异构数据环境下的联邦学习综述

汤尧[1,2]，刘健[1,2*]

（1. 浙江大学区块链与数据安全全国重点实验室，杭州 310063；
2. 杭州高新区（滨江）区块链与数据安全研究院，杭州 310051）

摘要：随着多模态、大语言模型的不断发展，参与人工智能（Artificial Intelligence，AI）训练的数据异质性逐渐增强，联邦学习（Federated Learning，FL）面临着新的挑战与机遇。对异构数据场景下的联邦学习相关研究进行了综述，从数据层面和模型层面总结了用于评估数据偏移性的指标和方法，并从多任务学习、数据蒸馏等多条技术路线对现有的联邦学习解决方案进行了全面的梳理。最后，探索了联邦学习与大模型、多模态等新兴技术的融合方向，并对未来的发展趋势进行了展望。

关键词：联邦学习；数据隐私；异构数据

中图分类号：TP393　　**文献标志码：**A

DOI: 10.20172/j.issn.2097-3136.250201

A survey on federated learning in heterogeneous data environments

TANG Yao[1,2], LIU Jian[1,2*]

（1. The State Key Laboratory of Blockchain and Data Security, Zhejiang University, Hangzhou 310063, China;
2. Hangzhou High-Tech Zone (Binjiang) Blockchain and Data Security
Research Institute, Hangzhou 310051, China）

Abstract: With the continuous development of multimodal and large language models, the heterogeneity of data involved in artificial intelligence (AI) training is gradually increasing. This has brought new challenges and opportunities to federated learning (FL). Relevant studies of federated learning in heterogeneous data scenarios were reviewed, and the indicators and methods for assessing data shift were summarized from the data and model levels with the existing federated learning solutions reviewed from multiple technical routes such as the multi-task learning and data distillation. Finally, the integration directions of federated learning with emerging technologies such as large models and multimodality were explored, and the future development trends were predicted.

Keywords: federated learning; data privacy; heterogeneous data

0 引言

在当今数字化时代，人工智能（Artificial Intelligence，AI）技术正以前所未有的速度发展，深刻地影响着各行各业。从自动驾驶汽车到智能家居，从个性化推荐系统到精准医疗诊断，人工智能的应用无处不在，其核心驱动力是数据。然而，随着数据量的激增和数据价值的提升，数据隐私保护问题日益凸显，成为社会关注的焦点。如何在利用数据推动技术进步的同时，确保个人隐私不被侵犯，是当前亟待解决的挑战。

联邦学习[1-2]（Federated Learning，FL）作为一种创新的分布式机器学习框架，为解决这一问题提供了新的思路。与传统的集中式机器学习不同，联邦学习允许多个机构或主体在不共享原始数据的情况下，共同构建和训练机器学习模型。这种“数据不

* 通信作者. E-mail: tangyaozju@zju.edu.cn

基金项目：国家重点研发计划青年科学家项目（2023YFB2704000）

引用格式：汤尧，刘健. 异构数据环境下的联邦学习综述 [J]. 网络空间安全科学学报，2025，3（2）：2 - 11.

Citation Format: TANG Y，LIU J. A survey on federated learning in heterogeneous data environments[J]. Journal of Cybersecurity，2025，3（2）：2 - 11.

动模型动、数据可用不可见”的特性，不仅保护了数据的隐私性，还确保了数据的安全性和合规性，使得联邦学习在隐私保护方面具有独特的优势。

联邦学习的核心思想是将模型训练过程分散到各个参与方（如移动设备、企业服务器等）。如图 1 所示，每个参与方仅在本地数据上进行模型训练，然后将训练得到的模型参数（如权重、梯度等）发送给中心服务器进行聚合。中心服务器负责协调整个训练过程，包括初始化模型、收集参数、进行聚合操作以及更新全局模型。通过这种方式，联邦学习能够在保护数据隐私的前提下，充分利用多个机构或主体的数据进行联合建模，实现数据价值的最大化。

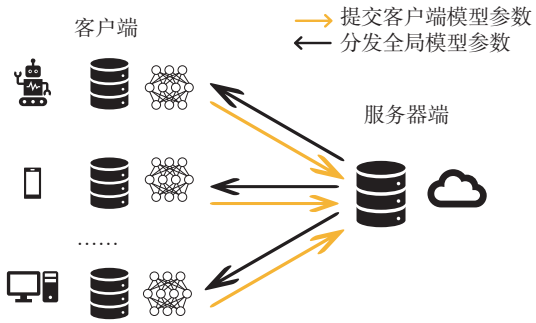

图 1　联邦学习流程示意图

Fig. 1　Schematic diagram of the federated learning process

然而，随着多模态、大语言模型以及通用模型的兴起，联邦学习面临着新的机遇和挑战。这些模型在处理异构数据时，需要高效的聚合技术来解决设备异质性、数据异质性（非独立同分布数据）、模型异质性（多模态/大模型/传统模型）以及通信效率与安全隐私等问题。

本综述针对异构场景下的联邦学习聚合方案这一主题进行总结探讨，梳理了现有异构场景的数据特点，全面总结了针对异构数据的聚合方案，重点关注了大语言模型以及多模态模型下的场景，探讨了现有技术的优缺点，并对未来研究方向提出了展望。本文主要贡献如下：

（1）对异构数据特点进行了分析讨论，并对其偏移性指标进行了总结。

（2）总结了不同技术路线的异构数据聚合方案，由常规分类任务拓展到文本生成任务和多模态检索任务场景。

（3）对联邦学习异构数据场景的发展趋势进行了展望，分析了其未来发展前景。

1　异构数据的特点

1.1　独立同分布数据的概念

在机器学习和统计学中，独立同分布（Independent and Identically Distributed，IID）是一个重要的假设条件，它是指数据样本之间相互独立，并且所有样本都来自同一分布。具体来说，IID 数据满足以下两个条件：

（1）独立性（Independent）。每个数据样本之间没有关联，一个样本的值不会影响其他样本的值。

（2）同分布（Identically Distributed）。所有数据样本都服从相同的概率分布。

在传统的集中式机器学习中，IID 假设简化了数据分布特征，使得联邦学习集合训练的效率提高。然而，随着更多样的应用场景和任务的出现，IID 假设在现实场景中往往难以得到满足，尤其是在数据分布离散化和模型结构多样化的场景下。

1.2　非独立同分布数据的成因

非独立同分布（Non-Indepen-dent and Identically Distributed，Non-IID）数据是指数据样本之间存在依赖关系，或者数据来自不同的分布[3-4]。Non-IID 数据的成因主要包括以下几种情况：

（1）数据来源的多样性。在联邦学习中，数据通常来自多个不同的客户端或机构，每个客户端的数据可能受到其自身业务、地理位置、用户群体等因素的影响，从而导致数据分布的差异。

（2）模型系统的异质性。联合网络中每个设备的存储、计算和通信功能可能会有所不同，导致其部署的模型规模也不尽相同，从而形成训练系统的不平衡性。

（3）数据特征的异质性。不同客户端的数据可能包含不同的特征集或特征分布，如某些客户端可能只采集了部分特征，而其他客户端采集了更全面的特征。

（4）目标任务的异质性。不同客户端可能面临不同的任务目标，导致数据分布的差异。

1.3　现实场景下非独立同分布数据的特点

在大语言模型[5]和多模态模型[6]中，Non-IID 数据主要表现为以下几种情况：

（1）主题分布差异。不同客户端的数据可能集中在不同的主题或领域。例如，某些客户端的数据主要涉及新闻报道，而另一些客户端的数据可能集中在社交媒体对话。

（2）语言风格差异。不同客户端的数据可能具

有不同的语言风格，如正式文本与口语化文本的差异。

（3）模态内容差异。不同模态数据所表示含义范围差异大，难以进行统一的编码模态对齐。

这些数据特性给联邦学习在异构数据环境中的高效解决方案带来了诸多挑战。

2 衡量数据偏移性的指标

为了更好地理解和处理 Non-IID 数据，研究者们从数据和模型两个层面提出了多种衡量数据异构性的方法。

2.1 数据层面的衡量方法

数据集熵[7]是一个用于衡量数据分布、信息量、不平衡结构以及 Non-IID 性质的重要指标，其计算与所使用的模型无关。数据集熵的计算基于信息熵的概念，通过广义聚类策略实现，利用集成了特征和监督输出的自定义相似性矩阵，这使其适用于分类和回归任务。然而，数据集熵的计算依赖聚类和自定义相似性矩阵，这可能导致较高的计算开销。

通用边界 s_G[8]是另一个衡量数据异构性的指标，用于指示本地数据分布的差异程度。当 $s_G=0$ 时，数据集满足 IID 条件；而较高的 s_G 则表示 Non-IID 特征的水平增加，反映了不同客户端数据之间的显著可变性。这一指标对于分析联邦学习算法（如 FedAvg）的收敛率至关重要，因为它能够揭示 Non-IID 条件如何影响模型的训练过程和整体性能。

考虑到每个客户端的类别数较少意味着数据集的数据分布不平衡和异质性大，Zawad 等[9]提出了异质性指数（Heterogeneity Index, HI）：

$$\mathrm{HI}=1-\frac{1}{C_{\max}-1}\cdot(c-1)$$

其中，c 是每个客户端的最大类别数，$C_{\max}$是数据集中的类别总数。请注意，HI 仅能反映不同客户的类别特征的不平衡性，无法捕获客户数据类别数量分布中的细微变化[10]。

不平衡比（Imbalance Ratio，IR）是文献 [11] 中提出的另一个指标：

$$\mathrm{IR}(\zeta)=\frac{\max_i \zeta_i}{\min_j \zeta_j}$$

其中，ζ_i表示类别 i 在数据集中的出现频率。该指标用于衡量多数阶层和少数阶层之间的不平衡性。IR 值越大，表示数据集中的类不平衡程度越高。IR 有两个主要限制：它主要适用于二元分类问题；它可能会通过忽略中间类别的分布过度简化多类不平衡性。

一些指标利用统计检验来评估标签分布差异的显著性，如 Kolmogorov-Smirnov 统计量[12]和卡方检验[9]，另一个替代检验是最大均值差异。后者通过识别连续函数 f、计算每个分布的平均值并测量这些平均值之间的差异，来比较数据的分布情况。均值之间的差异越大，表示数据分布差异越显著。

2.2 模型层面的衡量方法

除了单纯地从数据层面进行统计的方法，还有一些在特征空间或模型表现中提取特征的方法，这类特征的计算通常与客户端模型有关。

文献 [13] 提出了客户端 Non-IID 指数（Client-Wise Non-IID Index，CNI），用于衡量客户端 i 的数据分布与其他客户端的数据分布的差异。

$$\mathrm{CNI}(i)=\frac{\left\|\left(\frac{1}{|C_i|}\sum_k \mathrm{En}\left(D_i^k\right)\right)-\left(\frac{1}{|C_j|}\sum_{l\neq i}\mathrm{En}\left(D_j^l\right)\right)\right\|_2}{\sigma(\mathrm{En}(D))}$$

其中，D_i^k表示第 i 个参与者数据 D_i中属于第 k 类别的数据，C_i表示 D_i中的类别数量，σ是标准差，$\|\cdot\|_2$表示 l_2距离。CNI 背后的直觉是测量给定客户端上特征空间中不同类别的平均数据表示与所有其他客户端的对应数据表示之间的距离。

一些指标基于不同客户端数据的类别分布比例，使用广为人知的距离、相似性和散度衡量特征空间，而不是标签空间中数据分布的差异，如 Hellinger 距离[14,15]、Jensen-Shannon 散度[16]、Kullback-Leibler 散度[17]、余弦相似度[18]，以及 Jaccard[19]和 Wasserstein 距离[20-21]等相似性。

Dataskew[22]是直接衡量组合标签和属性倾斜对模型性能影响的唯一指标，定义如下：

$$\mathrm{Dataskew}=\frac{\max\left(\Delta\mathrm{Accuracy}_{\mathrm{pairwise}}\right)}{\frac{1}{K}\sum_{i=1}^{K}\mathrm{Accuracy}_i}$$

其中，$\max\left(\Delta\mathrm{Accuracy}_{\mathrm{pairwise}}\right)$是客户端之间准确性的最大配对偏差。分母 $\frac{1}{K}\sum_{i=1}^{K}\mathrm{Accuracy}_i$是所有客户端的平均准确率。高 Dataskew 值（接近 1）表示数据异质性强。它可能会在计算中引入偏差，因为它包括训练初始模型的客户端。如果该客户端的数据分布明显不同，则可能会扭曲指标的解释。

模型移动度量（Model Traveling Metric）[23]被用于估计模型在不同 Non-IID 数据分区中的泛化程度。在训练期间，模型会定期在不同的数据分区之间移动，以评估其在其他客户端上的准确性。将模型在其原始数据分区上的性能与其在新分区上的准确性

进行比较，可以估计准确性损失，这反映了 Non-IID 的程度。

3　现有联邦学习方案

在分布式训练领域，Non-IID 数据问题是一个长期存在的挑战。为了应对这一挑战，研究者们在传统机器学习、自然语言处理以及多模态模型等多个领域内，结合原型学习、知识蒸馏、多任务学习等技术路线探索并提出了一系列解决方案，表 1 总结了各类技术路线在原有任务场景下的核心思想。

表 1　现有技术的核心思想

Table 1　Core idea of the existing technologies

方案	核心思想
原型学习	通过交换代表性样本（原型）传递数据信息
知识蒸馏	将教师模型的知识迁移到学生模型
多任务学习	同时训练多个相关任务以提高泛化能力
对比学习	通过比较学习正负样本对来增强数据表示相似性
数据增强	通过数据生成增加训练数据的多样性，以缓解本地数据不平衡问题
预训练模型	使用预训练模型减少训练时间和提高模型准确性

本节依照技术路线对传统图像分类任务、自然语言场景和多模态场景下的异构联邦学习方案进行了总结。

3.1　图像分类任务

在联邦学习环境中，图像分类模型面临诸多挑战，包括数据的非独立同分布、模型异构性以及隐私保护等。为了解决这些问题，研究者们提出了一系列创新方法，本小节将概述这些方法的主要进展。

3.1.1　基于原型学习的方案

在联邦学习环境中，原型学习通过交换代表性样本（原型）执行分类、回归或聚类等任务，这种方法的灵感来自人类通过交换特定概念的原型来获得更多知识的方式。原型学习的优势在于客户端和服务器进行信息传递时只需要传递原型数据而非模型参数，能够有效降低通信成本。问题是用原型数据作为代表性样本，对长尾数据的学习能力较弱。

FedPCL 方案[24] 旨在通过类内原型高效地共享相似的高级语义，不会暴露每个参与者的本地模型和数据。该方法鼓励客户端从基础模型输出的丰富通用表示中捕获更多与类别相关的信息，从而提高表示能力。FedPCL 通过在本地训练期间进行对比学习，允许客户端从本地和全局原型中共享更多类别相关的知识。

现有的个性化联合学习（Personalized Federated Learning，PFL）算法大多使用以模型为中心的方式处理个性化问题，如个性化层分区、模型正则化和模型插值，这些算法都没有考虑分布式客户端的数据特征。文献 [25] 提出了一种用于图像分类任务的新型 PFL 框架，称为 pFedPT，它利用个性化的视觉提示来隐式表示客户端的本地数据分布信息，并将该信息提供给聚合模型以帮助完成分类任务。具体来说，在每一轮 pFedPT 训练中，每个客户端都会生成一个与本地数据分发相关的本地个性化提示。然后，根据由原始数据和视觉提示组成的输入对本地模型进行训练，以了解提示中包含的分布信息。

在联邦学习环境中，客户端可能在数据分布、网络延迟、输入/输出空间和/或模型架构方面有所不同，这很容易导致其局部梯度错位。为了提高对异构性的容忍度，文献 [26] 提出了一种新的联邦原型学习框架 FedProto，其中客户端和服务器交流抽象类原型而不是梯度。FedProto 聚合从不同客户端收集本地原型，然后将全局原型发送回所有客户端，以规范本地模型的训练。对每个客户端的训练旨在最大限度地减少本地数据的分类误差，同时保持生成的本地原型与相应的全局原型足够接近。此外，该文对非凸目标下 FedProto 的收敛率进行了理论分析。

3.1.2　基于知识蒸馏的方案

知识蒸馏是一种模型压缩技术，它将一个大型、复杂模型（教师模型）的知识迁移到一个更小、更简单的模型（学生模型）中，以提高后者的性能和泛化能力。在联邦学习中，经常将具有独特数据的客户端作为教师模型，将服务器端作为学生模型。基于知识蒸馏的联邦学习算法只需要客户端交换本地模型的软标签（如 logits），而无须上传模型参数或数据，从而显著降低潜在的隐私风险和通信成本。知识蒸馏的缺点在于服务器端需要一个公开数据集进行模型蒸馏，该数据集的数据分布会影响蒸馏客户端模型知识的全面性和有效性。

文献 [27] 提出了一种基于两步知识蒸馏的高效通信联邦学习框架 Fed2KD，它通过生成隐私保护数据提高了分类的准确性，同时通过注意力机制和度量学习赋能的新知识蒸馏方案提高了通信效率。

FedX[28] 是一个无监督联邦学习框架，其核心特点是采用双边知识蒸馏和无偏表示学习。在传统的联邦学习中，通常依赖监督信号，而在 FedX 中，模

型通过对比学习机制进行自我监督学习，从而在没有标签的情况下学习样本的向量表示。

3.1.3 基于多任务学习的方案

多任务学习通过联合训练多个相关任务，能够利用任务间的相关性来提高模型的泛化能力，从而缓解 Non-IID 数据带来的挑战。在联邦学习场景下，多个客户端模型的训练目标不一致，服务器端可以利用多任务学习的思路高效地进行模型聚合。同时，由于不同任务之间可能存在目标冲突，合理平衡任务权重以提高综合任务准确率是该方案的难点所在。

文献 [29] 提出了第一个有效协调和训练多个同步联邦学习任务的联邦学习系统。其首先将训练同步联邦学习任务的问题正式化并提出了新方法——合并和拆分（Merge and Split，MAS），以优化训练多个同步联邦学习任务的性能。MAS 首先将联邦学习任务合并为具有多任务架构的一体化联邦学习任务。经过几轮训练后，MAS 利用在一体化训练期间测量的任务之间的亲和力，将一体化联邦学习任务拆分为两个或多个联邦学习任务。然后，根据一体化训练中的模型参数继续训练联邦学习任务的每个分割。

3.1.4 基于对比学习的方案

对比学习可以有效控制全局模型和客户端模型的相似性，难点在于训练过程中可能存在过拟合问题。

MOON 方案[30] 通过引入对比学习来改善联邦学习的性能，尤其是在客户端之间数据分布差异较大的情况下。MOON 的主要目标是利用对比学习机制，通过最大化当前模型与全局模型的相似性，最小化当前模型与其历史模型的相似性，使得客户端在本地训练过程中保持对全局模型的学习方向，避免各客户端的模型偏离全局模型过多，从而提高全局模型的泛化能力。

3.1.5 基于数据增强的方案

在联邦学习中，数据增强是一种有效的方法，用于增加训练数据的多样性，从而缓解本地数据不平衡的问题。该方案的缺点在于需要额外的数据生成模型参与训练，增加了训练系统的复杂度。合成数据的质量和真实性直接影响模型性能，生成质量差的数据可能导致模型性能下降，引入新的偏差。

文献 [31] 提出了一个名为合成数据辅助联邦学习（Synthetic Data Aided Federated Learning，SDA-FL）的新框架，通过共享合成数据来解决 Non-IID 挑战。具体来说，每个客户端都会预先训练一个本地生成对抗网络（Generative Adversarial Network，GAN）以生成客户端私有合成数据，这些数据被上传到参数服务器（Parameter Server，PS）以构建全局共享合成数据集。为了为合成数据集生成可信的伪标签，还提出了一种由 PS 执行的迭代伪标签机制。具有置信度伪标签的合成数据集的辅助显著缓解了客户端之间的数据异构性，从而提高了本地更新之间的一致性，有利于全局聚合。

文献 [32] 研究了具有不同偏斜水平的 Non-IID 数据对联邦学习的影响。在此基础上，提出了一种基于合成少数过采样技术（Synthetic Minority Over-Sampling Technique，SMOTE）的数据增强联邦学习算法，以减少 Non-IID 数据的影响。在此基础上，还使用扩展的伯克利数据包过滤器（extended Berkeley Packet Filter，eBPF）技术开发了一个数据收集模块，以收集用于实验的数据集。

3.1.6 基于预训练模型的方案

在公开任务中预训练服务器模型可以有效提升联邦学习的训练效率，减少训练时间，与文本预训练模型的思路较为相似。预训练模型的性能依赖预训练数据的质量和相关性，因此预训练数据集是该方案的重点。

在联合学习的许多实际应用中，服务器可以访问训练任务的代理数据，这些数据可用于开始联合训练之前的预训练模型。文献 [33] 使用四个标准联合学习基准数据集实证研究了从预训练模型开始对联邦学习的影响。不出所料，从预训练模型开始可以减少达到目标错误率所需的训练时间，并且与从随机初始化开始时相比，能够训练出更准确的模型（准确率高达 40%）。令人惊讶的是，该文章还发现，从预训练的初始化开始联邦学习会降低数据和系统异构性的影响。

文献 [34] 专注于迁移学习，提出了一个联邦迁移学习和基础模型相结合的框架——联邦迁移基础模型（Federated Transfer Learning-Foundation Model，FTL-FM），使客户端能够从在联合环境中学到的一般知识中受益，并将特定领域的知识传回以改进联合学习。

3.1.7 针对模型收敛问题的方案

为了应对设备间的系统特性差异和数据分布不平衡性这两大挑战，FedProx[35] 通过引入近端项和不精确解来提高算法的鲁棒性和稳定性，从而在一定程度上解决了由于数据异质性导致的模型偏离问题，并允许不同设备根据其计算能力执行不同数量的本地训练轮次，以适应系统异构性。此外，FedProx 还

提供了理论上的收敛保证，并在实验中展示了其在异质网络环境中相对于 FedAvg 的优越性能。

SCAFFOLD[36] 是一种高效的联邦学习算法，主要关注梯度稀疏性和设备间的通信。它通过在本地更新 k 次才进行一次通信的方式，增加了修正项，使每次本地更新被拉回到理想的更新路径附近，从而解决了联邦学习中 Non-IID 数据使用户多轮本地训练容易越走越偏，最终降低模型精度和减慢收敛速度的问题。

FedNova[37] 是一种针对异构联邦优化问题提出的算法，它旨在解决由于客户端数据分布不平衡和计算能力差异导致的“目标不一致性”问题。FedNova 通过采用规范化平均策略消除了这一难题，同时保持了快速的误差收敛性。FedNova 的核心是对局部模型变化进行正则化聚合，从而避免传统方法中因不同步更新而导致的失配问题。其理论框架深入分析了异构环境下优化算法的收敛行为，揭示了目标不一致性和收敛速度下降的根本原因。

3.1.8　其他方案

文献 [38] 提出了一种新型个性化联邦学习方法 pFedBayes，该方法通过贝叶斯变分推理来缓解过拟合问题。为了实现个性化，每个客户端通过平衡其对私有数据的构造误差及其与来自服务器的全局分发的 KL（Kullback-Leibler）差异来更新其本地分发参数。该方法在客户端和服务器的神经网络中引入了权重不确定性，从而提高了模型的泛化能力。理论分析给出了平均泛化误差的上界，并表明泛化误差的收敛速度在对数因子内是最小二乘最优的。

在联邦学习中，模型性能通常会受到数据异构性引起的客户端漂移的影响，主流工作侧重于纠正客户端漂移。文献 [39] 提出了一种名为虚拟同质性学习（Virtual Homogeneity Learning，VHL）的不同方法来直接“纠正”数据异构性。特别地，VHL 使用虚拟同构数据集进行联邦学习，该数据集满足两个条件：不包含私人信息和可分离。虚拟数据集可以从客户端之间共享的纯噪声中生成，旨在校准来自异构客户端的特征，并从理论上证明了 VHL 可以在自然分布上实现可证明的泛化性能。

3.2　自然语言场景

在联邦学习环境中，大语言模型（Large Language Models，LLMs）的个性化和隐私保护是一个重要研究方向。本小节将概述大语言模型在联邦学习中的几种改进方法，包括基于低秩适配器（Low-Rank Adaptation，LoRA）的改进、基于提示调优（Prompt Tuning）的改进以及基于预训练模型的改进。

3.2.1　基于低秩适配器的改进

低秩适配器训练方法是一种高效的微调技术，通过在预训练语言模型中注入低秩矩阵对来显著减少可训练参数的数量，从而在保持模型性能的同时降低计算和存储成本。该方案能有效降低联邦学习中的计算和通信成本。

现有的模型异构个性化联邦学习（Model-Heterogeneous Personalized Federated Learning，MHPFL）方法具有较高的计算和通信成本。为了弥合这一差距，文献 [40] 提出了一种基于 LoRA 调优的新型高效模型异构个性化联邦学习框架 pFedLoRA。受流行的 LoRA 方法的启发，pFedLoRA 使用低秩模型（又名适配器）进行微调，即设计了一个同构的小型适配器，通过提出的用于全球-本地知识交换的迭代训练来促进联邦客户端的异构本地模型训练。在联邦学习服务器上，这些小型本地适配器进行聚合以生成全局适配器。

当 LoRA 应用于隐私保护联邦学习的设置时，可能会变得不稳定，原因如下：（1）数据异构性和多步骤本地更新的影响是不可忽视的；（2）在更新梯度上强制执行加性噪声以保证差分隐私（Differential Privacy，DP）可以被放大；（3）最终性能容易受到超参数的影响。导致这些现象的一个关键因素是本地客户端联合优化两个低秩矩阵与中央服务器单独聚合它们之间的不一致。因此，文献 [41] 提出了一种高效且有效的 LoRA 版本，即 FFA-LoRA（Federated Freeze A LoRA），以应对这些挑战，并进一步将联合微调大语言模型的成本减半。FFA-LoRA 的核心思想是固定随机初始化的非零矩阵，仅对零初始化的矩阵进行微调。与 LoRA 相比，FFA-LoRA 是出于在隐私保护联邦学习中实际和理论上的优势而提出的。

随着用户之间的数据变得更加多样化，完全微调模型和采用高效参数微调（Parameter-Efficient Fine-Tuning，PEFT）方法之间的差距会扩大。为了弥合这一性能差距，文献 [42] 提出了一种名为 SLoRA 的方法，该方法通过一种新的数据驱动初始化技术克服了 LoRA 在高异构数据场景中的关键限制。

3.2.2　基于提示调优的改进

提示调优是一种针对大语言模型的优化方法，通过设计特定的提示（Prompt）引导大语言模型生成更符合任务需求的输出，而无须对模型的内部参数进行大规模的微调。

文献 [43] 提出了一种具有自适应优化参数的高效提示调优方法 FedPepTAO，以实现大语言模型。首先，提出了一种高效的部分提示调优方法，以同时提高性能和效率。其次，开发了一种新的自适应优化方法来解决设备和服务器端的客户端漂移问题，以进一步提高性能。

为了在克服内存限制和保护隐私的同时以最佳方式利用每个本地数据集，文献 [44] 提出了联合黑盒提示调优（Federated Black-box Prompt Tuning，Fed-BPT）。这种创新方法避免了对参数架构和私有数据集访问的依赖，而是利用中央服务器来帮助本地用户通过定期聚合协作训练提示生成器。

3.2.3 基于预训练模型的改进

文献 [45] 提出了一种新颖的联邦学习策略，称为 FedYolo，它利用预训练转换器（Pretrained Transformers，PTF）的规模和模块化优势来应对 Non-IID 数据挑战。研究表明，扩大模型规模能够提高异构环境下的准确性和鲁棒性，同时减少通信需求。模块化设计进一步降低了通信成本，提升了泛化能力，并允许单个 PTF 同时处理多个任务，减少灾难性遗忘。在 FedYolo 中，客户端仅需要加载一次完整的 PTF 模型，后续更新通过高效模块完成，每个任务拥有独立模块，从而实现通信高效和模型稳健的学习过程。

3.3 多模态数据场景

随着多模态数据在人工智能领域的广泛应用，从跨模态数据中高效提取信息成为一项关键挑战。联邦学习作为一种有效的解决方案，能够聚合来自多个任务或模态的模型信息，构建出性能更强的集中式模型。本小节对多模态联邦学习中的多种优化方案进行了综述，涵盖了基于原型学习、知识蒸馏、对比学习以及其他创新技术的方法。

3.3.1 基于原型学习的方案

当前的多模态联邦学习（Multimodal Federated Learning，MFL）方法通常在所有模态之间统一分配计算频率，这对于资源有限的物联网设备来说效率低下。针对这一问题，文献 [46] 提出了 FlexMod，这是一种提高 MFL 计算效率的新方法，它根据每个模态编码器的重要性和训练要求自适应地分配训练资源。FlexMod 采用原型学习来评估模态编码器的质量，使用 Shapley 值来量化每种模态的重要性，并采用深度强化学习中的深度确定性策略梯度（Deep Deterministic Policy Gradient，DDPG）方法来优化训练资源的分配，从而优先考虑关键模态，优化模型性能和资源利用率。

文献 [47] 采用共注意力机制整合不同模态的互补信息，从而实现更有效的信息融合。在此基础上，提出了一种增强的联邦学习算法，能够学习不同模态中的有用全局特征，并通过联合训练的方式为所有客户端构建一个通用模型。此外，为了进一步优化模型性能，引入了基于模型不可知元学习（Model-Agnostic Meta-Learning，MAML）的个性化方法，针对每个客户端的具体需求对最终模型进行定制化调整。

3.3.2 基于知识蒸馏的方案

知识蒸馏是另一种在多模态联邦学习中提高效率和性能的技术。文献 [48] 提出了一个为异构多模态联邦学习量身定制的微调框架，称为联邦双适配器教师（Federated Dual-Aadapter Teacher，FedDAT）。具体来说，该框架利用双适配器教师（Dual-Adapter Teacher，DAT）来解决数据异构问题，方法是规范客户端本地更新并应用互知蒸馏（Mutual Knowledge Distillation，MKD）进行有效的知识转移。

现有的联邦学习算法通常要求客户端和服务器部署相同架构的模型，但受限于客户端有限的资源，难以训练大型模型。为此，文献 [49] 提出了一种名为 Fed-ET 的新型集成知识转移方法。Fed-ET 在客户端训练小型异构模型，并利用这些模型在服务器上训练大型模型。与传统集成学习不同，Fed-ET 利用客户端数据的异构性，通过多样性正则化的加权一致性蒸馏方案，从集成样本中提取可靠共识并提升泛化能力。

文献 [50] 提出了一个即插即用知识构成（Knowledge Composition，KC）模块，该模块允许在不共享原始数据的情况下在客户端之间交换知识，通过一种有效的方法来计算基于客户端之间的共享知识定义的一致性损失，这使得在不同客户端上训练的模型能够对相似数据实现类似的预测，从而解决多语言联邦自然语言理解中数据异构性的挑战。

3.3.3 基于对比学习的方案

现有的多模态联邦学习方法通常依赖单模态级别的模型聚合，这限制了同种模态下的服务器模型和客户端模型必须具有相同的模型架构。为了解决这一问题，文献 [51] 提出了多模态联邦学习的对比表示集成和聚合方法 CreamFL，这是一个多模态联邦学习框架，能够在具有异构模型架构和数据模态的客户端上训练更大的服务器模型，同时只在公共数据集上交流知识。为了实现更好的多模态表示融合，CreamFL 设计了一个全局-局部跨模态集成策略

来聚合客户端表示。为了减轻由多模态差异引起的两个前所未有的异质性因素（模态差距和任务差距）造成的局部模型漂移，又进一步提出了两种模态间和模态内对比方法来规范本地训练，补充了单模态客户的缺失模态信息，并使本地客户端向全球共识迈进。

3.3.4　其他方案

在联邦学习领域，传统的算法往往难以应对客户端之间普遍存在的域转移问题，这导致模型泛化能力受限。为了应对这一挑战，文献 [52] 提出了一种新方法，称为联合双提示调整（Federated Dual Prompt Tuning，Fed-DPT）。Fed-DPT 方法利用预先训练的视觉语言模型，通过应用视觉和文本提示调整来促进对分散数据的域适应。这种方法通过快速学习技术解决了域转移的问题，其广泛的实验结果证明了其在领域感知联邦学习中的显著有效性。

此外，文献 [53] 研究了命名实体识别（Named Entity Recognition，NER）的联合域适应问题，提出了一种从异构标签集进行蒸馏的方法，以实现更好的域适应。文献 [54] 提出了拆分学习（Split Learning，SL）来实现模块化分解，并使单模态局部模型能够互补聚合，进一步扩展了多模态联邦学习的应用范围。

4　未来展望

随着联邦学习在异构数据环境中的应用不断拓展，未来的研究方向将聚焦开发创新解决方案以应对 Non-IID 数据带来的挑战，以下是一些关键领域和新兴趋势。

4.1　评估与基准测试

未来研究需要开发更复杂的评估和基准方法，以应对现实世界中多种数据偏斜（如标签偏斜、特征偏斜和数量偏斜）同时存在的复杂情况。通过建立全面的分区协议和标准化的数据异构度量方法，可以更准确地评估算法性能，并推动更具适应性和鲁棒性的联邦学习算法的发展。

4.2　模型泛化与任务适应

随着人工智能对多模态信息融合的需求日益增长，联邦学习提供了一种有效的解决方案，能够将分散在不同边缘设备上的多个小型模型的知识整合到服务器端的大型模型中。这种方法不仅能够保护数据隐私，还能充分利用边缘设备的计算资源。

因此，研究者们应当探寻更高效的知识聚合机制，使得服务器端的大型模型能够更快地从客户端的小型模型中学习到有用的知识。这将促进跨设备、跨领域的知识共享，以适应不同模态数据的特点，推动人工智能技术在更广泛场景下的应用和发展，将其拓展到自然语言处理、语音识别和时间序列分析等多模态数据密集型领域。

4.3　通信效率优化

随着联邦学习系统规模的不断扩大和复杂性的增加，优化通信协议变得尤为关键，以应对服务器与客户端之间参数传递过程中耗时增加的问题。未来的研究方向可以集中在设计先进的数据压缩技术，这些技术将专门针对异构数据环境，以减少通信开销同时确保模型更新的完整性。此外，研究者们也将探索减少传递模型参数数量的方法，进一步使模型训练和参数传递过程更加轻量。

4.4　隐私保护增强

尽管联邦学习本身具有一定的隐私保护性，但随着模型规模的增加和应用场景的复杂化，仍然存在数据泄露的风险。差分隐私和同态加密等技术可以在此基础上进一步提高加密程度。

5　结束语

联邦学习作为一种分布式机器学习框架，在保护数据隐私的同时，能够充分利用异构数据进行联合建模。本文对于联邦学习中异构数据的处理进行了全面的技术调查，为未来在更多模态场景下的联邦学习方案研究奠定了坚实基础。隐私保护技术的不断创新将进一步巩固联邦学习在数据安全领域的优势。随着技术的不断突破和产业融合的加深，联邦学习有望在人工智能的发展中发挥更大的作用。

参考文献：

[1] MCMAHAN B，MOORE E，RAMAGE D，et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial Intelligence and Statistics. PMLR，2017：1273-1282.

[2] YUROCHKIN M，AGARWAL M，GHOSH S，et al. Bayesian nonparametric federated learning of neural networks[C]//International conference on machine learning. PMLR，2019：7252-7261.

[3] CHEN X，CHEN T，SUN H，et al. Distributed training with heterogeneous data：Bridging median-and mean-based algorithms[J]. Advances in Neural Information Processing Systems，2020，33：21616-21626.

[4] LI X，HUANG K，YANG W，et al. On the convergence of FedAvg on Non-IID data[J]. arXiv preprint，arXiv：1907.

02189，2019.

[5] CHEN C，FENG X，ZHOU J，et al. Federated large language model：A position paper[J]. arXiv preprint，arXiv：2307. 08925，2023.

[6] CHE L，WANG J，ZHOU Y，et al. Multimodal federated learning：A Survey[J]. Sensors，2023，23（15）：6986.

[7] AAMER B，CHERGUI H，BENJILLALI M，et al. Entropy-driven stochastic federated learning in Non-IID 6G edge-ran[J]. Frontiers in Communications and Networks，2021，2：739414.

[8] YANG H，FANG M，LIU J. Achieving linear speedup with partial worker participation in Non-IID federated learning[J]. arXiv preprint，arXiv：2101. 11203，2021.

[9] ZAWAD S，ALI A，CHEN P Y，et al. Curse or redemption? How data heterogeneity affects the robustness of federated learning[C]//Proceedings of the AAAI conference on artificial intelligence. 2021，35（12）：10807-10814.

[10] PARK C，CHOI T，KIM T，et al. FedGeo：Privacy-preserving user next location prediction with federated learning[C]//Proceedings of the 31st ACM International Conference on Advances in Geographic Information Systems. ACM，2023：1-10.

[11] ORTIGOSA-HERNÁNDEZ J，INZA I，LOZANO J A. Measuring the class-imbalance extent of multi-class problems[J]. Pattern Recognition Letters，2017，98：32-38.

[12] QU L，ZHOU Y，LIANG P P，et al. Rethinking architecture design for tackling data heterogeneity in federated learning[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. IEEE，2022：10061-10071.

[13] LI A，SUN J，WANG B，et al. LotteryFL：Personalized and communication-efficient federated learning with lottery ticket hypothesis on Non-IID datasets[J]. arXiv preprint，arXiv：2008. 03371，2020.

[14] JIMENEZ G D M，ANAGNOSTOPOULOS A，CHATZIGIANNAKIS I，et al. FedArtML：A tool to facilitate the generation of Non-IID datasets in a controlled way to support federated learning research[J]. IEEE Access，2024，12：2169-3536.

[15] TAN Q，WU S，TAO Y. Privacy-enhanced federated learning for Non-IID data[J]. Mathematics，2023，11（19）：4123.

[16] XU Y，LI Y，LUO H，et al. FBLG：A local graph based approach for handling dual skewed Non-IID data in federated learning[C]//Proceedings of the 33rd International Joint Conference on Artificial Intelligence. International Joint Conferences on Artificial Intelligence Organization. 2024，8：5289-5297.

[17] ZHANG L，GAO G，ZHANG H. Spatial-temporal federated learning for lifelong person re-identification on distributed edges[J]. IEEE Transactions on Circuits and Systems for Video Technology，2025，35（2）：1884-1896.

[18] SHU J，YANG T，LIAO X，et al. Clustered federated multitask learning on Non-IID data with enhanced privacy[J]. IEEE Internet of Things Journal，2022，10（4）：3453-3467.

[19] LUO G，CHEN N，HE J，et al. Privacy-preserving clustering federated learning for Non-IID data[J]. Future Generation Computer Systems，2024，154：384-395.

[20] HALLER M，LENZ C，NACHTIGALL R，et al. Handling Non-IID data in federated learning：An experimental evaluation towards unified metrics[C]//2023 IEEE International Conference on Dependable，Autonomic and Secure Computing，International Conference on Pervasive Intelligence and Computing，International Conference on Cloud and Big Data Computing，International Conference on Cyber Science and Technology Congress. IEEE，2023：762-770.

[21] CHEN A，FU Y，SHA Z，et al. An EMD-based adaptive client selection algorithm for federated learning in heterogeneous data scenarios[J]. Frontiers in Plant Science，2022，13：908814.

[22] ZHAO H. Non-IID quantum federated learning with one-shot communication complexity[J]. Quantum Machine Intelligence，2023，5（1）：3.

[23] HSIEH K，PHANISHAYEE A，MUTLU O，et al. The Non-IID data quagmire of decentralized machine learning[C]//International Conference on Machine Learning. PMLR，2020：4387-4398.

[24] TAN Y，LONG G，MA J，et al. Federated learning from pre-trained models：A contrastive learning approach[J]. Advances in Neural Information Processing Systems，2022，35：19332-19344.

[25] LI G，WU W，SUN Y，et al. Visual prompt based personalized federated learning[J]. arXiv preprint，arXiv：2303. 08678，2023.

[26] TAN Y，LONG G，LIU L，et al. FedProto：Federated prototype learning across heterogeneous clients[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2022，36（8）：8432-8440.

[27] WEN H，WU Y，HU J，et al. Communication-efficient federated learning on Non-IID data using two-step knowledge distillation[J]. IEEE Internet of Things Journal，2023，10（19）：17307-17322.

[28] HAN S，PARK S，WU F，et al. FedX：Unsupervised federated learning with cross knowledge distillation[C]//European Conference on Computer Vision. Cham：Springer Nature Switzerland，2022：691-707.

[29] ZHUANG W，WEN Y，LYU L，et al. MAS：Towards resource-efficient federated multiple-task learning[C]//Proceedings of the IEEE/CVF International Conference on Computer Vision. IEEE，2023：23414-23424.

[30] LI Q，HE B，SONG D. Model-contrastive federated learning[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. IEEE，2021：10713-10722.

[31] LI Z，SHAO J，MAO Y，et al. Federated learning with GAN-based data synthesis for Non-IID clients[C]//International Workshop on Trustworthy Federated Learning. Cham：Springer International Publishing，2022：17-32.

[32] GUO W，YAO Z，LIU Y，et al. A new federated learning model for host intrusion detection system under Non-IID data[C]//2023 IEEE International Conference on Systems，Man，and Cybernetics（SMC）. IEEE，2023：494-500.

[33] AVELINO J G, CAVALCANTI G D, CRUZ R M. Resampling strategies for imbalanced regression: A survey and empirical analysis[J]. Artificial Intelligence Review, 2024, 57(4): 82.

[34] KANG Y，FAN T，GU H，et al. Grounding foundation models through federated transfer learning：A general framework[J]. arXiv preprint，arXiv：2311. 17431，2023.

[35] LI T，SAHU A K，ZAHEER M，et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems，2020，2：429-450.

[36] KARIMIREDDY S P，KALE S，MOHRI M，et al. SCAFFOLD：Stochastic controlled averaging for federated learning[C]//International Conference on Machine Learning. PMLR，2020：5132-5143.

[37] WANG J，LIU Q，LIANG H，et al. Tackling the objective inconsistency problem in heterogeneous federated optimization[J]. Advances in Neural Information Processing Systems，2020，33：7611-7623.

[38] ZHANG X，LI Y，LI W，et al. Personalized federated learning via variational Bayesian inference[C]//International Conference on Machine Learning. PMLR，2022：26293-26310.

[39] TANG Z，ZHANG Y，SHI S，et al. Virtual homogeneity learning：Defending against data heterogeneity in federated learning[C]//International Conference on Machine Learning. PMLR，2022：21111-21132.

[40] YI L，YU H，WANG G，et al. pFedLoRA：Model-heterogeneous personalized federated learning with LoRA tuning[J]. arXiv preprint，arXiv：2310. 13283，2023.

[41] SUN Y，LI Z，LI Y，et al. Improving LoRA in privacy-preserving federated learning[J]. arXiv preprint，arXiv：2403. 12313，2024.

[42] BABAKNIYA S，ELKORDY A R，EZZELDIN Y H，et al. SLoRA：Federated parameter efficient fine-tuning of language models[J]. arXiv preprint，arXiv：2308. 06522，2023.

[43] CHE T，LIU J，ZHOU Y，et al. Federated learning of large language models with parameter-efficient prompt tuning and adaptive optimization[J]. arXiv preprint，arXiv：2310. 15080，2023.

[44] LIN Z，SUN Y，SHI Y，et al. Efficient federated prompt tuning for black-box large pre-trained models[J]. arXiv preprint，arXiv：2310. 03123，2023.

[45] ZHANG X，LI M，CHANG X，et al. FedYolo：Augmenting federated learning with pretrained transformers[J]. arXiv preprint，arXiv：2307. 04905，2023.

[46] BIAN J，WANG L，XU J. Prioritizing modalities：Flexible importance scheduling in federated multimodal learning[J]. arXiv preprint，arXiv：2408. 06549，2024.

[47] XIONG B，YANG X，QI F，et al. A unified framework for multi-modal federated learning[J]. Neurocomputing，2022，480：110-118.

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

[49] CHO Y J，MANOEL A，JOSHI G，et al. Heterogeneous ensemble knowledge transfer for training large models in federated learning[J]. arXiv preprint，arXiv：2204. 12703，2022.

[50] WANG H，ZHAO H，WANG Y，et al. FedKC：Federated knowledge composition for multilingual natural language understanding[C]//Proceedings of the ACM Web Conference 2022. 2022：1839-1850.

[51] YU Q，LIU Y，WANG Y，et al. Multimodal federated learning via contrastive representation ensemble[J]. arXiv preprint，arXiv：2302. 08888，2023.

[52] WEI G，WANG F，SHAH A，et al. Dual prompt tuning for domain-aware federated learning[J]. arXiv preprint，arXiv：2310. 03103，2023.

[53] WANG R，YU T，WU J，et al. Federated domain adaptation for named entity recognition via distilling with heterogeneous tag sets[C]//Findings of the Association for Computational Linguistics：ACL 2023. 2023：7449-7463.

[54] ZHANG Z，QI F，XU C. Enhancing storage and computational efficiency in federated multimodal learning for large-scale models[C]//41st International Conference on Machine Learning. PMLR，2024：59685-59699.