面向边缘计算场景的个性化联邦学习综述

何帆[1]，王勇[1,2]，杨静[1]，于旭[3]
（1.哈尔滨工程大学计算机科学与技术学院，黑龙江 哈尔滨 150001；
2.哈尔滨工程大学电子政务建模仿真国家工程实验室，黑龙江 哈尔滨 150001；
3.中国石油大学（华东）计算机科学与技术学院，山东 青岛 266580）

摘　要：针对传统联邦学习在边缘计算场景中面临边缘节点数据异质、个性化需求等挑战，导致全局模型难以适配多样化的边缘节点，对面向边缘计算场景的个性化联邦学习研究进展进行系统性的综述。首先，回顾个性化联邦学习的背景及意义并分析数据异质性对联邦学习的影响。其次，介绍数据异质性的概念，并归纳数据异质性的常见形式。然后，梳理现阶段面向边缘计算场景的个性化联邦学习研究方法，主要包括基于数据、基于客户端模型优化、基于服务器聚合优化、基于全局架构优化、基于大模型以及基于原型学习的5种关键方法。最后，对其发展趋势进行探讨并展望未来可能的研究方向，为未来个性化联邦学习领域的研究提供指引和方向。

关键词：边缘计算场景；模型协同训练；数据异质性；个性化联邦学习
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025131

Survey of personalized federated learning for edge computing scenarios

HE Fan[1], WANG Yong[1,2], YANG Jing[1], YU Xu[3]
1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
2. Modeling and Emulation in E-Government National Engineering Laboratory, Harbin Engineering University, Harbin 150001, China
3. College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266580, China

Abstract: In view of the challenges faced by traditional federated learning in edge computing scenarios, such as data heterogeneity and personalized requirements among edge nodes, limiting the adaptability of the global model. So, a comprehensive review of recent advances in personalized federated learning for edge computing scenarios was provided. Firstly, the background and scientific significance of personalized federated learning were elaborated, followed by rigorous analysis of data heterogeneity's impacts. Secondly, data heterogeneity was formally defined and classified. Subsequently, existing approaches were categorized into five key methodologies: data-based methods, client-side model optimization, server-side aggregation optimization, global architecture optimization, large model, and prototype-based learning methods. Finally, to guide ongoing developments in the field, future trends and outlines potential research directions were explored.

Keywords: edge computing scenario, collaborative model training, data heterogeneous, personalized federated learning

---

收稿日期：2025–05–26；**修回日期：**2025–07–10
通信作者：王勇，wangyongcs@hrbeu.edu.cn
基金项目：国家自然科学基金资助项目（No.62472441）；国家重点研发计划基金资助项目（No.2022YFC3301804）；教育部人文社会科学研究青年基金资助项目（No.20YJCZH172）；黑龙江省自然科学基金资助项目（No.LH2024F035）
Foundation Items: The National Natural Science Foundation of China (No.62472441), The National Key Research and Development Program of China (No.2022YFC3301804), The Youth Fund Project of Humanities and Social Sciences Research of the Ministry of Education of China (No.20YJCZH172), The Natural Science Foundation of Heilongjiang Province (No.LH2024F035)

0　引言

随着5G与物联网技术的崛起，以及人工智能与计算技术的快速发展，智能家居、车联网、智能制造以及智慧医疗等产业蓬勃发展。边缘计算通过在网络边缘部署计算和存储资源，成为推动上述产业落地的关键支撑技术。伴随物联网设备数量激增，边缘计算架构快速发展，促使大量智能终端被部署于网络边缘，也使边缘侧数据呈现指数级增长趋势[1]。这类数据往往蕴含大量敏感信息，不仅存在严重的隐私泄露风险，还可能违背数据主权、合规性等相关法律法规。因此，数据隐私与安全问题日益凸显[2]。如何在边缘计算场景中保证数据隐私安全与高效模型训练的同时，最大可能优化各边缘设备的模型性能，是当前智能物联网、工业互联网等领域的研究热点。联邦学习（FL, federated learning）[3]作为一种分布式机器学习方法，允许客户端在不暴露原始数据的情况下协同训练深度学习模型，具有巨大的应用潜力。典型的FL系统如图1所示。

当前，联邦学习在数据同质环境下，往往能够获得良好的模型训练效果。然而，在现实边缘计算场景下，由于各边缘设备的数据来源受其特定任务需求、数据获取策略和采样方法的影响，本地数据分布往往呈现出显著差异[4]。这种差异导致客户端存在数据异质性，即数据的非独立同分布（Non-IID, non-independent and identically distributed）[5]。大量研究表明，在边缘计算场景下，由于数据异质性的存在，传统联邦学习方法因其客户端的局部优化目标与全局优化目标不一致，全局模型难以适应不同客户端的个性化需求，因此模型的性能会受到严重影响[6]。

针对边缘计算场景中广泛存在的数据异质性问题，个性化联邦学习（PFL, personalized federated learning）作为一种有效的解决方案，在传统联邦学习的基础上，着重加强全局模型的泛化能力和本地模型的个性化水平，能够有效解决传统联邦学习中不同边缘节点间的数据异质性问题[7]。

1) 个性化联邦学习通过引入鲁棒性更强的优化方法，如数据增强、正则化等方法，增强全局模型对不同数据分布的适应性，从而缓解数据异质性导致的客户端漂移问题，提高模型的泛化性能。

2) 针对每个边缘节点的独特数据分布，个性化联邦学习能够结合参数解耦、客户端聚类等方法，为其定制个性化模型，提升本地模型的性能。

随着边缘终端数量持续增长、任务场景日益复杂，对PFL提出了更高要求，尤其在任务精度要求高、资源受限和数据差异显著的场景中，如医疗诊断、智能驾驶等，亟须深入研究具有高效性、可扩展性与适应性的个性化联邦学习模型，以支撑新一

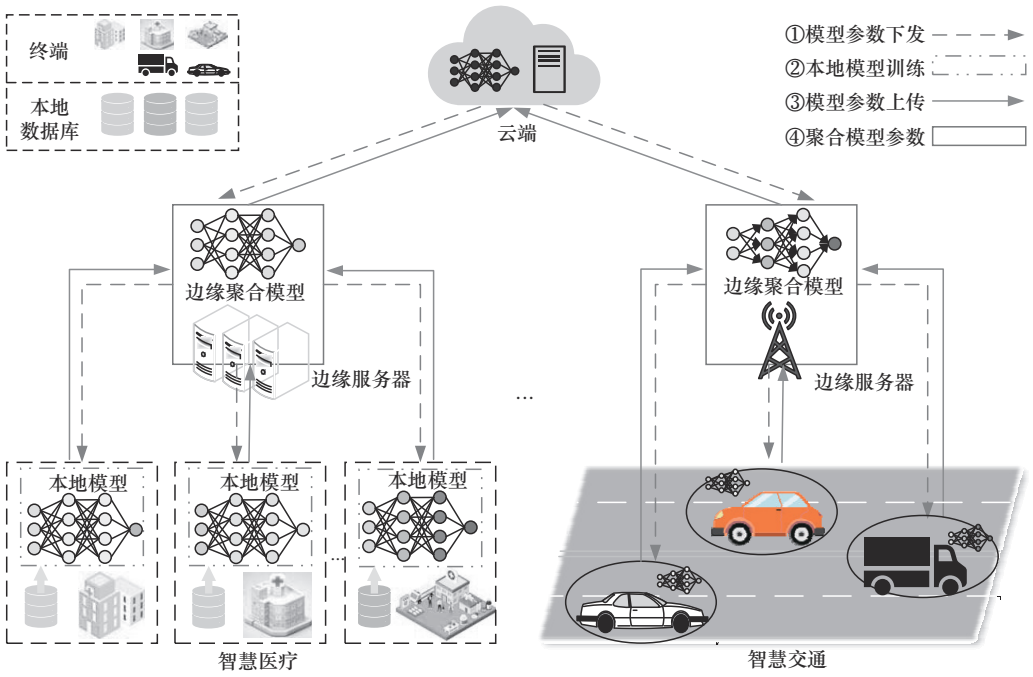


图1　面向边缘计算场景的个性化联邦学习

代智能边缘计算的广泛应用。

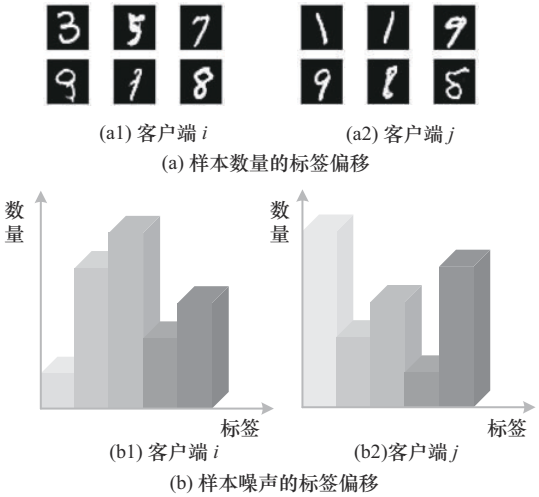
因此，个性化联邦学习逐渐成为联邦学习研究领域的热点方向，受到广泛关注。然而，目前国内针对边缘计算场景下个性化联邦学习的研究仍较为零散，缺乏系统性梳理与深入总结，亟须构建统一的研究框架与发展脉络。基于此，本文对面向边缘计算场景的个性化联邦学习进行了全面综述，旨在为该研究梳理出清晰的研究脉络，以便为研究人员了解或研究个性化联邦学习提供参考。

1　边缘计算场景下的数据异质性分析

在边缘计算场景下，不同边缘设备由于部署位置、硬件能力和应用任务的差异，往往会采集到分布各异的本地数据，主要表现为标签分布、特征分布、数据量及数据质量不均衡，严重影响模型的性能[8]。本节从分布的角度将数据异质性分为标签偏移、特征偏移、质量偏移和数量偏移，具体如下。

1) 标签偏移

标签偏移是指各边缘设备数据的标签分布存在差异，即存在$i \neq j$，使$P_i(y) \neq P_j(y)$。标签偏移通常表现为基于数量的标签偏移和基于分布的标签偏移[9]。前者体现在各边缘设备的本地数据集中数据类别显著不同，如一些边缘设备含有较多数据类别，另一些含有较少数据类别，即假设存在标签空间$y=\{y_1,y_1,\cdots,y_C\}$，设备i和j的标签空间y_i和y_j存在差异，从而影响模型的整体学习效率和性能。后者则是同一类别数据的分布不均匀，即$P_i(x|y)=P_j(x|y)$，如图2所示。



(a1) 客户端 i　(a2) 客户端 j

(a) 样本数量的标签偏移

(b1) 客户端 i　(b2)客户端 j

(b) 样本噪声的标签偏移

图2　标签偏移

2) 特征偏移

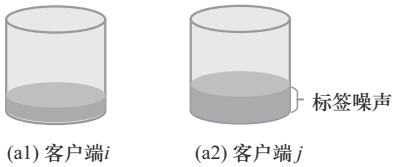
特征偏移意味着标签分布一致，但特征分布可能不同，即$P_i(y|x)=P_j(y|x)$，$P_i(x)\neq P_j(x)$，如图3所示。以手写数字识别为例，同一字符，不同书写者书写的样式、粗细、倾斜度和字体大小等方面可能存在巨大差异。这种特征的多样性导致模型面对来自不同分布的数据时，可能需要更复杂的适应性调整来保持识别准确性。

(a) 客户端i　(b) 客户端j

图3　特征偏移

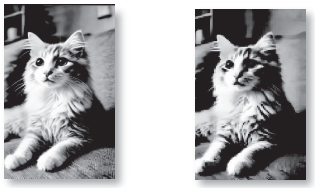
3) 质量偏移

质量偏移是指边缘设备所收集的数据集质量参差不齐，可能持有不同比例的噪声数据[10]，包括标签噪声偏移和样本噪声偏移，如图4所示。标签噪声偏移指本地数据中噪声标签的比例不同，设每个节点设备k上的数据分布为$D_k=\{(x_i,y_i)\}_{i=1}^{n_i}$，其中$y_i$可能受标签噪声的干扰。本文将标签噪声建模为条件概率分布的扰动，即存在某种转移矩阵$\boldsymbol{T}_k\in R^{C\times C}$，使真实标签$y$与观测标签$\tilde{y}$满足$P(\tilde{y}=j|y=i)=T_k(i,j)$，转移矩阵差异反映标签噪声偏移的差异。而样本噪声偏移则指数据收集过程中的样本噪声差异，即存在扰动$\delta_k\sim\mathcal{N}(0,\varepsilon_k)$，使观测样本$\tilde{x}=x+\delta_k$，其中方差$\varepsilon_k$在不同设备之间不一致。不同边缘设备的数据异质性使模型训练更加复杂和不确定。



(a1) 客户端i　(a2) 客户端j

(a) 标签噪声偏移



(b1) 客户端i　(b2) 客户端j

(b) 样本噪声偏移

图4　质量偏移

4) 数量偏移

数量偏移是指各边缘设备拥有的数据量不均衡，某些节点数据量远大于其他节点，即 $D_i \gg D_j$，如长尾分布式数据[11]，如图 5 所示。数量偏移会导致全局模型的训练偏向于数据量较大的边缘侧，削弱了小数据量边缘设备的适应能力，从而影响模型的公平性。在更极端情况下，一些边缘设备甚至存在数据稀缺的问题[12]，这对 FL 又提出了新的要求。

(a) 客户端 i　　(b) 客户端 j

图 5　数量偏移

5) 多重偏移

在理想状态下，数据异质性根据其特点可划分为标签、特征、质量和数量偏移。然而，在现实世界中，许多 Non-IID 数据包含双重甚至多重偏移[8]。以智慧医疗场景为例，不同医疗机构其等级、规模、资源配置等方面存在显著差异，导致其本地数据在多个维度上呈现出高度异质性。首先，受医疗机构等级和规模限制，各机构采集到的样本数量存在明显差异。其次，不同医疗机构诊疗重点不同，造成标签分布存在差异，表现为标签偏移。再次，由于采集设备、成像参数和检测流程的不一致，各机构本地数据存在明显的特征偏移。此外，设备精度、人工标注标准等方面的差异也会引入偏移问题。综上，医疗机构的数据存在包括标签、特征、数量及质量偏移的多重偏移。现有研究表明，双重甚至多重偏移对模型性能具有重大影响[13]。Xu 等[14]针对标签及数量双重偏移问题进行了研究。针对标签偏移问题，基于客户端的局部损失和 Jensen-Shannon 散度构建局部图，并在此基础上选择相似的客户端进行聚类。针对数量偏移问题，基于样本数量进行客户端选择，弥补样本数量偏差。然而，样本数量较少的客户端会被长期忽略。到目前为止，有关双重甚至多重偏移的研究仍非常有限，未来需要更复杂的数据异质性案例以及更深入的研究。

2　面向边缘计算场景的个性化联邦学习方法体系

部署在边缘侧的终端设备由于其所处地理位置不同、用户行为模式各异，所采集的数据分布存在巨大差异，进而对联邦学习模型的收敛性与跨节点泛化能力构成挑战。为了解决边缘计算场景下的数据异质性问题，近年来许多个性化联邦学习方法被提出[15]。本节从数据层面、客户端模型优化层面、服务器聚合优化层面、全局架构优化层面以及结合大模型的方法等几个方面总结和分析面向边缘计算场景的个性化联邦学习方法研究。

2.1　基于数据的个性化联邦学习方法

2.1.1　基于数据增强的方法

在边缘计算场景中，由于不同边缘节点所采集的数据具有显著异质性，联邦学习面临模型收敛缓慢与性能不稳等问题。为缓解这一问题，引入数据增强能够在客户端生成符合目标分布的样本，从而提高数据的统计同质性。典型方法包括生成对抗网络（GAN, generative adversarial network），Maliakel 等[16]针对 FL 中的数据类别缺失问题，利用 GAN 捕获数据分布并生成与现实世界数据非常相似的合成数据，以弥补本地数据集中的数据类别缺失问题。针对标签偏移问题，李志鹏等[17]提出了一种基于数据生成的类别均衡联邦学习方法。该方法包括类别均衡采样器和数据生成器：类别均衡采样器对客户端数据量不足的类别进行高概率采样；数据生成器生成虚拟数据以补充各客户端的数据类别。上述方法通过数据生成实现了客户端标签分布的初步均衡，然而却忽略了数据安全问题。为此，汤凌韬等[18]利用 GAN 生成虚拟样本，并通过梯度剪裁和添加噪声保护数据隐私。针对特征偏移问题，Yan 等[19]提出了一种轻量级的数据增强方法，在训练阶段通过随机选取全局统计信息进行数据归一化。

在数据层面，上述方法从底层解决数据异质性问题，但现有研究多聚焦于合成方法本身的设计，忽略了边缘节点的计算、通信受限等现实情况。另外，数据生成所导致的隐私泄露问题也需得到妥善解决。除此之外，如何防止对局部数据过度修改，导致客户端特有的信息丢失。如何保证合成数据的质量以及如何弥补数据生成带来的额外计算成本也是亟待解决的重要问题。

2.1.2 基于数据共享的方法

在边缘计算场景中，通过数据共享策略，在客户端之间共享部分公共数据或在全局范围内构建辅助数据集，能够减少数据分布差异对模型训练的负面影响。基于此思路，刘吉强等[20]将客户端划分为不同层级，并通过共享数据集来增强全局模型对Non-IID数据的适应能力，同时利用梯度补偿方法对不同层级的客户端模型进行调整，以降低模型训练中的偏差。此外，张红艳等[21]提出了通过部分数据共享来减少客户端之间的数据异质性，显著提升了全局模型的泛化能力和收敛速度。

尽管数据共享在技术实现上展现出了一定潜力，其应用仍面临隐私泄露风险。首先，全局共享数据集的构建依赖对整体数据分布的了解，而这恰恰违背了联邦学习“数据不可见”的初衷，也容易引发客户端数据隐私泄露风险。因此，此类方法研究有限且在隐私敏感场景下的适用性受到较大限制。

2.1.3 基于客户端选择的方法

面对边缘计算场景中终端设备算力有限、数据分布不均等挑战，通过精确选择参与训练的客户端，有助于缓解系统及数据异质性对模型训练的负面影响，从而提升全局模型表现。客户端选择的方法主要分为基于数据的选择和基于资源的选择[22]两类。

前者通过评估客户端本地数据的特征，如数据量、数据分布和损失等，选择对全局模型贡献较大的客户端。例如，Zou等[23]提出了一种基于信息价值（VoI, value of information）的选择方法，该方法通过强化学习估计每个客户端对全局模型的贡献度，并利用贪心算法选择VoI最高的客户端，以最大化全局模型的训练效果。Li等[24]提出了FedSAE方法，该方法在每一轮训练中自适应地选择局部训练损失较大的客户端，以加速模型收敛。

基于资源的选择重点考虑客户端的计算能力、通信带宽和能量消耗等系统资源，以优化训练时间和系统稳定性。例如，Lu等[25]提出了一种基于拍卖机制的集群联邦学习方法，首先利用均值漂移聚类算法对客户端进行分类，然后在每个集群内采用竞价拍卖机制进行选择。Chai等[26]提出了一种基于分层的方法，根据训练绩效将客户端划分为不同的层。该方法通过优化准确率和训练时间，自适应地在每轮训练中从同一层中选择参与训练的客户端。

数据驱动与资源驱动的客户端选择方法在选择参与训练的客户端时，更倾向于选择具备丰富本地数据或强大计算能力的终端参与联邦训练，导致资源受限或数据稀缺的客户端长期被边缘化，从而引发了训练过程中的公平性问题。这种选择机制在无意中强化了模型对特定数据分布的依赖，削弱了其在非理想环境中的泛化能力。此外，现有方法普遍缺乏对客户端动态接入和数据分布时变性的适应性建模，难以在复杂、多变的边缘计算环境中保障模型的鲁棒性。为应对上述挑战，未来需突破当前资源/数据导向的选择标准，引入长期贡献度、度量机制或博弈论机制，实现对“弱势客户端”的激励与保护。也可设计结合时间衰减和代表性回溯机制的动态调度算法，实现资源受限终端的周期性纳入训练。针对客户端动态接入和数据分布时变性问题，可引入时序建模或元学习框架，使模型具备对新节点的适应能力。基于数据的个性化联邦学习方法及其效果对比分别如表1和表2所示，其中，计算和通信开销相对于FedAvg进行对比，≈表示相当或开销可忽略不计，↑表示略有增加，↑↑表示显著增加。

2.2 基于客户端模型优化的个性化联邦学习方法

2.2.1 基于正则化的模型优化

在边缘计算场景下，由于终端节点间的数据分布高度异质，联邦学习中的局部模型易过拟合本地数据，从而影响全局模型的泛化能力。为缓解这一问题，引入正则化方法可有效约束本地模型的更新幅度，避免本地模型过度偏向本地数据分布。

SCAFFOLD[4]使用方差减少来缓解客户端漂移导致局部和全局模型之间的权重分歧的影响。在此基础上，Cheng等[27]通过引入动量机制优化FedAvg和SCAFFOLD算法，证明动量可以有效减少客户端数据异质性带来的影响。除此之外，Hu等[28]在损失函数中加入类平均特征范数作为正则项，以减少数据异质性导致的本地模型更新方向偏差。然而，上述方法在边缘计算场景下的应用性较差，因为数据不仅存在Non-IID问题，还可能包含标签噪声，进一步影响模型性能。为此，Ji等[29]提出了FedFixer模型，通过置信度正则化和距离正则化2种机制，减少了标签噪声在本地模型更新中的负向累积效应。

表1　基于数据的个性化联邦学习方法对比

方法体系	文献	解决问题	方法	优劣势
基于数据增强的方法	文献[16]	数据缺失	使用生成对抗网络生成缺失数据	优势：有效补充缺失数据 劣势：GAN 训练成本较高
	文献[17]	数据异质场景下标签偏移	基于数据生成技术，通过合成数据样本来均衡标签分布	优势：能够减少类别不均衡对模型的影响 劣势：生成数据质量影响最终模型效果
	文献[18]	数据异质性	结合 GAN 和差分隐私技术，在保护隐私安全的条件下生成数据	优势：减小了隐私泄露风险 劣势：生成数据的复杂性和可用性还有提升空间
	文献[19]	特征偏移	轻量级的数据增强技术	优势：轻量级数据增强策略的计算成本较低 劣势：不适用于极端 Non-IID 环境
基于数据共享的方法	文献[20]	数据异质性	共享数据集并引入梯度补偿以优化联邦学习训练过程	优势：有效抑制模型更新偏移问题 劣势：共享数据可能带来隐私泄露风险
	文献[21]	数据异质性	结合数据共享，并优化模型参数聚合策略	优势：提高联邦学习在数据异质环境下的适应性 劣势：有隐私泄露风险
基于客户端选择的方法	文献[23]	Non-IID 数据	通过 VoI 评估选择高质量客户端	优势：提高模型质量，选择最优客户端 劣势：信息价值评估成本较大，计算开销较高
	文献[24]	异构系统环境	设计自适应联邦学习框架优化客户端选择策略	优势：提高异构系统中的联邦学习适应性 劣势：系统适配性需进一步验证
	文献[25]	数据异质性	采用竞价机制优化客户端选择	优势：能够高效利用有限计算资源 劣势：竞价机制带来额外的计算开销
	文献[26]	数据异质性	通过训练绩效分层选择客户端	优势：支持多层聚合 劣势：层次划分策略有待优化

表2　基于数据的个性化联邦学习方法效果对比

方法体系	文献	数据集	准确率	计算开销	通信开销	收敛速度	隐私保护强度
基于数据增强的方法	文献[16]	Adult Intrusion Creditcard Bank Albert	52.00% 64.00% 71.00% 78.00% 93.00%	↑	↑	快	弱
	文献[17]	CIFAR-10 CIFAR-100 CINIC-10	51.02% 47.03% 43.43%	↑	↑	快	无
	文献[18]	MNIST FMNIST	85.99% 75.54%	↑↑	↑	快	强
	文献[19]	Office-Caltech-10 DomainNet	73.38% 45.01%	↑	≈	中	无
基于数据共享的方法	文献[20]	MNIST CIFAR-10	92.00% 64.00%	≈	≈	中	无
	文献[21]	EMNIST CIFAR-10	72.89% 71.04%	≈	≈	中	无
基于客户端选择的方法	文献[23]	MNIST FMNIST CIFAR-10 STL-10	95.60% 75.72% 58.37% 53.30%	↑	↑	中	无
	文献[24]	—	—	↑	↑	中	无
	文献[25]	FEMNIST MNIST	77.80% 89.40%	↑↑	↑	快	无
	文献[26]	—	—	↑	≈	快	无

综上，正则化方法在一定程度上缓解了数据异质性带来的模型更新漂移。然而仍存在局限性，一方面，现有正则化策略普遍建立在全局一致性假设之上，过度依赖正则化机制容易导致局部特征学习能力降低，特别是在存在明显领域偏移或任务差异的情况下，模型逐步收敛到对多数客户端有利但对少数客户端不利，从而降低模型整体的泛化能力与个性化水平；另一方面，现有方法大多采用固定或经验设定的超参数，未来应进一步研究对客户端数据分布、训练动态等因素的自适应调节方法，提高模型在不同数据异质性水平下的稳定性。

2.2.2 基于元学习的模型优化

受限于终端设备的计算能力和本地数据规模，模型训练常面临样本不足与分布差异显著的问题。元学习方法凭借其在低资源条件下的快速适应与良好泛化能力，能够有效提升边缘节点个性化模型的性能，增强其对本地数据分布的适应性。因此，研究人员提出了一种名为Per-FedAvg的模型[30]，该模型是建立在模型无关元学习（MAML, model-agnostic meta-learning）之上的FedAvg的变形。在此基础上，Dinh等[31]对Per-FedAvg模型进行了扩展，提出了一种使用Moreau Envelopes的联邦元学习方法。高雨佳等[32]结合注意力机制和元学习提出了注意力增强元学习网络，学习客户端之间的相似性，有效提高模型的个性化精度，但由于注意力模块引入了额外参数量与特征计算开销，在设备资源极其受限时仍存在部署瓶颈。与此同时，针对物联网环境下的健康监测等高异质性场景，Jia等[33]通过联合建模元学习与联邦学习框架，有效提升了在小样本、高个性化需求下的学习效果，进一步验证了元学习策略在边缘异构环境中的适用性与优势。

综上所述，元学习方法通过提高模型的快速适应能力，在处理边缘计算场景下的数据异质性和个性化需求方面展现出巨大的潜力。现有的元学习方法大多依赖于假设客户端之间的数据异质性相对固定，但在实际应用中，客户端数据分布可能会发生动态变化，这对模型的适应性提出了更高要求。

2.2.3 基于迁移学习的模型优化

近年来，迁移学习在联邦学习中的应用受到广泛关注，尤其在边缘计算场景中，通过在边缘节点间迁移共享知识，有助于提升模型对本地数据的适应性，从而增强联邦学习系统在边缘侧的稳定性与鲁棒性[34]。

Zhang等[35]提出了基于参数化知识迁移的个性化联邦学习方法，该方法允许客户端在模型更新过程中利用来自全局模型或其他客户端的知识，增强个性化模型的泛化能力。Xu等[36]提出了基于自适应群体个性化的联邦迁移学习方法。该方法首先对客户端进行聚类，以形成数据分布相似的集群，并在群组内部进行知识迁移，以提升个性化模型的性能。同时采用自适应策略动态调整群组划分，以应对数据分布的动态变化，进一步提高模型的稳定性。

针对图像分割任务中的数据异质性问题，Ma等[37]引入了风格迁移技术，以减少数据风格的分布差异，使不同客户端的特征表达更加一致，从而提升PFL在计算机视觉任务中的应用效果。

综上，结合迁移学习的个性化联邦学习方法能够有效提升联邦学习模型的个性化水平。然而，在极端Non-IID数据场景下的鲁棒性和计算开销仍然是一项挑战。未来研究可聚焦于开发鲁棒性更强的迁移策略，以应对复杂度更高和形式多变的数据异质性，并进一步探索模型轻量化技术以降低计算成本。

2.2.4 基于多任务学习的模型优化

基于多任务学习的模型优化方法通过在训练过程中建模边缘设备的任务关联性，能够有效提升模型在数据异质场景下的稳定性与个性化性能，从而增强联邦学习在边缘计算场景中的实用性与鲁棒性。为此，Jia等[38]研究了一种基于局部参数共享的异构联邦多任务学习方法。该方法采用局部参数共享机制，在全局聚合过程中仅共享任务无关参数，而任务相关参数则由各客户端本地优化，以实现个性化与泛化能力的平衡。

多任务学习优化策略能够有效提升个性化联邦学习的适应性，特别是在数据异质性强、任务需求多样的场景下，为个性化联邦学习提供了新的优化思路。基于客户端模型优化的个性化联邦学习方法及其效果对比分别如表3和表4所示。

2.3 基于服务器聚合优化的个性化联邦学习方法

2.3.1 基于客户端聚类的方法

考虑到终端设备分布广泛且数据来源高度异构，数据异质性成为制约个性化联邦学习模型训练效率与泛化性能的关键因素。为提升联邦学习在异构环境下的适应能力，近年来研究者提出了多种优

表3　基于客户端模型优化的个性化联邦学习方法对比

方法体系	文献	解决问题	方法	优劣势
基于正则化的模型优化	文献[27]	数据异质性	引入动量机制优化FedAvg和SCAFFOLD	优势：有效提高模型稳定性和收敛性 劣势：在数据分布极度偏差时表现不佳
	文献[28]	数据异质性	引入特征范数正则化	优势：在数据不均衡与分布偏移场景下提升模型鲁棒性 劣势：正则化参数需要根据具体任务进行调整
	文献[29]	标签噪声	引入置信度正则化和距离正则化	优势：有效抑制噪声样本对全局模型扰动 劣势：噪声建模依赖先验分布假设，实际标签噪声复杂性难以精准捕捉
基于元学习的模型优化	文献[30]	数据分布不一致	结合元学习优化个性化模型	优势：有效提高模型泛化能力 劣势：计算成本较高，收敛速度受影响
	文献[31]	数据异质性	使用Moreau Envelope作为客户正则化损失函数	优势：提升模型的稳定性，减少局部最优陷阱 劣势：收敛速度依赖初始设置
	文献[32]	数据异质性问题及隐私性	通过注意力增强元学习网络学习客户端之间的协同	优势：模型性能良好，并通过渐进式训练弥补训练元学习网络带来的计算开销 劣势：服务器和客户端之间的通信成本有待降低
基于迁移学习的模型优化	文献[35]	如何通过参数化知识迁移提升个性化联邦学习的训练效率	提出参数化知识迁移方法，在个性化联邦学习中共享知识	优势：有效提升模型泛化能力 劣势：参数迁移可能导致某些客户端过拟合
	文献[36]	如何自适应地进行群体个性化以优化联邦相互迁移学习	采用自适应群体个性化方法，以增强联邦相互迁移学习	优势：优化个性化联邦学习的协同训练，提高个体和群体模型效果 劣势：个性化程度较高的任务影响整体训练稳定性
	文献[37]	图像分割任务中的Non-IID数据	采用联邦风格迁移策略，使不同客户端的图像风格更加一致	优势：使图像特征更加一致，提升模型性能 劣势：对图像风格特征提取准确性依赖较高
基于多任务学习的模型优化	文献[38]	边缘设备资源受限、多任务部署和数据异质性	利用迁移学习，通过将本地模型划分为可共享的编码器和任务特定的预测器	优势：有效提高模型的泛化性能和计算效率 劣势：局部参数共享导致不同任务之间的信息干扰

化策略。其中，基于客户端聚类的方法旨在根据客户端数据分布的相似性对其进行分组，从而提高模型聚合的效率和性能。

许多研究人员通过客户端数据的不同层面进行聚类。例如，Diao等[39]根据客户端的标签分布对其进行分组，并在每个集群内协同训练模型。除此之外，朱素霞等[40]提出了一种基于相似度加速的自适应聚类联邦学习算法，基于客户端本地更新的几何特性和客户端训练时的正向反馈进行聚类。具体而言，首先基于本地模型的更新向量进行相似度计算并排序，然后在相似度序列中搜寻所有客户端成员，如果性能超过预设的正项激励阈值，即满足式(1)，并将该客户端划分到当前聚类中。相同簇中的客户端协同实现聚类联邦学习，从而提升模型性能。

$$\sum_{i=1}^{N}\left[\mathrm{eval}_{\mathrm{glo}}(i)-\mathrm{eval}(i)\right]\geqslant\beta \tag{1}$$

其中，$\mathrm{eval}(i)$表示客户端i本地训练后的准确率，$\mathrm{eval}_{\mathrm{glo}}(i)$表示通过联邦学习训练后获得的聚合模型在客户端本地测试集上的准确率。

Vahidian等[41]提出了一种基于主角度分析的聚类方法，该方法通过分析客户端数据子空间之间的主角度来有效地识别客户端之间的相似性。此外，也有一些聚类方法在训练开始时设置固定数量的集群。例如，Ghosh等[42]设置了K个集群，每个客户端被分配到K个集群中的一个，条件是该集群的全局模型在该客户端数据上的损失值最低。

综上，通过在联邦学习过程中引入基于相似度的客户端聚类，能够在一定程度上缓解数据异质性对模型优化产生的负面影响。现有方法主要通过梯度空间相似性、模型参数距离、数据分布统计量或表示空间投影等不同层次的相似性度量来划分客户端子群体，使簇内客户端进行聚合，从而提升模型在本地数据上的性能。传统相似性度量方法，如欧

表4 基于客户端模型优化的个性化联邦学习方法效果对比

方法体系	文献	数据集	准确率	计算开销	通信开销	收敛速度	隐私保护强度
基于正则化的模型优化	文献[27]	MNIST	90.89%	≈	≈	中	无
	文献[28]	CIFAR-10 MNIST FEMNIST	99.31% 99.43% 99.41%	↑	≈	快	无
	文献[29]	MNIST CIFAR-10	96.00% 59.01%	↑	≈	中	无
基于元学习的模型优化	文献[30]	FMNIST CIFAR100 Tiny-ImageNet	99.18% 56.80% 28.06%	↑	≈	中	无
	文献[31]	FMNIST CIFAR100 Tiny-ImageNet	99.35% 58.20% 27.71%	↑↑	↑	快	无
	文献[32]	V-MNIST W&A China	84.66% 84.16%	↑	↑	中	无
基于迁移学习的模型优化	文献[35]	EMNIST Fashion_MNIST CIFAR-10	84.65% 75.60% 43.82%	↑↑	≈	中	弱
	文献[36]	—	—	↑↑	↑	中	无
	文献[37]	Medical image Face image	92.33% 85.60%	↑↑	↑↑	快	无
基于多任务学习的模型优化	文献[38]	MNIST FashionMNIST SVHN CIFAR-10 CIFAR-100	96.67% 83.39% 88.00% 71.15% 47.70%	≈	≈	快	无

氏距离、余弦相似度等，无法充分捕捉复杂非线性特征分布差异，尤其在高维梯度空间或多模态数据场景下。未来可考虑引入核方法、流形学习或基于深度特征的表示学习，提升对数据分布的感知能力。此外，聚类过程中的隐私保护问题也需高度关注。现有大部分聚类方法需要客户端暴露模型梯度、数据分布特征甚至部分样本表示，存在被重建攻击或成员推理攻击风险。未来可考虑引入差分隐私聚类、安全多方计算或同态加密等隐私保护机制，实现隐私保护下的客户端聚类。

2.3.2 基于聚合策略优化的方法

聚合策略优化主要集中在如何通过服务器端的聚合过程优化来解决边缘计算中数据异质性带来的问题。通过优化聚合策略，可以更合理地调整全局模型聚合方式，解决数据异质性问题带来的负面影响，使全局模型既能保持一定的泛化能力，又能有效适应不同边缘设备的个性化需求。

因此，Tang等[43]基于客户端数据集质量评估，动态调整加权聚合策略。Zhang等[44]提出了FedALA模型，核心是自适应本地聚合模块，能够根据每个客户端的个性化需求，选择性地聚合全局模型和本地模型，以提高个性化性能。Jia等[45]提出了FedAHA模型，包含结构感知聚合和凸语义校准两阶段。前者对齐提取器，从而增强全局模型的对象感知能力，后者利用凸函数理论来平均语义特征，增强全局模型的本地化精度。

除此之外，还有部分研究着重于分层聚合策略。Ma等[46]通过更新聚合权重矩阵实现层粒度的参数聚合，并利用客户端的相似性实现模型个性化。

尽管上述多个方法有效减少了通信开销，但依赖动态加权和自适应聚合策略的算法仍然需要在不同客户端之间进行复杂的交互，增加了计算负担。基于服务器聚合优化的个性化联邦学习方法及其效果对比分别如表5和表6所示。

2.4 基于全局架构优化的个性化联邦学习方法

2.4.1 基于知识蒸馏的架构优化

在边缘计算场景中，终端设备其计算能力、

表5　基于服务器聚合优化的个性化联邦学习方法对比

方法体系	文献	解决问题	方法	优劣势
基于客户端聚类的方法	文献[39]	标签偏移	基于标签分布的相似性进行客户端聚类	优势：在标签偏移情况下模型性能表现优异 劣势：访问本地标签分布有隐私泄露风险
	文献[40]	数据异质性	基于客户端几何特征和正向反馈实现聚类	优势：收敛速度快 劣势：依赖于相似度计算，有隐私泄露风险
	文献[41]	数据异质性	采用主角度分析度量客户端数据子空间相似性，实现高效聚类	优势：有效减少数据异质性对模型的影响 劣势：容易受计算资源限制
	文献[42]	数据异质性	设施固定数量的集群进行迭代聚类	优势：有效缓解大规模系统异构性聚合收敛难题 劣势：聚类更新需频繁通信，增加带宽负担
基于聚合策略优化的方法	文献[43]	数据异质性	采用适应性加权聚合方法，根据数据质量动态调整权重	优势：有效缓解极端客户端间样本量失衡现象 劣势：聚合权重计算复杂度随客户端数量上升
	文献[44]	Non-IID数据	提出本地自适应聚合模块	优势：提高了模型个性化水平 劣势：训练效率较低
	文献[45]	Non-IID数据	通过结构感知的聚合对齐提取器，增强全局模型的对象感知能力，利用凸函数理论来平均语义特征	优势：提升了全局模型的感知能力 劣势：没有考虑隐私风险
	文献[46]	数据异质性	分层参数聚合	优势：通过细粒度的聚合提高了模型的性能 劣势：通信成本有待降低

表6　基于服务器聚合优化的个性化联邦学习方法效果对比

方法体系	文献	数据集	准确率	计算开销	通信开销	收敛速度	隐私保护强度
基于客户端聚类的方法	文献[39]	CIFAR10 SVHN FMNIST	57.70% 87.50% 87.70%	↑	↑	中	无
	文献[40]	MNIST EMNIST	91.90% 69.70%	↑↑	≈	快	无
	文献[41]	FMNIST CIFAR-10 CIFAR-100 SVHN	97.54% 89.30% 73.10% 95.77%	↑↑	↑	中	无
	文献[42]	Rotated MNIST Rotated CIFAR	94.20% 81.51%	↑	↑	中	无
基于聚合策略优化的方法	文献[43]	CMNIST	80.00%	↑	≈	中	无
	文献[44]	FMNIST CIFAR100 Tiny-ImageNet	99.57% 67.83% 40.31%	↑	≈	快	无
	文献[45]	VOC 2007 NWPU VHR-10 BCCD	74.72% 92.77% 87.82%	≈	≈	中	无
	文献[46]	MNIST FashionMNIST CIFAR-10 CIFAR-100	94.11% 95.47% 60.02% 46.47%	↑↑	≈	中	无

模型架构及本地数据分布存在差异。随着知识蒸馏（KD, knowledge distillation）[47]技术的发展，其逐渐应用于面向边缘计算场景的联邦学习。基于KD的联邦学习能够为客户端提供更大程度的灵活性，以适应各终端设备的模型架构及数据分布差异。

Lu 等[48]针对标签偏移问题提出了FedLMD模型。该模型在训练过程中，将标签划分为多数类和

少数类，本地模型从本地数据学习多数类标签知识，而服务器端则通过标签掩码蒸馏引导模型学习少数类标签知识，以降低模型更新的偏移。设第k个本地模型的输出为p_k，全局模型的输出为p_g，则损失可表示为

$$\mathcal{L}_k = \mathcal{L}_{\mathrm{CE}}(p_k,1_y) + \beta\mathcal{L}_{\mathrm{LMD}}(p'_k,p'_g) \tag{2}$$

其中，$\mathcal{L}_{\mathrm{CE}}$为学习多数类标签知识的交叉熵损失，标签掩蔽蒸馏损失$\mathcal{L}_{\mathrm{LMD}}$为KL（Kullback-Leibler）散度，$\beta$为控制蒸馏损失的超参数。

Yao等[49]提出了FedGKD模型。该模型通过融合历史全局模型的知识指导本地训练，以减少模型更新方向上的偏移。FedGKD采用自蒸馏策略，使本地模型能够更稳定地学习来自过去全局模型的知识，而不需要额外的代理数据。模型的优化目标可表示为

$$\min_{\boldsymbol{w}} F_k(\boldsymbol{w}) + \frac{\gamma}{2n_k}\sum_{i=1}^{n_k}\mathrm{KL}(h_k(\boldsymbol{w}_t,x_{ki})\|h_k(\boldsymbol{w},x_{ki})) \tag{3}$$

其中，$\boldsymbol{w}$表示本地模型，$\boldsymbol{w}_t$表示第t轮的全局模型，γ表示控制蒸馏损失的超参数，n_k表示客户端k的训练样本数，$h_k()$函数计算式为

$$h(\boldsymbol{w},x) = \frac{\exp\left(\frac{z(\boldsymbol{w},x)}{\tau}\right)}{\sum_d \exp\left(\frac{z(\boldsymbol{w},x)}{\tau}\right)} \tag{4}$$

其中，τ为温度系数。

该方法在不需要代理数据的条件下能有效缓解模型漂移与灾难性遗忘问题，但在长期迭代过程中仍可能受限于历史模型累积噪声。

此外，Zhang等[50]提出了一种基于GAN的数据无关知识蒸馏方法，该方法在服务器端部署生成，并在客户端复用本地模型作为判别器，以生成共享的特征表示，从而实现高效的知识蒸馏。Zhu等[51]提出了一个无数据的蒸馏框架FedGen。在服务器中训练生成模型并广播给客户端，然后每个客户端使用学习到的知识作为归纳偏差在特征空间上生成增强表示，以调节其局部模型。

针对知识蒸馏在FL中的超参数优化问题，Alballa等[52]通过实验分析了温度参数权重参数、蒸馏数据集等因素对知识传递的影响。该研究表明，不同客户端的最佳超参数组合可能存在显著差异，合理的超参数调优可以在平均情况下提升5倍的知识传递效果。该研究为优化联邦知识蒸馏提供了理论和实验支持，并提出了一种动态超参数调优方法，以提高联邦学习的收敛速度和精度。

在基于知识蒸馏的个性化联邦学习方法中，知识转移的有效性不仅取决于模型参数，还取决于模型架构。如果大型教师模型和小型学生模型之间存在巨大的容量差距，学生模型可能很难很好地学习，因此如何找到教师模型和学生模型之间的最佳平衡是亟待解决的问题。

2.4.2 基于参数解耦的架构优化

针对边缘计算场景下终端设备面临数据分布异构和计算资源受限等挑战，参数解耦通过将个性化参数与全局参数解耦来实现个性化联邦学习，提升模型在边缘设备的适应能力。

倪宣明等[53]将模型参数划分为全局参数与个性化参数，在提取全局知识的同时，实现个性化模型构建。此外，该方法采用弹性权重巩固来保留重要的全局共享参数，从而增强模型的适应能力。Wu等[54]采用参数加法分解，将每个模型参数分解为全局参数和个性化参数的和，并采用低秩矩阵约束来减少计算开销。Gao等[55]通过正交投影技术，实现全局参数与个性化参数的解耦。该方法采用双特征提取器，确保全局参数的共享，同时允许个性化参数在本地保持独立。针对时间序列分类任务中的空间-时间特征异构性问题，Wu等[56]结合多视角正交训练，在训练阶段通过正交投影解耦全局特征和个性化特征，并在测试阶段使用基于原型的预测进行自适应推理。

综上，参数解耦方法在面向边缘计算场景的个性化联邦学习中已取得了良好的效果，私有参数和全局参数的分类能够控制泛化和个性化性能之间的平衡，但确定最佳的解耦策略仍是一项挑战。基于全局架构优化的个性化联邦学习方法及其效果对比分别如表7和表8所示。

2.5 基于大模型的个性化联邦学习方法

大模型凭借其强大的特征提取能力、知识迁移能力以及对复杂数据的建模能力，在自然语言处理及计算机视觉等多个领域展现出显著优势，也逐渐应用于联邦学习研究。在个性化联邦学习中，由于各节点所持数据存在高度异质性，大模型具备的强表征能力使其能够更精准地捕捉客户端间数据的差异性与潜在的共性结构，从而实现更细粒度的模型定制与更强的泛化能力，满足多样化用户需求。

表7　基于全局架构优化的个性化联邦学习方法对比

方法体系	文献	解决问题	方法	优劣势
基于知识蒸馏的架构优化	文献[48]	标签偏移	设计标签掩盖蒸馏方法，在全局模型中专注于少数标签的知识	优势：避免传输完整标签，降低隐私泄露风险 劣势：影响少量样本的学习效率
	文献[49]	系统和数据异质性	提出FedGKD模型，利用历史全局知识训练本地模型	优势：不需要访问本地数据，保证隐私安全 劣势：依赖全局历史模型质量
	文献[50]	数据和模型异质	提出数据无关知识蒸馏，通过GAN合成共享特征表示进行模型训练	优势：提升模型准确性且通信开销较低 劣势：生成样本质量直接影响蒸馏效果
	文献[51]	数据异质性	无数据知识蒸馏	优势：在较少的通信轮次下能取得较好的模型效果 劣势：蒸馏误差累积影响模型性能
	文献[52]	数据异质性	分析蒸馏超参数对联邦知识蒸馏性能的影响，并提出优化方案	优势：模型性能较好 劣势：超参数选择和调整过程需要大量实验验证
基于参数解耦的架构优化	文献[53]	数据异质性	通过弹性权重巩固保留全局知识	优势：降低了模型冗余 劣势：持续学习过程需合理设计知识更新与遗忘平衡，存在灾难性遗忘风险
	文献[54]	参数解耦不彻底	采用参数加法解耦，将每个参数分解为全局参数与个性化参数的加和形式	优势：充分捕获全局泛化知识与个性化特征 劣势：加法解耦在数据量有限时可能导致泛化能力不足
	文献[55]	特征偏移	在双特征提取器的结构下使用正交投影来解耦全局特征和个性化特征	优势：提升了特征偏斜情况下的模型性能 劣势：正交约束引入额外计算开销
	文献[56]	时空数据异质性	提出多视图正交训练方法	优势：有效提高训练效率与收敛速度 劣势：多视图协同训练需精确建模视图间关联性

通常来说，基础模型具有广泛的泛化能力，提取基础模型的部分结构并针对特定任务或场景进行再训练成为一种高效的解决方案。Zeng等[57]针对联邦学习中数据异质性引发的偏见问题，提出了FF-DVP框架，以CLIP为基础模型，结合2种去偏模块，包括视觉提示模块和客户端特定知识模块，以保证即使在数据异质环境下，训练出的模型在保持公平性的同时能有效收敛。此外，Shi等[58]设计了一种基于CLIP模型的联邦学习框架，有效缓解了数据异质和长尾数据问题，提升了模型对少数类别的识别能力。Moskvoretskii等[59]针对低资源语言的机器翻译问题，提出了基于个性化联邦优化的MeritOpt方法。以M2M100为基础模型，根据客户端翻译效果动态分配聚合权重，显著提升多语言翻译任务中的公平性与翻译质量。

提示学习作为近年来基础模型应用中的重要范式，已在自然语言处理、计算机视觉等多个领域得到广泛关注。其核心思想在于，通过在模型输入中设计合理的提示，引导预训练大模型在下游任务中更有效地激活已有的知识与能力。pFedPT[60]首次将prompt学习引入联邦学习，在原始数据和提示组成的输入中训练本地大模型，学习提示包含的数据分布信息，使模型具有自适应“微调”的能力，从而提高解决客户端数据异质性等综合能力。Yang等[61]提出了一种高效的客户端特定提示生成方法，在Vit模型的基础上，利用个性化prompt引导模型在各客户端上更好地适应本地数据，实现了低通信代价下的模型个性化。Cui等[62]进一步探讨了在提示学习范式下，个性化与泛化能力之间的权衡，提出联合调和机制，在保证全局模型泛化能力的同时，实现对各客户端个性化需求的自适应调优。

除此之外，多模态学习也逐渐应用于联邦学习，旨在隐私保护与资源受限的约束下，有效融合图像、文本等多模态信息以提升模型泛化与适应能力。Chen等[63]实现了基础模型在视觉−语言多模态下的高效分布式调优。该方法设计了双适配器教师模块，通过冻结全局适配器与本地适配器协同优化，兼顾了客户端特异性知识与客户端无关知识的平衡。同时，引入互助知识蒸馏机制，在提升模型迁移能力的同时有效抑制了过拟合现象。该方法展

表8 基于全局架构优化的个性化联邦学习方法效果对比

方法体系	文献	数据集	准确率	计算开销	通信开销	收敛速度	隐私保护强度
基于知识蒸馏的架构优化	文献[48]	MNIST CIFAR-10 CIFAR-100 CINIC-10	88.48% 60.76% 32.34% 54.13%	↑	≈	快	弱
	文献[49]	CIFAR-10 CIFAR-100 Tiny-ImageNet	73.06% 33.42% 35.72%	↑	≈	快	强
	文献[50]	CIFAR-10 CIFAR-100 CINIC-10	46.89% 37.60% 49.58%	↑	≈	快	无
	文献[51]	MNIST EMNIST	91.30% 68.53%	↑	≈	快	无
	文献[52]	—	—	↑	≈	快	无
基于参数解耦的架构优化	文献[53]	MNIST FEMNIST CIFAR-10	81.28% 71.20% 62.56%	↑	≈	中	无
	文献[54]	CIFAR-10 CIFAR-100 Tiny-ImageNet	69.09% 42.98% 25.55%	↑	≈	快	无
	文献[55]	Office-Caltech-10 DomainNet Digits-Five CIFAR-100	60.60% 37.32% 96.94% 58.00%	↑↑	≈	快	无
	文献[56]	HAR HHAR WISDM Sleep-EDF Epilepsy	93.02% 78.82% 81.19% 93.49% 94.82%	↑↑	↑	快	无

现出了良好的收敛性与可扩展性，为联邦学习场景下多模态大模型的高效适配与应用提供了有力支撑。

然而，大模型通常伴随着高昂的计算与通信成本，在边缘计算场景中，边缘设备往往存在计算、存储与通信资源限制，传统大模型的直接部署面临诸多挑战[64]。为此，如何在有限资源条件下充分释放大模型的潜力，成为当前研究的关键问题。为解决上述问题，亟须对大模型进行压缩以减轻计算、存储与通信负担。目前，关于大模型的压缩技术主要包括模型量化、参数剪枝、知识蒸馏和低秩分解等。模型量化通过将模型中的高精度数值转化为低精度数值表示，大幅减少模型计算开销。Xiao等[65]研究表明，模型量化技术能够有效压缩模型规模并提升推理速度。然而，量化会引起模型性能退化，尤其在极低比特情况下，可进一步引入量化感知训练，在保证精度的条件下降低计算和存储成本。参数剪枝通过去除部分模型参数实现压缩，如Frantar等[66]将参数剪枝视作广义稀疏回归问题，在大规模GPT系列模型达到60%的非结构化稀疏度，实现模型的高效推理。参数剪枝的优势在于可移除不重要参数以实现最大化模型压缩，但硬件条件会限制稀疏运算的加速。知识蒸馏则利用教师−学生模型迁移知识以训练轻量化模型[67]。低秩分解通过矩阵分解技术降低模型参数维度，在保持性能的前提下实现了百亿参数规模模型的高效压缩与快速推理[68]。研究者通常将低秩分解技术与其他技术相结合，包括上述参数剪枝与模型量化技术，实现更有效的模型压缩。

综上所述，大模型强化了边缘计算场景下联邦学习在复杂真实环境中的泛化能力。轻量化技术进一步为大模型在资源受限环境下的部署与推理提供了有效支撑，也为联邦学习场景下的大模型高效本地化适配奠定了基础。基于大模型的个性化联邦学习方法及其效果对比分别如表9和表10所示。

表 9　　基于大模型的个性化联邦学习方法对比

方法体系	文献	解决问题	方法	优劣势
基于大模型的方法	文献[57]	数据异质性	引入公平性损失函数，对不同客户端做偏差校正	优势：提升多客户端间性能公平性 劣势：没有考虑通信和计算资源有限问题
	文献[58]	个性化联邦学习中通信和计算成本高	服务器端生成个性化提示，冻结主干模型参数	优势：不需要微调主干模型，通信开销小 劣势：提示生成器训练需额外设计
	文献[59]	联邦提示学习中泛化与个性化的平衡	联合优化个性化与泛化提示，设计融合机制	优势：同时保持良好的泛化与个性化性能 劣势：融合策略复杂，调参敏感
	文献[60]	数据异质性和长尾分布	利用CLIP特征指导个性化微调	优势：增强模型对少数类和异构数据的适应能力 劣势：依赖CLIP等大模型的表示能力
	文献[61]	低资源语言翻译中联邦个性化优化	根据性能动态分配客户端聚合权重	优势：显著提升低资源语言下的翻译性能 劣势：语言间迁移效果存在差异
	文献[62]	个性化与泛化能力权衡	联合调和机制	优势：兼顾个性化与泛化 劣势：需设计合理的调和权重
	文献[63]	多模态数据异质性	设计双适配器教师和互助知识蒸馏机制	优势：适应视觉-语言多模态任务，兼顾客户端特异性与共性知识 劣势：训练过程需协调多模块优化

表 10　　基于大模型的个性化联邦学习方法效果对比

方法体系	文献	数据集	准确率	计算开销	通信开销	收敛速度	隐私保护强度
基于大模型的方法	文献[57]	CelebA FairFace	90.50% 84.80%	↑ ↑	↑	快	无
	文献[58]	CIFAR-10-LT CIFAR-100-LT	73.37% 37.56%	↑ ↑	↑	快	无
	文献[59]	Inari Sami Skolt Sami South Sami North Sami	52.08% 50.27% 13.26% 38.53%	↑ ↑	↑	中	无
	文献[60]	CIFAR-10 CIFAR-100	74.92% 36.88%	↑ ↑	↑	快	无
	文献[61]	Office-Caltech10 DomainNet	96.81% 71.64%	↑ ↑	↑	快	无
	文献[62]	Office-Caltech10 DomainNet	96.54% 86.76%	↑ ↑	↑ ↑	快	无
	文献[63]	VizWiz COCO Art GQA Abstract	60.99% 63.81% 71.36% 48.65% 60.75%	↑	↑ ↑	快	无

2.6　基于原型学习的个性化联邦学习方法

近年来，基于原型学习的方法被应用于联邦学习。该方法通过抽象化的类别表示代替梯度或模型参数进行传输，增强联邦学习的鲁棒性和可扩展性。

针对数据和模型异质性问题，Tan 等[69]提出了一种原型聚合方法。该方法通过交换类原型来替代梯度更新，使不同模型架构的客户端仍然能够共享知识。Zhang 等[70]提出了一种基于自适应边距增强对比学习的联邦学习方法。该方法通过训练全局可学习的原型，在服务器端利用对比学习增强原型的可分性，同时保持语义一致性。针对原型冗余、原型失败以及原型质量下降等问题，Yan 等[71]采用 SoftPool 机制，并引入拜占庭容错检测聚合算法，以提高原型聚合的安全性和稳定性。针对特征偏移问题，Li 等[72]提出了固定原型约束，提高全局模

型的泛化能力。

综上所述，基于原型学习的方法在个性化联邦学习中展现出显著的优势，能够在数据和模型异质性环境下减少全局模型的优化偏差，提高个性化适应能力，并降低通信成本。但当前方法仍面临原型冗余、原型质量不佳以及动态环境下适应能力不足等挑战，亟须在原型质量及动态原型演化等方面进一步突破。基于原型学习的个性化联邦学习方法及其效果对比如表11和表12所示。

除上述方法外，还有一些方法可用于解决数据异质性问题，如神经架构搜索（NAS, neural architecture search），近年来在个性化联邦学习中引起了广泛关注。NAS能够自动化地探索适合每个客户端的模型架构，提高个性化联邦学习的效率和准确性。

基于此，Yao等[73]提出了一体化个性化联邦神经架构搜索框架，旨在解决联邦学习中的异质性问题。该框架通过NAS，自动化地为每个客户端设计个性化模型架构，并优化其模型权重。该方法能够自适应地调整模型中需要个性化的部分，以优化不同客户端的模型结构并提高其对本地数据分布的适应性。另外，该框架采用强化学习技术动态优化模型架构，使每个客户端在本地模型更新过程中能够根据自身数据的特征进行调整，从而提升个性化联邦学习的准确性和效率。

3　研究展望

1) 数据要素隐私安全机制

随着数据要素在数字经济中的核心地位日益凸显，联邦学习作为“数据可用不可见”理念的重要实现形式，在边缘计算场景中展现出独特优势，已成为保障用户隐私、实现分布式协同训练的关键技术路径。然而，在处理边缘计算场景下数据异质性问题时，部分方法通过上传类别梯度或部分真实数据来提升模型性能，这在无形中加剧了隐私泄露

表11　基于原型学习的个性化联邦学习方法对比

方法体系	文献	解决问题	方法	优劣势
基于原型学习的方法	文献[69]	数据异质性和模型异质性	引入原型聚合机制，通过交换类原型实现跨客户端知识共享	优势：实现模型架构无关的高效聚合，提升异构系统适配性 劣势：初始原型构建过于依赖数据分布
	文献[70]	数据异质性	结合自适应边距增强对比学习提升原型可分性与语义一致性	优势：提高复杂场景下模型稳健性 劣势：对比学习参数调整复杂，模型训练开销较大
	文献[71]	原型冗余、失败与质量退化	采用SoftPool机制减少原型冗余，引入拜占庭容错检测聚合算法提升稳定性	优势：增强对异常原型的适应能力 劣势：需要大量计算资源支撑
	文献[72]	特征偏移	固定原型约束	优势：显著提升类别不平衡场景下的模型性能 劣势：对齐过程依赖分布假设，泛化能力存在局限

表12　基于原型学习的个性化联邦学习方法效果对比

方法体系	文献	数据集	准确率	计算开销	通信开销	收敛速度	隐私保护强度
基于原型学习的方法	文献[69]	FMNIST CIFAR100 Tiny-ImageNet	99.49% 69.18% 36.78%	↑	↑	中	无
	文献[70]	CIFAR-10 CIFAR-100 Flowers102 Tiny-ImageNet	88.15% 46.94% 53.68% 27.37%	↑	↑	快	无
	文献[71]	MNIST FEMNIST CIFAR-10	97.17% 94.53% 79.47%	↑↑	↑	快	无
	文献[72]	CIFAR-10 FMNIST EMNIST	58.50% 83.80% 88.70%	↑	≈	快	无

风险。

目前，主流的隐私保护方法是将经典的机器学习隐私保护技术融入联邦学习中，包括同态加密[74]、秘密共享[75]、安全多方计算[2]等密码学技术，然而，这些密码学技术给联邦学习引入了额外的计算和通信开销，在边缘计算场景设备及通信受限情况下无法达到较好的效果。未来的研究应发展兼具高效性与安全性的轻量化加密机制，具体来说，针对资源受限的边缘终端，通过优化加密算子以及稀疏编码等技术压缩同态加密、秘密共享以及安全多方计算中的计算与存储负载。也应进一步结合优化同态加密、秘密共享以及安全多方计算技术，如文献[2]设计了安全两方计算在客户端本地模型的加密方法，并结合同态哈希和加法秘密共享增强隐私保护。此外，也应从数据采集、本地训练、模型聚合、结果应用等多个环节出发，构建覆盖数据生成−使用−治理全过程的隐私保障体系。

除此之外，差分隐私也被用于联邦学习中的隐私保护，但这类加噪的隐私增强学习通常需要在牺牲模型效用的条件下保护参与方数据隐私安全。因此，如何实现隐私增强学习与个性化模型之间的协同优化，也是当前研究的重点。Noble 等[76]将差分隐私约束纳入 SCAFFOLD 算法，实现隐私增强学习与个性化联邦学习的融合。Wei 等[77]通过改变人工噪声的方差以及动态裁剪阈值实现用户级差分隐私。张少波等[78]通过定义衰减系数动态调整每轮差分隐私噪声的大小，以合理分配隐私噪声大小并提升模型可用性。然而，由于隐私预算与噪声标准差之间成反比的固有限制，以及当前缺乏精细化的裁剪阈值策略，仍可能对模型性能产生不利影响。未来，可进一步强化对不同数据主体、数据类型的区分管理，隐私增强机制可按需动态调整粒度，根据个体用户对隐私的敏感程度，引入个性化差分隐私预算分配策略，也可通过模型结构设计将隐私敏感部分与个性化层解耦，降低隐私保护对个性化建模的干扰。

2) 通信效率

在 FL 系统中，客户端与服务器之间频繁的通信是不可避免的。在个性化联邦学习场景下，需要在全局模型和每个客户端的本地模型之间不断地交换信息与更新。随着联邦学习规模的不断扩大，通信开销成为制约模型训练效率的关键因素之一。特别是在网络、通信和计算资源的限制下，节点掉线和慢节点现象普遍存在，对 FL 系统的鲁棒性提出了严峻挑战。因此，设计一种能够应对这些挑战的鲁棒联邦学习系统显得尤为重要。目前，研究者提出了几种常见的通信优化策略，如梯度压缩和异步模型更新。尽管这些策略在一定程度上缓解了通信瓶颈，但如何在保证个性化效果的同时有效减少通信负担，如何处理节点异构性带来的不平衡计算负载，如何在分布式环境中快速响应网络波动和节点动态变化等，都需要进一步的理论研究和实践探索。因此，未来要对通信信息（如梯度、模型参数）进行压缩，采用低秩分解、知识蒸馏或轻量网络结构，在保证训练精度的前提下降低总体资源开销。除此之外，可进一步引入时间衰减因子以及动态的异步调度等，发展更高效的异步优化策略，以应对客户端掉线或响应时延等问题。

3) 平衡个性化和泛化性能

由于本地数据分布之间的差异，模型的个性化性能和泛化性能难以平衡，一些研究者通过参数解耦，将模型粗粒度地拆分为特征提取器和分类器，通过共享一个组件并个性化另一个组件实现二者平衡[79]。在此基础上，一些研究者更细粒度地在特征提取器内部对部分参数进行划分，以提取同时具备泛化与个性化特征的表示[55]。尽管如此，现有方法在设计上仍不可避免地涉及泛化与个性化性能之间的权衡。如何兼顾泛化与个性化性能成为一个挑战。未来应利用参数解耦进一步优化个性化与泛化的协同策略，充分挖掘和利用泛化和个性化信息。另外，也可以结合博弈论探索泛化和个性化性能之间的平衡。

4) 个性化模型的多任务与跨场景适应性

在个性化联邦学习中，模型训练通常依赖于多个客户端，每个客户端基于其本地数据进行更新。然而，个性化模型往往无法适应多任务和跨场景的复杂需求，尤其在数据非独立同分布且任务目标差异显著的情况下，个性化模型的迁移与泛化效果严重受限。例如，从智能交通场景中的交通流量预测到工业互联网中的异常流量检测[80]，两者在数据以及任务目标等方面存在显著差异，这类跨场景迁移任务不仅对模型的鲁棒性提出挑战，也对其结构的可扩展性和泛化能力提出更高要求。因此，如何提升个性化模型的多任务和跨场景适应性，成为个性化联邦学习中亟待解决的核心问题。

迁移学习在一定程度上可以解决上述问题，然而，当源域与目标域存在显著分布偏移或目标域完全无标签时，传统迁移学习方法容易出现负迁移现象。在此背景下，领域自适应技术被广泛关注，其核心思想是通过对齐源域和目标域的数据分布，使在有标签源域中训练的模型可以直接迁移到没有标签的目标域，且最大程度地避免模型性能下降。其中，无监督域自适应技术，为联邦学习本地数据不共享提供了可行的技术路径。在近期的研究中，Chi等[81]提出了一种协同对抗式训练机制，用于在不共享原始数据的前提下缓解联邦学习系统中的领域偏移问题。这一机制展示出在复杂场景中进行无监督对抗训练的巨大潜力。未来研究可进一步结合神经架构搜索技术，构建适配不同场景的模型，提升个性化模型的跨场景泛化能力。

5) 真实情况下的Non-IID数据

当前，个性化联邦学习研究多聚焦于单一类型的Non-IID数据。然而，在实际应用中，数据分布存在多种偏移的现象。与单一偏移相比，双重偏移甚至多重偏移对模型性能的削弱作用更为显著，对模型的泛化能力构成更大的威胁。多重偏移进一步加剧了数据异质性，使应对Non-IID问题变得更加棘手。目前，涉及双重或多重偏移的Non-IID问题研究较为有限，因此未来有必要深入探索其影响与应对策略。

除此之外，个性化联邦学习实验通常依赖于预设或人工划分的数据集，以模拟特定的Non-IID情境。然而，仅依靠这样的实验环境难以真实反映复杂的现实场景，因此未来应研究更加贴近真实世界的数据分布特征，如智慧医疗中多医疗机构的患者数据，由于其所服务的患者群体、医疗设备、诊疗标注标准以及规模的不同，天然存在着标签、特征、质量以及数量偏移。也应探索更具代表性的多样化数据分布特征，如时间维度上的Non-IID特性[82]，在真实数据的基础上进一步提升PFL算法的适应性和稳健性，并构建更完善的个性化联邦学习研究生态。除此之外，部分基于数据、客户端模型优化、原型学习等方法尤其是基于大模型的方法其计算开销较大，边缘设备的资源异构性会对上述方法产生严重影响。在此情况下，聚合策略优化方法或许是最优解，也可采取模型压缩技术降低计算和通信开销。

4 结束语

在边缘计算场景下，节点间的数据异质性以及个性化需求对联邦学习提出了更高的要求。个性化联邦学习作为应对数据异质性挑战的有效途径，在提升模型收敛性及本地适应性方面展现出显著优势。为了帮助研究者更全面地了解面向边缘计算场景的个性化联邦学习的最新研究进展，系统地梳理了现有个性化联邦学习的研究方案，并分析现有方法的优缺点。另外，针对现有方法的局限性，提出了个性化联邦学习的未来研究方向，为解决边缘计算场景下联邦学习中的数据异质性、个性化需求等问题提供理论支撑和实践指引，进一步推动个性化联邦学习技术的发展以及在自动驾驶、智能制造、智慧城市等领域的应用。

参考文献：

[1] 王义君, 李嘉欣, 闫志颖, 等. 基于深度强化学习的移动边缘计算安全传输策略研究[J]. 通信学报, 2025, 46(4): 272-281.
WANG Y J, LI J X, YAN Z Y, et al. Research on secure transport strategy of mobile edge computing based on deep reinforcement learning[J]. Journal on Communications, 2025, 46(4): 272-281.

[2] 高鸿峰, 黄浩, 田有亮. 基于多方计算的安全拜占庭弹性联邦学习[J]. 通信学报, 2025, 46(2): 108-122.
GAO H F, HUANG H, TIAN Y L. Secure Byzantine resilient federated learning based on multi-party computation[J]. Journal on Communications, 2025, 46(2): 108-122.

[3] 林伟伟, 石方, 曾岚, 等. 联邦学习开源框架综述[J]. 计算机研究与发展, 2023, 60(7): 1551-1580.
LIN W W, SHI F, ZENG L, et al. Survey of federated learning open-source frameworks[J]. Journal of Computer Research and Development, 2023, 60(7): 1551-1580.

[4] GAO M, ZHENG H F, FENG X X, et al. Multimodal fusion using multi-view domains for data heterogeneity in federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2025, 39(16): 16736-16744.

[5] 马鑫迪, 李清华, 姜奇, 等. 面向Non-IID数据的拜占庭鲁棒联邦学习[J]. 通信学报, 2023, 44(6): 138-153.
MA X D, LI Q H, JIANG Q, et al. Byzantine-robust federated learning over Non-IID data[J]. Journal on Communications, 2023, 44(6): 138-153.

[6] 黄聿辰, 赵彦超, 郝江山, 等. 面向数据异构的联邦学习性能优化研究[J]. 小型微型计算机系统, 2024, 45(4): 777-783.
HUANG Y C, ZHAO Y C, HAO J S, et al. Research on performance optimization of federated learning for data heterogeneity[J]. Journal of Chinese Computer Systems, 2024, 45(4): 777-783.

[7] 刘淼, 林婉茹, 王琴, 等. 车联网联邦学习的数据异质性问题及基于个性化的解决方法综述[J]. 通信学报, 2024, 45(10): 207-224.
LIU M, LIN W R, WANG Q, et al. Survey on data heterogeneity problems and personalization based solutions of federated learning in Inter-

net of vehicles[J]. Journal on Communications, 2024, 45(10): 207-224.

[8] YE M, FANG X W, DU B, et al. Heterogeneous federated learning: state-of-the-art and research challenges[J]. ACM Computing Surveys, 2024, 56(3): 1-44.

[9] GUO K P, DING Y H, LIANG J, et al. Exploring vacant classes in label-skewed federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2025, 39(16): 16960-16968.

[10] YANG S, PARK H, BYUN J, et al. Robust federated learning with noisy labels[J]. IEEE Intelligent Systems, 2022, 37(2): 35-43.

[11] GUO C, HE Q Q, TANG X Y, et al. Parameterized data-free knowledge distillation for heterogeneous federated learning[J]. Knowledge-Based Systems, 2025, 317: 113502.

[12] HUANG W K, YE M, DU B, et al. Few-shot model agnostic federated learning[C]//Proceedings of the 30th ACM International Conference on Multimedia. New York: ACM Press, 2022: 7309-7316.

[13] HSIEH K, PHANISHAYEE A, MUTLU O, et al. The non-IID data quagmire of decentralized machine learning[J]. arXiv Preprint, arXiv: 1910.00189, 2019.

[14] XU Y, LI Y, LUO H Y, et al. FBLG: a local graph based approach for handling dual skewed non-IID data in federated learning[C]//Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence. International Joint Conferences on Artificial Intelligence Organization, 2024: 5289-5297.

[15] 万伟, 胡胜山, 陆建荣, 等. 联邦学习在高度数据异构场景下的泛化鲁棒性增强[J]. 中国科学: 信息科学, 2024, 54(3): 566-581.
WAN W, HU S S, LU J R, et al. Enhancing generalization robustness of federated learning in highly heterogeneous environments[J]. Scientia Sinica (Informationis), 2024, 54(3): 566-581.

[16] MALIAKEL P J, ILAGER S, BRANDIC I. FLIGAN: enhancing federated learning with incomplete data using GAN[C]//Proceedings of the 7th International Workshop on Edge Systems, Analytics and Networking. New York: ACM Press, 2024: 1-6.

[17] 李志鹏, 国雍, 陈耀佛, 等. 基于数据生成的类别均衡联邦学习[J]. 计算机学报, 2023, 46(3): 609-625.
LI Z P, GUO Y, CHEN Y F, et al. Class-balanced federated learning based on data generation[J]. Chinese Journal of Computers, 2023, 46(3): 609-625.

[18] 汤凌韬, 王迪, 刘盛云. 面向非独立同分布数据的联邦学习数据增强方案[J]. 通信学报, 2023, 44(1): 164-176.
TANG L T, WANG D, LIU S Y. Data augmentation scheme for federated learning with non-IID data[J]. Journal on Communications, 2023, 44(1): 164-176.

[19] YAN Y L, FU H Z, LI Y X, et al. A simple data augmentation for feature distribution skewed federated learning[J]. arXiv Preprint, arXiv: 2306.09363, 2023.

[20] 刘吉强, 王雪微, 梁梦晴, 等. 基于共享数据集和梯度补偿的分层联邦学习框架[J]. 信息网络安全, 2023, 23(12): 10-20.
LIU J Q, WANG X W, LIANG M Q, et al. A hierarchical federated learning framework based on shared dataset and gradient compensation[J]. Netinfo Security, 2023, 23(12): 10-20.

[21] 张红艳, 张玉, 曹灿明. 一种解决数据异构问题的联邦学习方法[J]. 计算机应用研究, 2024, 41(3): 713-720.
ZHANG H Y, ZHANG Y, CAO C M. Effective method to solve problem of data heterogeneity in federated learning[J]. Application Research of Computers, 2024, 41(3): 713-720.

[22] 张瑞麟, 杜晋华, 尹浩. 跨设备联邦学习中的客户端选择算法[J]. 软件学报, 2024, 35(12): 5725-5740.
ZHANG R L, DU J H, YIN H. Client selection algorithm in cross-device federated learning[J]. Journal of Software, 2024, 35(12): 5725-5740.

[23] ZOU Y F, SHEN S K, XIAO M B, et al. Value of information: a comprehensive metric for client selection in federated edge learning[J]. IEEE Transactions on Computers, 2024, 73(4): 1152-1164.

[24] LI L, DUAN M M, LIU D, et al. FedSAE: a novel self-adaptive federated learning framework in heterogeneous systems[C]//Proceedings of the 2021 International Joint Conference on Neural Networks (IJCNN). Piscataway: IEEE Press, 2021: 1-10.

[25] LU R H, ZHANG W Z, WANG Y, et al. Auction-based cluster federated learning in mobile edge computing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(4): 1145-1158.

[26] 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.

[27] CHENG Z H, HUANG X M, WU P F, et al. Momentum benefits non-IID federated learning simply and provably[C]//International Conference on Learning Representations. Vancouver: ICLR, 2024: 6265-6298.

[28] HU K, XIANG L Y, TANG P, et al. Feature norm regularized federated learning: utilizing data disparities for model performance gains[C]//Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence. International Joint Conferences on Artificial Intelligence Organization, 2024: 4136-4146.

[29] JI X Y, ZHU Z W, XI W, et al. FedFixer: mitigating heterogeneous label noise in federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(11): 12830-12838.

[30] FALLAH A, MOKHTARI A, OZDAGLAR A. Personalized federated learning with theoretical guarantees: a model-agnostic meta-learning approach[J]. Advances in Neural Information Processing Systems, 2020, 33: 3557-3568.

[31] DINH C T, TRAN N H, NGUYEN T D. Personalized federated learning with Moreau envelopes[J]. arXiv Preprint, arXiv: 2006.08848, 2020.

[32] 高雨佳, 王鹏飞, 刘亮, 等. 基于注意力增强元学习网络的个性化联邦学习方法[J]. 计算机研究与发展, 2024, 61(1): 196-208.
GAO Y J, WANG P F, LIU L, et al. Personalized federated learning method based on attention-enhanced meta-learning network[J]. Journal of Computer Research and Development, 2024, 61(1): 196-208.

[33] JIA Z G, ZHOU T R, YAN Z Y, et al. Personalized meta-federated learning for IoT-enabled health monitoring[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2024, 43(10): 3157-3170.

[34] 崔腾, 张海军, 代伟. 基于分布共识的联邦增量迁移学习[J]. 计算机学报, 2024, 47(4): 821-841.
CUI T, ZHANG H J, DAI W. Federated incremental transfer learning based on distributed consensus[J]. Chinese Journal of Computers, 2024, 47(4): 821-841.

[35] ZHANG J, GUO S, MA X S, et al. Parameterized knowledge transfer for personalized federated learning[J]. arXiv Preprint, arXiv: 2111.02862, 2021.

[36] XU H Q, SHEN D, WANG M, et al. Adaptive group personalization for federated mutual transfer learning[C]//Proceedings of the 41st International Conference on Machine Learning. New York: PMLR, 2024: 55225-55240.

[37] MA B Y, YIN X, TAN J, et al. FedST: federated style transfer learning for non-IID image segmentation[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(5): 4053-4061.

[38] JIA Y Z, ZHANG X Y, BEHESHTI A, et al. FedLPS: heterogeneous federated learning for multiple tasks with local parameter sharing[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(11): 12848-12856.

[39] DIAO Y Q, LI Q B, HE B S. Exploiting label skews in federated learning with model concatenation[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(10): 11784-11792.

[40] 朱素霞, 顾玢珂, 孙广路. 基于相似度加速的自适应聚类联邦学习[J]. 通信学报, 2024, 45(3): 197-207.
ZHU S X, GU B K, SUN G L. Adaptive clustering federated learning via similarity acceleration[J]. Journal on Communications, 2024, 45(3): 197-207.

[41] VAHIDIAN S, MORAFAH M, WANG W J, et al. Efficient distribution similarity identification in clustered federated learning via principal angles between client data subspaces[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(8): 10043-10052.

[42] GHOSH A, CHUNG J, YIN D, et al. An efficient framework for clustered federated learning[J]. IEEE Transactions on Information Theory, 2022, 68(12): 8076-8091.

[43] TANG Y T. Adapted weighted aggregation in federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(21): 23763-23765.

[44] ZHANG J Q, HUA Y, WANG H, et al. FedALA: adaptive local aggregation for personalized federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(9): 11237-11244.

[45] JIA R F, XIE W Y, LEI J, et al. Adaptive hierarchical aggregation for federated object detection[C]//Proceedings of the 32nd ACM International Conference on Multimedia. New York: ACM Press, 2024: 3732-3740.

[46] MA X S, ZHANG J, GUO S, et al. Layer-wised model aggregation for personalized federated learning[C]//Proceedings of the 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2022: 10082-10091.

[47] 刘松, 罗杨宇, 许佳培, 等. 基于轻量自蒸馏的低成本联邦学习[J]. 电子学报, 2025, 53(1): 259-269.
LIU S, LUO Y Y, XU J P, et al. Low-cost federated learning based on lightweight self-distillation[J]. Acta Electronica Sinica, 2025, 53(1): 259-269.

[48] LU J H, LI S K, BAO K X, et al. Federated learning with label-masking distillation[C]//Proceedings of the 31st ACM International Conference on Multimedia. New York: ACM Press, 2023: 222-232.

[49] YAO D Z, PAN W N, DAI Y T, et al. FedGKD: toward heterogeneous federated learning via global knowledge distillation[J]. IEEE Transactions on Computers, 2024, 73(1): 3-17.

[50] ZHANG J, GUO S, GUO J C, et al. Towards data-independent knowledge transfer in model-heterogeneous federated learning[J]. IEEE Transactions on Computers, 2023, 72(10): 2888-2901.

[51] ZHU Z D, HONG J Y, ZHOU J Y. Data-free knowledge distillation for heterogeneous federated learning[J]. Proceedings of Machine Learning Research, 2021, 139: 12878-12889.

[52] ALBALLA N, CANINI M. A first look at the impact of distillation hyper-parameters in federated knowledge distillation[C]//Proceedings of the 3rd Workshop on Machine Learning and Systems. New York: ACM Press, 2023: 123-130.

[53] 倪宣明, 沈鑫圆, 张海. 面向异构数据的自适应个性化联邦学习: 一种基于参数分解和持续学习的方法[J]. 中国科学: 信息科学, 2022, 52(12): 2306-2320.
NI X M, SHEN X Y, ZHANG H. Adaptive personalized federated learning for heterogeneous data: a method based on parameter decomposition and continual learning[J]. Scientia Sinica (Informationis), 2022, 52(12): 2306-2320.

[54] WU X H, LIU X F, NIU J W, et al. Decoupling general and personalized knowledge in federated learning via additive and low-rank decomposition[C]//Proceedings of the 32nd ACM International Conference on Multimedia. New York: ACM Press, 2024: 7172-7181.

[55] GAO L Z, LI Z X, LU Y, et al. FediOS: decoupling orthogonal subspaces for personalization in feature-skew federated learning[J]. arXiv Preprint, arXiv: 2311.18559, 2023.

[56] WU C R, WANG H S, ZHANG X, et al. Spatio-temporal heterogeneous federated learning for time series classification with multi-view orthogonal training[C]//Proceedings of the 32nd ACM International Conference on Multimedia. New York: ACM Press, 2024: 2613-2622.

[57] ZENG H M, YUE Z R, ZHANG Y, et al. Fair federated learning with biased vision-language models[C]//Proceedings of the Findings of the Association for Computational Linguistics ACL 2024. Stroudsburg: ACL Press, 2024: 10002-10017.

[58] SHI J M, ZHENG S S, YIN X B, et al. CLIP-guided federated learning on heterogeneity and long-tailed data[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(13): 14955-14963.

[59] MOSKVORETSKII V, TUPITSA N, BIEMANN C, et al. Low-resource machine translation through the lens of personalized federated learning[C]//Proceedings of the Findings of the Association for Computational Linguistics: EMNLP 2024. Stroudsburg: ACL Press, 2024: 8806-8825.

[60] LI G H, WU W S, SUN Y, et al. Visual prompt based personalized federated learning[J]. arXiv Preprint, arXiv: 2303.08678, 2023.

[61] YANG F E, WANG C Y, WANG Y F. Efficient model personalization in federated learning via client-specific prompt generation[C]//Proceedings of the 2023 IEEE/CVF International Conference on Computer Vision (ICCV). Piscataway: IEEE Press, 2023: 19102-19111.

[62] CUI T Y, LI H X, WANG J Y, et al. Harmonizing generalization and personalization in federated prompt learning[J]. arXiv Preprint, arXiv: 2405.09771, 2024.

[63] CHEN H K, ZHANG Y, KROMPASS D, et al. FedDAT: an approach for foundation model finetuning in multi-modal heterogeneous federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(10): 11285-11293.

[64] DONG S, XIA Y J, KAMRUZZAMAN J. Quantum particle swarm optimization for task offloading in mobile edge computing[J]. IEEE Transactions on Industrial Informatics, 2023, 19(8): 9113-9122.

[65] XIAO G X, LIN J, SEZNEC M, et al. Smoothquant: accurate and efficient post-training quantization for large language models[C]//International Conference on Machine Learning. New York: PMLR, 2023:

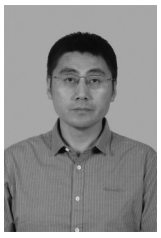
38087-38099.
[66] FRANTAR E, ALISTARH D. Sparsegpt: massive language models can be accurately pruned in one-shot[C]//International Conference on Machine Learning. New York: PMLR, 2023: 10323-10337.
[67] GU Y X, DONG L, WEI F R, et al. MiniLLM: knowledge distillation of large language models[J]. arXiv Preprint, arXiv: 2306.08543, 2023.
[68] YU H, WU J X. Compressing transformers: features are low-rank, but weights are not![J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(9): 11007-11015.
[69] TAN Y, LONG G D, LIU L, et al. FedProto: federated prototype learning across heterogeneous clients[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2022, 36(8): 8432-8440.
[70] ZHANG J Q, LIU Y, HUA Y, et al. FedTGP: trainable global prototypes with adaptive-margin-enhanced contrastive learning for data and model heterogeneity in federated learning[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(15): 16768-16776.
[71] YAN B W, ZHANG H L, XU M H, et al. FedRFQ: prototype-based federated learning with reduced redundancy, minimal failure, and enhanced quality[J]. IEEE Transactions on Computers, 2024, 73(4): 1086-1098.
[72] LI L, ZHAN D C, LI X C. Aligning model outputs for class imbalanced non-IID federated learning[J]. Machine Learning, 2024, 113(4): 1861-1884.
[73] YAO D X, LI B C. PerFedRLNAS: one-for-all personalized federated neural architecture search[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(15): 16398-16406.
[74] SU H D, DONG S, ZHANG T. A hybrid blockchain-based privacy-preserving authentication scheme for vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2024, 73(11): 17059-17072.
[75] XIA Y J, LIU Y N, DONG S, et al. SVCA: secure and verifiable chained aggregation for privacy-preserving federated learning[J]. IEEE Internet of Things Journal, 2024, 11(10): 18351-18365.
[76] NOBLE M, BELLET A, DIEULEVEUT A. Differentially private federated learning on heterogeneous data[C]//International Conference on Artificial Intelligence and Statistics. New York: PMLR, 2022: 10110-10145.
[77] WEI K, LI J, DING M, et al. User-level privacy-preserving federated learning: analysis and performance optimization[J]. IEEE Transactions on Mobile Computing, 2022, 21(9): 3388-3401.
[78] 张少波, 张激勇, 朱更明, 等. 基于Bregman散度和差分隐私的个性化联邦学习方法[J]. 软件学报, 2024, 35(11): 5249-5262.
ZHANG S B, ZHANG J Y, ZHU G M, et al. Personalized federated learning method based on bregman divergence and differential privacy[J]. Journal of Software, 2024, 35(11): 5249-5262.
[79] 刘洋, 吴旭, 刘承坤. 工业物联网中的个性化联邦学习算法的研究[J]. 小型微型计算机系统, 2025, 46(1): 209-216.
LIU Y, WU X, LIU C K. Research on personalized federated learning algorithm in industrial Internet of things[J]. Journal of Chinese Computer Systems, 2025, 46(1): 209-216.
[80] XIA Q Y, DONG S, PENG T. An abnormal traffic detection method for IoT devices based on federated learning and depthwise separable convolutional neural networks[C]//Proceedings of the 2022 IEEE International Performance, Computing, and Communications Conference (IPCCC). Piscataway: IEEE Press, 2022: 352-359.
[81] CHI H, ZHANG Y Q, XU S, et al. Collaborative adversarial learning for unsupervised federated domain adaptation[C]//International Conference on Knowledge Science, Engineering and Management. Berlin: Springer, 2024: 346-357.
[82] FAN J M, WU K, TANG G M, et al. Taking advantage of the mistakes: rethinking clustered federated learning for IoT anomaly detection[J]. IEEE Transactions on Parallel and Distributed Systems, 2024, 35(6): 862-876.

[作者简介]

何帆（1998– ），女，山东济宁人，哈尔滨工程大学博士生，主要研究方向为联邦学习、机器学习、数据安全等。

王勇（1983– ），男，河南信阳人，博士，哈尔滨工程大学副教授，主要研究方向为机器学习、隐私计算、数据安全等。

杨静（1962– ），女，黑龙江哈尔滨人，博士，哈尔滨工程大学教授，主要研究方向为人工智能、隐私保护、社会计算等。



于旭（1982– ），男，山东青岛人，博士，中国石油大学（华东）教授，主要研究方向为机器学习、工业互联网、推荐系统等。