群体智能中的联邦学习算法综述

杨强[1,2]，童咏昕[3]，王晏晟[3]，范力欣[1]，王薇[3]，陈雷[2]，王魏[4]，康焱[1]

（1. 深圳前海微众银行股份有限公司，广东 深圳 518063；
2. 香港科技大学，香港 999077；
3. 北京航空航天大学，北京 100191；
4. 南京大学，江苏 南京 210033）

摘　要：群体智能是在互联网高速普及下诞生的人工智能新范式。然而，数据孤岛与数据隐私保护问题导致群体间数据共享困难，群体智能应用难以构建。联邦学习是一类新兴的打破数据孤岛、联合构建群智模型的重要方法。首先，介绍了联邦学习的基础概念以及其与群体智能的关系；其次，基于群体智能视角对联邦学习算法框架进行了分类，从隐私、精度与效率 3 个角度讨论了联邦学习算法优化技术；而后，阐述了基于线性模型、树模型与神经网络模型的联邦学习算法模型；最后，介绍了联邦学习代表性开源平台与典型应用，并对联邦学习研究进行总结展望。

关键词：群体智能；联邦学习；隐私保护

中图分类号：TP39

文献标志码：A

doi: 10.11959/j.issn.2096−6652.202218

A survey on federated learning in crowd intelligence

YANG Qiang[1,2], TONG Yongxin[3], WANG Yansheng[3], FAN Lixin[1], WANG Wei[3], CHEN Lei[2], WANG Wei[4], KANG Yan[1]

1. Qianhai WeBank Co., Ltd., Shenzhen 518063, China
2. The Hong Kong University of Science and Technology, Hong Kong 999077, China
3. Beihang University, Beijing 100191, China
4. Nanjing University, Nanjing 210033, China

Abstract: Crowd intelligence is emerging as a new artificial intelligence paradigm owing to the rapid development of the Internet. However, the data isolation and data privacy preservation problems make it difficult to share data among the crowd and to build crowd intelligent applications. Federated learning is a novel solution that aims to collaboratively build models by breaking the data barriers in crowd. Firstly, the basic ideas of federated learning and a comparison with crowd intelligence were introduced. Secondly, federated learning algorithms were divided into three categories according to the crowd organization, and further optimization techniques on privacy, accuracy and efficiency were discussed. Thirdly, federated learning operators based on linear models, tree models and neural network models were presented respectively. Finally, mainstream federated learningopensource platforms and typical applications were introduced, followed by the conclusion.

Key words: crowd intelligence, federated learning, privacy preservation

---

收稿日期：2021−12−16；**修回日期：**2022−03−04

通信作者：童咏昕，yxtong@buaa.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2018AAA0101100）；国家自然科学基金资助项目（No.U21A20516，No.61822201，No.U1811463，No.62076017）；微众学者计划

Foundation Items: The National Key Research and Development Program of China (No.2018AAA0101100), The National Natural Science Foundation of China (No.U21A20516, No.61822201, No.U1811463, No.62076017), WeBank Scholars Program

0 引言

近年来，人工智能技术的发展进入了新时代，诞生了以AlphaGo为代表的能够模拟出强大个体智慧的成功案例。同时，随着互联网高速普及，人与人之间的信息碰撞交流更加密切，群体智慧的联结开始发挥越来越重要的作用，群体智能（crowd intelligence）也初现端倪。所谓群体智能，就是指通过特定的组织结构吸引、汇聚和管理大规模参与者完成任务时，所涌现出的超越个体智力的智能。在互联网环境下，群体智能面临着许多不同于主流人工智能范式的新挑战。例如，构建传统人工智能应用依赖于大量的训练数据，而在更贴近真实的群体智能场景中，数据往往分散在不同的企业、机构群体，甚至大规模个人移动用户群体中。这些散布于群体的数据之间存在壁垒，很难用常规手段去打通，由此诞生了数据孤岛（data isolation）问题。与此同时，对数据隐私安全的重视也成为世界趋势。欧盟在 2018 年通过并开始实施堪称史上“最严”的数据隐私保护法规《通用数据保护条例》（general data protection regulation，GDPR），专门针对大数据、移动互联网、人工智能新背景制定了一系列数据隐私安全保护措施。我国也相继出台了《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等包含数据隐私保护的法规。总之，在当前全球数据隐私保护的大浪潮之下，数据孤岛问题变得异常严峻，联合群体数据构建智能模型，使群体智能技术得以落地的需求变得愈加难以实现。

为了应对群体间存在数据孤岛、难以联合构建群智模型的挑战，联邦学习（federated learning，FL）[1-7]的概念被提出，它旨在使群体原始数据在不离开本地的前提下联合构建机器学习模型。在谷歌公司较早的联邦学习构想中[1-2]，学习的对象是大规模群体移动设备用户，这些用户的智能手机、移动终端中存储着可用于构建智能模型的个人隐私数据，谷歌公司设想仅通过传递模型梯度或加密后的梯度来实现联合模型的构建。后来，联邦学习场景中的个体也从个人推广到企业或机构[3]，即大量拥有数据的公司或部门，如互联网公司、银行、政府机构等，在各自数据都不离开本地的前提下，弥补各自数据的短板，联合构建智能模型，实现互利共赢。

无论哪种场景，联邦学习算法的实现都离不开群体间的智能协作。本文将从群体智能的角度对联邦学习算法展开深入讨论，从基于群体智能视角的联邦学习算法框架、联邦学习算法优化与联邦学习算法模型 3 个方面阐述设计联邦学习算法的几大重要步骤与相关前沿工作。

1 联邦学习概述

本节首先简要地介绍联邦学习的基础概念；然后，从相似性和独特性角度讨论联邦学习与群体智能的关系；最后，对本文的内容结构进行概览。

1.1 基础概念

联邦学习的基本范式可表述如下[3,8]：当多个数据拥有方 $F_i(i=1,\cdots,N)$ 想要联合它们的数据集 D_i 共同训练机器学习模型 M 时，传统方案通常先将数据整合，得到总数据集 $D=D_1\cup\cdots\cup D_N$，然后在 D 上训练，得到模型 M_{sum}。这种做法存在隐私泄露的隐患，甚至可能违反相关法律规定。联邦学习则是在数据拥有方 F_i 不需要直接提供数据 D_i 的情况下，只通过传输安全处理后的中间结果来训练联邦模型 M_{fed}，联邦学习通用框架如图 1 所示。联邦学习能够使联邦模型 M_{fed} 的性能 V_{fed} 接近直接训练模型 M_{sum} 的性能 V_{sum}，即：

$$\left|V_{\text{fed}}-V_{\text{sum}}\right|<\delta \tag{1}$$

其中，δ 是一个小正数，用来衡量隐私保护引起的机器学习模型精度损失。

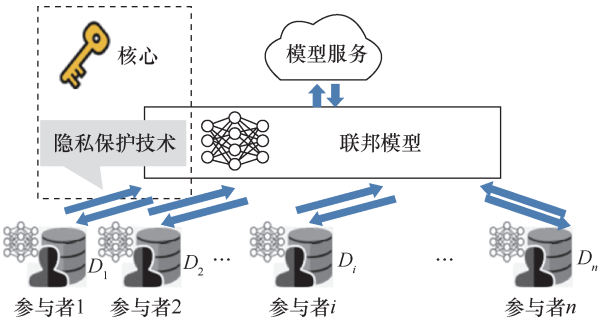


图 1 联邦学习通用框架

用于训练机器学习模型的数据包含用户 U 和用户特征 X 两部分（有些数据还会包含标签特征 Y）。以两个数据拥有方参与的联邦学习为例，它们各自的用户 U_1,U_2 与用户特征 X_1,X_2 很可能并不相同，具体按照特征与用户的重叠情况，可以把联邦学习分为横向联邦学习、纵向联邦学习与联邦迁移学习 3 类[3]。现有联邦学习综述通常按照上述横向、纵向、迁移的角度进行分类，本文不再赘述。本文在第 2 节从群体组织架构的视角对联邦学习算

法架构重新分类，该分类与横向、纵向、迁移的分类属于正交关系。

1.2　联邦学习与群体智能的关系

联邦学习是目前群体智能研究的新兴方向之一。回顾群体智能的发展历史不难发现，许多相关领域都对当前联邦学习的发展产生了一定的启发作用，同时联邦学习也存在其独特性。下面将从相似性与独特性两方面阐述二者关系。

（1）相似性

群体智能的思想古已有之。我国自古就有“众人拾柴火焰高”的谚语，这与联邦学习“合作共赢”的思想是一致的。20 世纪 90 年代由维克托 • 莱瑟（Victor Lesser）教授创立的多智体系统领域是群体智能的代表性传统领域[9]，而联邦学习本身也可被视为一个多智体系统，有研究工作就结合多智体系统和与博弈论相关的技术来解决联邦学习中的激励建模等[10]问题。21 世纪初诞生了群体智能的另一个重要领域——众包[11]，其主要思想是把复杂的任务分解成简单的任务交给广大互联网用户来完成。联邦学习思想与其不谋而合，在隐私保护、激励机制、质量控制等多个方面都借助或延伸了传统众包中的相关方法，Tong Y X 等人[12]就从众包的角度重新对联邦学习进行了全面的解读。近年来诞生了许多面向多方的机器学习方法，如联合学习（joint learning）[13]、多任务学习（multitask learning）[14-15]、分布式机器学习（distributed machine learning）[16]等，这类方法由于涉及多方共同构建智能应用，也常被划入群体智能范畴，其研究的分布式大规模数据场景与联邦学习类似，其多方协作学习的方法对于联邦学习的研究也有一定启发作用。

（2）独特性

虽然联邦学习与群体智能中的许多其他领域具有密切的关联，并受到了许多相似领域的启发，但是其同样具有独特性。首先，联邦学习是当前群体智能领域解决隐私限制下大规模协同学习问题的重要方法，其旨在在各参与方所拥有的原始数据不离开本地的情况下，通过传输安全处理后的数据或中间结果，达到隐私保护要求下集成多方数据训练模型的效果，因此对数据或模型隐私安全的关注是许多其他群体智能领域未曾考虑的，也是其核心的技术特点之一。此外，虽然联邦学习常常被视为一种分布式机器学习方法，但是二者的最大区别在于联邦学习中参与学习的多方自治，从而导致计算设备异构、数据异质（即非独立同分布）等挑战，在这些挑战下，模型的精度与可用性大大降低，同时过大的计算与通信开销也使得算法难以落地，因此需要针对性的优化方法。

1.3　综述概览

本文重点介绍与联邦学习算法相关的研究，整体架构如图 2 所示。首先，在第 1 节介绍联邦学习基本概念的基础上，第 2 节讨论以群体智能组织架构为分类标准的 3 类联邦学习的基础算法框架，即中心化联邦学习、半中心化联邦学习和去中心化联邦学习；然后，在算法框架基础上，第 3 节进一步重点阐述目前主流联邦学习算法为应对隐私、精度与效率 3 类挑战而设计的优化算法；随后，第 4 节介绍联邦学习的主流模型，包括线性模型（linear model，LM）、树模型与神经网络（neural network，NN）模型，这些模型一般与算法框架以及优化算法相互正交，但不同模型在联邦学习场景下也有其特有的设计要点；最后，第 5 节介绍现有的联邦学习主流开源平台与相关应用，第 6 节进行总结。

图 2　联邦学习算法整体架构

2　基于群体智能视角的联邦学习算法框架

本节介绍基于群体智能视角的 3 类联邦学习算法框架。根据群体组织结构可将联邦学习算法划分为存在中心的群体（中心化结构）算法、存在多中

心的群体（半中心化结构）算法、不存在中心的群体（去中心化结构）算法 3 类，而不同的群体组织结构也会对联邦学习的模型训练过程产生影响，基于群体智能视角的联邦学习算法框架如图 3 所示。下面分别介绍中心化、半中心化、去中心化群体组织结构下的联邦学习框架。

2.1 中心化联邦学习

大部分现有的联邦学习模型都假设联邦学习过程中存在一个协调构建群体学习模型的中心服务器，其余联邦参与方可以在中心服务器进行模型聚合、模型分发、收敛判定等联邦模型训练的基础操作。

以联邦学习中的联邦平均（federated averaging，FedAvg）算法[2]为例，典型的中心化联邦学习模型构建过程如下：首先，由中心服务器$\mathcal{C}$初始化全局联邦模型 M_{fed}；然后，在所有参与方中随机选择一部分可交互的参与方 U，被选参与方从中心服务器下载模型 M_{fed}；随后，被选中参与方基于本地数据继续训练并更新全局模型，并将联邦参与方 i 的本地模型 M_i 上传至中心服务器$\mathcal{C}$；最后，中心服务器聚合各方上传的本地模型。重复上述联邦模型构建过程，直至全局联邦模型 M_{fed} 满足收敛条件。

2.2 半中心化联邦学习

现有半中心化联邦学习可以分为两类：基于聚类划分的联邦学习（clustered federated learning）[17-18]、基于层次划分的联邦学习（hierarchical federated learning）。基于聚类划分的联邦学习主要考虑参与方具有不同的任务，并通过全局模型来优化本地模型的情景，其通过推断参与方的任务类型进行聚类划分，然后使用多个聚类中心聚合各方模型；基于层次划分的联邦学习则主要考虑如何降低无线网络中的通信时延，其先在中间层节点进行局部模型聚合，避免所有参与方直接与远程中心服务器进行长距离通信，从而能够有效降低参与方的总体通信开销。

下面分别具体介绍两类半中心化联邦学习框架。

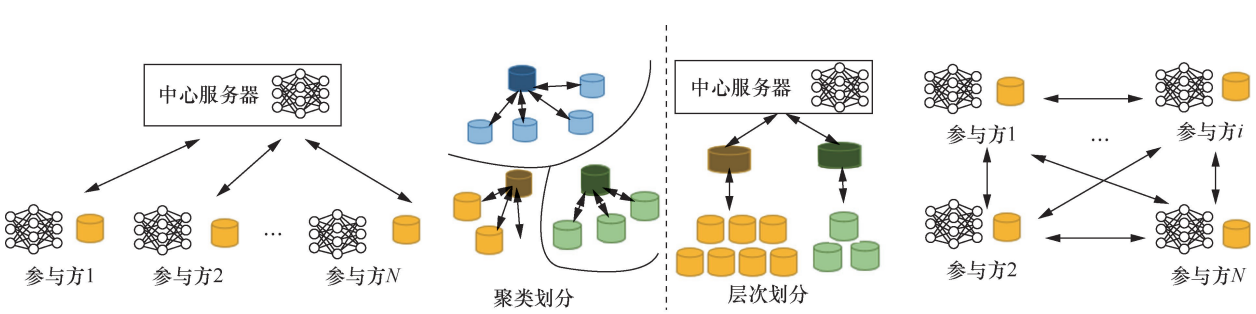
（1）基于聚类划分的联邦学习

Ghosh A 等人[19]较早研究了在多中心群体结构场景下的联邦学习算法，其假设所有 N 个联邦参与方的模型适用于 K 类任务，即存在 K 个聚类中心 $\mathcal{C}_1,\mathcal{C}_2,\cdots,\mathcal{C}_K$。通过聚类划分能够避免不相关的联邦参与方之间相互干扰，提升联合构建的群体模型的精度。基于聚类划分的联邦学习框架包括两部分。一是中心化联邦学习模块，其根据各联邦参与方上传的梯度参数，在 K 个聚类中心 $\mathcal{C}_1,\mathcal{C}_2,\cdots,\mathcal{C}_K$ 上进行模型聚合，得到全局模型 $\theta=\{\theta_1,\theta_2,\cdots,\theta_K\}$。二是聚类迭代划分模块，首先计算各全局模型关于目标函数的梯度，然后计算各参与方的相似度，并根据各方距离更新群体聚类划分，最后重复上述过程，直至收敛。

Sattler F 等人[17]提出了类似的联邦学习框架，其不明确计算各参与方之间的距离（相似度），而是通过评估不同聚类所提升的本地模型准确度，来确定各个联邦参与方具体归属于哪一个类别。

（2）基于层次划分的联邦学习

在移动网络中，由于链接距离不同，所有联邦成员参与方均直接与中心服务器相互传输数据通常容易导致较高的通信成本[18]。为了解决上述问题，Abad M S H 等人[18]提出了基于层次划分的联邦学习框架，通过划分层级并选择区域中心降低通信时延。本文以参考文献[4]中的框架为例（如图 3（b）的右半部分所示），介绍基于层次划分的联邦学习的典型框架。根据地理位置与时延大小，将联邦节点（参与方）划分为 3 级，自底向上依次为：①数据节点（worker），具有本地数据的联邦学习参与方；②中间节点（cluster head），负责聚合部



(a) 中心化联邦学习 (b) 半中心化联邦学习 (c) 去中心化联邦学习

图 3 基于群体智能视角的联邦学习算法框架

分数据节点的训练结果；③模型节点（model owner），负责聚合中间节点的局部模型，并获得最终的联邦模型。基于层次划分的联邦学习模型训练过程与中心化联邦学习的模型训练过程相似：首先，由底层的数据节点训练得到本地模型 M_i；然后，中间节点将其负责区域的本地模型进行聚合，得到新的中间层模型 M_{mid}，并且分发给各数据节点继续训练；经过 T 轮迭代之后，将各中间层模型 M_{mid} 上传至模型节点进行聚合，并将新模型分发至各中间节点；如此迭代，直至得到收敛后的联邦学习模型 M_{fed}。

2.3　去中心化联邦学习

去中心化群体组织结构允许联邦参与方中不存在聚合各方模型的协调者。因此，需要设计模型聚合的联邦网络，现有工作也将联邦学习与区块链结合，基于区块链技术，设计去中心化的模型聚合方法[20-22]。其核心在于设计支持模型聚合的对等网络（peer-to-peer network）。

Warnat-Herresthal S 等人[21]提出了一种典型的去中心化联邦学习框架，如图 3（c）所示。首先，基于区块链技术对联邦参与方的权限进行预定义，只有具有事务权限的参与方才能够共同训练联邦模型。其中，对于新加入对等网络的节点，只有满足预定义的权限条件，才能加入联邦学习训练过程，并通过智能合约（smart contract）获得当前的联邦模型。然后，模型参数可以通过专用的应用程序接口（application programming interface，API）进行聚合，并得到新的联邦学习模型。最后，重复上述过程，直至模型收敛。

Kim H 等人[22]同样基于区块链技术提出了去中心化的联邦学习框架，并且利用区块链可验证和可激励的特点对学习框架进行了优化。具体地，通过分布式记账机制对模型进行异步更新，这也能够避免同步更新时单点故障导致的等待问题。同时，区块链的可验证性能够支持验证本地模型训练结果，这也能够将联邦学习参与方的范围扩展到不可信的公网环境中。此外，区块链中的工作量证明机制（proof-of-work）能够提供与训练样本规模成比例的奖励，进而促进各方贡献数据。

3　联邦学习算法优化

联邦学习为解决数据孤岛问题以及应对群体智能领域的挑战带来了新的方案。现有的联邦学习算法主要在算法隐私、算法精度和算法效率 3 个方面进行优化。下文将主要阐述和总结联邦学习算法在上述 3 类优化上的前沿进展，联邦学习的算法优化见表 1。

3.1　隐私优化

隐私保护一直是联邦学习的核心挑战，这也是其不同于其他传统群体智能技术的明显特点。目前，联邦学习采用的隐私保护优化方法可以主要分为 3 类：基于同态加密的方法、基于安全多方计算的方法与基于差分隐私的方法。下面对 3 类方法分别进行介绍。

（1）基于同态加密的方法

同态加密[23]是一种加密形式，它能够对密文进行特定形式的代数运算，并得到加密的运算结果，将其解密所得结果与对明文进行同样运算的结果相同，这样就实现了在不泄露用户数据的情况下进行密文运算。若使用 Enc 表示加密函数，m 表示明

表 1　　**联邦学习的算法优化**

联邦学习的算法优化分类			参考文献
算法隐私优化	同态加密	优化安全性	[23-25]
		优化加密效率	[26-27]
	安全多方计算	基于混淆电路	[28-31]
		基于秘密共享	[32-36]
	差分隐私	基于中心化差分隐私	[37-43]
		基于本地化差分隐私	[44-48]
算法精度优化	泛化界优化		[2]、[49-51]
	收敛性优化		[17]、[52-55]
算法效率优化	模型压缩		[56-60]
	客户端选择		[2]、[61-65]

文，c 表示密文，pk 表示私钥，则同态加密的形式化定义如下：

$$\forall m_1, m_2 \in \mathcal{M}$$
$$\mathrm{Enc}_{\mathrm{pk}}(m_1 \odot_{\mathcal{M}} m_2) \leftarrow \mathrm{Enc}_{\mathrm{pk}}(m_1) \odot_c \mathrm{Enc}_{\mathrm{pk}}(m_2) \quad (2)$$

同态加密与联邦学习框架中的模型聚合操作十分契合，能够实现中心服务器在对模型数值未知的情况下聚合各方本地模型。因此，已有大量学者对基于同态加密的联邦学习进行了研究。Phong L T 等人[24]首次在联邦学习框架中使用同态加密保护梯度进行计算，参与方使用本地数据更新模型参数，对梯度进行加密后发送给中心服务器，中心服务器对梯度密文进行聚合，参与方可以对聚合后的模型进行解密，该方法可以有效保护恶意中心服务器的推断攻击。Chen Y Q 等人[26]在联邦学习中使用了加法同态加密，参与方对模型参数进行加密后发送给中心服务器，服务器将模型聚合后，分发给参与方解密模型参数，并且使用本地数据更新模型参数。除此以外，还有使用全同态加密来优化算法隐私保护性[25]，使用批加密来优化计算效率[27]等扩展性工作。

（2）基于安全多方计算的方法

安全多方计算[28]由 A.M.图灵奖得主姚期智先生提出，是一种为了解决隐私保护下的协同计算问题而提出的算法框架。其允许 N 个参与方使用自己的数据 $D_1, D_2, \cdots, D_N$ 共同计算一个目标函数 $f(D_1, D_2, \cdots, D_N)$。该方法通常基于混淆电路方法，能够在不需要可信第三方参与的情况下进行带有隐私保护的计算，但同时也有较高的计算复杂度和通信开销。

混淆电路方法相比同态加密允许更丰富的运算操作，例如集合求交集、数值大小比较等。目前已有多种研究结合了联邦学习与安全多方计算。Cock M D 等人[29]提出了一种带有隐私保护的集合交集计算方法，用于联邦学习文本分类问题。Sharma S 等人[30]提出了一种用于非线性深度学习的动态安全方法，该方法可以为大部分参与方不诚实的场景提供隐私安全保护。Zhu H F 等人[31]研究了基于安全多方计算的 FedAvg 算法，提出了一种面向联邦学习的安全聚合算法。

秘密共享[32]也是一种联邦学习中广泛采用的安全多方计算方法，其核心思想是将秘密分割存储。秘密共享将原始数据分为若干份，只有拥有大于一定份数的数据才能重构原始数据，因此可以将秘密分散在所有客户端中，避免中心服务器在聚合模型时的攻击，从而实现隐私保护。Bonawitz K 等人[33]提出了基于秘密共享的联邦学习算法，该算法允许安全聚合参与方的模型参数。然而上述算法易受到不诚实服务器或恶意参与方的攻击，为了解决上述问题，Xu G W 等人[34]提出了一种支持验证的联邦学习框架，该方法使用秘密共享来保护模型训练过程中本地梯度的隐私。除了经典的联邦学习算法框架 FedAvg，也有学者结合了秘密共享与其他机器学习算法来构建联邦学习方法，例如基于秘密共享的异构数据联邦迁移学习算法[35]和结合了秘密共享与联邦 K 均值聚类（K-means）的算法[36]等。然而上述方法会导致极高的时间复杂度和通信开销，因此优化计算效率一直是该方向的研究重点。

（3）基于差分隐私的方法

差分隐私同样是目前联邦学习中被广泛采用的隐私保护方法，该方法最早由 Dwork C 提出[37]，其主要思想是在原始数据上添加噪声，使得两个相似数据在概率上满足不可区分性，同时保留数据集的统计学性质，便于进行数据分析或机器学习，具体定义如下：

$$\Pr[M(D) = o] \leqslant \mathrm{e}^{\epsilon} \Pr[M(D') = o] + \delta \quad (3)$$

其中，M 表示隐私保护机制，D 和 D' 表示两个相似的数据集（两个数据集仅有 1 条数据不同），o 表示机器学习任务的输出结果，ϵ 和 δ 为隐私粒度参数。若算法满足上述不等式，则称该隐私保护方法符合 (ϵ, δ)-差分隐私。根据该方法的隐私保护对象，又可以将差分隐私算法分为两类，分别是用来保护共享模型的中心化差分隐私和用来保护每条数据的本地化差分隐私。后者的隐私保护效果更强，但同时也会损失更多数据可用性，导致联邦学习模型准确率降低。

目前基于差分隐私的方法可分为中心化差分隐私与本地化差分隐私，下面分别进行介绍。

① 中心化差分隐私。中心化差分隐私可以在保护用户隐私的前提下，获得较高的数据可用性，从而获得准确率较高的联邦学习模型。Geyer R C 等人[38]将联邦学习框架与差分隐私技术结合（如图 4 所示），在所提方法中，参与方会将模型梯度上传给中心服务器，服务器会在聚合模型参数时添加高斯噪声，以防恶意参与方从共享模型中推断出其他参

与方所用数据。然而模型仍可能受到恶意服务器的攻击，为此，Hao M 等人[44]提出了一种为本地梯度增加噪声的方法，但其仍属于中心化差分隐私范畴。目前，基于中心化差分隐私的联邦学习在多类场景中得到了应用，如语言模型[39]、排序学习模型[40]、主题模型[41-43]等。

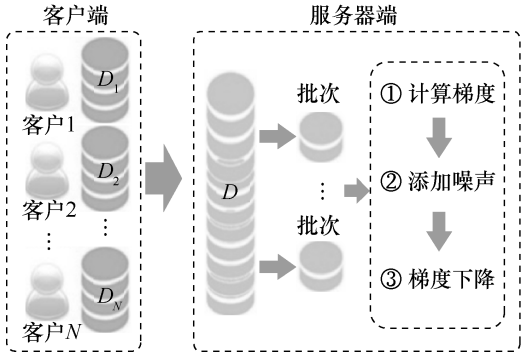


图 4　基于差分隐私的联邦学习算法优化

② 本地化差分隐私。本地化差分隐私对隐私的保护更严苛，该方法在参与方上传数据之前增加噪声，使得任意两个参与方的数据不可区分，不需要可信的第三方进行数据收集。该方法较早由 Abadi M 等人[45]提出，用来在隐私保护的前提下训练深度神经网络，通过梯度截断和增加噪声来保护样本隐私。Bhowmick A 等人[46]首次结合了本地化差分隐私和联邦学习框架来防止推断攻击，在参与方本地通过差分隐私保护每个样本的隐私安全，在服务器端使用差分隐私保护全局模型的隐私安全。Lu Y L 等人[47]提出了一种面向移动设备的联邦学习算法，该算法使用了本地化差分隐私来保护移动设备数据的安全。Wang Y S 等人[48]提出了一个带有本地差分隐私的文本数据挖掘联邦学习算法，实验结果表明，该方法可以保护参与方隐私并保持较高的准确率。本地化差分隐私目前主要面临噪声过大导致结果可用性低的问题，因此相关工作通常致力于设计新的机制以在隐私保护性与结果可用性之间进行更好的权衡。

3.2　精度优化

现实场景中数据的异质性（非独立同分布）导致联邦学习算法精度无论在理论还是在实际上都难以达到传统分布式机器学习的效果，这也成为其重要挑战。下面从算法泛化界优化和收敛性优化两个维度介绍当前联邦学习精度优化方面的前沿进展。

（1）泛化界优化

联邦学习的本质是通过多客户端协作产生在具体任务上拥有较强泛化能力的机器学习模型，其能够使各客户端在保障数据安全的前提下协同训练机器学习模型，实现数据拥有方可以共享数据价值而不共享数据本身。在联邦学习的实际应用场景中，数据异质性给算法的泛化性能带来了挑战。为了减小数据异质性对模型性能的影响，谷歌研究院的 Mcmahan H B 等人[2]首先提出了 FedAvg 算法。该算法在混合分布 $\bar{D}=\sum_{i=1}^{N} w_i D_i$ 上训练模型，设置权重 $w_i = D_i / D$ 为客户端对应的数据规模比例，其中 D 为各方总数据规模。然而这样产生的模型将偏向持有较大数据量的客户端，从而对模型的泛化性能造成影响。Mohri M 等人[49]提出了不可知联邦学习（agnostic federated learning）框架，用于分析数据异质场景下联邦学习的泛化性能。对于多客户端分布 $\{D_1,\cdots,D_N\}$，不可知联邦学习在所有可能的测试分布 $\bar{D}=\sum_{i=1}^{N} \lambda_i D_i$ 上构建模型，其中权重 λ 属于 N 维单纯形 Δ_N，基于权重 λ_i 与样本比例 N_i / N 之间的偏度以及拉德马赫尔（Rademacher）复杂度给出了不可知联邦学习的泛化误差界。不可知联邦学习通过求解对应的最小最大（minmax）优化问题，能够产生在任意目标分布上性能鲁棒的全局模型。然而对于分布与全局分布差异较大的客户端来说，单一的全局模型在该客户端上的性能通常较差。为了弥补单一模型的局限性，Mansour Y 等人[50]提出 3 种能够为客户端定制个性化模型的方法，分别为客户端聚类、数据插值以及模型插值，并给出了相应的泛化误差界；Deng Y 等人[51]又针对客户端的模型插值进行改进，提出了一种自适应泛化误差界的学习方法。

（2）收敛性优化

异质数据还会影响联邦学习的训练效率，导致模型收敛速度降低。在联邦学习的每一轮模型训练中，中央服务器都需要聚合并发送客户端的模型参数，因此客户端之间分布的偏移将影响联邦模型的收敛速率。Li T 等人[52]的研究表明，当参与者的数据分布与平均分布之间存在较大偏差时，FedAvg 算法的收敛速率会大幅下降。

为了解决上述问题，Karimireddy S P 等人[53]借助控制变量纠正 FedAvg 算法在处理非独立同分布数据时产生的客户端偏移现象，并从理论上证明了所提随机控制平均（stochastic controlled averaging for federated learning，SCAFFOLD）方法具有更高的收

敛速率。然而，SCAFFOLD 方法仅考虑降低通信代价，模型精度无法得到很好的保证。Rothchild D 等人[54]提出了基于略图的联邦梯度下降方法 FetchSGD，试图解决因客户端参与的稀疏性导致收敛速率缓慢的难题，并从理论上证明在保证一定泛化性能的前提下，FetchSGD 方法能够通过压缩梯度降低通信代价，从而提高收敛速率；Hamer J 等人[55]基于集成学习的思想提出了高效的 FedBoost（federated boosting）方法，并针对密度估计这一特定任务，从理论上分析了 FedBoost 的泛化误差界。尽管 Rothchild D 等人[54]和 Hamer J 等人[55]的工作在模型性能以及训练效率方面有较好的提升，但这些方法在一定程度上增加了模型复杂度，为方法的实际部署带来了困难。

3.3 效率优化

联邦学习受到参与方设备异构、网络带宽有限等影响，导致计算与通信效率成为阻碍其落地的最大挑战。影响联邦学习算法效率的主要因素是客户端和中央服务之间传递参数的通信成本。目前的研究主要通过模型压缩和客户端选择方法来分别降低单次通信成本和总通信次数，从而降低算法的通信复杂度。

（1）模型压缩方法

由传递深度学习模型带来的巨额通信成本已经成为联邦学习和分布式机器学习落地应用的瓶颈。模型压缩可以在牺牲一定模型性能的情况下减少模型交互带来的通信开销，优化联邦学习的算法效率。Suresh A T 等人[56]首先在分布式场景下提出了基于随机旋转的通信编码算法，证明了在不需要对数据特征做出任何假设的前提下可以达到最小的均方误差，并将其应用到了分布式的劳埃德（Lloyd）算法中，实验结果表明，所提算法可以大大减少通信成本，同时保持模型精度不变。Caldas S 等人[57]在对模型进行压缩的基础上，提出了联邦随机失活（dropout）的方式来选择全局模型的子集，从而进行参数更新，相比已有工作，通信成本被降低到 1/14。Xu J J 等人[58]针对联邦学习算法中存在大量冗余参数需要更新的问题，提出了一种联邦三元量化（federated trained ternary quantization，FTTQ）算法，通过自学习的方式来优化客户端中的学习模型，并证明了所提算法的收敛性。Haddadpour F 等人[59]针对同质和异质的联邦学习分别提出了周期性压缩算法——带压缩的联邦平均（federated averaging with compression，FedCOM）与带压缩和局部梯度跟踪的联邦平均（federated averaging with compression and local gradient tracking，FedCOMGATE），并给出了在非凸、强凸等不同假设下的算法收敛界。Cui L Z 等人[60]在模型压缩的基础上实现了基于区块链的联邦学习算法——用于内容缓存的联邦学习压缩算法（compressed algorithm of federated learning for content caching，CREAT），进一步保护了客户端节点数据的安全性。

（2）客户端选择方法

在客户端数量规模较大的场景中，联邦学习算法需要与每一个客户端进行通信，导致算法效率较低。

现有研究针对此问题，通过在众多客户端中选择一定数量的客户端，并将其作为代表进行训练来减少通信开销，优化算法效率。根据联邦学习过程中客户端的在线状态是否动态变化可以将客户端选择算法分为两类：静态客户端选择和动态客户端选择。

在静态客户端选择中，联邦学习的客户端不存在中途宕机、突然退出的现象，仅需要在联邦学习过程中挑选一次参与训练的客户端，就可以持续进行本地迭代与模型聚合。Mcmahan H B 等人[2]提出的 FedAvg 算法采取简单的随机采样策略，在数据分布满足独立同分布假设的情况下也可以实现不错的训练效果。Wei S Y 等人[61]和 SONG T S 等人[66]的研究中将夏普利值（Shapley value）的概念引入联邦学习中，通过高效计算联邦学习参与者的夏普利值来评估数据质量，从而有效选择客户端。Chai Z 等人[62]提出了基于层的联邦学习（tier-based federated learning，TiFL）系统，将联邦学习参与方基于训练性能分层，在训练中依照参与者所属的层次进行选择，提高了异质场景下联邦学习的收敛速度。在动态客户端选择中，客户端的状态是动态变化的，每一个联邦学习的参与方都有可能因为网络、硬件等出现离线的情况。Huang T S 等人[63]基于多臂老虎机在每一轮中动态选择客户端；Lai F 等人[64]在此基础上进一步实现了一个基于探索–利用策略的联邦学习客户端选择算法。Wang H 等人[65]通过额外训练一个深度强化学习模型在每一轮评估客户端的价值，选择当前价值最高的 K 个参与方进行联邦学习训练，但这种方法需要在联邦模型的基础上进行额外的深度模型训练，对计算资源提出了更高的要求。

4　联邦学习算法模型

现有工作在上述联邦学习框架下设计了多种机器学习的基础模型，包括线性模型、树模型与神经网络模型等，联邦学习算法模型见表 2。

4.1　线性模型

线性模型是机器学习模型中的基础模型之一，其通常适用于朴素的线性数据的回归与分类问题。在线性模型的基础上，通过增加非线性映射层或高维映射，也可以对非线性的数据进行高效的处理，例如逻辑回归（logistic regression，LR）模型等。相比于其他的联邦学习模型，线性模型由于结构简单，通常具有较好的收敛性，下面对具有代表性的两类线性模型进行介绍。

Yang Q 等人[3]介绍了使用线性回归和同态加密进行纵向联邦学习模型训练的方法。该方法使用梯度下降方法训练线性回归模型，对模型的梯度进行安全计算。Hardy S 等人[67]提出了保护隐私的逻辑回归模型纵向联邦学习训练算法，通过保护隐私的实体解析进行逻辑回归模型的训练；此外，该算法对梯度函数进行泰勒逼近，以满足同态加密中的整值计算条件。

现有工作也针对联邦学习场景中线性模型的收敛性进行了实验与理论分析。Konečný J 等人[68]提出了一种联邦随机方差梯度算法，并通过实验对所提线性模型的收敛性进行了验证。Ghosh A 等人[19]提出了迭代联邦聚类算法（iterative federated clustering algorithm，IFCA），该算法交替估计参与方的任务类别，并证明了模型的收敛性在线性模型中是有保障的。

4.2　树模型

机器学习中的树模型具有部署灵活、解释性强等优点，是应用非常广泛的一类机器学习模型。树模型可以分为决策树模型和随机森林模型（random forest，RF）模型两类：决策树模型通过构造一个树状的分类器完成预测任务；而随机森林模型则通过集成训练多棵决策树模型，优化模型的预测准确率。

（1）决策树模型

联邦决策树（decision tree，DT）模型的现有研究主要关注在隐私保护的前提下，对决策树的各数据节点和特征进行训练。Truex S 等人[69]研究了面向横向联邦场景的迭代二叉树 3 代（iterative dichotomiser 3，ID3）决策树的构建。具体地，在决

表 2　　**联邦学习算法模型**

算法	数据划分	适用模型	模型类型	隐私保护机制
VFL-LM[3]	纵向	线性模型	线性回归	同态加密
VFL-LR[67]	纵向		逻辑回归	同态加密
IFCA[19]	横向		线性回归	无
FSVRG[68]	横向		线性回归/逻辑回归	无
PDTL[69]	横向	树模型	决策树	多方安全计算/差分隐私
Pivot[70]	纵向		决策树/随机森林	多方安全计算
SecureBoost[71]	纵向		决策树	同态加密
FRF[72]	纵向		随机森林	加密/混淆
RevFRF[73]	纵向		随机森林	加密/混淆
FedAvg[2]	横向	神经网络模型	多层感知机/卷积神经网络	无
FedProx[74]	横向		多层感知机/卷积神经网络	无
PFNM[75]	横向		多层感知机	无
FedMA[76]	横向		多层感知机/循环神经网络	无
FedGKT[77]	横向		卷积神经网络	无
IncFed[78]	横向		循环神经网络	无

策树模型进行节点分裂时，聚合节点向每个参与方发出查询请求，参与方在本地查询结果的基础上添加差分隐私噪声，返回聚合节点完成信息增益计算，并对决策树节点进行分裂。Wu Y C 等人[70]研究了面向纵向联邦学习的决策树构建，提出了隐私保护纵向决策树（privacy preserving vertical decision tree，Pivot）方法，解决了纵向联邦学习中各客户方的标签数据不互通的问题。Pivot 方法不需要依赖可信第三方，并且能够确保除了客户同意发布的信息（即最终的决策树模型和预测输出），不会泄露任何中间信息。Cheng K W 等人[71]提出了一种新的联邦学习纵向决策树模型——安全提升树模型 SecureBoost，SecureBoost 构建框架如图 5 所示。SecureBoost 在训练过程中，由拥有标签数据的一方对损失函数的一阶导数和二阶导数进行计算后加密传输，随后其他联邦参与方基于加密对梯度计算每个分裂点的信息增益值，并发送给标签拥有方，再由拥有标签数据的一方选出最佳分裂。

（2）随机森林模型

随机森林模型通过对决策树进行模型集成（bootstrap aggregating）来求解分类/回归问题。Wu Y C 等人[70]提出的用于纵向联邦决策树的 Pivot 方法可以被扩展到树集成模型中。将树集成模型中的单棵决策树视为构建块，以此在纵向联邦场景下构建随机森林模型。Liu Y 等人[72-73]提出了可撤销的联邦随机森林（revocable federated random forest，RevFRF）。若某个参与方退出联邦，其原始数据仍然可能被联邦模型记录。而在 RevFRF 中，被撤销的数据既不供其余联邦参与方使用，也不会被训练模型记录，进而增强了随机森林的结构安全性。

4.3 神经网络模型

神经网络模型是目前人工智能中应用非常广泛的机器学习模型之一。其中多层感知机（multi-layer perceptron，MLP）模型、卷积神经网络（convolutional neural network，CNN）模型、循环神经网络（recurrent neural network，RNN）模型是 3 个具有代表性的神经网络模型，而且已经在图像识别、自然语言处理[79-80]等许多领域都实现了落地应用。因此，在联邦学习场景中实现神经网络模型具有巨大的潜力，现有工作也对此方向展开了广泛的探索。下面分别介绍联邦学习场景中对上述 3 类典型的神经网络模型的探索。

（1）MLP 模型

目前主流的支持随机梯度下降算法的联邦学习框架都能够实现多层感知机模型，如经典的 FedAvg 算法[2]和联邦近端梯度法（federated proximal gradient，FedProx）算法[74]等。还有一些现有工作专门研究了如何高效地构建联邦 MLP 模型。Yurochkin M 等人[75]提出了一种非参数贝叶斯框架概率联邦神经匹配（probabilistic federated neural matching，PFNM）算法，如图 6 所示。该算法能够根据联邦参与方提供的本地 MLP 模型的参数权重进行推理，实现了在单轮通信的情况下聚合全局神经网络。一方面，中心服务器收到本地模型后，利用贝塔–伯努利过程将本地 MLP 模型参数与全局模型进行匹配，得到新的全局联邦模型；另一方面，该算法将本地训练与模型聚合解耦，聚合过程只依赖本地模型参数本身，对局部模型的训练方式以及额外信息不作要求，实现了根据参与方的数据和算力选择训练策略的功能。同时，该算法利用贝叶斯框架的特性减小了模型参数，并提高了通信效率。

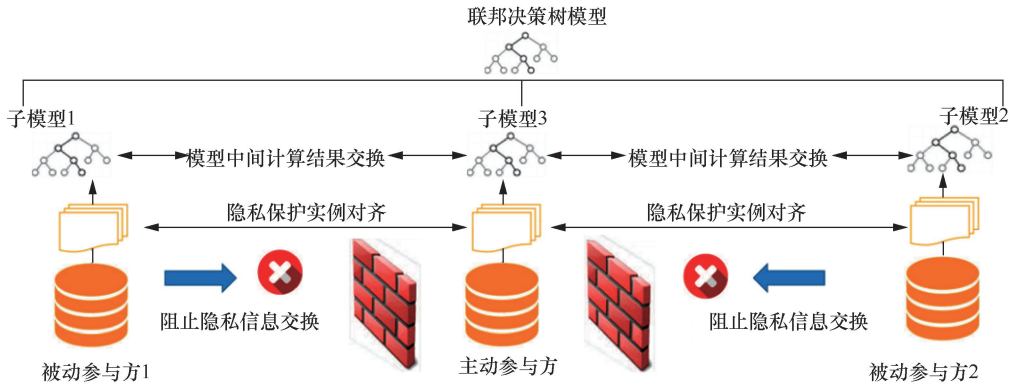


图 5 SecureBoost 构建框架

（2）CNN 模型

CNN 模型是一类包含卷积计算且具有深度结构的前馈神经网络，是深度学习中的代表算法之一。为了高效地构建联邦场景中的 CNN 模型，Wang H Y 等人[76]对上述仅支持 MLP 模型的 PFNM 算法进一步拓展，提出了联邦学习匹配平均（federated learning with matched averaging，FedMA）算法。FedMA 算法基于神经元排列的不变性，通过匹配和平均具有相似的特征提取签名的隐藏元素（即 CNN 中的通道），逐层构建全局模型。在 CNN 模型上的实验表明，除了在性能上领先通用型的 FedAvg 与 FedProx 等流行联邦学习框架，FedMA 同样能够有效降低联邦学习中的总体通信负担。

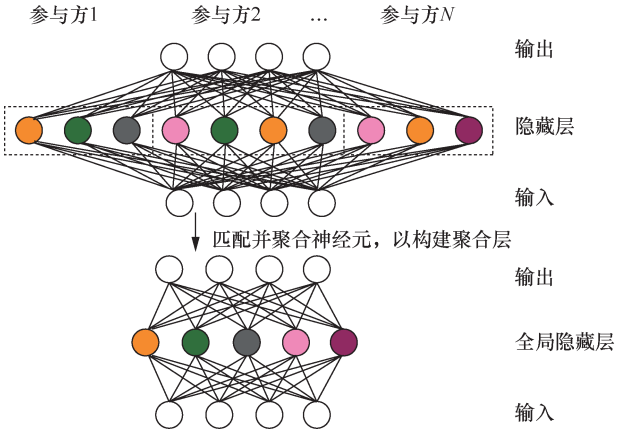


图 6　PFNM 算法

为了解决大型联邦 CNN 模型在边缘设备上的计算资源不足问题，He C Y 等人[77]提出了基于组知识迁移训练的联邦组知识迁移（federated group knowledge transfer，FedGKT）算法。FedGKT 算法实现了一种交替最小化方法的变体，能够用于在边缘节点上训练小型 CNN，并通过知识蒸馏周期性将知识转移到中心服务器端的大型 CNN 上。

（3）RNN 模型

RNN 被广泛用于处理时序数据，也被广泛用于自然语言处理中的语音识别、机器翻译、文本分类等领域[81-84]。RNN 模型在每一时刻的输出同时取决于此刻的输入和上一时刻网络的状态，如长短期记忆（long short term memory，LSTM）[80]等都属于 RNN 模型。

在联邦 RNN 模型方面，Shukla S 等人[85]在 FedMA 算法的基础上，使用基于信息增益的采样策略，根据学习期间测量的信息增益选择部分参数发送给服务器，有效减少了参与方发送的模型参数。Bacciu D 等人[78]针对 RNN 中的回声状态网络模型提出了增量联邦学习（incremental federated learning，IncFed）算法。IncFed 算法避免了 FedAvg 算法中将模型参数直接平均化的朴素方案，而是通过改进聚合过程，生成最优的全局模型。但 IncFed 算法只适用于回声状态网络模型，尚未扩展至通用的 RNN 模型。

5　开源平台与典型应用

本节首先按照发布时间，介绍联邦学习 5 个主要的开源平台；然后，介绍目前联邦学习在智慧交通、智慧金融和智慧医疗 3 个领域的典型应用。

5.1　联邦学习的开源平台

目前业界已搭建了多个联邦学习的开源平台，包括 FATE[86]、TFF（TensorFlow federated）[87]、PySyft[88]、FedML[89]、Flower[90]等，联邦学习开源平台发布时间如图 7 所示。开源平台的目的是为多设备部署或实验提供通信接口和隐私保护机制，这能够极大地简化联邦学习算法的编写及部署难度。大部分联邦学习平台通常不包含计算平台，而是以 TensorFlow 或 PyTorch 等机器学习框架为底层计算平台，在其上实现了联邦学习接口，即将用户编写的联邦模型转换为相应的模型进行训练与推断。在模型方面，目前大部分平台通常能够支持线性模型和神经网络模型，FATE 能够支持决策树等树形模型。在隐私保护优化方面，5 个开源平台均支持至少一种隐私保护方法，包括差分隐私、同态加密等。其中，Flower 和 PySyft 均通过第三方库 Opacus 实现隐私保护技术。

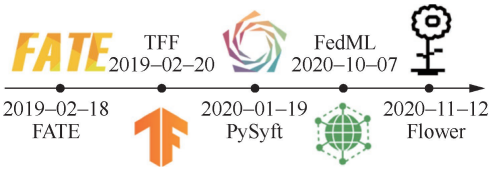


图 7　联邦学习开源平台发布时间

（1）FATE 开源平台

FATE[86]是由深圳前海微众银行股份有限公司开发的首个联邦学习工业级开源平台。FATE 底层由三部分组成，分别是计算、联邦、存储，其中计算模块同时适配了 TensorFlow 及 PyTorch。在底层之上，FATE 使用安全多方计算和同态加密技术构建了安全协议，支持不同种类机器学习算法的安全计算。FATE 还提供了联邦学习高级 API，支持线性模型、决策树、

深度学习和迁移学习等多种机器学习方法。除此之外，FATE 还支持图形交互界面，用于联邦学习可视化、客户端集群管理与监控以及任务调度与管理。

（2）TFF 开源平台

TFF[87]是谷歌公司开发的分布式机器学习与计算平台。以 TensorFlow 为底层计算平台，简化了开发者调用已有算法和设计新的联邦学习算法的开发难度。与 FedML 类似，TFF 将 API 分为低层 API 与高层 API，具有良好的可扩展性，低层 API 提供了丰富的接口，允许研究者设计不同的联邦学习算法；高层 API 为调用库中包含的算法进行训练提供支持。同时 TFF 也支持使用 TensorFlow Privacy 中的组件对联邦学习算法进行隐私保护。

（3）PySyft 开源平台

PySyft[88]是由 OpenMined 组织开发的联邦学习开源平台。该开源平台实现了隐私保护与模型训练解耦，重写了 PyTorch 中张量的运算符，分布于多台设备上的数据可以通过安全求和函数轻松计算，中心化的机器学习代码也可以轻松迁移为联邦学习，而无须考虑客户端中的通信过程。该平台支持多种隐私保护方法，包括差分隐私以及安全多方计算，以保护联邦学习客户端的数据安全。

（4）FedML 开源平台

FedML 是 He C Y 等人[89]开发的联邦学习平台和基准测试库，该平台以 PyTorch 为底层计算平台，提供了灵活并且通用的接口，支持调用库中实现的基准算法（包括 FedAvg、FedProx 等），降低了研究者进行联邦学习算法实验的难度，具有较好的可扩展性。同时，该平台为非独立同分布场景提供了全面的联邦数据集，用于算法的公平比较。FedML 平台同时支持单机模拟、移动设备部署与物联网设备部署 3 种计算范式。但是 FedML 中的大部分算法尚未提供与隐私保护相关的组件，开发者需要自己实现同态加密、差分隐私等方法以保护联邦学习中的数据隐私。

（5）Flower 开源平台

Flower[90]是一个可拓展性高的联邦学习平台，同时支持本地模拟与多设备部署。联邦学习系统间通常具有较大的差异，Flower 允许根据不同的使用场景进行一系列自定义设置，以满足使用需求。该平台可以适配任何机器学习框架，不同机器学习框架具有不同的优点，开发者可根据需求自由选择，只需要实现机器学习模型参数到 Python 的数值计算库 NumPy 的转换即可适配。同时，该平台包含了部分基准测试算法，包括联邦批次正则化（federated batch normalization，FedBN）、联邦优化（federated optimization，FedOpt）等。在隐私保护方面，该平台支持使用 Pytorch 的 Opacus 库对模型进行差分隐私保护。

5.2 联邦学习的典型应用

目前，联邦学习的技术优势已经在多个真实应用场景中发挥了重要作用，本节以智慧交通、智慧金融与智慧医疗 3 类典型应用为例，介绍联邦学习的产业化应用。

（1）智慧交通领域应用

在过去几年中，人工智能技术的发展带动了交通领域的智慧化发展。智慧交通系统多采用中心化系统架构，其“中心–终端”模式无可避免地带来了隐私保护问题。在交通规划方面，Liu Y 等人[91]提出了一种基于联合声明协议的联邦聚合算法，避免了交换原始数据，在保护车辆隐私的前提下实现了交通流量预测。在车辆资源管理方面，Yu S 等人[92]提出了一种双时间尺度的联邦学习模型，利用联邦学习方法对该强化学习模型进行分布式数据分析，以保护车辆端的数据隐私，实现了在隐私保护基础上的交通决策和资源分配。Zhao N 等人[93]将双深度 Q-learning 方法与联邦学习结合，在有效保护车辆时空隐私的前提下，实现了对车辆运载能力与交通负载的计算，从而进行车辆资源管理。在共享交通方面，Shi D Y 等人[94]提出了一种基于联邦计算价值函数的交通资源调度方法，该方法显著提升了出行效率和群体公平性。

（2）智慧金融领域应用

金融行业是另一个对数据隐私有较高要求的领域，其中风险评估、欺诈检测等方面对隐私保护具有较高要求，联邦学习在智慧金融领域的应用为金融隐私提供了解决方案，是促进智慧金融发展的有效手段。Hardy S 等人[67]设计了一个端到端的安全联邦逻辑回归（secure federated logistics regression，SFLR）方案，联合两个参与方对同一批样本的不同特征进行建模，并应用加法同态加密来保护模型的安全和数据的隐私。该算法被深圳前海微众银行股份有限公司集成到 FATE[86]框架中并应用于小微企业信用风险评估等风控场景。Zheng W B 等人[95]提出了结合度量学习的联邦学习方法来解决信用卡欺诈中的隐私保护问题，并被有效应用到金融欺诈检测中。

（3）智慧医疗领域应用

在医疗物联网和通信技术的支持下，现代医疗体系的发展趋向智能化和高效化。联邦学习技术被应用于智慧医疗领域，解决了电子健康记录管理、远程健康监测、医疗影像分析以及新冠肺炎防治等方面的隐私保护问题，推动了大数据驱动的智慧医疗发展。Hao M 等人[96]介绍了一种联合多家医院通过云计算的方式共享电子健康记录数据的联邦模型。Brisimi T S 等人[97]提出了一种结合联邦学习和心脏病人过往电子健康记录，预测病人未来因心脏病就医的地点，以实现稀缺医疗资源管理优化的方法。在医疗影像分析方面，联邦学习被用于解决数据异质性问题和实现隐私保护。近两年，新冠肺炎在全球范围内快速传播，面对此类突发疾病，联邦学习在快速获得大量训练数据、快速更新模型方面具有较大优势。Zhang W S 等人[98]提出了一种动态的联邦学习方法，用于 CT（computed tomography）影像分析和新冠肺炎核酸检测。

6　结束语

联邦学习作为破解数据孤岛问题的群体智能新研究方向，近年来在数据隐私保护的大背景下受到了学术界与工业界广泛的关注。本文从群体组织结构划分的角度对联邦学习算法框架进行了分类，并介绍了优化算法与基础模型。本文还介绍了目前主流的联邦学习开源平台与典型应用。作为群体智能在互联网环境下的重要研究方向，未来的联邦学习研究充满了挑战与机遇，克服这些困难将有助于建立一套新的基于互联网的群体智能理论与方法体系，从而促进人工智能红利的落实，为现代社会的繁荣发展注入新的动力。

参考文献：

[1] KONEČNÝ J, MCMAHAN H B, YU F X, et al. Federated learning: strategies for improving communication efficiency[J]. arXiv preprint, 2016, arXiv:1610.05492.

[2] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv preprint, 2016, arXiv:1602.05629.

[3] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning[J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19.

[4] YANG Q, LIU Y, CHENG Y, et al. Federated learning-synthesis lectures on artificial intelligence and machine learning[M]. [S.l:s.n.], 2019.

[5] YANG Q, FAN L X, YU H. Federated learning[M]. Cham: Springer International Publishing, 2020.

[6] 杨强, 刘洋, 程勇, 等. 联邦学习[M]. 北京: 电子工业出版社, 2020.
YANG Q, LIU Y, CHENG Y, et al. Federated learning[M]. Beijing: Publishing House of Electronics Industry, 2020.

[7] 杨强, 黄安埠, 刘洋, 等. 联邦学习实战[M]. 北京: 电子工业出版社, 2021.
YANG Q, HUANG A B, LIU Y, et al. Practicing federated learning[M]. Beijing: Publishing House of Electronics Industry, 2021

[8] 杨强, 刘洋, 陈天健, 等. 联邦学习[J]. 中国计算机学会通讯, 2018, 14(11): 49-55.
YANG Q, LIU Y, CHEN T J, et al. Federated learning[J]. Communications of the CCF, 2018, 14(11): 49-55.

[9] REYNOLDS C W. Flocks, herds and schools: a distributed behavioral model[C]//Proceedings of the 14th Annual Conference on Computer Graphics and Interactive Techniques. New York: ACM Press, 1987: 25-34.

[10] PANDEY S R, TRAN N H, BENNIS M, et al. A crowdsourcing framework for on-device federated learning[J]. IEEE Transactions on Wireless Communications, 2020, 19(5): 3241-3256.

[11] SINDINGER T S. Crowdsourcing: why the power of the crowd is driving the future of business[J]. Human Resource Management International Digest, 2010, 18(3): 11-16.

[12] TONG Y X, WANG Y S, SHI D Y. Federated learning in the lens of crowdsourcing[J]. Data Engineering, 2020: 26.

[13] FINKEL J R, MANNING C D. Joint parsing and named entity recognition[C]//Proceedings of 2009 Annual Conference of the North American Chapter of the Association for Computational Linguistics. Morristown: Association for Computational Linguistics, 2009.

[14] RICH C. Multitask learning[J]. Machine Learning,1997, 28(1): 41-75.

[15] ZHANG Y, YANG Q. An overview of multi-task learning[J]. National Science Review, 2017, 5(1): 30-43.

[16] LI M. Scaling distributed machine learning with the parameter server[C]//Proceedings of 2014 International Conference on Big Data Science and Computing. New York: ACM Press, 2014: 583-598.

[17] SATTLER F, MÜLLER K R, SAMEK W. Clustered federated learning: model-agnostic distributed multitask optimization under privacy constraints[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 32(8): 3710-3722.

[18] ABAD M S H, OZFATURA E, GUNDUZ D, et al. Hierarchical federated learning ACROSS heterogeneous cellular networks[C]//Proceedings of 2020 IEEE International Conference on Acoustics, Speech and Signal Processing. Piscataway: IEEE Press, 2020: 8866-8870.

[19] GHOSH A, CHUNG J, YIN D, et al. An efficient framework for clustered federated learning[J]. Advances in Neural Information Processing Systems, 2020, 33: 19586-19597.

[20] LIM W Y B, NG J S, XIONG Z H, et al. Decentralized edge intelligence: a dynamic resource allocation framework for hierarchical federated learning[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(3): 536-550.

[21] WARNAT-HERRESTHAL S, SCHULTZE H, SHASTRY K L, et al. Swarm learning for decentralized and confidential clinical machine learning[J]. Nature, 2021, 594(7862): 265-270.

[22] KIM H, PARK J, BENNIS M, et al. Blockchained on-device federated learning[J]. IEEE Communications Letters, 2020, 24(6): 1279-1283.

[23] RIVEST R L, ADLEMAN L M, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[24] PHONG L T, AONO Y, HAYASHI T, et al. Privacy-preserving deep learning via additively homomorphic encryption[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(5): 1333-1345.

[25] HAO M, LI H W, LUO X Z, et al. Efficient and privacy-enhanced federated learning for industrial artificial intelligence[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6532-6542.

[26] CHEN Y Q, QIN X, WANG J D, et al. FedHealth: a federated transfer learning framework for wearable healthcare[J]. IEEE Intelligent Systems, 2020, 35(4): 83-93.

[27] ZHANG C L, LI S Y, XIA J Z, et al. Batchcrypt: efficient homomorphic encryption for cross-silo federated learning[C]//Proceedings of 2020 USENIX Conference on Usenix Annual Technical Conference. [S.l.:s.n.], 2020: 493-506.

[28] YAO A C. Protocols for secure computations[C]//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1982: 160-164.

[29] COCK M D, DOWSLEY R, NASCIMENTO A C A, et al. Privacy-preserving classification of personal text messages with secure multi-party computation: an application to hate-speech detection[J]. Advances in Neural Information Processing Systems 32, 2019: 3752.

[30] SHARMA S, XING C P, LIU Y, et al. Secure and efficient federated transfer learning[C]//Proceedings of 2019 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2019: 2569-2576.

[31] ZHU H F, MONG GOH R S, NG W K. Privacy-preserving weighted federated learning within the secret sharing framework[J]. IEEE Access, 2020, 8: 198275-198284.

[32] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[33] BONAWITZ K, IVANOV V, KREUTER B, et al. Practical secure aggregation for privacy-preserving machine learning[C]//Proceedings of 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1175-1191.

[34] XU G W, LI H W, LIU S, et al. VerifyNet: secure and verifiable federated learning[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 911-926.

[35] GAO D S, LIU Y, HUANG A B, et al. Privacy-preserving heterogeneous federated transfer learning[C]//Proceedings of 2019 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2019: 2552-2559.

[36] LIU Y, MA Z, YAN Z, et al. Privacy-preserving federated K-means for proactive caching in next generation cellular networks[J]. Information Sciences, 2020, 521: 14-31.

[37] DWORK C. Differential privacy[C]//Proceedings of the International Colloquium on Automata, Languages, and Programming. Heidelberg: Springer, 2006: 1-12.

[38] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective[J]. arXiv preprint, 2017, arXiv:1712.07557.

[39] MCMAHAN H B, RAMAGE D, TALWAR K, et al. Learning differentially private recurrent language models[J]. arXiv preprint, 2017, arXiv:1710.06963.

[40] WANG Y S, TONG Y X, SHI D Y, et al. An efficient approach for cross-silo federated learning to rank[C]//Proceedings of 2021 IEEE 37th International Conference on Data Engineering. Piscataway: IEEE Press, 2021: 1128-1139.

[41] SHI Y X, TONG Y X, SU Z Y, et al. Federated topic discovery: a semantic consistent approach[J]. IEEE Intelligent Systems, 2020.

[42] JIANG D, TONG Y X, SONG Y F, et al. Industrial federated topic modeling[J]. ACM Transactions on Intelligent Systems and Technology, 2021, 12(1): 1-22.

[43] JIANG D, SONG Y F, TONG Y X, et al. Federated topic modeling[C]//Proceedings of the 28th ACM International Conference on Information and Knowledge Management. New York: ACM Press, 2019: 1071-1080.

[44] HAO M, LI H W, XU G W, et al. Towards efficient and privacy-preserving federated deep learning[C]//Proceedings of 2019 IEEE International Conference on Communications. Piscataway: IEEE Press, 2019: 1-6.

[45] ABADI M, CHU A, GOODFELLOW I, et al. Deep learning with differential privacy[C]//Proceedings of 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 308-318.

[46] BHOWMICK A, DUCHI J, FREUDIGER J, et al. Protection against reconstruction and its applications in private federated learning[J]. arXiv preprint, 2018, arXiv:1812.00984.

[47] LU Y L, HUANG X H, DAI Y Y, et al. Differentially private asynchronous federated learning for mobile edge computing in urban informatics[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2134-2143.

[48] WANG Y S, TONG Y X, SHI D Y. Federated latent dirichlet allocation: a local differential privacy based framework[J]. Proceedings of the AAAI Conference on Artificial Intelligence. [S.l.:s.n.], 2020, 34(4): 6283-6290.

[49] MOHRI M, SIVEK G, SURESH A T. Agnostic federated learning[C]//Proceedings of the 36th International Conference on Machine Learning. [S.l.:s.n.], 2019:4615–4625.

[50] MANSOUR Y, MOHRI M, RO J, et al. Three approaches for personalization with applications to federated learning[J]. arXiv preprint, 2020, arXiv:2002.10619.

[51] DENG Y, KAMANI M M, MAHDAVI M. Adaptive personalized federated learning[J]. arXiv preprint, 2020, arXiv:2003.13461.

[52] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[J]. arXiv preprint, 2018, arXiv:1812.06127.

[53] KARIMIREDDY S P, KALE S, MOHRI M, et al. SCAFFOLD: stochastic controlled averaging for federated learning[C]//Proceeding of the International Conference on Machine Learning. [S.l.:s.n.], 2020: 5132-5143.

[54] ROTHCHILD D, PANDA A, ULLAH E, et al. FetchSGD: communication-efficient federated learning with sketching[C]//Proceedings of the 37th International Conference on Machine Learning. [S.l.:s.n.], 2020: 8253-8265.

[55] HAMER J, MOHRI M, SURESH A T. FedBoost: a communication-efficient algorithm for federated learning[C]//Proceedings of the 37th International Conference on Machine Learning. [S.l.:s.n.], 2020:

3973-3983.

[56] SURESH A T, YU F X, KUMAR S, et al. Distributed mean estimation with limited communication[C]//Proceedings of 2017 International Conference on Machine Learning. [S.l.:s.n.], 2017: 3329-3337.

[57] CALDAS S, KONEČNY J, MCMAHAN H B, et al. Expanding the reach of federated learning by reducing client resource requirements[J]. arXiv preprint, 2018, arXiv:1812.07210.

[58] XU J J, DU W L, JIN Y C, et al. Ternary compression for communication-efficient federated learning[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 33(3): 1162-1176.

[59] HADDADPOUR F, KAMANI M M, MOKHTARI A, et al. Federated learning with compression: unified analysis and sharp guarantees[C]// Proceedings of the International Conference on Artificial Intelligence and Statistics. [S.l.:s.n.], 2021: 2350-2358.

[60] CUI L Z, SU X X, MING Z X, et al. CREAT: blockchain-assisted compression algorithm of federated learning for content caching in edge computing[J]. IEEE Internet of Things Journal, 2020, 4370(99): 1.

[61] WEI S Y, TONG Y X, ZHOU Z M, et al. Efficient and fair data valuation for horizontal federated learning[M]//Federated learning. Cham: Springer, 2020.

[62] CHAI Z, ALI A, ZAWAD S, et al. TiFL: a tier-based federated learning system[C]//Proceedings of the 29th International Symposium on High-Performance Parallel and Distributed Computing. New York: ACM Press, 2020: 125-136.2020.

[63] HUANG T S, LIN W W, WU W T, et al. An efficiency-boosting client selection scheme for federated learning with fairness guarantee[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1552-1564.

[64] LAI F, ZHU X F, MADHYASTHA H, et al. Oort: informed participant selection for scalable federated learning[J]. arXiv preprint, 2020, arXiv:2010.06081.

[65] WANG H, KAPLAN Z, NIU D, et al. Optimizing federated learning on non-IID data with reinforcement learning[C]//Proceedings of 2020 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 1698-1707.

[66] SONG T S, TONG Y X, WEI S Y. Profit allocation for federated learning[C]//Proceedings of 2019 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2019: 2577-2586.

[67] HARDY S, HENECKA W, IVEY-LAW H, et al. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption[J]. arXiv preprint, 2017, arXiv:1711.10677.

[68] KONEČNÝ J, MCMAHAN H B, RAMAGE D, et al. Federated optimization: distributed machine learning for on-device intelligence[J]. arXiv preprint, 2016, arXiv:1610.02527.

[69] TRUEX S, BARACALDO N, ANWAR A, et al. A hybrid approach to privacy-preserving federated learning[C]//Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security. New York: ACM Press, 2019: 1-11.

[70] WU Y C, CAI S F, XIAO X K, et al. Privacy preserving vertical federated learning for tree-based models[J]. Proceedings of the VLDB Endowment, 2020, 13(12): 2090-2103.

[71] CHENG K W, FAN T, JIN Y L, et al. SecureBoost: a lossless federated learning framework[J]. IEEE Intelligent Systems, 2021, 36(6): 87-98.

[72] LIU Y, LIU Y T, LIU Z J, et al. Federated forest[J]. IEEE Transactions on Big Data, 2020, 2755(99): 1.

[73] LIU Y, MA Z, LIU X M, et al. Revocable federated learning: a benchmark of federated forest[J]. arXiv preprint, 2019, arXiv:1911.03242.

[74] SAHU A K, LI T, SANJABI M, et al. On the convergence of federated optimization in heterogeneous networks[J]. arXiv preprint, 2018, arXiv: 1812.06127.

[75] YUROCHKIN M, AGARWAL M, GHOSH S, et al. Bayesian nonparametric federated learning of neural networks[C]//Proceedings of the International Conference on Machine Learning. [S.l.:s.n.], 2019: 7252-7261.

[76] WANG H Y, YUROCHKIN M, SUN Y K, et al. Federated learning with matched averaging[J]. arXiv preprint, 2020, arXiv:2002.06440.

[77] HE C Y, ANNAVARAM M, AVESTIMEHR S. Group knowledge transfer: federated learning of large CNNs at the edge[J]. arXiv preprint, 2020, arXiv:2007.14513.

[78] BACCIU D, DI SARLI D, FARAJI P, et al. Federated reservoir computing neural networks[C]//Proceedings of 2021 International Joint Conference on Neural Networks. Piscataway: IEEE Press, 2021: 1-7.

[79] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[80] SUNDERMEYER M, SCHLÜTER R, NEY H. LSTM neural networks for language modeling[C]//Proceedings of the 13th Annual Conference of The International Speech Communication Association. [S.l.:s.n.], 2012.

[81] GRAVES A, MOHAMED A R, HINTON G. Speech recognition with deep recurrent neural networks[C]//Proceedings of 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. Piscataway: IEEE Press, 2013: 6645-6649.

[82] SUTSKEVER I, VINYALS O, LE Q V. Sequence to sequence learning with neural networks[J]. Advances in Neural Information Processing Systems, 2014.

[83] WANG R S, LI Z, CAO J, et al. Recurrent convolutional neural networks for text classification[C]//Proceedings of 2019 International Joint Conference on Neural Networks. [S.l.:s.n.], 2015.

[84] CHO K, VAN MERRIENBOER B, BAHDANAU D, et al. On the properties of neural machine translation: encoder–decoder approaches[C]//Proceedings of the 8th Workshop on Syntax, Semantics and Structure in Statistical Translation. Stroudsburg: Association for Computational Linguistics, 2014.

[85] SHUKLA S, SRIVASTAVA N. Federated matched averaging with information-gain based parameter sampling[C]//Proceedings of the 1st International Conference on AI-ML-Systems. [S.l.:s.n.], 2021: 1-7.

[86] LIU Y, FAN T, CHEN T J, et al. FATE: an industrial grade platform for collaborative learning with data protection[J]. Journal of Machine Learning Research, 2021, 22(226): 1-6.

[87] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: system design[J]. Proceedings of Machine Learning and Systems, 2019, 1: 374-388.

[88] ZILLER A, TRASK A, LOPARDO A, et al. PySyft: a library for easy federated learning[M]//Federated learning systems. Cham: Springer, 2021.

[89] HE C Y, LI S Z, SO J, et al. FedML: a research library and benchmark for federated machine learning[J]. arXiv preprint, 2020, arXiv:

2007.13518.

[90] BEUTEL D J, TOPAL T, MATHUR A, et al. Flower: a friendly federated learning research framework[J]. arXiv preprint, 2020, arXiv:2007.14390.

[91] LIU Y, YU J J Q, KANG J W, et al. Privacy-preserving traffic flow prediction: a federated learning approach[J]. IEEE Internet of Things Journal, 2020, 7(8): 7751-7763.

[92] YU S, CHEN X, ZHOU Z, et al. When deep reinforcement learning meets federated learning: intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network[J]. IEEE Internet of Things Journal, 2021, 8(4): 2238-2251.

[93] ZHAO N, WU H, YU F R, et al. Deep-reinforcement-learning-based latency minimization in edge intelligence over vehicular networks[J]. IEEE Internet of Things Journal, 2022, 9(2): 1300-1312.

[94] SHI D Y, TONG Y X, ZHOU Z M, et al. Learning to assign: towards fair task assignment in large-scale ride hailing[C]//Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. [S.l.:s.n.], 2021: 3549-3557.

[95] ZHENG W B, YAN L, GOU C, et al. Federated meta-learning for fraudulent credit card detection[C]//Proceedings of the 29th International Joint Conference on Artificial Intelligence. California: International Joint Conferences on Artificial Intelligence Organization, 2020: 4654-4660.

[96] HAO M, LI H W, XU G W, et al. Privacy-aware and resource-saving collaborative learning for healthcare in cloud computing[C]//Proceedings of 2020 IEEE International Conference on Communications. Piscataway: IEEE Press, 2020: 1-6.

[97] BRISIMI T S, CHEN R D, MELA T, et al. Federated learning of predictive models from federated electronic health records[J]. International Journal of Medical Informatics, 2018, 112: 59-67.

[98] ZHANG W S, ZHOU T, LU Q H, et al. Dynamic fusion-based federated learning for COVID-19 detection[J]. IEEE Internet of Things Journal, 2021, 8(21): 15884-15891.

[作者简介]

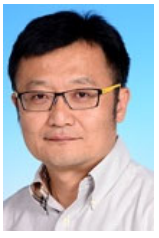
杨强（1961− ），男，博士，深圳前海微众银行股份有限公司首席人工智能官，香港科技大学教授，主要研究方向为联邦学习、迁移学习、群体智能等。

童咏昕（1982− ），男，博士，北京航空航天大学教授，主要研究方向为联邦学习、群体智能、数据库与数据挖掘。

王晏晟（1994− ），男，北京航空航天大学博士生，主要研究方向为联邦学习。

范力欣（1971− ），男，博士，深圳前海微众银行股份有限公司人工智能首席科学家，主要研究方向为机器学习、联邦学习、计算机视觉。

王薇（1983− ），女，博士，北京航空航天大学教授，主要研究方向为群智系统协同控制与优化、攻击检测与安全控制。



陈雷（1972− ），男，博士，香港科技大学教授，主要研究方向为时空大数据、空间众包、不确定数据、数据驱动的机器学习。

王魏（1983− ），男，博士，南京大学副教授，主要研究方向为机器学习、弱监督学习、计算学习理论。

康焱（1984− ），男，博士，深圳前海微众银行股份有限公司人工智能算法研究员，主要研究方向为隐私保护机器学习、联邦迁移学习。