneous devices//Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Washington, USA, 2022: 3398-3406

[34] Yoshida N, Nishio T, Morikura M, et al. Hybrid-FL for wireless networks: Cooperative learning mechanism using non-IID data//Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC). 2020: 1-7

[35] Ji Z, Chen L, Zhao N, et al. Computation offloading for edge-assisted federated learning. IEEE Transactions on Vehicular Technology, 2021, 70(9): 9330-9344

[36] Ye Y, Li S, Liu F, et al. EdgeFed: Optimized federated learning based on edge computing. IEEE Access, 2020, 8: 209191-209198

[37] Zhao J, Han R, Yang Y, et al. Federated learning with heterogeneity-aware probabilistic synchronous parallel on edge. IEEE Transactions on Services Computing, 2021, 15(2): 614-626

[38] Li X, Huang K, Yang W, et al. On the convergence of FedAvg on non-IID data//Proceedings of the International Conference on Learning Representations (ICLR). Addis Ababa, Ethiopia, 2020: 1-26

[39] Charles Z, Konečný J. Convergence and accuracy trade-offs in federated learning and meta-learning//Proceedings of the International Conference on Artificial Intelligence and Statistics. 2021: 2575-2583

[40] Wu W, He L, Lin W, et al. SAFA: A semi-asynchronous protocol for fast federated learning with low overhead. IEEE Transactions on Computers, 2020, 70(5): 655-668

[41] Nguyen J, Malik K, Zhan H, et al. Federated learning with buffered asynchronous aggregation//Proceedings of the International Conference on Artificial Intelligence and Statistics. 2022: 3581-3607

[42] Li J, He L, Ren S, et al. Developing a loss prediction-based asynchronous stochastic gradient descent algorithm for distributed training of deep neural networks//Proceedings of the 49th International Conference on Parallel Processing (ICPP). Edmonton, Canada, 2020: 1-10

[43] Abdelmoniem A M, Ho C Y, Papageorgiou P, et al. Empirical analysis of federated learning in heterogeneous environments //Proceedings of the 2nd European Workshop on Machine Learning and Systems. Rennes, France, 2022: 1-9

[44] Chai Z, Fayyaz H, Fayyaz Z, et al. Towards taming the resource and data heterogeneity in federated learning//Proceedings of the 2019 USENIX Conference on Operational Machine Learning (OpML 19). Santa Clara, USA, 2019: 19-21

[45] Xu C, Qu Y, Xiang Y, et al. Asynchronous federated learning on heterogeneous devices: A survey. arXiv preprint arXiv: 2109.04269, 2021

[46] Chai Z, Ali A, Zawad S, et al. TiFL: A tier-based federated learning system//Proceedings of the 29th International Symposium on High-Performance Parallel and Distributed Computing (HPDC). Stockholm, Sweden, 2020: 125-136

[47] Li G, Hu Y, Zhang M, et al. FedHiSyn: A hierarchical synchronous federated learning framework for resource and data heterogeneity//Proceedings of the 51st International Conference on Parallel Processing. 2022: 1-11

[48] Chen Y, Ning Y, Slawski M, et al. Asynchronous online federated learning for edge devices with non-IID data//Proceedings of the 2020 IEEE International Conference on Big Data (Big Data). Atlanta, USA, 2020: 15-24

[49] Kairouz P, McMahan B, Song S, et al. Practical and private (deep) learning without sampling or shuffling//Proceedings of the International Conference on Machine Learning. 2021: 5213-5225

[50] Nadiradze G, Markov I, Chatterjee B, et al. Elastic consistency: A practical consistency model for distributed stochastic gradient descent//Proceedings of the AAAI Conference on Artificial Intelligence. 2021: 2-9

[51] Lu Y, Huang X, Dai Y, et al. Differentially private asynchronous federated learning for mobile edge computing in urban informatics. IEEE Transactions on Industrial Informatics, 2019, 16(3): 2134-2143

[52] Xie C, Koyejo S, Gupta I. Asynchronous federated optimization. arXiv preprint arXiv: 1903.03934, 2019

[53] Dean J, Corrado G, Monga R, et al. Large scale distributed deep networks//Proceedings of the 25th International Conference on Neural Information Processing Systems. Lake Tahoe, USA, 2012: 1223-1231

[54] Kall S, Trabelsi S. An asynchronous federated learning approach for a security source code scanner//Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP). 2021: 572-579

[55] Wang S, Tuor T, Salonidis T, et al. Adaptive federated learning in resource constrained edge computing systems. IEEE Journal on Selected Areas in Communications, 2019, 37(6): 1205-1221

[56] Abadi M, Chu A, Goodfellow I, et al. Deep learning with differential privacy//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 308-318

[57] Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for federated learning on user-held data. arXiv preprint arXiv: 1611.04482, 2016

[58] Wu W, He L, Lin W, et al. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1539-1551

[59] Li T, Sahu A K, Zaheer M, et al. Federated optimization in heterogeneous networks//Proceedings of the Machine Learning and Systems. Austin, USA, 2020, 2: 429-450

[60] Dhakal S, Prakash S, Yona Y, et al. Coded federated learning //Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps). Hawaii, USA, 2019: 1-6

[61] Xie M, Long G, Shen T, et al. Multi-center federated learning. arXiv preprint arXiv:2005.01026, 2020

[62] Ghosh A, Hong J, Yin D, et al. Robust federated learning in a heterogeneous environment. arXiv preprint arXiv:1906.06629, 2019

[63] Mohri M, Sivek G, Suresh A T. Agnostic federated learning //Proceedings of the International Conference on Machine Learning. Long Beach, USA, 2019: 4615-4625

[64] Fang M, Cao X, Jia J, et al. Local model poisoning attacks to byzantine-robust federated learning//Proceedings of the 29th USENIX Security Symposium (USENIX Security 2020). 2020: 1605-1622

[65] Nishio T, Yonetani R. Client selection for federated learning with heterogeneous resources in mobile edge//Proceedings of the 2019 IEEE International Conference on Communications (ICC). Shanghai, China, 2019: 1-7

[66] Luo M, Chen F, Hu D, et al. No fear of heterogeneity: Classifier calibration for federated learning with non-IID data//Proceedings of the Advances in Neural Information Processing Systems. 2021: 5972-5984

[67] Mitra A, Jaafar R, Pappas G J, Hassani H. Linear convergence in federated learning: Tackling client heterogeneity and sparse gradients//Proceedings of the Advances in Neural Information Processing Systems. 2021: 14606-14619

[68] Li Z, He Y, Yu H, et al. Data heterogeneity-robust federated learning via group client selection in industrial IoT. IEEE Internet of Things Journal, 2022, 9(18): 17844-17857

[69] Vahidian S, Morafah M, Chen C, et al. Rethinking data heterogeneity in federated learning: Introducing a new notion and standard benchmarks. IEEE Transactions on Artificial Intelligence, 2024, 5(3): 1386-1397

[70] Goetz J, Malik K, Bui D, et al. Active federated learning. arXiv preprint arXiv:1909.12641, 2019

[71] Cho Y J, Wang J, Joshi G. Client selection in federated learning: Convergence analysis and power-of-choice selection strategies. arXiv preprint arXiv:2010.01243, 2020

[72] Wang H, Kaplan Z, Niu D, et al. Optimizing federated learning on non-IID data with reinforcement learning// Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications. 2020: 1698-1707

[73] Zhan Y, Li P, Guo S. Experience-driven computational resource allocation of federated learning by deep reinforcement learning//Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS). New Orleans, USA, 2020: 234-243

[74] Chen W, Horvath S, Richtarik P. Optimal client sampling for federated learning. arXiv preprint arXiv: 2010.13723, 2020

[75] Nguyen H T, Sehwag V, Hosseinalipour S, et al. Fast-convergent federated learning. IEEE Journal on Selected Areas in Communications, 2021, 39(1): 201-218

[76] Reddi J, Hefny S, Sra A, et al. On variance reduction in stochastic gradient descent and its asynchronous variants// Proceedings of the Advances in Neural Information Processing Systems. Montreal, Canada, 2015: 2647-2655

[77] Tran D Q, Liu D, Nguyen L. Hybrid variance-reduced SGD algorithms for minimax problems with nonconvex-linear function//Proceedings of the Advances in Neural Information Processing Systems. 2020: 11096-11107

[78] Haddadpour F, Kamani M M, Mokhtari A, et al. Federated learning with compression: Unified analysis and sharp guarantees//Proceedings of the International Conference on Artificial Intelligence and Statistics. 2021: 2350-2358

[79] Rothchild D, Panda A, Ullah E, et al. FetchSGD: Communication-efficient federated learning with sketching//Proceedings of the International Conference on Machine Learning. 2020: 8253-8265

[80] Liu W, Chen L, Chen Y, et al. Accelerating federated learning via momentum gradient descent. IEEE Transactions on Parallel and Distributed Systems, 2020, 31(8): 1754-1766

[81] Acar D A E, Zhao Y, Navarro R M, et al. Federated learning based on dynamic regularization. arXiv preprint arXiv:2111.04263, 2021

[82] Huo Z, Yang Q, Gu B, et al. Faster on-device training using new federated momentum algorithm. arXiv preprint arXiv: 2002.02090, 2020

[83] Wang J, Tantia V, Ballas N, et al. SlowMo: Improving communication-efficient distributed SGD with slow momentum. arXiv preprint arXiv:1910.00643, 2019

[84] Das R, Acharya A, Hashemi A, et al. Faster non-convex federated learning via global and local momentum. arXiv preprint arXiv:2012.04061, 2020

[85] Karimireddy S P, Kale S, Mohri M, et al. SCAFFOLD: Stochastic controlled averaging for federated learning// Proceedings of the International Conference on Machine Learning. 2020: 5132-5143

[86] Hamer J, Mohri M, Suresh A T. FedBoost: A communication-efficient algorithm for federated learning//Proceedings of the International Conference on Machine Learning. 2020: 3973-3983

[87] Wang H, Yurochkin M, Sun Y, et al. Federated learning with matched averaging//Proceedings of the International Conference on Learning Representations. 2020: 1-16

[88] Wang J, Liu Q, Liang H, et al. Tackling the objective inconsistency problem in heterogeneous federated optimization //Proceedings of the Advances in Neural Information Processing Systems. 2020: 7611-7623

[89] Defazio A, Bach F, Lacoste-Julien S. SAGA: A fast incremental gradient method with support for non-strongly convex

composite objectives//Proceedings of the 27th International Conference on Neural Information Processing Systems. Montreal, Canada, 2014: 1646-1654

[90] Dragomir R A, Even M, Hendrikx H. Fast stochastic bregman gradient methods: Sharp analysis and variance reduction//Proceedings of the International Conference on Machine Learning. 2021: 2815-2825

[91] Reisizadeh A, Farnia F, Pedarsani R, et al. Robust federated learning: The case of affine distribution shifts//Proceedings of the Advances in Neural Information Processing Systems. 2020: 21554-21565

[92] Li T, Sanjabi M, Beirami A, et al. Fair resource allocation in federated learning. arXiv preprint arXiv: 1905.10497, 2019

[93] Fallah A, Mokhtari A, Ozdaglar A. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach//Proceedings of the Advances in Neural Information Processing Systems. 2020: 3557-3568

[94] Ruan Y, Zhang X, Liang S C, et al. Towards flexible device participation in federated learning//Proceedings of the International Conference on Artificial Intelligence and Statistics. 2021: 3403-3411

[95] Liu S, Yu G, Yin R, et al. Adaptive batchsize selection and gradient compression for wireless federated learning//Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference. Taipei, China, 2020: 1-6

[96] Chen C, Wang W, Li B. Round-robin synchronization: Mitigating communication bottlenecks in parameter servers//Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications. Paris, France, 2019: 532-540

[97] Bengio Y, Courville A, Vincent P. Representation learning: A review and new perspectives. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013, 35(8): 1798-1828

[98] Tan A Z, Yu H, Cui L, et al. Towards personalized federated learning. IEEE Transactions on Neural Networks and Learning Systems, 2023, 34(12): 9587-9603

[99] Yao C H, Gong B, Qi H, et al. Federated multi-target domain adaptation//Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. Waikoloa, USA, 2022: 1424-1433

[100] Li Q, He B, Song D. Model-contrastive federated learning//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2021: 10713-10722

[101] Wu W, He L, Lin W, et al. FedProf: Selective federated learning with representation profiling. IEEE Transactions on Parallel and Distributed Computing, 2023, 34(6): 1942-1953

[102] Park H, Hosseini H, Yun S. Federated learning with metric loss//Proceedings of the International Workshop on Federated Learning for User Privacy and Data Confidentiality in Conjunction with ICML 2021(FL-ICML'21). 2021: 1-6

[103] Hosseini H, Park H, Yun S, et al. Federated learning of user verification models without sharing embeddings//Proceedings of the International Conference on Machine Learning(ICML). 2021: 4328-4336

[104] Yu F, Rawat A S, Menon A, et al. Federated learning with only positive labels//Proceedings of the International Conference on Machine Learning (ICML). 2020: 10946-10956

[105] Peng X, Huang Z, Zhu, Y, et al. Federated adversarial domain adaptation. arXiv preprint arXiv: 1911.02054, 2019

[106] Sirohi D, Kumar N, Rana P S, et al. Federated learning for 6G-enabled secure communication systems: A comprehensive survey. Artificial Intelligence Review, 2023, 56(10): 11297-11389

[107] Lim W Y B, Luong N C, Hoang D T, et al. Federated learning in mobile edge networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2020, 22(3): 2031-2063

[108] Konečný J, McMahan H B, Yu F, et al. Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv: 1610.05492, 2016

[109] Sun Y, Zhou S, Niu Z, et al. Time-correlated sparsification for efficient over-the-air model aggregation in wireless federated learning//Proceedings of the ICC 2022-IEEE International Conference on Communications. 2022: 3388-3393

[110] Sattler F, Wiedemann S, Müller K R, et al. Robust and communication-efficient federated learning from non-IID data. IEEE Transactions on Neural Networks and Learning Systems, 2019, 31(9): 3400-3413

[111] Liu L, Zhang J, Song S, et al. Hierarchical quantized federated learning: Convergence analysis and system design. arXiv preprint arXiv: 2103.14272, 2021

[112] Shlezinger N, Chen M, Eldar Y C, et al. UVeQFed: Universal vector quantization for federated learning. IEEE Transactions on Signal Processing, 2020, 69: 500-514

[113] Chen M, Shlezinger N, Poor H V, et al. Communication-efficient federated learning. Proceedings of the National Academy of Sciences, 2021, 118(17): 1-8

[114] Cui L, Su X, Zhou Y, et al. Slashing communication traffic in federated learning by transmitting clustered model updates. IEEE Journal on Selected Areas in Communications, 2021, 39(8): 2572-2589

[115] Thapa C, Chamikara MAP, Camtepe SA. SplitFed: When federated learning meets split learning. arXiv preprint arXiv: 2004.12088, 2020

[116] Li X, Jiang M, Zhang X, et al. FedBN: Federated learning on non-IID features via local batch normalization. arXiv preprint arXiv: 2102.07623, 2021

[117] Wang X, Han Y, Wang C, et al. In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning. IEEE Network, 2019, 33(5): 156-165

[118] Jere S, Fan Q, Shang B, et al. Federated learning in mobile edge computing: An edge-learning perspective for beyond 5G. arXiv preprint arXiv:2007.08030, 2020

[119] Chen M, Poor H V, Saad W, et al. Convergence time optimization for federated learning over wireless networks. IEEE Transactions on Wireless Communications, 2021, 20(4): 2457-2471

[120] Shi W, Zhou S, Niu, Z. Device scheduling with fast convergence for wireless federated learning//Proceedings of the 2020 IEEE International Conference on Communications (ICC). 2020: 1-6

[121] Amiri M M, Gündüz D. Federated learning over wireless fading channels. IEEE Transactions on Wireless Communications, 2020, 19(5): 3546-3557

[122] Yang H H, Liu Z, Quek T Q, et al. Scheduling policies for federated learning in wireless networks. IEEE Transactions on Communications, 2020, 68(1): 317-333

[123] Xu C, Liu S, Yang Z, et al. Learning rate optimization for federated learning exploiting over-the-air computation. IEEE Journal on Selected Areas in Communications, 2021, 39(12): 3742-3756

[124] Elgabli A, Park J, Issaid C B, et al. Harnessing wireless channels for scalable and privacy-preserving federated learning. IEEE Transactions on Communications, 2021, 69(8): 5194-5208

[125] Zhao Z, Xia J, Fan L, et al. System optimization of federated learning networks with a constrained latency. IEEE Transactions on Vehicular Technology, 2022, 71(1): 1095-1100

[126] Wang L, Wang W, Li B. CMFL: Mitigating communication overhead for federated learning//Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems(ICDCS). Piscataway, USA, 2019: 954-964

[127] Niknam S, Dhillon H S, Reed J H. Federated learning for wireless communications: Motivation, opportunities, and challenges. IEEE Communications Magazine, 2020, 58(6): 46-51

[128] Aledhari M, Razzak R, Parizi R M, et al. Federated learning: A survey on enabling technologies, protocols, and applications. IEEE Access, 2020, 8: 140699-140725

[129] Liu Y, Yuan X, Xiong Z, et al. Federated learning for 6G communications: Challenges, methods, and future directions. China Communications, 2020, 17(9): 105-118

[130] Mothukuri V, Parizi R M, Pouriyeh S, et al. A survey on security and privacy of federated learning. Future Generation Computer Systems, 2021, 115: 619-640

[131] Ma C, Li J, Ding M, et al. On safeguarding privacy and security in the framework of federated learning. IEEE Network, 2020, 34(4): 242-248

[132] Xu G, Li H, Liu S, et al. VerifyNet: Secure and verifiable federated learning. IEEE Transactions on Information Forensics and Security, 2019, 15: 911-926

[133] So J, Güler B, Avestimehr A S. Byzantine-resilient secure federated learning. IEEE Journal on Selected Areas in Communications, 2021, 39(7): 2168-2181

[134] Hao M, Li H, Luo X, et al. Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Transactions on Industrial Informatics, 2019, 16(10): 6532-6542

[135] Pettai M, Laud P. Combining differential privacy and secure multiparty computation//Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC). Los Angeles, USA, 2015: 421-430

[136] Girgis A, Data D, Diggavi S, et al. Shuffled model of differential privacy in federated learning//Proceedings of the International Conference on Artificial Intelligence and Statistics. 2021: 2521-2529

[137] Adnan M, Kalra S, Cresswell J C, et al. Federated learning and differential privacy for medical image analysis. Scientific Reports, 2022, 12(1): 1-10

[138] Fereidooni H, Marchal S, Miettinen M, et al. SAFELearn: Secure aggregation for private FEderated learning//Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW). 2021: 56-62

[139] So J, Yang C S, Li S, et al. LightSecAgg: A lightweight and versatile design for secure aggregation in federated learning//Proceedings of the Machine Learning and Systems. Santa Clara, USA, 2022: 694-720

[140] Yang Q, Huang A, Fan L, et al. Federated learning with privacy-preserving and model IP-right-protection. Machine Intelligence Research, 2023, 20(1): 19-37

[141] So J, Güler B, Avestimehr A S. Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning. IEEE Journal on Selected Areas in Information Theory, 2021, 2(1): 479-489

[142] Gentry C. Fully homomorphic encryption using ideal lattices//Proceedings of the 41st Annual ACM Symposium on Theory of Computing. Bethesda, USA, 2009: 169-178

[143] Paillier P. Public-key cryptosystems based on composite degree residuosity classes//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany, 1999: 223-238

[144] Truex S, Baracaldo N, Anwar A, et al. A hybrid approach to privacy-preserving federated learning//Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security. London, UK, 2019: 1-11

[145] Zhao C, Zhao S, Zhao M, et al. Secure multi-party computation: Theory, practice and applications. Information Sciences, 2019, 476: 357-372

[146] Knott B, Venkataraman S, Hannun A, et al. CrypTen: Secure multi-party computation meets machine learning//Proceedings of the Advances in Neural Information Processing Systems. 2021, 34: 4961-4973

[147] Patra A, Srinivasan A. Three-round secure multiparty computation from black-box two-round oblivious transfer//Proceedings of the Annual International Cryptology Conference. 2021: 185-213

[148] Xu R, Baracaldo N, Zhou Y, et al. HybridAlpha: An efficient approach for privacy-preserving federated learning//Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security. London, UK, 2019: 13-23

[149] Liu Y, Peng J, Kang J, et al. A secure federated learning framework for 5G networks. IEEE Wireless Communications, 2020, 27(4): 24-31

[150] Chai D, Wang L, Zhang J, et al. Practical lossless federated singular vector decomposition over billion-scale data//Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Washington, USA, 2022: 46-55

[151] Zhao B, Mopuri K R, Bilen, H. iDLG: Improved deep leakage from gradients. arXiv preprint arXiv:2001.02610, 2020

[152] Zhang H, Hong J, Deng Y, et al. Understanding deep gradient leakage via inversion influence functions//Proceedings of the Advances in Neural Information Processing Systems. New Orleans, USA, 2023, 36: 3921-3944

[153] Gu Y, Bai Y, Xu S. CS-MIA: Membership inference attack based on prediction confidence series in federated learning. Journal of Information Security and Applications, 2022, 67: 1-15

[154] Yin X, Zhu Y, Hu J. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. ACM Computing Surveys (CSUR), 2021, 54(6): 1-36

[155] Song S, Chaudhuri K, Sarwate A D. Stochastic gradient descent with differentially private updates//Proceedings of the 2013 IEEE Global Conference on Signal and Information Processing. Texas, USA, 2013: 245-248

[156] Wei K, Li J, Ding M, Ma C, et al. Federated learning with differential privacy: Algorithms and performance analysis. IEEE Transactions on Information Forensics and Security, 2020, 15: 3454-3469

[157] Wang H, Sreenivasan K, Rajput S, et al. Attack of the tails: Yes, you really can backdoor federated learning//Proceedings of the Advances in Neural Information Processing Systems. 2020: 16070-16084

[158] Bagdasaryan E, Veit A, Hua Y, et al. How to backdoor federated learning//Proceedings of the International Conference on Artificial Intelligence and Statistics. 2020: 2938-2948

[159] Mao Y, Yuan X, Zhao X, et al. Romoa: Robust model aggregation for the resistance of federated learning to model poisoning attacks//Proceedings of the 26th European Symposium on Research in Computer Security. 2021: 476-496

[160] Lyu L, Yu H, Ma X, et al. Privacy and robustness in federated learning: Attacks and defenses. IEEE Transactions on Neural Networks and Learning Systems, 2024, 35(7): 8726-8746

[161] Sun J, Li A, DiValentin L, et al. FL-WBC: Enhancing robustness against model poisoning attacks in federated learning from a client perspective. Advances in Neural Information Processing Systems, 2021, 34: 12613-12624

[162] Tolpegin V, Truex S, Gursoy M E, et al. Data poisoning attacks against federated learning systems//Proceedings of the European Symposium on Research in Computer Security. Cham: Springer, 2020: 480-501

[163] Li S, Cheng Y, Wang W, et al. Learning to detect malicious clients for robust federated learning. arXiv preprint arXiv: 2002.00211, 2020

[164] Fang X, Ye M. Robust federated learning with noisy and heterogeneous clients//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. New Orleans, USA, 2022: 10072-10081

[165] Sun Z, Kairouz, P, Suresh A T, et al. Can you really backdoor federated learning?. arXiv preprint arXiv:1911.07963, 2019

[166] Zhu Z, Fan P, Peng C, et al. ISFL: Trustworthy federated learning for non-IID data with local importance sampling. arXiv preprint arXiv:2210.02119, 2022

[167] Guo X, Liu Z, Li J, et al. VeriFL: Communication-efficient and fast verifiable aggregation for federated learning. IEEE Transactions on Information Forensics and Security, 2020, 16: 1736-1751

[168] Jiang C, Xu C, Zhang Y. PFLM: Privacy-preserving federated learning with membership proof. Information Sciences, 2021, 576: 288-311

[169] Hahn C, Kim H, Kim M, et al. VerSA: Verifiable secure aggregation for cross-device federated learning. IEEE Transactions on Dependable and Secure Computing, 2021, 20(1): 36-52

[170] Chowdhury A R, Guo C, Jha S, et al. EIFFeL: Ensuring integrity for federated learning//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. Copenhagen, Denmark, 2022: 2535-2549

[171] Tang Ling-Tao, Chen Zuo-Ning, Zhang Lu-Fei, et al. Research progress of privacy issues in federated learning. Journal of Software, 2023, 34(1): 197-229(in Chinese)
(汤凌韬，陈左宁，张鲁飞等. 联邦学习中的隐私问题研究进展. 软件学报，2023，34(1)：197-229)

[172] Rehman M H, Dirir A M, Salah K, et al. TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT. IEEE Transactions on Industrial Informatics, 2021, 17(12): 8485-8494

[173] Otoum S, Al Ridhawi I, Mouftah H T. Blockchain-supported federated learning for trustworthy vehicular networks//Proceedings of the 2020 IEEE Global Communications Conference. 2020: 1-6

[174] Otoum S, Al Ridhawi I, Mouftah H. Securing critical IoT infrastructures with blockchain-supported federated learning. IEEE Internet of Things Journal, 2022, 9(4): 2592-2601

[175] Zhang Q, Ding Q, Zhu J, et al. Blockchain empowered reliable federated learning by worker selection: A trustworthy reputation evaluation method//Proceedings of the 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). 2021: 1-6

[176] Mothukuri V, Parizi R M, Pouriyeh S, et al. FabricFL: Blockchain-in-the-loop federated learning for trusted decentralized systems. IEEE Systems Journal, 2021, 16(3): 3711-3722

[177] Li B, Fan L, Gu H, et al. FedIPR: Ownership verification for federated deep neural network models. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(4): 4521-4536

[178] Fink O, Netland T, Feuerriegelc S. Artificial intelligence across company borders. Communications of the ACM, 2021, 65(1): 34-36

[179] Wilson G, Cook D. A survey of unsupervised deep domain adaptation. ACM Transactions on Intelligent Systems and Technology (TIST), 2020, 11(5): 1-46

[180] Cheng K, Fan T, Jin Y, et al. SecureBoost: A lossless federated learning framework. IEEE Intelligent Systems, 2021, 36(6): 87-98

[181] Scannapieco M, Figotin I, Bertino E, et al. Privacy preserving schema and data matching//Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data. Beijing, China, 2007: 653-664

[182] Nock R, Hardy S, Henecka W, et al. Entity resolution and federated learning get a federated resolution. arXiv preprint arXiv:1803.04035, 2018

[183] Ji S, Saravirta T, Pan S, et al. Emerging trends in federated learning: From model fusion to federated x learning. arXiv preprint arXiv:2102.12920, 2021

[184] Liu X, Deng Y, Nallanathan A, et al. Federated learning and meta learning: Approaches, applications, and directions. IEEE Communications Surveys & Tutorials, 2024, 26(1): 571-618

[185] Yang Y, Ye X, Sakurai T. Multi-view federated learning with data collaboration//Proceedings of the 14th International Conference on Machine Learning and Computing (ICMLC). 2022: 178-183

[186] Attota D C, Mothukuri V, Parizi R M, et al. An ensemble multi-view federated learning intrusion detection for IoT. IEEE Access, 2021, 9: 117734-117745

[187] Marfoq O, Neglia G, Bellet A, et al. Federated multi-task learning under a mixture of distributions//Proceedings of the Advances in Neural Information Processing Systems, 2021, 34: 15434-15447

[188] Corinzia L, Beuret A, Buhmann J M. Variational federated multi-task learning. arXiv preprint arXiv: 1906.06268, 2019

[189] Wu Q, He K, Chen X. Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. IEEE Open Journal of the Computer Society, 2020, 1: 35-44

[190] Wu J, Liu Q, Huang Z, et al. Hierarchical personalized federated learning for user modeling//Proceedings of the Web Conference 2021. 2021: 957-968

[191] Deng Y, Kamani M M, Mahdavi M. Adaptive personalized federated learning. arXiv preprint arXiv:2003.13461, 2020

[192] Li T, Hu S, Beirami A, et al. Ditto: Fair and robust federated learning through personalization//Proceedings of the International Conference on Machine Learning. 2021: 6357-6368

[193] Zhang J, Hua Y, Wang H, et al. FedALA: Adaptive local aggregation for personalized federated learning//Proceedings of the AAAI Conference on Artificial Intelligence. Washington, USA, 2023, 37(9): 11237-11244

[194] Dinh C T, Tran N, Nguyen J. Personalized federated learning with moreau envelopes//Proceedings of the Advances in Neural Information Processing Systems. 2020: 21394-21405

[195] Arivazhagan M G, Aggarwal V, Singh A K, et al. Federated learning with personalization layers. arXiv preprint arXiv: 1912.00818, 2019

[196] Liang P P, Liu T, Ziyin L, et al. Think locally, act globally: Federated learning with local and global representations. arXiv preprint arXiv:2001.01523, 2020

[197] Hanzely F, Richtárik P. Federated learning of a mixture of global and local models. arXiv preprint arXiv:2002.05516, 2020

[198] Mansour Y, Mohri M, Ro J, et al. Three approaches for personalization with applications to federated learning. arXiv preprint arXiv:2002.10619, 2020

[199] Ghosh A, Chung J, Yin D, et al. An efficient framework for clustered federated learning//Proceedings of the Advances in Neural Information Processing Systems. 2020: 19586-19597

[200] Briggs C, Fan Z, Andras P. Federated learning with hierarchical clustering of local updates to improve training on non-IID data//Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN). Glasgow, UK, 2020: 1-9

[201] Hu C, Jiang J, Wang Z. Decentralized federated learning: A segmented gossip approach. arXiv preprint arXiv:1908.07782, 2019

[202] Roy A G, Siddiqui S, Pölsterl S, et al. BrainTorrent: A peer-to-peer environment for decentralized federated learning. arXiv preprint arXiv:1905.06731, 2019

[203] Hegedüs I, Danner G, Jelasity M. Gossip learning as a decentralized alternative to federated learning//Proceedings of the IFIP International Conference on Distributed Applications and Interoperable Systems. Kongens Lyngby, Denmark, 2019: 74-90

[204] Lalitha A, Kilinc O C, Javidi T, et al. Peer-to-peer federated learning on graphs. arXiv preprint arXiv:1901.11173, 2019

[205] Pappas C, Chatzopoulos D, Lalis S, et al. IPLS: A framework for decentralized federated learning//Proceedings of the 2021 IFIP Networking Conference (IFIP Networking), 2021: 1-6

[206] Wu X, Wang Z, Zhao J, et al. FedBC: Blockchain-based decentralized federated learning//Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). Dalian, China, 2020: 217-221

[207] Warnat-Herresthal S, Schultze H, Shastry K L, et al. Swarm learning for decentralized and confidential clinical machine learning. Nature, 2021, 594(7862): 265-270

[208] Li Y, Chen C, Liu N, et al. A blockchain-based decentralized federated learning framework with committee consensus. IEEE Network, 2021, 35(1): 234-241

[209] Ma Y, Yu D, Wu T, et al. PaddlePaddle: An open-source deep learning platform from industrial practice. Frontiers of Data and Computing, 2019, 1(1): 105-115

[210] He C, Li S, So J, et al. FedML: A research library and benchmark for federated machine learning. arXiv preprint arXiv:2007.13518, 2020

[211] Zhang T, He C, Ma T, et al. Federated learning for Internet of Things: A federated learning framework for On-device anomaly data detection. arXiv preprint arXiv: 2106.07976, 2021

[212] Lin B, He C, Zeng Z, et al. FedNLP: A research platform for federated learning in natural language processing. arXiv preprint arXiv:2104.08815, 2021

[213] He C, Balasubramanian K, Ceyani E, et al. FedGraphNN: A federated learning system and benchmark for graph neural networks. arXiv preprint arXiv:2104.07145, 2021

[214] He C, Annavaram M, Avestimehr S. Towards Non-IID and invisible data with fednas: Federated deep learning via neural architecture search. arXiv preprint arXiv: 2004.08546, 2020

[215] He C, Annavaram M, Avestimehr S. Group knowledge transfer: Federated learning of large CNNs at the edge// Proceedings of the Advances in Neural Information Processing Systems. 2020: 14068-14080

[216] Reddi S J, Charles Z, Zaheer M, et al. Adaptive federated optimization. arXiv preprint arXiv:2003.00295, 2021

[217] He C, Shah A D, Tang Z, et al. FedCV: A federated learning framework for diverse computer vision tasks. arXiv preprint arXiv:2111.11066, 2021

[218] Kong Q, Yin F, Lu R, et al. Privacy-preserving aggregation for federated learning-based navigation in vehicular fog. IEEE Transactions on Industrial Informatics, 2021, 17(12): 8453-8463

[219] Yin F, Lin Z, Kong Q, et al. FedLoc: Federated learning framework for data-driven cooperative localization and location data processing. IEEE Open Journal of Signal Processing, 2020, 1: 187-215

[220] Li Y, Tao X, Zhang X, et al. Privacy-preserved federated learning for autonomous driving. IEEE Transactions on Intelligent Transportation Systems, 2021, DOI: 10.1109/TITS.2021.3081560

[221] Hegedüs I, Danner G, Jelasity M. Decentralized recommendation based on matrix factorization: A comparison of gossip and federated learning//Proceedings of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Wurzburg, Germany, 2019: 317-332

[222] Zhao S, Bharati R, Borcea C, et al. Privacy-aware federated learning for page recommendation//Proceedings of the 2020 IEEE International Conference on Big Data (Big Data). 2020: 1071-1080

[223] Yang L, Tan B, Zheng V W, et al. Federated Learning: Federated Recommendation Systems. Cham: Springer, 2020

[224] Hard A, Rao K, Mathews R, et al. Federated learning for mobile keyboard prediction. arXiv preprint arXiv: 1811.03604, 2018

[225] Chen M, Mathews R, Ouyang T, et al. Federated learning of out-of-vocabulary words. arXiv preprint arXiv: 1903.10635, 2019

[226] Ramaswamy S, Mathews R, Rao K, et al. Federated learning for Emoji prediction in a mobile keyboard. arXiv preprint arXiv:1906.04329, 2019

[227] Yang T, Andrew G, Eichner H, et al. Applied federated learning: Improving Google keyboard query suggestions. arXiv preprint, arXiv:1812.02903, 2018

[228] Brinda C. Google Ads blog. Building a privacy-first future for web advertising. https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/, 2021

[229] Ravichandran D, Vassilvitski S. Google Research & Ads. Evaluation of cohort algorithms for the FloC API. https://github.com/google/ads-privacy/raw/master/proposals/FLoC/FLOC-Whitepaper-Google.pdf, 2020

[230] Brisimi T S, Chen R, Mela T, et al. Federated learning of predictive models from federated electronic health records. International Journal of Medical Informatics, 2018, 112: 59-67

[231] Xu J, Glicksberg B S, Su C, et al. Federated learning for healthcare informatics. Journal of Healthcare Informatics Research, 2021, 5(1): 1-19

[232] Rieke N, Hancox J, Li W, et al. The future of digital health with federated learning. NPJ Digital Medicine, 2020, 3(1): 1-7

[233] Sheller M J, Edwards B, Reina G A, et al. Federated learning in medicine: Facilitating multi-institutional collaborations without sharing patient data. Scientific Reports, 2020, 10(1): 1-12

[234] Mothukuri V, Khare P, Parizi R M, et al. Federated learning-based anomaly detection for IoT security attacks. IEEE Internet of Things Journal, 2022, 9(4): 2545-2554

[235] Liu Y, James J Q, Kang J, et al. Privacy-preserving traffic flow prediction: A federated learning approach. IEEE Internet of Things Journal, 2020, 7(8): 7751-7763

[236] Liu Y, Huang A, Luo Y, et al. FedVision: An online visual object detection platform powered by federated learning// Proceedings of the AAAI Conference on Artificial Intelligence. New York, USA, 2020, 34(8): 13172-13179

[237] Chen J, Li K, Deng Q, et al. Distributed deep learning model for intelligent video surveillance systems with edge computing. IEEE Transactions on Industrial Informatics. 2019, DOI: 10.1109/JIOT.2021.3077803

[238] Ye D, Yu R, Pan M, et al. Federated learning in vehicular edge computing: A selective model aggregation approach. IEEE Access, 2020, 8: 23920-23935

[239] Lu Y, Huang X, Dai Y, et al. Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Network, 2020, 34(3): 50-56

[240] Caldas S, Duddu S M K, Wu P, et al. LEAF: A benchmark for federated settings. arXiv preprint arXiv: 1812.01097, 2018

[241] Deng L. The MNIST database of handwritten digit images for machine learning research. IEEE Signal Processing Magazine, 2012, 29(6): 141-142

[242] Krizhevsky A, Hinton G. Learning multiple layers of features from tiny images. http://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf, 2009

[243] Deng J, Dong W, Socher R, et al. ImageNet: A large-scale hierarchical image database//Proceedings of 2009 the IEEE Conference on Computer Vision and Pattern Recognition. Miami, USA, 2009: 248-255

[244] Morafah M, Vahidian S, Wang W, et al. FLIS: Clustered federated learning via inference similarity for non-IID data distribution. IEEE Open Journal of the Computer Society, 2023, 4: 109-120

[245] Pandey S R, Tran N H, Bennis M, et al. A crowdsourcing framework for on-device federated learning. IEEE Transactions on Wireless Communications, 2020, 19(5): 3241-3256

[246] Wang Y, Su Z, Zhang N, et al. Learning in the air: Secure federated learning for UAV-assisted crowdsensing. IEEE Transactions on Network Science and Engineering, 2020, 8(2): 1055-1069

[247] Kang J, Xiong Z, Niyato D, et al. Incentive design for efficient federated learning in mobile networks: A contract theory approach//Proceedings of the 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS). Singapore, 2019: 1-5

[248] Kang J, Xiong Z, Niyato D, et al. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714

[249] Kang J, Xiong Z, Niyato D, et al. Reliable federated learning for mobile networks. IEEE Wireless Communications, 2020, 27(2): 72-80

[250] Zhang J, Wu Y, Pan R. Incentive mechanism for horizontal federated learning based on reputation and reverse auction// Proceedings of the Web Conference. Ljubljana Slovenia, 2021: 947-956

[251] Liu Z, Chen Y, Yu H, et al. GTG-shapley: Efficient and accurate participant contribution evaluation in federated learning. ACM Transactions on Intelligent Systems and Technology (TIST), 2022, 13(4): 1-21

[252] Qu Y, Gao L, Luan T, et al. Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet of Things Journal, 2020, 7(6): 5171-5183

[253] Wang G, Dang C X, Zhou Z. Measure contribution of participants in federated learning//Proceedings of the 2019 IEEE International Conference on Big Data (Big Data). Los Angeles, USA, 2019: 2597-2604

[254] Wang T, Rausch J, Zhang C, et al. Federated Learning: A Principled Approach to Data Valuation for Federated Learning. Cham: Springer, 2020

[255] Song T, Tong Y, Wei S. Profit allocation for federated learning//Proceedings of the 2019 IEEE International Conference on Big Data. Los Angeles, USA, 2019: 2577-2586

[256] Chen J H, Chen M R, Zeng G Q, et al. BDFL: A byzantine-fault-tolerance decentralized federated learning method for autonomous vehicle. IEEE Transactions on Vehicular Technology, 2021, 70(9): 8639-8652

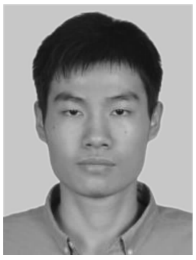
[257] Lu S, Zhang Y, Wang Y. Decentralized federated learning for electronic health records//Proceedings of the 2020 54th Annual Conference on Information Sciences and Systems (CISS). Princeton, USA, 2020: 1-5

[258] Posner J, Tseng L, Aloqaily M, et al. Federated learning in vehicular networks: Opportunities and solutions. IEEE Network, 2021, 35(2): 152-159

[259] Nguyen D C, Ding M, Pathirana P N, et al. Federated learning for Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2021, 23(3): 1622-1658

[260] Sun W, Lei S, Wang L, et al. Adaptive federated learning and digital twin for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2021, 17(8): 5605-5614

[261] Lu Y, Huang X, Zhang K, et al. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology, 2020, 69(4): 4298-4311



WU Wen-Tai, Ph. D., associate professor. His main research interests include distributed systems, collaborative machine learning, and sustainable computing.

WU Ying-Liang, Ph. D., professor, Ph. D. supervisor. His main research interests include information systems, data-driven decision-making, and digital ecosystem.

LIN Wei-Wei, Ph. D., professor, Ph. D. supervisor. His main research interests include cloud computing, big data analytics, and AI applications.

ZUO Wen-Ming, Ph. D., professor, Ph. D. supervisor. His main research interests include electronic commerce, data mining, business intelligence, and digital economy.

Background

Since the release of the general data protection regulation (GDPR) in the European Union, various countries and regions have strengthened or planned to strengthen the control of user data in the region. This makes traditional data-centralized model training methods no longer feasible in user privacy-sensitive scenarios such as autonomous vehicles, digital health care, and Internet of Things. With the support of 5G and the increasing capacity of mobile devices, AI applications have been popularized to the edge of the network, and end devices including smart phones, drones and wearable devices are capable to perform machine learning tasks. These factors together call for a new paradigm of machine learning that matches the decentralized nature of data and computation whilst offers strong privacy protection to users.

As a promising solution, Horizontal Federated Learning (HFL) can adapt to diverse optimization strategies and technologies for distributed machine learning. HFL has emerged as a popular direction of research and also attracted much attention from the industry in recent years. This in a large part comes down to the fact that HFL has great potential to facilitate a variety of emerging application scenarios such as edge computing, industrial IoT, smart cities and medical diagnostics. The research on horizontal federated learning also spans a broad spectrum that involves multiple fields of study such as machine learning, distributed systems, wireless communication, and information security. It features a diversified and intersected map of techniques. In the meantime, the advance of research in the relevant field has catalyzed the development of open-source FL frameworks, libraries, prototype systems, developer platforms, and various applications.

Existing reviews of FL mainly focus on the progress of research or the branch of studies in regards to one specific subject (such as communication, machine learning, or information security). A comprehensive survey of the entire spectrum of techniques for HFL is still missing. Existing work hardly covers the engineering factors and applications of HFL from a systematic standpoint.

This survey points out the gap between the research of HFL and the development of HFL systems in the real-world environment, analyzes the key challenges we face in the design and implementation of such systems and the related applications powered by HFL, and provides useful insights for the engineering practice and future research of HFL.

This survey is part of our research supported by the National Natural Science Foundation of China (Nos. 61872150, 62072187, 62402198), the National Social Science Foundation of China Post-funded project (No. 20FGLB034), the Guangdong Major Project of Basic and Applied Basic Research (No. 2021B0101420002), the Guangdong Natural Science Foundation (No. 2020A1515010830), the Young Scholar Funding Project of Pazhou Laboratory (No. PZL2021KF0027). This work facilitates our further study on optimized machine learning in distributed systems as well as the development of AI-driven applications in the tide of digital economy.