



福建工程学院  
Fujian University of Technology

# GFL: Federated Learning on Non-IID Data via Privacy-preserving Synthetic Data

汇报人: 黄其涵      导师: 章静教授

2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)

June 6, 2023



# 目录

► 研究背景

► 问题定义

► 研究方法

► 实验分析

► 研究总结



## 1.1 联邦学习

- 联邦学习是一种分布式机器学习方法, 其利用一个中央服务器 (也称为服务器端) 协调各终端设备 (也称为客户端), 协同训练一个各客户端共享的全局模型。
- 与传统中心化训练方法不同, **联邦学习不需要各设备发送自身隐私数据至数据中心, 因此有利于保护数据隐私**。具体而言, 联邦学习在客户端和服务端之间通过多轮通信迭代优化模型。
- 每轮通信包含两个阶段:
  - (1) 各客户端从服务器端下载全局模型, 并在本地数据上进行训练以获得本地模型;
  - (2) 服务器端接收并聚合各客户端的本地模型参数以获得性能更优的全局模型。然而, 现有联邦学习机制尚面临两大不足。

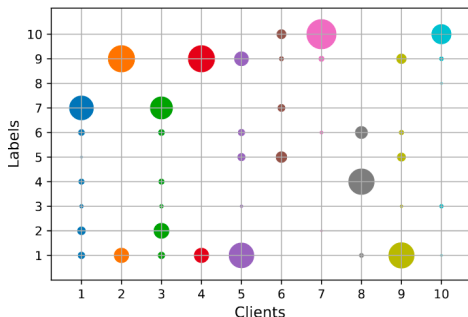


## 1.1 联邦学习

- 联邦学习是一种分布式机器学习方法, 其利用一个中央服务器 (也称为服务器端) 协调各终端设备 (也称为客户端), 协同训练一个各客户端共享的全局模型。
- 与传统中心化训练方法不同, **联邦学习不需要各设备发送自身隐私数据至数据中心, 因此有利于保护数据隐私**。具体而言, 联邦学习在客户端和服务端之间通过多轮通信迭代优化模型。
- 每轮通信包含两个阶段:
  - (1) 各客户端从服务器端下载全局模型, 并在本地数据上进行训练以获得本地模型;
  - (2) 服务器端接收并聚合各客户端的本地模型参数以获得性能更优的全局模型。然而, 现有联邦学习机制尚面临两大不足。



## 1.2 现有问题



- **类别不均衡。**全局模型需考虑多个客户端的数据, 但各客户端往往仅包含部分类别数据且类别间数据量严重不均衡, 使得全局模型难以训练。所训练的本地模型容易过拟合本地数据而在全局数据上往往取得较差性能。更重要的是, 这些性能较差的本地模型严重影响全局模型的训练, 导致难以构建高性能全局模型。
- **数据分布差异。**由于各客户端的功能和用户使用习惯不同, 不同客户端往往产生不同类别的数据, 导致各客户端数据之间的类别分布差异较大。



## 1.3 主要贡献

- 本文提出基于 GAN 的 GFL 框架以解决 FL 中数据异构性问题，并为 FL 系统构建高性能全局模型。GFL 促进了 FL 训练过程，同时保持了成员身份的隐私和原始数据在客户中的分布。
- 本文提出了一种保护隐私的数据生成工作流程，以生成符合我们隐私设置的合成样本。DPGAN 用于生成满足差分隐私的样本，以保护客户端免受成员推理攻击。本文生成大量合成数据并选择一个随机分布的子集来隐藏客户端的真实数据分布。
- 本文对合成数据进行“iidify”处理，以 iid 方式训练全局模型，并使用 Epoch Decay 参数来解决模式崩溃问题并避免使用低质量的合成数据。

研究背景  
○○○○○

问题定义  
●○

研究方法  
○○○○○

实验分析  
○○○○○○○

研究总结  
○○○



## 目录

► 研究背景

► 问题定义

► 研究方法

► 实验分析

► 研究总结



## 2 优化目标

为解决上述难题, 本文提出在客户端构造类别均衡的数据集进行训练的策略。令  $\mathcal{D}$  表示所构造的类别均衡数据集,  $M$  表示全局数据的类别数, 则

$$\mathcal{D} = \left\{ (x, y) \mid P(y = i) = \frac{1}{M}, \quad i \in \{0, 1, \dots, M-1\} \right\}$$

其中  $p(\mathcal{D})$  表示数据集  $\mathcal{D}$  所代表的经验分布. 因此, 本文旨在解决如下优化问题:

$$\min_{\mathbf{W}_T} \mathbb{E}_k \left[ \mathbb{E}_{x_k \sim p(\mathcal{D})} [\mathcal{L}(x_k; \mathbf{W}_T)] \right]$$

与仅仅利用客户端本地数据进行训练的方式相比, 基于类别均衡的数据集进行训练使得各客户端本地模型之间的差异大大减少。

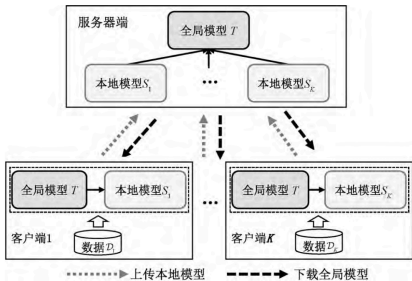


图 2 联邦学习流程





# 目录

► 研究背景

► 问题定义

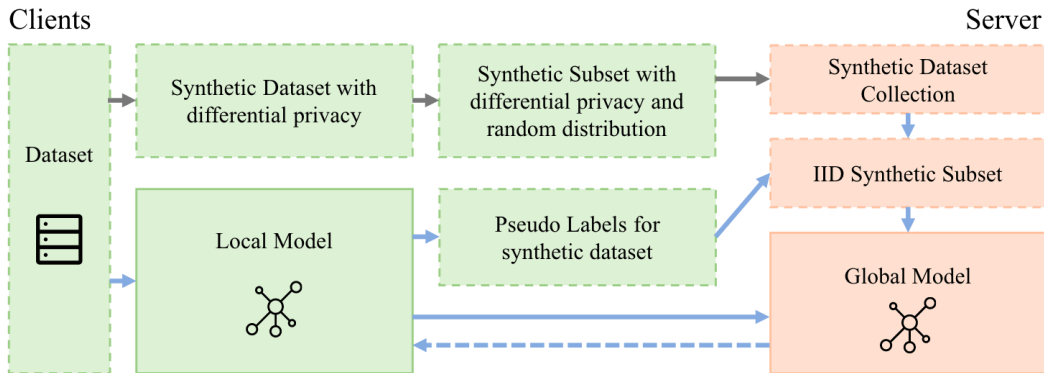
► 研究方法

► 实验分析

► 研究总结



## 3.1 Overview of Generative Federated Learning (GFL)





## 3.2 Synthetic Data Generation

### Threat Model

将 GAN 引入 GFL 中的联邦学习。但是，GAN 提供的合成数据可能会泄露客户的隐私信息。GAN 中最严重的漏洞之一是成员关系问题。例如，即使他/她参加了 GAN 训练，也没有人希望他/她的脸出现在生成的图像中。



## 3.2 Synthetic Data Generation

### Privacy-preserving Data Generation

---

**Algorithm 2:** Privacy-preserving Data Generation
 

---

**Input** : The synthetic data amount  $n_{S_k}$ .

**Output:** The synthetic dataset  $S_k$ .

**Data** : The local dataset  $\mathcal{P}_k$  with size  $n_k$ .

1 **Client  $k$  executes:**

```

2    $P_{S_k} \leftarrow$  (a random distribution)
3    $d_k, g_k \leftarrow \text{DPGANTraining}(\mathcal{P}_k)$ 
4    $S'_k \leftarrow \emptyset$ 
5   while not EnoughData( $S'_k, n_{S_k}, P_{S_k}$ ) do
6        $noises \leftarrow$  (random noises)
7        $S'_k \leftarrow S'_k \cup g_k(noises)$ 
8    $S_k \leftarrow \text{CutData}(S'_k, n_{S_k}, P_{S_k})$ 
```

---

**Algorithm 2:** Privacy-preserving Data Generation
 

---

**Input** : The synthetic data amount  $n_{S_k}$ .

**Output:** The synthetic dataset  $S_k$ .

**Data** : The local dataset  $\mathcal{P}_k$  with size  $n_k$ .

1 **Client  $k$  executes:**

```

2    $P_{S_k} \leftarrow$  (a random distribution)
3    $d_k, g_k \leftarrow \text{DPGANTraining}(\mathcal{P}_k)$ 
4    $S'_k \leftarrow \emptyset$ 
5   while not EnoughData( $S'_k, n_{S_k}, P_{S_k}$ ) do
6        $noises \leftarrow$  (random noises)
7        $S'_k \leftarrow S'_k \cup g_k(noises)$ 
8    $S_k \leftarrow \text{CutData}(S'_k, n_{S_k}, P_{S_k})$ 
```



### 3.3 Federated Learning with Synthetic Data

#### 数据生成器

通过类别均衡采样器, 客户端可获得各类别的采样量。然而, 如何根据所采样的类别获得相应的数据以用于本地模型的训练仍然是一个难题。为解决该问题, 本文引入了数据生成器  $G$ 。该数据生成器的输入为类别标签  $y$  和噪声矢量  $z$ 。其中  $y \in \{0, 1, \dots, M-1\}$ ,  $z$  服从高斯分布  $N(0, 1)$ 。数据生成器  $G$  根据噪声矢量  $z$  和类别标签  $y$  生成相应的数据  $\hat{x}$ , 即

$$\hat{x} = G(z \mid y), z \sim N(0, 1)$$

数据生成器和类别均衡采样器构造完成后, 客户端首先根据类别均衡采样器采样类别  $m$ , 然后利用数据生成器生成类别为  $m$  的虚拟数据。最后, 客户端结合本地数据和生成的虚拟数据, 从而构造类别均衡的数据集来训练本地模型。



# 目录

- ▶ 研究背景
- ▶ 问题定义
- ▶ 研究方法
- ▶ 实验分析
- ▶ 研究总结



## 4.1 数据集

在我们的实验中，我们使用 DPGAN 作为 Local GAN 模型，ResNet18 作为 EMNIST 和 CIFAR-10 联邦学习的训练模型。

- 1) EMNIST。在实验中使用它的“Digits”子集。它包含 10 个类，总共 280,000 个样本，分为 240,000 个训练样本和 40,000 个测试样本。与 MNIST 相比，它拥有更多数据并且完全平衡。
- 2) CIFAR-10。它包含 10 个不同类别的 60,000 个  $32 \times 32$  彩色图像，与 EMNIST 相比，这是一项更复杂的任务。我们使用这个数据集来衡量 GFL 在艰巨任务中的稳定性。



## 4.2 对比模型

本文将 GFL 与目前最新的方法进行比较, 即 FedAvg、FedPoxr、SCAFFOLD 和 FedNvae。本实验通过狄利克雷分布  $\text{Dir}(0.1)$  模拟各客户端数据的类别分布。

GFL 在合成数据生成阶段训练了 200 个 epoch。然后, 我们从每个客户端  $k$  中随机选择  $n_{S_k} = 500$  个合成样本。在联邦学习阶段, 初始全局训练 epoch  $E_s$  设置为 10, 如果未指定, epoch decay 参数  $\tau$  设置为 0.1。

上述所有算法共享相同的基本训练设置。训练包含 100 轮通信, 每轮每个客户端训练 20 个 epoch, 服务器和客户端的批大小都设置为 128。





## 4.3 实验结果

### Result Analysis

TABLE II

THE ACCURACY RESULTS OF DIFFERENT METHODS ON EMNIST AND CIFAR-10. GFL IS THE BEST IN MOST SITUATIONS, ESPECIALLY WHEN THE DATA IS EXTREMELY NON-IID SUCH AS  $\alpha \rightarrow 0, 1$ . AS THE DATA DISTRIBUTION MOVES TOWARDS IID, GFL MAINTAINS THE ACCURACY SIMILAR TO FEDAVG.

EMNIST	$\alpha \rightarrow 0$		$\alpha \rightarrow 1$		$\alpha \rightarrow 10$		$\alpha \rightarrow \infty$	
FedAVG	30.84%	(x1.00)	66.05%	(x1.00)	98.55%	(x1.00)	98.65%	(x1.00)
FedProx	64.72%	(x2.10)	77.66%	(x1.18)	98.94%	(x1.00)	<b>98.89%</b>	<b>(x1.00)</b>
SCAFFOLD	51.35%	(x1.67)	78.38%	(x1.19)	97.88%	(x0.99)	98.03%	(x0.99)
GFL	<b>78.78%</b>	<b>(x2.55)</b>	<b>89.77%</b>	<b>(x1.36)</b>	<b>99.39%</b>	<b>(x1.01)</b>	98.13%	(x0.99)

CIFAR-10	$\alpha \rightarrow 0$		$\alpha \rightarrow 1$		$\alpha \rightarrow 10$		$\alpha \rightarrow \infty$	
FedAVG	13.43%	(x1.00)	46.67%	(x1.00)	78.15%	(x1.00)	89.84%	(x1.00)
FedProx	38.55%	(x2.87)	46.19%	(x0.99)	83.63%	(x1.07)	89.31%	(x0.99)
SCAFFOLD	38.90%	(x2.90)	56.82%	(x1.22)	<b>88.50%</b>	<b>(x1.13)</b>	89.48%	(x1.00)
GFL	<b>56.22%</b>	<b>(x4.19)</b>	<b>67.42%</b>	<b>(x1.44)</b>	84.26%	(x1.08)	<b>89.93%</b>	<b>(x1.00)</b>

1. GFL 在所有设置中都优于其他算法;
2. non-iid 程度越大, GFL 的优势越明显;
3. 数据集越复杂, GFL 越优越。



## 4.3 实验结果

### Result Analysis

TABLE III  
ACCURACY COMPARISON OF FEDAVG AND GFL WITH DIFFERENT EPOCH  
DECAY PARAMETER  $\tau$ .

CIFAR-10	$\tau$	$\alpha \rightarrow 0$	$\alpha \rightarrow 1$
FedAVG	$\infty$	13.43%	46.67%
GFL	0.1	<b>56.22%</b>	<b>67.42%</b>
	0	32.77%	38.21%
	$-\infty$	17.26%	24.94%

1. Epoch Delay 参数在 GFL 中是必不可少的;
2. 只使用合成数据的方法是没有用的。



## 4.3 实验结果

### Result Analysis

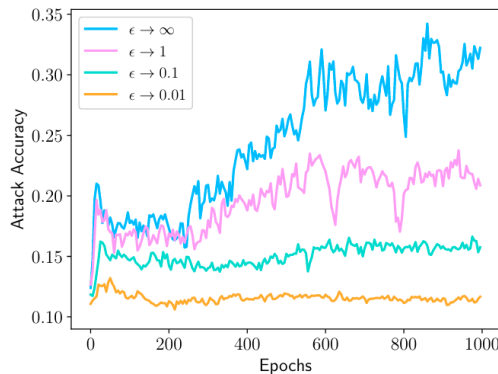


Fig. 3. The line chart of the privacy evaluation results on different privacy level  $\epsilon$ . The membership inference attack accuracy drops as  $\epsilon$  decreases.



## 4.3 实验结果

### Result Analysis

TABLE IV  
THE TABLE OF THE PRIVACY EVALUATION AND FL TRAINING RESULTS ON  
DIFFERENT PRIVACY LEVEL  $\epsilon$ .

CIFAR-10	$\epsilon$	Attack Acc	FL Acc
GFL	$\infty$	31.16%	69.31%
	1	21.58%	68.12%
	0.1	14.80%	67.42%
	0.01	11.66%	52.79%
FedAVG	—	—	46.67%

根据图 3 和表 IV 中的实验，选择  $\epsilon = 0.1$ ，这可以防止成员推理攻击，同时保持良好的性能。



# 目录

- ▶ 研究背景
- ▶ 问题定义
- ▶ 研究方法
- ▶ 实验分析
- ▶ 研究总结



## 研究总结

本文提出了一个称为生成联合学习 (GFL) 的新框架来处理非独立同分布问题。我们将 DPGAN 引入 GFL 以应对潜在的隐私攻击，尤其是成员推理攻击。

大量实验表明，GFL 可以在非 iid 情况下工作，也可以在 iid 情况下工作，并且在大多数情况下优于其他框架，如 FedProx 和 SCAFFOLD。隐私评估表明，通过在 DPGAN 的训练中加入适当的噪声，我们可以有效地防御成员推理攻击。我们还分析了 GFL 引入的 Epoch Decay 参数的必要性，这对于防止模式崩溃和高质量样本损害全局模型很重要。



*Q&A*

感谢您的聆听和反馈

## **Temporary page!**

L<sup>A</sup>T<sub>E</sub>X was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, because L<sup>A</sup>T<sub>E</sub>X now knows how many pages to expect for this document.