arXiv:2305.00771v1 [cs.LG] 1 May 2023

迈向联邦开放世界半监督学习中的无偏训练

Jie Zhang [1] **Xiaosong Ma** [1] **Song Guo** [1] **Wenchao Xu** [1]

摘要

联邦半监督学习（FedSSL）已成为一种新范式，使分布式客户端能够利用稀缺的有标签数据和丰富的无标签数据协同训练机器学习模型。然而，现有的 FedSSL 研究依赖于封闭世界假设，即所有本地训练数据和全局测试数据均来自有标签数据集中已观察到的已见类。至关重要的是，我们还需更进一步：使联邦学习模型适应开放世界设置，其中无标签数据中存在未见类别。本文提出一种新颖的**联邦开**放世界**半**监督**学**习**习**框架（**FedoSSL**），可解决分布式开放世界设置中的关键挑战，即针对异质分布未见类别的训练过程存在偏差。具体而言，由于某个未见类别是否出现取决于客户端，本地未见类别（存在于多个客户端）相比全局未见类（仅存在于一个客户端）可能获得差异化的更优聚合效果。我们采用不确定性感知抑制损失，以缓解本地未见类别与全局未见类之间的训练偏差。此外，我们在全局聚合中加入校准模块，以避免不同客户端之间数据分布不一致所导致的潜在冲突性知识迁移。所提出的 FedoSSL 可轻松适配最先进的联邦学习方法，并通过在基准数据集和真实世界数据集（CIFAR-10、CIFAR-100 和 CINIC-10）上进行的大量实验得到验证。

1. 引言

为解决分布式机器学习中的隐私问题，联邦学习（FL）（McMahan 等人，2017年；Zhang 等人，2021b）已成为一种颇具前景的范式，通过多个客户端协同训练共享模型，而无需泄露其私有原始数据。在联邦学习中，通常由中心化服务器定期对来自分布式客户端的更新后模型参数求平均，以获得全局模型。现有联邦学习方法假设客户端的数据均带有标签，因此可在各客户端进行监督学习以更新本地模型；然而，在一些真实世界应用中，数据标注过程可能因开销巨大且需要相应的专业知识而难以实施（Ouali 等人，2020年），例如医学诊断（Ng 等人，2021年）和目标检测（Liu 等人，2021年）。

稀缺的有标签数据和丰富的无标签数据促成了联邦半监督学习（联邦半监督学习，FedSSL）的兴起（Jeong 等人，2021年；Liang 等人，2022年），它能够同时利用有标签和无标签数据，在分布式环境中优化全局模型。现有的联邦半监督学习方案已证明，可以基于少量有标签数据，在客户端或服务器端训练模型（Jin 等人，2020年；Long 等人，2020年）。然而，这些工作依赖封闭世界假设，即所有本地训练数据和全局测试数据都来自有标签数据集中包含的同一组类别（Zhou，2022年；Boult 等人，2019年），这在实际场景中往往并不成立。相比之下，开放世界设置允许进行新类别发现，因此常见于真实场景数据。例如，在医学图像分类任务中，某些疾病本就较为罕见，且从未被标注过，而模型可能既需要将图像分类到预定义类型（已见类），又需要发现新的未知疾病（未见类别）。因此，一个新的基本问题随之产生：如何在开放世界设置下，基于分布式数据协同训练模型，使其能够对已见类和未见类别进行分类？

为此，我们首先构建了一个新的联邦半监督学习基准，将传统的封闭世界训练框架扩展到开放世界设置。令人惊讶的是，研究表明，由于

[1]香港理工大学计算学系，中国香港。通讯作者：Song Guo<song.guo@polyu.edu.hk>。

arXiv 预印本。

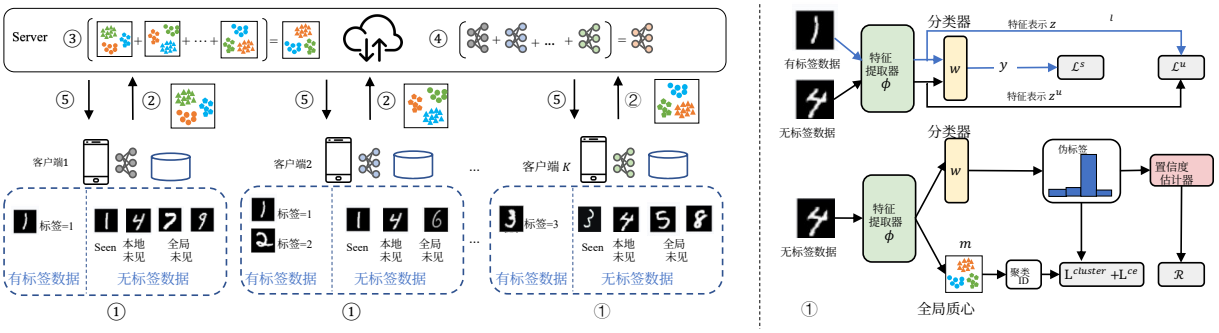


图 1：所提出的 FedoSSL 算法框架。 **流程**： ① **本地训练：** 每个客户端首先在其私有数据集上进行若干轮本地训练（即通过优化公式（1）中的损失函数），然后通过基于 Sinkhorn-Knopp 的聚类算法计算本地质心（Genevay 等人， 2019年）。 ② 将模型参数和本地质心上传至服务器。 ③ 服务器执行标准的模型聚合。 ④ 服务器再次使用 Sinkhorn-Knopp 聚类执行质心聚合，以获得全局质心。 ⑤ 全局模型和全局质心会返回给客户端，客户端使用它们进行本地训练。

训练过程中无标签数据中存在未见类别，模型性能会显著下降。尽管已有少数研究探讨未见类别问题，以避免将来自未见类别的无标签样本误分类为已见类别，同时缓解已见类与未见类别之间不理想的性能差距（Cao等人，2022年；Guo等人，2022年），但尚无文献在分布式环境中考虑这一问题。在存在多个参与方的情况下，问题定义有所不同：从全局视角来看，一个客户端中的某些未见类别可能在其他客户端中存在，因此需要对未见类别进行新颖的细粒度定义，并为不同类型的样本/类别设计训练机制。值得一提的是，由于不同客户端之间的类别分布存在异质性，简单地按照传统联邦学习机制聚合参数，可能导致拥有不同未见类别的客户端在训练过程中产生偏差。

为应对上述挑战，本文提出了一种全新的**联邦开**放世界**半**监督**学习**框架（FedoSSL），能够在不同类型的样本之间实现无偏训练过程。具体而言，我们首先将本地客户端中的未见类别重新定义为局部未见类别和全局未见类别。随后，我们设计了一种不确定性感知抑制损失，以自适应地控制局部未见类别与全局未见类别之间不期望的训练偏差；也就是说，由于跨客户端协作，局部未见类别通常比全局未见类别具有更高的训练效率。此外，考虑到不同客户端之间异质分布的未知类别可能在聚合阶段导致潜在的冲突性知识迁移，我们引入了一个校准模块，以生成相应的全局质心，从而在每个客户端上执行专门的本地调整。实验表明，我们的方法能够显著提升开放世界场景下的模型准确率；与广泛使用的模型（即 ResNet-18）和下游任务（即 CIFAR-10、CIFAR-100、CINIC-10）上的最先进基线方法相比，均取得了更好的性能。本文的贡献总结如下。

- 据我们所知，我们是首个考虑 FedSSL 中开放世界设置的研究，其中未见类别存在于未标记数据中；由于未见类别呈异质分布，这一设置极具挑战性。
- 我们设计了一种全新的 FedoSSL 框架，可在不同类型的类别（即局部未见类和全局未见类）之间实现无偏学习，并在数据分布异构的情况下实现校准的知识聚合。
- 我们在三种典型的图像分类任务上进行了大量实验。实验结果表明，FedoSSL 的性能优于现有最先进的方法。

2. 相关工作

2.1. 联邦学习

联邦学习（FL）已成为一种颇具前景的范式，能够在保护隐私的同时，利用去中心化训练数据协同训练机器学习模型。作为最流行的监督式联邦学习训练框架，FedAvg（McMahan 等人，2017年）会定期在服务器端聚合本地更新，并将平均后的模型传回本地客户端，以进行下一轮训练。在联邦学习中，非独立同分布数据是主要挑战之一，因为它会导致权重发散和性能下降（Li 等人，2020b年）。人们已提出许多解决这一问题的方法，例如：

表1：我们提出的 FedoSSL 与其他半监督学习相关方法的比较。

方法	训练数据集 已见类	训练数据集 未见类别	测试数据集 已见类	测试数据集 未见类别	联邦学习环境?
SSL	存在	不存在	分类	-	×
开放集半监督学习	存在	存在	分类	检测并拒绝	×
新类别发现	存在	存在	-	发现与聚类	×
开放世界半监督学习	存在	存在	分类	发现与聚类	×
联邦半监督学习	存在	不存在	分类	-	√
FedoSSL	存在	存在	分类	发现与聚类	√

在客户端之间共享公共数据集，以获得近似独立同分布的数据（Zhao 等人，2018年；Yoshida 等人，2019年）、数据增强（Jeong 等人，2018年）、知识蒸馏（Li 和 Wang，2019年；Lin 等人，2020年）、基于正则化的方法（Fallah 等人，2020年；Li 等人，2020a年），甚至个性化联邦学习（Collins 等人，2021年；Zhang 等人，2021a）。然而，半监督设置下的联邦学习尚未得到充分研究。

2.2. 半监督学习

半监督学习（SSL）是指利用部分标注数据进行学习的一般问题，尤其是在有标签数据量远小于无标签数据量时（Zhou & Li，2005年；Rasmuset al.，2015年）。半监督学习主要可分为两类：伪标签和一致性正则化。伪标签方法（Lee et al.，2013年；Pham et al.，2021年；Zou etal.，2020年）通常利用在有标签数据上训练的模型为无标签数据生成人工标签，并将筛选出的高置信度标签作为无标签数据训练的监督信号。一致性正则化方法（Tar-vainen & Valpola，2017年；Weiet al.，2020年；Lee et al.，2022年）着重通过最小化同一输入的不同扰动输出之间的距离来训练模型。上述所有文献都假设处于封闭世界设置中，即有标签数据和无标签数据来自同一组预定义类别。然而，这一假设在现实世界的应用数据中很少成立，即无标签数据中会出现未见类别。近期有两条与不同场景相关的研究路线：

开放集半监督学习。开放集半监督学习认为，无标签样本中的未见类别仅存在于训练数据中，而不存在于测试数据中（Chen等人，2020b年；Guo等人，2020年；Huang等人，2021年；Saito等人，2021年）。其目标是检测这些未见类别并将其拒绝，以确保已见类的性能不会下降。

新类别发现（NCD）。与无法对未见类别进行分类的开放集半监督学习不同，NCD（Han等人，2019年；Hsu等人，2019年；Zhong等人，2021年）旨在测试阶段对已见类和未见类别进行分类，但假设训练数据中的所有无标签实例都属于未见类别。

为了将未见类别扩展到更实际的场景，开放世界半监督学习（Cao等人，2022年；Guo等人，2022年）致力于解决有标签数据与无标签数据之间的类别不匹配问题；在测试时，每个测试样本都应被分类为现有类别之一或新的未见类别。

2.3. 联邦半监督学习

在保护数据隐私的同时从去中心化数据中学习表示仍然是一个新兴领域。现有的联邦半监督学习框架根据有标签数据的位置可分为两类：1）标签位于服务器（Labels-at-Server）假设客户端拥有纯无标签数据，而服务器包含少量有标签数据（Lin等人，2021年；He等人，2021年；Zhang等人，2021c年；Diao等人，2022年）；2）标签位于客户端（Labels-at-Client）认为本地客户端拥有有标签数据（Jeong等人，2021年；Lin等人，2021年；Liang等人，2022年），该类型还可进一步细分为两种场景：a）每个客户端同时包含有标签数据和无标签数据（Jeong等人，2021年）；b）部分客户端拥有全部有标签数据，而部分客户端仅包含无标签样本（Lin等人，2021年；Liang等人，2022年；Liu等人，2021年）。本文关注类型2.a，因为这一类型在很大程度上被忽视了，并且在真实世界的联邦学习场景中更为普遍。

2.4. 总结

总而言之，在联邦半监督学习中考虑未见类别的存在仍是一项空白。更重要的是，多个客户端之间的数据异质性为开放世界框架与传统联邦半监督学习框架的结合带来了新的挑战：如何高效地处理客户端之间异质的未见类别？受上述观察启发，我们致力于开发一种新颖的联邦开放世界半监督学习框架，以在已见类和未见类别上均取得优异性能。我们提出的 FedoSSL 与其他半监督学习相关方法之间的详细比较如表1所示。

3. 方法

本节首先定义问题，并详细介绍所提出的 FedoSSL 框架。该框架包含用于本地训练的不确定性感知抑制损失，以及用于模型聚合的校准模块。随后，我们将在第3.3节介绍优化过程。

3.1. 预备知识与问题定义

我们关注开放世界设定下的联邦半监督学习，其中每个客户端的数据均为部分有标签，且有标签数据与无标签数据中的类别集合并不相同，即无标签数据中存在未见类别。假设有 K 个客户端，每个客户端 i 持有一个私有分类数据集，其中包含有标签部分 $\mathcal{D}_i^l = \{(x_j,\ y_j)\}_{j=1}^{n_i^l}$ 和无标签部分$\mathcal{D}_i^u = \{(x_j)\}_{j=1}^{n_i^u}$，其中 $n_i^l \ll n_i^u$，$x \in \mathbb{R}^N$，$1 \le i \le K$。整个有标签数据集和无标签数据集分别表示为 $\mathcal{D}^l = \{\mathcal{D}_i^l\}_{i=1}^K$ 和 $\mathcal{D}^u = \{\mathcal{D}_i^u\}_{i=1}^K$。我们将全部有标签数据中已见类别的集合记为 $\mathcal{C}^l$，将无标签测试数据中的类别集合记为 $\mathcal{C}^u$。不同于传统的（封闭世界）联邦半监督学习，即 $\mathcal{C}^l = \mathcal{C}^u$，本文考虑 $\mathcal{C}^l \neq \mathcal{C}^u$，并分别用 $\mathcal{C}_{seen} = \mathcal{C}^l \cap \mathcal{C}^u$、$\mathcal{C}_{unseen} = \mathcal{C}^u \setminus \mathcal{C}_{seen}$ 表示已见类别和未见类别的集合。

FedSSL 的目标是利用多个去中心化客户端训练一个泛化的全局模型f，其参数为 θ，即 $\min_\theta \mathcal{L}(\theta)$: $= \sum_{i=1}^K \frac{n_i}{n} \mathcal{L}_i(\theta)$，其中 $n_i = n_i^l + n_i^u$和$n = \sum_{i=1}^K n_i$ 是数据总量。 $\mathcal{L}_i(\theta)$ 是客户端 i的训练损失函数。具体而言，模型 f可分解为一个参数为ϕ的特征提取器 g：$\mathbb{R}^N \to \mathbb{R}^d$，用于学习低维特征 z；以及一个参数为 w的分类器 h： $\mathbb{R}^d \to \mathbb{R}^{|\mathcal{C}_{seen} \cup \mathcal{C}_{unseen}|}$。每个客户端 i 上的半监督学习算法的训练损失通常包含有监督损失 $\mathcal{L}_i^s$ 和无监督损失 $\mathcal{L}_i^u$，其权重参数为 α、 $\alpha > 0$:

$$\mathcal{L}_i = \mathcal{L}_i^s + \alpha \mathcal{L}_i^u \tag{1}$$

通常， $\mathcal{L}_i^s$ 对带标签的样本应用标准交叉熵损失:

$$\mathcal{L}_i^s = \frac{1}{n_i^l} \sum_{(x_j, y_j) \in \mathcal{D}_i^l} \mathcal{H}(y_j, p(x_j; \theta)) \tag{2}$$

其中， $p(x;\ \theta)$ $=$Softmax($f(x;\ \theta)$) 表示模型 f 对输入 x生成的预测概率，而$\mathcal{H}(\cdot,\ \cdot)$ 是交叉熵函数。

在无监督损失方面 $\mathcal{L}_i^u$，有两种典型形式：**伪标签**(Sohn等人，2020年），基于有标签数据；以及一**致性正则化**(Xie等人，2020年），基于数据增强。然而，在开放世界场景中，未见类别的存在使上述方法无法对已见类和未见类别进行分类。因此，与 ORCA（Cao等人，2022年）和 NACH（Guo等人，2022年）类似，我们将成对目标用作无标签数据上的无监督损失，以对未见类别进行分类:

$$\mathcal{L}_i^u = -\frac{1}{n_i^l + n_i^u} \sum_{\substack{z_j, \bar{z}_j \in \\ (Z_i^l \cup Z_i^u, \bar{Z}_i^l \cup \bar{Z}_i^u)}} \mathcal{H}(p(w^\top \cdot z_j), p(w^\top \cdot \bar{z}_j)) \tag{3}$$

其中， Z_i^l和 Z_i^u分别是有标签数据和无标签数据的全部特征表示集合。 $\bar{Z}_i^l \cup \bar{Z}_i^u$是通过计算所有特征表示对之间的余弦距离，在一个小批量中与 $Z_i^l \cup Z_i^u$最接近的集合。

3.2. FedoSSL 概述

以往的联邦半监督学习方法未考虑每个客户端上未见类别的存在，这导致大量来自未见类别的数据被误分类为已见类。此外，不同客户端之间不一致的数据分布又带来了另一个新问题：某些未见类别可能存在于多个客户端中，导致不同未见类别之间的训练存在偏差，例如，在图 1 中，客户端1、2和 K 都拥有类别4，而类别5、6、7、8和9只存在于其中一个客户端。在这种情况下，我们需要从全局视角对未见类别进行更细粒度的定义。

定义 1（局部未见类和全局未见类）。 在 FedoSSL 中，客户端 i 上的未见类别 $\mathcal{C}_{i,unseen}$ 可分为两种类型：局部未见类$\mathcal{C}_{i,lu}$，其中$\mathcal{C}_{i,lu} = \mathcal{C}_{1,unseen} \cap \cdots \cap \mathcal{C}_{K,unseen}$；以及全局未见类 $\mathcal{C}_{i,gu}$，其中 $\mathcal{C}_{i,gu} = \mathcal{C}_{i,unseen} \setminus \mathcal{C}_{i,lu}$。

当 Fe-doSSL 中多个客户端存在未见类别时，需要考虑两个主要挑战。首先，由于客户端协作有助于学习局部未见类，局部未见类的学习速度可能快于全局未见类。现有的无监督成对损失 $\mathcal{L}_i^u$对每个类别一视同仁，而未见类别之间不均衡的训练进度会导致伪标签生成出现较大偏差，甚至使已见类的性能下降。因此，我们提出一种不确定性感知正则化损失，以缓解不同类别之间的训练偏差。此外，对无标签数据使用特征级无监督成对损失，会导致不同客户端生成的聚类/类别标识符不一致，因为有标签数据和无标签数据都需要输入同一个模型分类器。在模型聚合阶段，设计一种校准策略来对齐同一未见类的输出至关重要。

3.2.1. 目标

为了在联邦半监督学习中实现不同未见类别之间的无偏训练，我们提出了 FedoSSL 方法。整体目标由三部分组成：1）基础

适用于全部数据的半监督损失；2）不确定性感知正则化损失，用于缩小局部未见类别与全局未见类别之间的训练差距；3）校准损失，用于实现高效的模型聚合：

$$\mathcal{L}_i^* = \mathcal{L}_i + \beta\mathcal{R}_i + \gamma\mathcal{L}_i^{cal} \tag{4}$$

其中，β 和 γ 为权衡超参数。

3.2.2. 不确定性感知损失

考虑到不同类型的未见类别具有不同的训练进度，即本地未见类别可以通过模型协作得到促进，我们尝试添加一个正则化项，以减轻本地未见类别与全局未见类别之间的训练偏差。具体而言，我们使用生成的聚类/类别标识符的不确定性来反映训练进度，并对不确定性较高的样本施加更大的惩罚项。因此，不确定性感知损失可定义为：

$$\mathcal{R}_i = \frac{1}{n_i^u}\sum_{x_j^u \in \mathcal{D}_i^u} |\pi(x_j^u)| \tag{5}$$

其中，$\pi(\cdot)$为数据不确定性函数。为了精确评估不确定性，我们同时依据由Softmax函数输出计算出的伪标签置信度，以及属于相关伪标签的样本比例，即，

$$\pi(x_j^u) = \rho(n^c|\arg\max_c p(x_j^u;\theta))[1-\max_c p(x_j^u;\theta)] \tag{6}$$

其中，$\rho(n^c) = -\tau^{1-\frac{n^c}{n_{\text{最大}}}}$是类别 c的权重，可根据有标签数据估计，$\tau \in (0,1]$。n^c 是模型预测为类别 c 的训练样本数。$n_{\max}$ 是样本数最多的类别的样本数。注意，$\rho(n^c)$ 可以是与 n^c成反比的任意函数。本文更关注本地未见类别与全局未见类别之间的无偏训练，而忽略已见类别与未见类别之间的训练不一致性，因为 ORCA（Cao等人，2022年）和 NACH（Guo等人，2022年）均已解决这一问题。

3.2.3. 校准模块

由于未见类别会在成对目标函数的作用下被划分到新的簇中，即 $\mathcal{L}_i^u$，而该目标函数只能确保相似样本被划分到同一组/簇，因此同一个未见类别在不同客户端上可能被赋予不同的簇标识符。例如，在图 2中，由于缺少有标签数据的监督，未见类 4、5 和 6 可能被赋予4~9 之间的任意标签。这种标签异质性会显著降低聚合性能。因此，需要设计一个校准模块，在聚合阶段之前对齐本地分类器的异构输出。

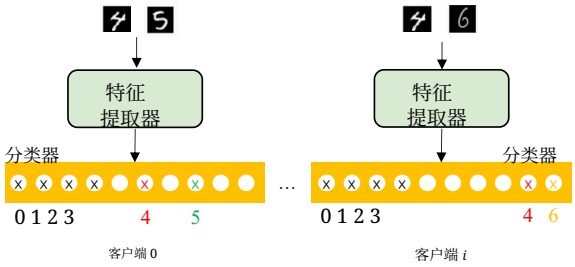


图2：FedoSSL 中标签异质性的示意图。在一个 10 类分类示例中，类别 {0, 1, 2, 3} 是已见类，而类别 {4, 5, 6} 是未见类别。由于对无标签数据使用了特征级成对无监督损失（即 $\mathcal{L}_i^u$），同一未见类别在不同客户端上可能会被分类为不同的标签标识符，例如，未见类别 4 在客户端 0 的分类器中会被分类到第六个位置，而在客户端 i 的分类器中，类别 4 会被分类到第八个位置。

受一种基于聚类的联邦学习技术（Lubana 等人，2022年）的启发，该技术旨在通过增加全局质心聚合机制来对齐不同客户端的本地聚类性能，我们将其扩展到 FedoSSL 场景，并使用全局质心作为自监督信号，引导未见类别的分类过程。校准模块的损失可表示为

$$\mathcal{L}_i^{cal} = \mathcal{L}_i^{ce} + \mathcal{L}_i^{cluster} \tag{7}$$

具体而言，我们首先汇总所有客户端的本地质心，在服务器端生成全局簇，即采用 Sinkhorn-Knopp（Genevay 等人，2019年）聚类。随后将全局质心返回给客户端，以进行进一步校准。以全局质心为指导，通过交叉熵损失使分类器在未见类别上的输出趋近于簇分配，从而进行更新：

$$\mathcal{L}_i^{ce} = \frac{1}{n_i^u}\sum_{z_j \in Z_i^u} \mathcal{H}(q(z_j;m), p(w^\top \cdot z_j)) \tag{8}$$

其中，m 表示全局质心。此外，为了防止某一类别的簇分配在训练过程中发生剧烈变化，我们还设计了以下损失函数，以提升特征表示的可聚类性：

$$\mathcal{L}_i^{cluster} = \frac{1}{n_i^u}\sum_{z_j,\bar{z}_j \in Z_i^u, \bar{Z}_i^u} \mathcal{H}(q(z_j;m), q(\bar{z}_j;m)) \tag{9}$$

其中，$q(z_j;m)$ 和 $q(\bar{z}_j;m)$ 是对应的聚类分配，通过将表示与全局质心进行匹配计算得出。

算法1 FedoSSL算法

输入： 客户端数量 K，学习率 η，本地训练周期 E，有标签数据 $\{\mathcal{D}_1^l, \mathcal{D}_2^l, \ldots, \mathcal{D}_K^l\}$，无标签数据 $\{\mathcal{D}_1^u, \mathcal{D}_2^u, \ldots, \mathcal{D}_K^u\}$，超参数 α，β，γ
输出： 最终模型 θ

初始化模型参数 θ
重复
  抽取一组客户端 $\mathcal{S}$。
  对 每个客户端 $i \in \mathcal{S}$ 并行 **执行**
    对 $j = 1$**至** E **执行**
      更新本地模型：$\theta_i \leftarrow \theta_i - \eta \nabla_\theta \mathcal{L}_i^*(\theta_i)$
    end for
    计算本地质心 m_i
  结束循环。
  更新全局模型：$\theta \leftarrow \frac{n_i}{\sum_{i \in \mathcal{S}} n_i n} \sum_{i \in \mathcal{S}} \theta_i$
  更新全局质心 m
  将 θ 和 m 分发给全部客户端。
直到模型收敛

3.3. 算法流程

在本小节中，我们介绍 FedoSSL 的整体学习框架，该框架总结于算法 1。

客户端更新。 在每个通信轮次中，客户端从服务器下载全局模型和全局质心。在客户端更新阶段，每个客户端会进行若干次本地基于梯度的更新（例如，E 个训练轮次），以优化公式（4）中的本地目标函数。随后，通过基于 Sinkhorn-Knopp 的聚类算法计算本地质心（Genevay 等人，2019年）。

服务器聚合。 在客户端完成本地模型训练后，更新后的模型和本地质心都会发送到服务器进行进一步聚合。具体而言，服务器首先对本地模型进行加权平均聚合。然后，通过聚合本地质心（即再次使用 Sinkhorn-Knopp 聚类）计算全局质心。上述步骤将重复进行，直至模型收敛。

4. 实验

4.1. 实验设置

数据集。 我们在三个数据集 CIFAR-10、CIFAR-100 和 CINIC-10 上评估 FedoSSL 框架（Darlow 等人，2018年）。CINIC-10 是一个由 CIFAR-10 和 ImageNet 构建而成的更大数据集。对于所有数据集，我们首先将类别划分为 60% 已见类和 40% 未见类别，然后从已见类中选取 50% 作为有标签数据，其余作为无标签数据。对于 CIFAR-10 和 CINIC-10 数据集，在未见类别中选取一个类别作为全局未见类别，其余 3 个类别作为局部未见类别，每个客户端拥有全部 6 个已见类、一个全局未见类别和一个局部未见类别。对于 CIFAR-100 数据集，在未见类别中选取 10 个类别作为全局未见类别，其余 30 个类别作为局部未见类别；每个客户端拥有全部 60 个已见类、10 个全局未见类别和 10 个局部未见类别。

基线方法。 为了将我们提出的 FedoSSL 与最先进的方法进行比较，我们从两个角度开展实验：1）将现有的开放世界半监督学习方法扩展到联邦学习环境；2）将现有的联邦半监督学习方法扩展到开放世界场景。

针对前者，我们通过分别采用两种具有代表性的联邦学习算法，即 Fe- dAvg（McMahan 等人，2017年）和 FedRep（Collins 等人，2021年），将 ORCA 和 NACH 扩展为适用于联邦学习场景。具体而言，扩展后的基线方法命名为 Fe- dAvg+ORCA（**Fed-AO**）、FedRep+ORCA（**Fed-RO**）、Fe- dAvg+NACH（**Fed-AN**）和 FedRep+NACH（**Fed-RO**）。请注意，FedRep 是一种个性化联邦学习算法，它会在本地持续更新每个客户端的分类器，同时将其他部分聚合到服务器上。之所以实现 FedRep，是因为将 ORCA 和 NACH 扩展到分布式环境时，不同客户端之间缺乏统一的标签，因此同一个未见类别可能会在不同分类器上被赋予不同标签。为避免聚合本地分类器所造成的混淆，FedRep 不会聚合分类器。

对于联邦半监督学习方法，我们采用一种最先进的方法 **SemiFL**（Diao 等人，2022年），并通过以下方式将其用于开放世界设置：我们使用 SemiFL 将样本分类到已见类中，并根据 softmax置信度分数估计分布外（OOD）样本。请注意，SemiFL 已显示出优于 FedMatch（Jeong 等人，2021年）的性能，因此本文不将 FedMatch 作为基线。

为确保性能比较的公平性，我们还分别在不进行聚合的集中式（即 **Cen-O**、**Cen-N**）和分布式（即 **Local-O**、**Local-N**）环境中运行开放世界半监督学习方法（即 ORCA、NACH），以表明我们提出的 FedoSSL 方法性能的上界和下界。

实现细节。 对于所有数据集，我们均使用 ResNet-18 作为骨干模型，并采用标准随机梯度下降进行模型训练，动量设为 0.9，权重衰减设为5×10^{-4}。分类器的维度对应于各数据集中的类别数。除非另有明确说明，α、β、γ均设为 1。模型训练 50 个全局轮次，每轮包含 5 个本地训练周期。所有实验的批大小均为 512。与 ORCA（Cao等人，2022年）类似，为避免过拟合，我们仅在第二阶段训练中更新 ResNet 最后一层的参数。对于其中的 Sinkhorn-Knopp 聚类（Genevay 等人，2019年）

表 2：在三个基准数据集上，10 个客户端对已见类、未见类和全部类别进行分类时，各对比方法的分类准确率。 * SemiFL 中的星号（∗）表示原始方法无法对未见类别进行分类（因此我们对其进行了扩展）。对于未见类别，*LU.* 表示局部未见类，而*GU.* 表示全局未见类。*AU.* 表示所有未见类的总体准确率。灰色行表示 FedoSSL 模型性能的上界。

#方法	CIFAR-10（%）					CIFAR-100（%）					CINIC-10（%）				
	All	Seen	未见			All	Seen	未见			All	Seen	未见		
			LU.	GU.	AU.			LU.	GU.	AU.			LU.	GU.	AU.
Cen-O	78.26	86.63	-	-	71.95	56.92	73.68	-	-	44.28	69.32	83.18	-	-	58.86
Cen-N	81.02	89.47	-	-	74.64	58.98	75.10	-	-	46.82	71.89	83.82	-	-	62.89
Local-O	65.98	79.57	-	-	45.60	43.10	54.33	-	-	26.25	55.33	65.23	-	-	40.48
Local-N	67.67	83.95	-	-	43.26	45.28	57.24	-	-	27.34	57.31	65.70	-	-	44.73
Fed-AO	69.46	81.01	89.38	42.03	52.15	47.91	59.67	38.07	29.12	30.26	54.85	63.22	71.31	37.88	42.29
Fed-RO	71.72	82.22	89.84	53.43	55.96	47.72	59.79	44.13	28.86	29.62	57.16	62.26	72.24	42.09	49.50
Fed-AN	66.58	84.18	78.76	37.58	40.15	47.25	58.24	42.11	30.44	30.77	53.49	63.61	66.78	36.06	38.32
Fed-RN	68.83	**85.52**	79.84	41.79	43.81	48.02	59.4	**48.77**	30.36	30.96	58.11	65.97	68.81	39.01	46.33
*SemiFL	64.91	81.57	86.33	31.16	39.92	42.28	54.94	31.68	21.46	23.29	52.27	62.72	64.53	37.21	37.34
FedoSSL	**76.26**	84.29	**90.68**	**59.69**	**64.22**	**51.58**	**61.12**	45.76	**33.82**	**31.13**	**63.82**	**68.40**	**79.79**	**47.78**	**56.96**

表 3：损失函数分析：CIFAR-10 上的分类准确率（客户端数量：10）。

方法	SEEN	未见	ALL
Fed-AO	81.01	52.15	69.46
FEDOSSL-$\mathcal{R}_i$-$\mathcal{L}_i^{ce}$	83.53	52.24	71.01
FEDOSSL-$\mathcal{R}_i$	83.13	62.98	75.07
FEDOSSL	84.29	64.22	76.26

表 4：损失函数分析：CINIC-10 上的分类准确率（客户端数量：10）。

方法	SEEN	未见	ALL
FED-AO	63.22	42.29	54.85
FEDOSSL-$\mathcal{R}_i$-$\mathcal{L}_i^{ce}$	69.10	40.31	57.58
FEDOSSL-$\mathcal{R}_i$	67.59	47.73	59.65
FEDOSSL	68.40	56.69	63.82

我们的 FedoSSL，为 CIFAR-10 和 CINIC-10 计算 32 个本地质心和 10 个全局质心，为 CIFAR-100 计算 128 个本地质心和 100 个全局质心。我们在两种设置下评估所有基线方法和 FedoSSL：10 个客户端，参与率为 50%；以及 50 个客户端，参与率为 10%。所有客户端的最终平均模型准确率取自所有全局轮次中表现最佳的一轮。所有对比方法均基于使用对比学习算法 SimCLR（Chen等人，2020a年）实现。

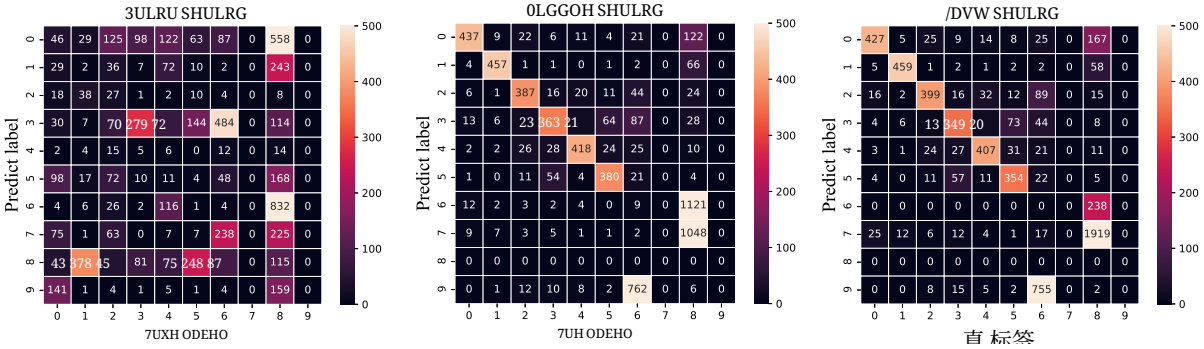
我们在配备 RTX 2080Ti GPU、3.6 GHz Intel Core i9-9900KF CPU 和 64GB 内存的工作站上模拟所有客户端和服务器。

说明。我们知道，许多技巧，例如用于避免平凡解的多样性约束正则化损失(Cao等人, 2022年; Guo等人, 2022年)或用于筛选置信度较低样本的动态阈值 (Guo等人, 2022年)等，都可以加入我们的 FedoSSL 框架中。不过，为避免偏离重点，本文不采用这些技巧。

4.2. 性能比较

首先，我们在三个基准数据集上将提出的 FedoSSL 方法与基线方法进行比较。类别在 CIFAR-10、CIFAR-100 和 CININ-10 数据集上的分类准确率列于表 2. 需要注意的是，整体未见准确率（AU.）并不总是本地未见准确率（LU.）和全局未见类（GU.）的加权平均值。有时，某个局部未见类别的大多数样本和某个全局未见类别的大多数样本会被分类为同一标签。在这种情况下，计算整体未见准确率时，我们必须为这两个类别中的一个选择另一个标签（即样本数量第二多的标签）。

从结果可以看出，在全部三个数据集上，与基线方法和本地训练版本（即 Local-O、Local-N）相比，我们提出的 FedoSSL 在整体分类准确率方面表现更优。在大多数情况下，FedoSSL 在已见类和局部未见类别上均保持稳健表现。在全局未见类和整体未见类别上，FedoSSL 则取得了显著的性能提升。例如，在全局未见类别上，FedoSSL 的表现比最佳基线方法在 CIFAR-10 上高出 11.72%，在 CIFAR-100 上高出 11.10%，在 CINIC-10 上高出 13.52%。在整体未见类别上，FedoSSL 的表现比最佳基线方法在 CIFAR-10 上高出 14.76%，在 CINIC-10 上高出 15.07%。此外，我们证明了局部未见类别与全局未见类别之间的性能差距在



(a) 在初始阶段。 (b) 在中间阶段。 (c) 在最终阶段。

图3： β (a) 和 γ (b) 在不同设置下的分类准确率。

表5：在三个基准数据集上，50个客户端参与时各对比方法在已见、未见及全部类别上的分类准确率。

	CIFAR-10（%）			CIFAR-100（%）			CINIC-10（%）		
#方法	All	Seen	未见	All	Seen	未见	All	Seen	未见
Fed-AO	70.22	83.34	50.54	45.63	56.25	29.69	53.81	60.49	43.80
Fed-RO	71.36	84.31	51.93	45.18	56.78	27.79	57.26	61.70	50.61
Fed-AN	69.89	85.36	46.68	45.22	56.30	28.59	53.42	63.62	38.13
Fed-RN	71.49	**86.28**	49.30	45.57	56.79	28.73	57.81	65.29	46.60
FedoSSL	**76.41**	85.71	**62.46**	**47.01**	**58.34**	**30.17**	**64.02**	**69.56**	**55.71**

与其他方法相比，FedoSSL 显著缩小了这一差距：例如，Fed-AO 中局部未见类别与全局未见类别之间存在 47% 的差距，而 FedoSSL 在 CIFAR-10 上将这一差距缩小至 31%。

4.3. 消融实验

在本小节中，我们将进行详细分析，以帮助理解所提出的 FedoSSL 框架的优越性，包括对两个额外模块 $\mathcal{R}_i$ 和 $\mathcal{L}_i^{cal}$ 的分析、已见类数量的影响、大规模联邦学习场景下的鲁棒性，以及超参数敏感性分析。

目标函数分析。我们评估了所提出的两个目标函数 $\mathcal{R}_i$ 和 $\mathcal{L}_i^{cal}$（即， $\mathcal{L}_i^{cal}$由 $\mathcal{L}_i^{ce}$和 $\mathcal{L}_i^{cluster}$组成）在 CIFAR-10 和 CINIC-10 数据集上的表现。我们使用 Fed-AO 作为基础基线。首先，FedoSSL-$\mathcal{R}_i$-$\mathcal{L}_i^{ce}$表示仅在基线中添加 $\mathcal{L}_i^{cluster}$，可以观察到已见类的准确率有所提升。接着，FedoSSL-$\mathcal{R}_i$ 表示同时添加 $\mathcal{L}_i^{ce}$和 $\mathcal{L}_i^{cluster}$，这能够大幅提升未见类别的准确率。最后，使用全部两个目标函数，即完整的 FedoSSL，可进一步提升未见类别的准确率并取得最佳性能。表3 和4 中的结果清晰地展示了消融实验，证明了所提出目标函数的有效性。此外，我们记录了初始阶段、中间阶段计算得到的聚类分配

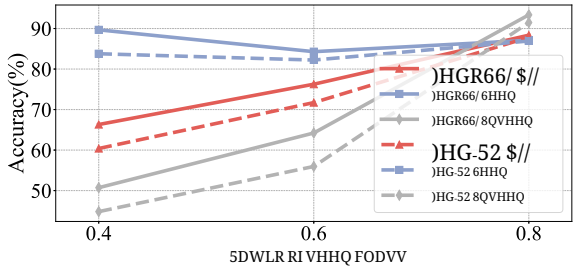


图 4：在 CIFAR-10 上，具有不同数量已见类时 Fed-RO 和 FedoSSL 的性能。

和最终阶段。图3 表明，共享本地质心能够显著帮助校准分类器在未见类别上的异质输出。

已见类别数量。 为展示所提出的 FedoSSL 的有效性，我们在 CIFAR-10 数据集上使用 10 个客户端，系统评估了改变已见类别比例时的性能。选择 Fed-RO 作为基线方法，是因为它在 4 种基线方法中表现最佳。图4 显示，FedoSSL 在所有情况下始终优于 Fed-RO。例如，在已见类别比例为 40% 时，FedoSSL 相较于 Fed-RO 的总体准确率提升了 9.8%。此外，FedoSSL 在所有比例取值下的性能都较为稳定，并且随着已见类别比例的增加而显著提升。

FedoSSL 鲁棒性分析。为进一步展示我们提出的 FedoSSL 在不同

表6：CIFAR-10 上对本地簇数量的敏感性。全局质心的数量为 10。

L	All	Seen	未见		
			LU.	GU.	AU.
8	74.28	84.26	88.90	54.09	59.29
16	75.76	84.17	89.28	58.36	63.15
32	76.26	84.29	90.68	59.69	64.22

实验规模下的鲁棒性，我们在其他客户端设置相同的 50 客户端场景中对其进行了评估，如表 5 所示。结果表明，FedoSSL 在全部数据集上仍具有最高的总体准确率，且在未见类别上的性能优势依然显著。对于 CIFAR-10 数据集，FedoSSL 的总体准确率比最佳基线方法高 6.88%，未见类别准确率高 20.28%；对于 CINIC-10，这两项指标分别高出 10.74% 和 10.08%。总体而言，我们的结果表明，FedoSSL 在大规模联邦学习场景中具有良好的鲁棒性。

本地质心数量。 在校准模块中，关键思路是上传本地质心，而不是所有数据的表示，以便计算全局簇。本地聚类方法可以根据系统的约束灵活选择，例如，为了提供强隐私保证，即使可能会导致效用大幅降低，也可以使用本地差分隐私（Local-DP）聚类方法（即 DP-k-均值（Balcan 等人，2017年）、Local-DP（Chang 等人，2021年）；对于保证稍弱但效用更高的情况，可以使用 K-匿名聚类方法（即 r-Gather 聚类（Aggarwal 等人，2010年）、基于 Sinkhorn-Knopp 的聚类（Genevay 等人，2019年））。为了进一步展示 FedoSSL 的有效性，我们研究了 FedoSSL 对本地质心数量（即L）的敏感性。表 6 显示，只要本地簇数量略高于类别数量，FedoSSL 就能保持对本地簇数量的稳健性，并在所有设置下取得相近的性能。

隐私分析。 我们提出的 FedoSSL 使用基于 Sinkhorn-Knopp 的聚类算法来计算 L大小相等的本地簇。该操作使所有 n/L-匿名性隐私保证适用于客户端上的 n 存在样本（Lubana 等人，2022年）。此外，也可以使用其他基于 Local-DP 的聚类方法来替代基于 Sinkhorn-Knopp 的聚类，从而提供更强的隐私保证。因此，我们将提出的 K-匿名性保证的 FedoSSL 与不提供隐私保证的版本进行比较（即，将基于 Sinkhorn-Knopp 的聚类替换为通用
k均值方法）。从表 7中可以看出，FedoSSL 的性能仅有小幅下降（相对于 K匿名性。

超参数分析。我们进一步分析了超参数的影响 β 以及 γ 在包含 10 个客户端的 CINIC-10 数据集上的影响。图5(a) 和 5(b) 展示了性能

表 7：在 CIFAR-10 上使用不同隐私保证版本的 FedoSSL 所获得的准确率。“无隐私”表示将本地表征共享给服务器的理想化设置。全局质心数量为 10。

	All	Seen	未见		
			LU.	GU.	AU.
无隐私	77.19	85.95	89.76	58.77	64.05
K-匿名性	76.26	84.29	90.68	59.69	64.22

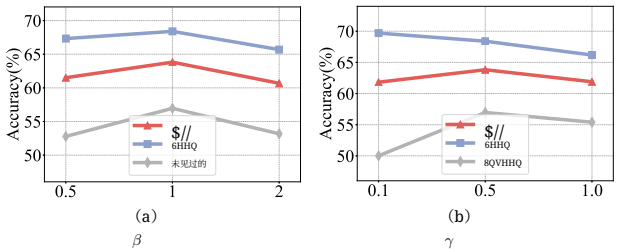


图5： β(a) 和 γ (b) 在不同设置下的分类准确率。

分别对应不同的 β 和 γ。对于 β，数值越大，表示 $\mathcal{R}_i$ 的影响越大。当 $\beta = 1$时，该方法在三项准确率指标上均取得最佳表现，而且随着 β 变化，性能不会显著下降。这表明 FedoSSL 对 β的选择具有很强的鲁棒性。对于 γ，数值越大，表示 $\mathcal{L}_i^{cal}$的影响越大，也就是说，模型受全局质心的影响越大。结果表明，当 $\gamma = 0.5$ 时，该方法的总体准确率最高。当 $\gamma = 0.1$时，未见类别的准确率会大幅下降，这表明 γ 的值不应过小。

5. 结论

本文研究了开放世界设置下的一种新的联邦半监督学习框架**FedoSSL**，旨在为有标签数据和无标签数据提供无偏训练。具体而言，我们根据相关未见类别是否仅存在于一个客户端，将未见类别划分为局部未见类和全局未见类。随后，我们分别设计了不确定性感知抑制损失和校准模块，以平衡局部未见类与全局未见类之间的训练进度，并补充全局模型聚合阶段。我们证明了 FedoSSL 是一个通用的联邦半监督学习框架，并且能够轻松兼容最先进的联邦学习方法。我们在各种模型和数据集上进行了大量实证实验，以验证 FedoSSL 框架的有效性和优越性能。

致谢

本研究获得了以下资助：广东省重点领域研发计划（编号：2021B0101400003）、香港研究资助局研究影响基金（编号：R5060-19）、优配研究金（152203/20E、152244/21E 和 152169/22E）、深圳市科技创新委员会（JCYJ20200109142008673）以及卓越领域计划（AoE/E-601/22-R）。

参考文献

Aggarwal, G., Panigrahy, R., Feder, T., Thomas, D., Kentha- padi, K., Khuller, S. 和 Zhu, A. 通过聚类实现匿名性。*ACM 算法汇刊 (TALG)*，6(3):1–19，2010年。

Balcan, M.-F., Dick, T., Liang, Y., Mou, W. 和 Zhang, H. 高维欧几里得空间中的差分隐私聚类。发表于国际机器学习会议，第 322–331 页。PMLR，2017年。

Boult, T. E., Cruz, S., Dhamija, A. R., Gunther, M., Henry- doss, J. 和 Scheirer, W. J. 学习与未知：综述迈向开放世界识别的步骤。发表于*AAAI* 人工智能会议论文集，第 33 卷，第 9801–9807 页，2019年。

Cao, K., Brbic, M. 和 Leskovec, J. 开放世界半监督学习。载于国际学习表征会议，2022年。网址 https://openreview.net/forum?id=O-r8LOR-CCA。

Chang, A., Ghazi, B., Kumar, R. 和 Manurangsi, P. 单轮局部隐私 k-means。载于 国际机器学习会议，第 1441–1451 页。PMLR，2021年。

Chen, T., Kornblith, S., Norouzi, M. 和 Hinton, G. 用于视觉表征对比学习的简单框架。载于 国际机器学习会议，第 1597–1607 页。PMLR，2020a年。

Chen, Y., Zhu, X., Li, W. 和 Gong, S. 类别分布失配下的半监督学习。载于 *AAAI* 人工智能会议论文集，第 34 卷，第 3569–3576 页，2020b年。

Collins, L., Hassani, H., Mokhtari, A., 和 Shakkottai, S. 利用共享表征实现个性化联邦学习。在国际机器学习会议，第 2089–2099 页。PMLR，2021年。

Darlow, L. N., Crowley, E. J., Antoniou, A. 和 Storkey, A. J. CINIC-10 既不是 ImageNet，也不是 CIFAR-10。*arXiv* 预印本 *arXiv:1810.03505*，2018年。

Diao, E., Ding, J. 和 Tarokh, V. SemiFL：面向无标签客户端的交替训练半监督联邦学习。神经信息处理系统进展，35:17871–17884，2022年。Fallah, A., Mokhtari, A. 和 Ozdaglar, A. E. 具有理论保证的个性化联邦学习：一种与模型无关的元学习方法。载于 *NeurIPS*，2020年。Genevay, A., Dulac-Arnold, G. 和 Vert, J.-P. 带聚类大小约束的可微深度聚类。*arXiv* 预印本 *arXiv:1910.09036*，2019年。Guo, L.-Z., Zhang, Z.-Y., Jiang, Y., Li, Y.-F. 和 Zhou, Z.-H. 面向未见类别无标签数据的安全深度半监督学习。载于国际机器学习会议，第3897–3906页。PMLR，2020年。

Guo, L.-Z., Zhang, Y.-G., Wu, Z.-F., Shao, J.-J., 和 Li, Y.-F. 并非所有类别都有标签时的鲁棒半监督学习。载于 Oh, A. H., Agarwal, A., Belgrave, D., 和 Cho, K.（编），神经信息处理系统进展，2022年。网址 https://openreview.net/forum?id=lDohSFOHr0。

Han, K., Vedaldi, A., 和 Zisserman, A. 通过深度迁移聚类学习发现新的视觉类别。在*IEEE/CVF* 国际计算机视觉会议论文集，第 8401–8409 页，2019年。

He, C., Yang, Z., Mushtaq, E., Lee, S., Soltanolkotabi, M., 和 Avestimehr, S. SSFL：通过个性化自监督解决联邦学习中的标签不足问题。*arXiv* 预印本 *arXiv:2110.02470*，2021年。

Hsu, Y.-C., Lv, Z., Schlosser, J., Odom, P. 和 Kira, Z. 无需多类别标签的多类别分类。*arXiv*预印本 *arXiv:1901.00544*，2019年。

Huang, J., Fang, C., Chen, W., Chai, Z., Wei, X., Wei, P., Lin, L. 和 Li, G. 变废为宝：通过跨模态匹配挖掘 OOD 数据，用于开放集半监督学习。发表于*IEEE/CVF*国际计算机视觉会议论文集，第8310–8319页，2021年。

Jeong, E., Oh, S., Kim, H., Park, J., Bennis, M. 和 Kim, S.- L. 非独立同分布私有数据下通信高效的端侧机器学习：联邦蒸馏与增强。*CoRR*，2018年。

Jeong, W., Yoon, J., Yang, E., and Hwang, S. J. 采用客户端间一致性与不相交学习的联邦半监督学习。发表于国际学习表征会议 *(ICLR) 2021*年。国际学习表征会议 (ICLR)，2021年。

Jin, Y.、Wei, X.、Liu, Y. 和 Yang, Q.《在联邦学习中利用无标签数据：综述与展望》。*arXiv*预印本 *arXiv:2002.11545*，2020年。

Lee, D.、Kim, S.、Kim, I.、Cheon, Y.、Cho, M. 和 Han, W.- S.《用于半监督学习的对比正则化》。载于*IEEE/CVF*计算机视觉与模式识别会议论文集，第3911–3920页，2022年。

Lee, D.-H. 等。伪标签：一种简单高效的深度神经网络半监督学习方法。发表于表征学习挑战研讨会，国际机器学习大会，第3卷，第896页，2013年。

Li, D. 和 Wang, J. Fedmd：通过模型蒸馏实现异构联邦学习。*arXiv*预印本 *arXiv:1910.03581*，2019年。Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A. 和 Smith, V. 异构网络中的联邦优化。发表于《机器学习与系统》会议论文集，2:429–450，2020a年。Li, X., Huang, K., Yang, W., Wang, S. 和 Zhang, Z. 关于 FedAvg 在非独立同分布数据上的收敛性。发表于*ICLR*论文集，2020b年。Liang, X., Lin, Y., Fu, H., Zhu, L. 和 Li, X. Rscfed：随机采样共识联邦半监督学习。发表于*IEEE/CVF*计算机视觉与模式识别会议论文集，第10154–10163页，2022年。Lin, H., Lou, J., Xiong, L. 和 Shahabi, C. Semifed：结合一致性与伪标签的半监督联邦学习。*arXiv*预印本 *arXiv:2108.09412*，2021 年。Lin, T., Kong, L., Stich, S. U. 和 Jaggi, M. 用于联邦学习中稳健模型融合的集成蒸馏。发表于*NeurIPS*，2020年。Liu, Q., Yang, H., Dou, Q. 和 Heng, P.-A. 通过客户端间关系匹配实现联邦半监督医学图像分类。发表于医学图像计算与计算机辅助干预国际会议，第325–335页。施普林格，2021年。Long, Z., Che, L., Wang, Y., Ye, M., Luo, J., Wu, J., Xiao, H. 和 Ma, F. Fedsiam：迈向自适应联邦半监督学习。*arXiv*预印本 *arXiv:2012.03292*，2020年。Lubana, E. S., Tang, C. I., Kawsar, F., Dick, R. P. 和 Mathur, A. Orchestra：通过全局一致聚类实现无监督联邦学习。*arXiv*预印本 *arXiv:2205.11506*，2022年。McMahan, B., Moore, E., Ramage, D., Hampson, S. 和 y Arcas, B. A. 基于去中心化数据的深度网络通信高效学习。发表于人工智能与统计学会议（*AISTATS*）论文集，2017年。

Ng, D.、Lan, X.、Yao, M. M.-S.、Chan, W. P. 和 Feng, M. 联邦学习：为拥有少量有标签数据的各个站点协作构建更优医学成像模型。定量医学影像与外科，11(2):852，2021年。Ouali, Y.、Hudelot, C. 和 Tami, M. 深度半监督学习综述。*arXiv*预印本 *arXiv:2006.05278*，2020年。Pham, H.、Dai, Z.、Xie, Q. 和 Le, Q. V. 元伪标签。载于*IEEE/CVF*计算机视觉与模式识别会议论文集，第11557–11568页，2021年。Rasmus, A.、Berglund, M.、Honkala, M.、Valpola, H. 和 Raiko, T. 使用阶梯网络进行半监督学习。神经信息处理系统进展，28，2015年。Saito, K.、Kim, D. 和 Saenko, K. OpenMatch：通过开放集一致性正则化实现的开放集半监督学习。神经信息处理系统进展，34:25956–25967，2021年。Sohn, K.、Berthelot, D.、Carlini, N.、Zhang, Z.、Zhang, H.、Raffel, C. A.、Cubuk, E. D.、Kurakin, A. 和 Li, C.-L. FixMatch：利用一致性和置信度简化半监督学习。神经信息处理系统进展，33:596–608，2020年。Tarvainen, A. 和 Valpola, H. 均值教师是更好的榜样：权重平均的一致性目标改善半监督深度学习结果。神经信息处理系统进展，30，2017年。Wei, C.、Shen, K.、Chen, Y. 和 Ma, T. 深度网络在无标签数据上进行自训练的理论分析。载于国际学习表征会议，2020年。Xie, Q.、Dai, Z.、Hovy, E.、Luong, T. 和 Le, Q. 无监督数据增强用于一致性训练。神经信息处理系统进展，33:6256–6268，2020年。Yoshida, N.、Nishio, T.、Morikura, M.、Yamamoto, K. 和 Yonetani, R. Hybrid-FL：无线网络中利用非独立同分布数据的协作学习机制。*CoRR*，2019年。Zhang, J.、Guo, S.、Ma, X.、Wang, H.、Xu, W. 和 Wu, F. 面向个性化联邦学习的参数化知识迁移。神经信息处理系统进展，34，2021a。Zhang, J.、Qu, Z.、Chen, C.、Wang, H.、Zhan, Y.、Ye, B. 和 Guo, S. 边缘学习：边缘分布式大数据分析的赋能技术。*ACM*计算调查（*CSUR*），54(7):1–36，2021b。

Zhang, Z.、Yang, Y.、Yao, Z.、Yan, Y.、Gonzalez, J. E.、Ramchandran, K. 和 Mahoney, M. W. 通过减少模型的梯度多样性改进半监督联邦学习。载于 *2021*年 *IEEE* 大数据国际会议（*Big Data*），第 1214–1225 页。IEEE，2021年c。

Zhao, Y.、Li, M.、Lai, L.、Suda, N.、Civin, D. 和 Chandra, V. 使用非独立同分布数据的联邦学习。*CoRR*，2018年。

Zhong, Z.、Fini, E.、Roy, S.、Luo, Z.、Ricci, E. 和 Sebe, N. 用于新类别发现的邻域对比学习。载于 *IEEE/CVF*计算机视觉与模式识别会议论文集，第10867–10875页，2021年。

Zhou, Z.-H. 开放环境机器学习。《国家科学评论》，9(8):nwac123，2022年。

Zhou, Z.-H. 和 Li, M. 三重训练：利用三个分类器使用无标签数据。*IEEE Transactions on knowl-edgeandDataEngineering*，17(11):1529–1541，2005年。

Zou, Y., Zhang, Z., Zhang, H., Li, C.-L., Bian, X., Huang, J.- B., and Pfister, T. Pseudoseg：为语义分割设计伪标签。*arXiv*预印本 *arXiv:2010.09713*，2020年。