基于联邦学习的推荐系统综述

梁锋[1†]，羊恩跃[1†]，潘微科[1*]，杨强[2*]，明仲[1*]

{liangfeng2018, yangenyue2021}@email.szu.edu.cn , panweike@szu.edu.cn,
qyang@cse.ust.hk, mingz@szu.edu.cn

[1]深圳大学计算机与软件学院 深圳 518060

[2]香港科技大学计算机科学及工程学系 香港

目录

背景

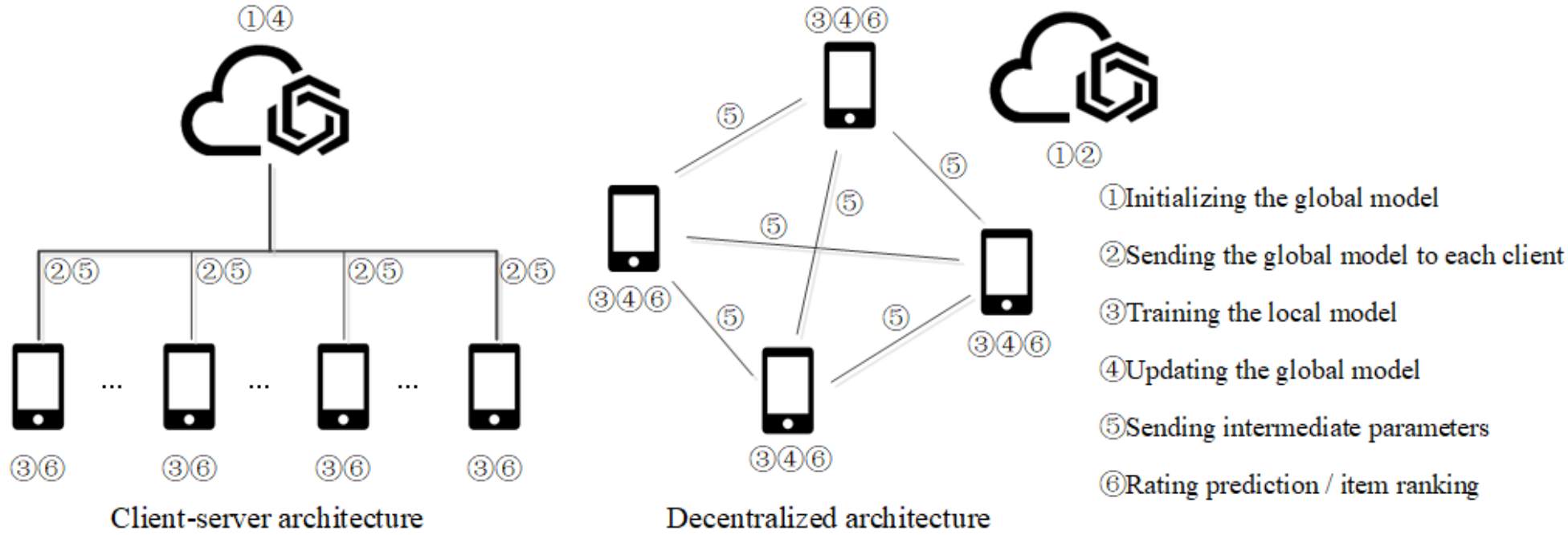
- 在传统的推荐算法中，为了构建一个全局的模型，通常需要收集所有用户的原始数据并上传至服务端，这样的做法往往存在用户隐私泄漏的问题。
- 联邦学习使得在模型训练的整个过程中，用户的原始数据始终保留在用户（客户端）本地，服务端和用户之间通过共享加密的或不包含隐私信息的中间参数的方式，进行模型训练和参数更新，进而在保护用户隐私的前提下构建一个有效的机器学习模型。
- 随着联邦学习技术的发展，对基于联邦学习的推荐算法（以下称“联邦推荐”）的研究也越发受到工业界和学术界的关注。
- 本文主要对基于联邦学习的推荐系统的研究进行综述。

联邦学习概述(1/3)

- 联邦学习本质上是一种既联合多方又不共享各方原始数据的分布式学习框架，在保护各个参与方数据中的隐私的前提下，联合各个参与方共同训练，得到一个共享的模型。
- 与传统的分布式学习框架相比：联邦学习中的各个参与方通常对自己的数据具有绝对的控制权。
- 联邦学习可按模型的架构、模型的联邦化、模型的优化和隐私保护技术的应用4个角度进行分类。

	类别	特点或经典算法
模型的架构	客户端-服务端架构	能够利用服务端的计算资源，减少客户端的计算压力；容易发生单点故障。
	去中心化架构	匿名性；节省服务端的资源；高可用性。
模型的联邦化	机器学习	线性回归[1]，提升树[2]，基于矩阵分解的聚类[3]…
	深度学习	图神经网络[4]，双向表征编码器[5]，卷积神经网络[6]，长短时间记忆网络[7]…
	迁移学习	文献[8，9]
	强化学习	文献[10]
	元学习	文献[11，12]
模型的优化	模型压缩	文献[13，14]
	通信策略的改进	文献[15，16–20]
	激励机制	文献[21–23]
	客户端采样	文献[23–27]
隐私保护技术的应用	同态加密	支持密文之间的运算；计算复杂度高
	差分隐私	权衡隐私保护强度和模型性能
	本地差分隐私	由客户端自动添加噪声
	安全多方计算	包括秘密共享、同态加密和混淆电路

联邦学习概述(3/3)



联邦学习的模型架构示意图

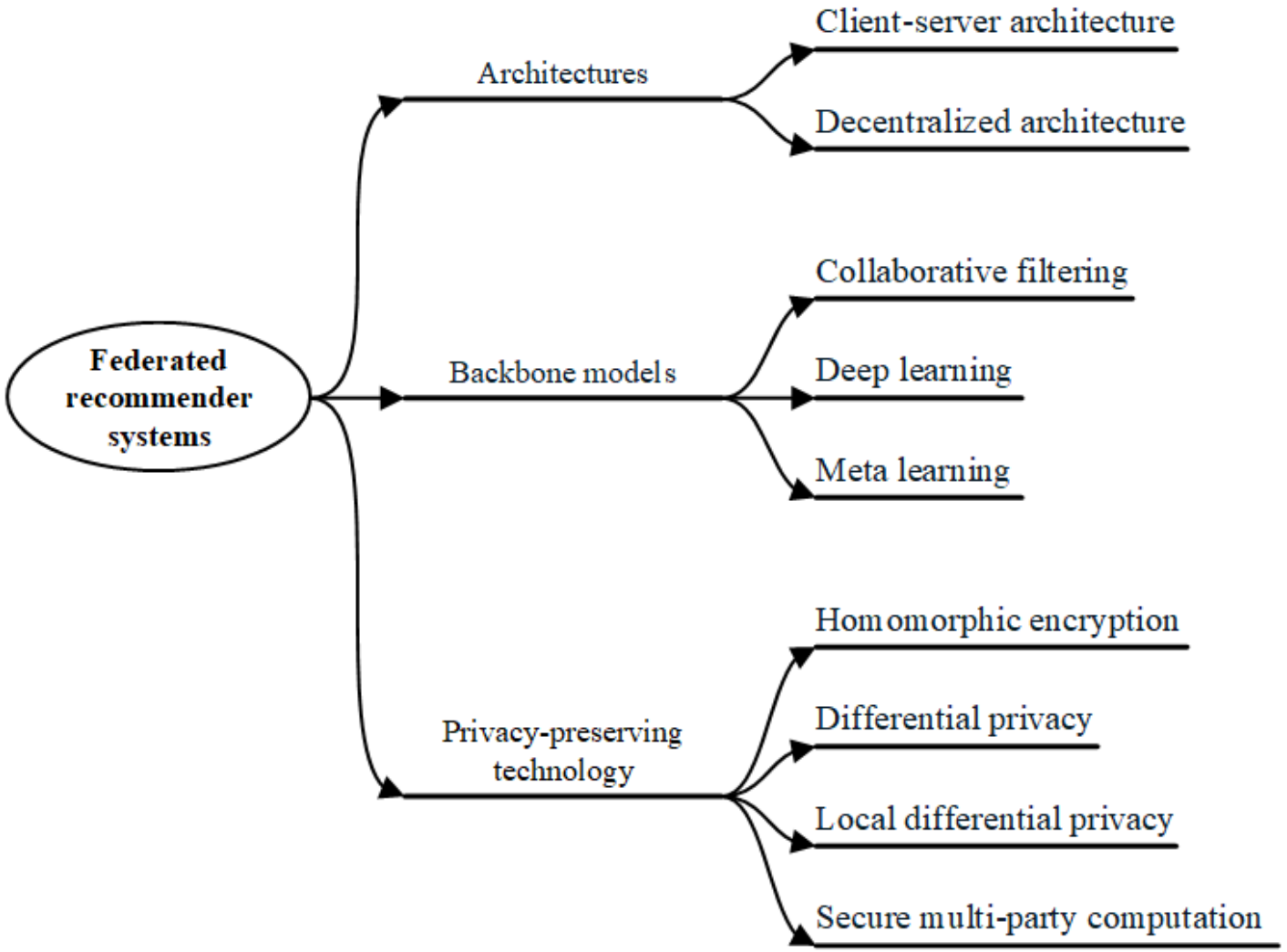
客户端-服务端架构和去中心化架构的相同之处在于：

- 客户端的原始数据不离开本地，通过服务端与客户端之间的通信或客户端与客户端之间的通信，以发送中间参数的训练方式来得到一个共享的模型。

联邦推荐概述(1/2)

- 与联邦学习的分类类似，我们从架构设计、系统的联邦化和隐私保护技术的应用3个角度，论述基于联邦学习的推荐系统的研究进展。
- 对于模型的优化，由于目前在联邦推荐系统方面的相关工作较少，我们将在未来工作部分进行讨论。

联邦推荐概述(2/2)



联邦推荐系统的分类

目录

客户端-服务端架构(1/3)

在一般联邦学习领域中，对于客户端-服务端架构，较为通用的训练流程为：

(1) 服务端初始化模型参数，并将模型参数发送给各个客户端；

(2) 客户端利用本地数据和最新的模型参数进行训练，并将中间参数发送给服务端；

(3) 服务端聚合中间参数，更新全局模型，再把模型回传给客户端；

(4) 重复步骤（2）和（3），直到模型收敛。

客户端-服务端架构(2/3)

我们以FCF（federated collaborative filtering）[28]为例，介绍客户端-服务端架构在面向传统协同过滤算法时较为通用的训练流程。

FCF使用用户特征向量和物品特征向量的内积来表示用户对物品的评分，即

$$\hat{r}_{ui} = U_{u\cdot} V_{i\cdot}^{\mathrm{T}},$$

其中，$U_{u\cdot}$表示用户u的特征向量，$V_{i\cdot}$表示物品i的特征向量。

- 用户和物品的交互数据需要保留在客户端本地；
- $U_{u\cdot}$表征用户的偏好信息，也需要保留在客户端本地。

客户端-服务端架构(3/3)

（1）服务端初始化物品特征矩阵V并发送给每个客户端；

（2）在每一轮迭代中，客户端使用本地数据，基于最小二乘法计算得到$U_{u\cdot}$的解析解，即

$$U_{u\cdot} = \frac{\sum_{i=1}^{m} y_{ui} V_{i\cdot}(1 + \lambda y_{ui})}{\sum_{i=1}^{m}(V_{i\cdot}^{\mathrm{T}} V_{i\cdot} + \lambda y_{ui} V_{i\cdot}^{\mathrm{T}} V_{i\cdot} + \alpha I)},$$

其中，$y_{ui} \in \{0,1\}$是指示变量，$1 + \lambda y_{ui}$是置信度权重，α是正则化项上的权衡参数，I为单位矩阵；

（3）客户端计算并上传所有物品特征向量的梯度给服务端；

（4）服务端聚合客户端上传的物品特征向量的梯度，更新物品特征矩阵，并将最新的物品特征矩阵发送给所有客户端；

（5）重复多轮的迭代训练，直到模型收敛。

去中心化架构(1/4)

在一般联邦学习领域中，对于去中心化架构，较为通用的训练流程为：

（1）服务端初始化模型参数，然后将模型参数发送给各个客户端；

（2）客户端利用本地数据进行模型训练，并将中间参数发送给其他客户端；

（3）客户端接收其他客户端的中间参数，更新本地的模型；

（4）重复步骤（2）和（3），直到模型收敛。

去中心化架构(2/4)

去中心化的分布式矩阵分解框架(DMF)[29]解决了面向兴趣点(POI)推荐中的物品排序问题中的隐私问题，其训练流程如下：

- 首先，DMF基于用户的位置信息构建用户邻接图；
- 然后，通过随机游走方法选择一些邻居用户进行通信；
- 进一步，每个用户u计算用户特征向量的梯度（用于本地更新用户特征向量$U_{u\cdot}$）、本地物品特征向量的梯度（用于本地更新物品特征向量$V_{i\cdot}^{\mathrm{lcl},u}$）和全局物品特征向量的梯度（发送给邻居用户，用于更新全局的物品特征向量$V_{i\cdot}^{\mathrm{glb},u'}$）。

特点：保护了用户的原始评分数据，节省了服务端的资源，且DMF的模型效果优于MF和BPR。

局限性：构建用户邻接图时需要收集用户的地理位置信息，这种做法泄露了用户的隐私。

去中心化架构(3/4)

用户能自主调节自身隐私级别的去中心化分布式矩阵分解框架（PDMFRec）[30]解决了DMF在构建用户邻接图时暴露用户地理位置的问题。PDMFRec的训练流程如下：

- 首先，PDMFRec在一些可信的客户端上根据用户之间共同评过分的物品构建用户邻接图；
- 然后，每个客户端执行本地训练，更新用户特征向量和物品特征向量；
- 进一步，每个客户端将物品特征向量的梯度发送给邻居用户；
- 最后，每个客户端接收其他客户端发送过来的物品特征向量的梯度，并更新本地物品特征向量。

特点：

- 在构建用户邻接图时，每个客户端可以隐藏自己的部分数据，以此构建不同的用户邻接图；
- 在模型训练阶段用户还能够选择不使用这部分数据，以达到更好地保护用户隐私的目的；
- 客户端之间能够直接传递信息，且客户端具有匿名性。

去中心化架构(4/4)

Hegedus等[31]基于矩阵分解将八卦学习（gossip learning）和联邦学习在一个特定的任务上进行对比：

- 通过实验验证，发现在客户端数量较多且通信成本相同的情况下两者的效果相近；
- 在都使用子采样压缩技术（即每次客户端随机采样一部分已评分物品和未评分物品的物品特征向量发送给其他客户端）的情况下八卦学习更具有优势。

目录

协同过滤推荐算法的联邦化(1/17)

联邦协同过滤推荐算法（FCF）[28]解决了基于ALS的协同过滤算法在计算物品特征向量时会泄露用户与物品的交互行为的问题。

- 在FCF中，用户的隐式反馈数据保留在用户本地，用于用户特征向量的更新和物品特征向量的梯度的计算；
- 物品特征向量的梯度需要上传到服务端进行物品特征向量的更新。

特点：在保护用户的隐私的同时，FCF能达到和CF一样的推荐性能。

局限性：将其扩展到评分预测问题时，模型会产生偏差，并且客户端通信成本较大。

协同过滤推荐算法的联邦化(2/17)

面向显式反馈的联邦协同过滤推荐算法（FedRec）[32]解决了FCF扩展到评分预测问题时模型会产生偏差的问题。FedRec中使用了混合填充方法：

- 首先，客户端u在本地随机采样部分未评过分的物品I'_u。

  其中，$|I'_u| = \rho|I_u|$，I_u表示客户端u已评分物品的集合，ρ为采样参数；

- 其次，客户端u对随机采样的物品填充虚假的评分值（在训练的前t次迭代填充已评分物品的分值的平均值，第t次迭代以后填充未评分物品的预测评分）；

- 最后，客户端u计算梯度，并将已评分物品和虚假采样的物品的特征向量的梯度一起上传到服务端。

特点：避免服务端得知客户端u评过分的物品，提高了通信效率。

协同过滤推荐算法的联邦化(3/17)

与FCF、FedRec不同，联邦矩阵分解算法（FederatedMF）[33]的物品特征向量在本地更新，具体地：

- 首先，客户端u在本地进行用户特征向量$U_{u.}$和物品特征向量$V_{i.}$的更新；
- 其次，客户端u将物品特征矩阵发送给服务端；
- 然后，服务端对接收到的物品特征矩阵进行加权平均，从而得到最新的物品特征矩阵。

在特定场景中，FederatedMF需要使用用户特征向量来创建或调整内容，因此Dolu等人[71]建议使用数据匿名化和差分隐私技术对用户特征向量进行处理，再发送给服务端。

特点：不仅保护了用户的评分数据，还节省了服务端的计算成本。

局限性： FederatedMF泄露了用户的评分行为(即用户对哪个物品评过分)。

协同过滤推荐算法的联邦化(4/17)

安全的联邦矩阵分解框架（FedMF）[34]使用加法同态加密技术来加密客户端要上传到服务端的物品特征向量的梯度。

- Chai等人[34]证明，在连续两次迭代中，在客户端上传同一物品的特征向量梯度的情况下，服务端能够推断出该用户对这一物品的评分信息。
- 与FederatedMF不同，在FedMF中，客户端上传的是物品特征向量的梯度，而不是物品特征向量。

特点：保护了用户的评分信息。

局限性： FedMF泄露了用户的评分行为；计算复杂度高。

协同过滤推荐算法的联邦化(5/17)

与FedMF不同，共享矩阵分解方法（SharedMF）[35]使用秘密共享技术来聚合梯度。

- 首先，客户端u在其本地使用秘密共享技术将要发送给服务端的物品特征向量的梯度分成n份梯度分片，即$\nabla V_{i\cdot} = \nabla V_{i\cdot}^{(1)} + \nabla V_{i\cdot}^{(2)} + \cdots + \nabla V_{i\cdot}^{(n)}$。其中，$n$表示客户端的数量，$\nabla V_{i\cdot}$表示物品$i$的特征向量的梯度；
- 其次，客户端u保留一份在本地，并将剩下的$n-1$份发送给其他客户端；
- 同时，客户端u接收到来自其他客户端的物品特征向量的梯度分片；
- 最后，客户端u将这些分片与本地保留的梯度分片进行求和运算，并将求和运算后得到的物品特征向量的梯度发送给服务端。

特点：保护了用户的评分分数和评分行为。

局限性：客户端之间需要能够相互通信；增加了客户端的通信成本。

协同过滤推荐算法的联邦化(6/17)

联邦成对学习算法(FPL)[36]是第一个将成对学习应用于联邦学习的研究工作。

- FPL能够让用户控制自己的敏感数据(即用户交互过物品的特征向量的梯度)的共享程度来平衡隐私保护和模型效果;
- 具体地，FPL通过引入了一个概率参数$\pi \in [0,1]$，使得用户能够控制自己交互过的物品的梯度与服务端共享的数量，即二元组$(\nabla V_{i.}, \nabla b_{i.})$以概率$\pi$被客户端上传到服务端，从而隐藏了部分互为相反数关系的梯度，其中，$i \in I_u$为用户评过分的物品。

特点：防止服务端重构出用户的评分行为。

协同过滤推荐算法的联邦化(7/17)

FedRecSys[37]是基于FATE平台建立的一个在线的联邦推荐系统。

- FedRecSys通过同态加密和秘密共享技术，实现了一些比较经典的推荐算法（例如，矩阵分解算法、分解机算法和基于广度&深度学习的推荐算法等）。
- Tan等人[37]还在2020年推荐系统大会（ACM RecSys）上公开演示了FedRecSys。

协同过滤推荐算法的联邦化(8/17)

基于位置敏感哈希的联邦推荐算法[38]（FRecLSH）解决了已有的位置敏感哈希算法（LSH）难以量化隐私保护预算的问题。

定义两个数据来源方A和B，以A方为例，FRecLSH的实现主要有以下3个步骤：

（1）A方在本地使用位置敏感的哈希函数，根据每个用户u的数据分别计算得到对应的哈希值S_u；

（2）用户u使用本地差分隐私技术处理哈希值S_u，得到扰乱后的哈希值S'_u；

（3）A方将哈希值S'_u发送给B方。同理，B方也要执行上述3个步骤。

特点：FRecLSH通过本地差分隐私技术，在联合多方数据建模的过程中给用户提供不同的隐私保护等级，在较小的隐私预算下，FRecLSH能够达到较高的时间效率和准确性。

协同过滤推荐算法的联邦化(9/17)

PP-NMF[39]是一个基于非负矩阵分解（NMF）的POI推荐框架，它保护POI推荐中用户的地理位置等隐私信息。

- 首先，服务端挑选一批志愿者对一些地点进行签到；
- 其次，服务端使用这些用户的匿名数据训练得到用户和物品的特征向量；
- 然后，使用k-均值(k -means)算法对用户的特征向量进行聚类，将用户分成k个群体；
- 最后，使用同一群体中的用户的数据来构建群体偏好。

协同过滤推荐算法的联邦化(10/17)

联邦多视图矩阵分解算法（FED-MVMF）[40]通过集成来自多个数据源的信息来解决冷启动问题，它包含多个客户端（用于存储本地数据信息以及计算私有的模型参数）、一个物品服务器（用于存储物品信息） 和一个联邦服务器（用于聚合模型参数的梯度以及更新共享的模型参数）。

每个客户端具有（用户，物品）交互矩阵和（用户，特征）矩阵，物品服务器具有（物品，特征）矩阵。

- 首先，客户端使用本地数据，通过ALS算法计算本地用户潜在因子向量，然后通过SGD算法计算用户属性因子向量的梯度和物品潜在因子向量的梯度，并发送给联邦服务器；
- 同时，物品服务器在本地使用物品属性因子特征和联邦服务器发送的物品潜在因子矩阵，通过ALS和SGD算法，分别计算得到物品属性因子向量和物品潜在因子向量的梯度，并将物品潜在因子向量的梯度发送给联邦服务器；
- 然后，联邦服务器聚合客户端发送的用户属性因子向量的梯度和物品服务器发送的物品潜在因子向量的梯度，分别用于更新用户属性因子向量和物品潜在因子向量，最后再将更新后的向量发送回客户端用于物品推荐。

特点：使用了多视图矩阵分解的方法，有效地利用了用户属性和物品属性数据，从而提高了模型的推荐效果。

协同过滤推荐算法的联邦化(11/17)

Gao等人[41]总结了不同的推荐场景中的矩阵分解算法存在的隐私问题，并且针对这些问题提出了相应的解决方案（请看后面三页的内容） 。

协同过滤推荐算法的联邦化(12/17)

（1）在A和B两个参与方能够共享用户特征空间和物品特征空间的推荐场景中：

- 首先，双方各自使用本地数据来计算物品特征向量的梯度和用户特征向量的梯度，并分别用于更新物品特征向量和用户特征向量；
- 然后，使用模型平均算法，对双方的用户特征向量和物品特征向量进行聚合，得到全局的用户特征向量和全局的物品特征向量，即

$$U_{u\cdot}^{\mathrm{glb}} = \frac{(U_{u\cdot}^{\mathrm{A}} + U_{u\cdot}^{\mathrm{B}})}{2},$$
$$V_{u\cdot}^{\mathrm{glb}} = \frac{(V_{i\cdot}^{\mathrm{A}} + V_{i\cdot}^{\mathrm{B}})}{2}.$$

隐私问题：A方能够反推出B方的用户特征向量梯度$\nabla U_{u\cdot}^{\mathrm{B}}$和物品特征向量梯度$\nabla V_{i\cdot}^{\mathrm{B}}$。

解决方案：可以使用同态加密和安全多方计算等技术来保护全局的用户特征向量和物品特征向量。

协同过滤推荐算法的联邦化(13/17)

（2）在A方具有（用户，物品）交互矩阵，而B方只有一些用户或物品的辅助信息以及用户对物品的评分的推荐场景中：

- A方可以利用B方所具有的辅助信息来丰富用户特征。

隐私问题：在对齐用户ID时，会泄露B方的用户特征信息。

解决方案：建议B方对用户特征信息进行加密再发送给A方。

协同过滤推荐算法的联邦化(14/17)

（3）在A方和B方具有不同的用户集合和相同的物品集合的推荐场景中：

- 虽然A方能够反推出B方的用户u对物品的真实评分，但是用户ID是匿名的。
- 只需要对物品特征向量进行加密再发送给A方，而不需要加密用户特征向量。

协同过滤推荐算法的联邦化(15/17)

隐私保护的推荐系统框架（PPRSF）[42]是一个适用于基于内容的推荐算法模型、基于协同过滤的推荐算法模型和基于神经网络的推荐算法模型的框架，其分为4层：

- 召回层：处于服务端，输入为用户的公共数据和物品信息，输出为每个用户的召回物品(物品子集)；
- 排序层：处于客户端，输入为用户的本地数据和服务端生成的召回物品，通过本地排序模型，输出有序的候选物品列表；
- 重排层：输入为客户端的候选物品列表，通过一个可选方法来输出考虑了新鲜度和公平性等因素的候选物品列表；
- 服务层：处于客户端，展示最终的推荐结果，收集用户对物品的交互行为。

特点：召回层→减少发送物品列表时的通信成本；服务层→保护了用户的隐私。

协同过滤推荐算法的联邦化(16/17)

算法	基准算法	中间参数	特点
FCF	MF	物品梯度	保护了用户的原始评分、用户特征向量和用户的评分行为
FedRec	PMF, SVD++	物品梯度	使用了混合填充方法，采样了没有评过分的样本
FederatedMF	MF	物品特征向量	使用了数据匿名技术和差分隐私技术
FedMF	MF	物品梯度密文	使用了加法同态加密
SharedMF	MF	物品梯度密文	使用了秘密共享技术
FPL	BPR	物品梯度	第一个基于矩阵分解的联邦成对学习方法
FedRecSys	Wide&Deep, SVD, FM	模型参数	使用了同态加密和秘密共享技术
FRecLSH	LSH-based ANN	哈希签名	基于差分隐私，使用了本地敏感的哈希函数
PP-NMF	NMF	用户组特征向量	使用了匿名和k-means聚类，对用户组偏好进行了建模
FED-MNMF	MVMF	梯度	引入了第三方服务器，使用了物品属性数据和用户属性数据
PPRSF	CF, NN	模型参数	通过召回层，降低了通信成本

表 一些联邦协同过滤推荐算法的对比

协同过滤推荐算法的联邦化(17/17)

隐私问题	算法
用户的原始数据	FCF, FederatedMF, FedMF, SharedMF, FPL, FedRec, PPRSF, FRecLSH
用户的评分行为	FCF, FPL, SharedMF, FedRec
用户特征向量中隐含的用户偏好	FCF, FederatedMF, FedMF, FPL, FedRec
物品特征向量中隐含的用户评分分数	FedMF, SharedMF, FedRec

表 联邦协同过滤推荐算法解决的隐私问题

深度学习推荐算法的联邦化(1/7)

基于深度学习的联邦云视频推荐框架（JointRec）[43]使用卷积神经网络从用户和视频的属性以及用户对视频的评论中提取用户和视频的特征，并构建用户和视频的特征向量；然后将它们应用到PMF中来预测用户对视频的评分，进而为用户推荐视频。

特点：（1）减少多个云服务器之间协同训练时的通信成本：使用了权重参数压缩算法，即先使用低秩矩阵分解算法将权重参数分解成两个低秩的矩阵，然后再使用8位量化算法对这两个矩阵进行压缩；（2）JointRec仍能达到近似无损的推荐性能。

局限性：用户的原始数据保存在云服务器；没有分析多个云服务器在协同训练过程中所传递的参数可能存在的隐私问题

深度学习推荐算法的联邦化(2/7)

安全的联邦子模型学习框架（SFSL）[44]基于随机响应、安全聚合和布隆过滤器等技术实现了一个能支持百亿物品规模的深度学习推荐系统模型。

（1）在每轮训练过程中，随机采样的n个客户端使用布隆过滤器来表示已评分物品的索引；

（2）服务端通过安全聚合技术来获取所有客户端的物品索引的并集，并发送给这n个参与模型训练的客户端；

（3）每个客户端使用满足本地差分隐私的二次随机响应技术来选择需要下载的物品的特征向量。

特点：在多次随机应答后，服务端无法推测出客户端真实的评分行为；减少客户端的存储压力；减低了客户端和服务端之间的通信成本。

深度学习推荐算法的联邦化(3/7)

基于GMF的深度联邦推荐模型（FedFast）[45]通过客户端采样技术和安全聚合技术，加快了模型的收敛速度。客户端采样技术的技术细节：

- 在采样客户端之前，服务端使用k-均值算法，根据用户嵌入对用户进行聚类；
- 然后，客户端轮流从每一个聚类好的用户群中随机采样一个客户端参与模型训练，直到采样满足一定数目的客户端；
- 在每次算法迭代过程中都需要根据更新后的用户嵌入来更新用户群，然后重新选择参与模型训练的客户端；
- 参与训练的客户端A需将接收到的模型参数发送给处于同一群中的其他客户端，其他客户端利用客户端A发送的模型参数来加速自己的模型训练。

深度学习推荐算法的联邦化(4/7)

基于内容的联邦多视图框架（FL-MV-DSSM）[46]解决了冷启动的问题，还联合学习了多个视图的用户特征。

- 每个客户端有多个视图，每个视图可以看做一个应用程序(APP)，且不同应用程序的原始数据不能直接进行共享；
- 客户端在本地共享多个视图的用户和物品的特征向量梯度；
- 为了保护共享的梯度中蕴含的敏感信息，FL-MV-DSSM使用差分隐私技术向各个视图的物品特征向量的梯度中加入高斯噪声。

深度学习推荐算法的联邦化(5/7)

在基于GRU4Rec模型的通用的联邦序列推荐模型(DeepRec)[47]中，服务端可以收集一些必要的商业数据(例如，用户的购买记录)，同时，在GDPR条例颁布前收集到的数据仍可保存。

- 首先，服务端使用GDPR条例颁布前的数据，以及GDPR条例颁布后的商业数据，训练得到一个全局的模型；
- 其次，客户端下载全局模型，并根据本地数据进行微调，得到一个符合用户偏好的个性化联邦学习模型；
- 同时，在推荐物品之前，服务端会根据收集到的数据，使用基于物品相似度的协同过滤算法，计算得到物品的候选集；
- 最后，客户端只需要根据本地的个性化模型，对候选集进行排序，从而完成对物品的排序。

特点：客户端不需要上传任何中间参数给服务端。

局限性：DeepRec没有根据点击、购买等微观行为背后隐含的不同的偏好程度进行建模；

客户端的点击数据仅参与本地的模型训练，没有很好地帮助其他客户端训练有效的模型。

深度学习推荐算法的联邦化(6/7)

通用的GNN联邦推荐学习框架（FedGNN）[48]引入了第三方服务器

- 在对第三方服务器隐藏物品ID的情况下，第三方服务器帮助客户端匹配邻居用户，并以匿名的方式发送邻居用户的特征向量给客户端；
- 根据用户对物品的交互信息以及邻居用户的特征向量，客户端在本地构建（用户，物品）子图；
- 在模型训练时，客户端需要将计算好的物品特征向量的梯度发送给服务端聚合，为了保护用户的交互行为以及梯度信息，客户端采样部分没有交互过的物品，并使用本地差分隐私技术对参数的梯度加入噪声，再上传到服务端。

深度学习推荐算法的联邦化(7/7)

算法	基准算法	中间参数	特点
JointRec	CNN	权重参数	压缩了权重参数
SFSL	DIN	物品梯度	引入了子模型的概念，使用了二次随机响应技术
FedFast	GMF	模型参数	使用$k-means$聚类方法来加快模型训练
FL-MV-DSSM	DSSM	梯度	解决了DSSM的冷启动问题，使用了多个视图的用户特征，使用了差分隐私技术
DeepRec	GRU4Rec	-	假设商业数据可以被服务端收集
FedGNN	GNN	梯度	引入了第三方服务器，并对其隐藏物品ID，使用了虚假采样未交互过的物品的策略，使用了本地差分隐私技术

表 一些联邦深度学习推荐算法的对比

元学习推荐算法的联邦化(1/4)

基于Reptile元学习算法的联邦推荐框架（SEFR）[49]解决了推荐系统中的评分预测中的隐私问题。

- 该框架在经过多次全局训练以后，再在每个客户端进行局部训练，以微调全局模型使之适应客户端，达到个性化推荐的目的。

特点：保护用户的原始评分信息。

局限性：泄露了用户的评分行为。

元学习推荐算法的联邦化(2/4)

基于联邦学习的元矩阵分解框架（MetaMF）[50]解决了现有联邦推荐研究中生成的推荐模型较大而消耗较多客户端资源的问题。

- MetaMF能够为每个客户端生成一个私有的物品嵌入和一个较小的评分预测模型。
- 在MetaMF中，协同记忆（CM）模块和元推荐（MR）模块都部署在服务端，评分预测（RP）模块部署在客户端。其中，CM模块用于生成协作向量，MR模型以协作向量为输入，生成客户端私有的物品嵌入和RP模型，RP模块使用RP模型为用户进行评分预测。

元学习推荐算法的联邦化(3/4)

基于元学习的联邦推荐框架（Fed4Rec）[51]解决了页面推荐场景中共享数据给服务端的公共用户和将数据保留在客户端本地的私有用户如何进行协同训练的问题。

- 首先，服务端初始化模型参数，随后将模型参数发送给参与模型训练的客户端；
- 其次，客户端使用本地数据来训练模型参数，并将更新后的参数发送到服务端；
- 然后，服务端使用MAML元学习算法，利用公共用户的数据和私有用户上传的模型参数训练全局模型；
- 最后，服务端将全局模型发送给每个客户端，继续进行下一次的迭代训练，直到模型收敛。

特点：只有少数用户共享数据，而其他用户共享模型参数。

局限性：没有考虑在模型参数上传给服务端的过程中存在的隐私问题。

元学习推荐算法的联邦化(4/4)

算法	基准算法	中间参数	特点
SEFR	Reptile meta learning	模型参数	通过微调全局模型来适应每个客户端，从而构建个性化的联邦推荐模型
MetaMF	MF	梯度	结合了协同过滤和元学习
Fed4Rec	MAML	模型参数	解决了在只有少部分用户共享数据，而其他用户共享模型参数的场景中客户端协同训练的问题

表 一些联邦元学习推荐算法的对比

目录

基于同态加密的推荐算法(1/4)

同态加密技术（homomorphic encryption, HE）支持密文之间的运算，即解密后的密文运算结果与明文的运算结果相等，其包括加法同态加密算法、乘法同态加密算法和全同态加密算法。定义x和x_1为两个实数，E为加密算法，D为解密算法，$\oplus$为加法运算算法，$\otimes$为乘法运算算法。

- 加法同态加密：

$$D\big(E(x) \oplus E(x_1)\big) = x + x_1,$$

- 乘法同态加密：

$$D\big(E(x) \otimes E(x_1)\big) = xx_1,$$

- 全同态加密则同时具有加法同态加密算法和乘法同态加密算法的特性。

基于同态加密的推荐算法(2/4)

CryptoRec[52]假设云服务器是不可信的，因此客户端上传给云服务器的是经过同态加密技术处理后的用户偏好数据，服务端利用加密后的评分数据计算物品梯度并更新物品特征向量，在模型收敛后服务端返回预测评分给用户。

- 为了进一步提高模型的推荐效果，服务端在计算模型梯度之前使用用户的加密数据对模型进行微调。
- 为了减少通信成本以及加密后的数据的乘法次数，CryptoRec还使用了稀疏量化重用算法，其通过删除一些不在特定阈值范围内的模型参数来降低通信成本。
- 同时，在不影响模型准确率的情况下，通过复用两个加密数据的乘法计算结果来减少乘法次数。

基于同态加密的推荐算法(3/4)

Lyu等[53]针对地点推荐问题，基于物品的协同过滤方法和同态加密技术，提出了一个基于隐私保护的推荐框架，其主要包括3大部分：提供隐私保护推荐的服务器（PPRS），提供公钥和私钥的隐私服务提供方（PSP），加密的数据库（ED）。

- 首先，PSP将同态加密的公钥发送给用户和PPRS，同态加密的私钥仅自己拥有；
- 接着，用户使用地点访问信息，基于同态加密技术生成共生矩阵，并将其存储在ED中，然后将地点和偏好进行加密，分别发送给PSP和PPRS；
- 紧接着，PPRS使用加密后的用户地点和共生矩阵生成加密后的推荐列表，并将其发送给PSP；
- 最后，PSP对推荐列表进行解密并筛选出与用户有关的推荐地点，并将其推荐给用户。
- 此外，如果用户的行为有变化，那么需要更新存储在ED中的共生矩阵，从而对推荐列表进行更新。

基于同态加密的推荐算法(4/4)

Kim等人[54]将全同态加密技术应用于矩阵分解算法中，提出了一个基于虚假评分的推荐算法。

- 首先，客户端使用同态加密算法加密用户的真实评分数据和虚假评分数据后上传到服务端；
- 其次，服务端在密文中加上随机掩码后再发送给加密服务提供方（CSP）；
- 然后，CSP将密文解密，并使用定点算法处理，对处理结果加密并发送给服务端；
- 最后，服务端在消除虚假评分数据后使用梯度下降算法，与CSP进行联合计算，得到加密的用户和物品画像。

特点：（1）服务端与CSP的协同计算能提高全同态加密算法的性能，从而提高模型的计算效率；

（2）保护用户的原始评分数据、用户和物品的画像、用户的评分行为、用户已评分物品的数量以及用户的模型参数。

基于差分隐私的推荐算法(1/2)

差分隐私技术（differential privacy，DP）是一种在统计分析数据集信息时，用来保护数据集中的个体信息的加密技术。

给定任何两个相邻数据集$D_1, D_2 \in D$，它们最多只有一条数据记录不同，对于一个随机算法A，其所有可能的输出的任一子集S_A，如果存在如下不等式，则称算法A满足ϵ-差分隐私（即很难推断出是D_1 还是D_2 生成了S_A）：

$$\Pr[A(D_1) \in S_A] \leq e^{\epsilon} \Pr[A(D_2) \in S_A],$$

其中，ϵ是隐私预算，ϵ的值越小表示隐私保护强度越高，引入的噪声也就越多，通常需要设置合理的ϵ值来权衡隐私保护强度和模型性能。

基于差分隐私的推荐算法(1/2)

基于差分隐私的本地协同过滤算法（DPLCF）[55]解决了基于隐私保护的协同过滤算法无法较好地处理隐式反馈数据的问题，其主要包括3个计算步骤：

（1）客户端对隐式反馈数据使用满足差分隐私的随机翻转技术进行翻转，并上传给服务端；

当用户对物品的交互$r_{ui} = 1$时以概率p保留原来的值，以概率$1 - p$翻转为0；

当用户对物品的交互$r_{ui} = 0$时以概率$1 - q$保留原来的值，以概率q翻转为1；

（2）服务端使用这些数据，基于差分隐私的集合操作的分布式基数估计算法计算$|I_u^{\text{flip}} \cap I_{u_1}^{\text{flip}}|$和$|I_u^{\text{flip}} \cup I_{u_1}^{\text{flip}}|$，进而计算杰卡德物品相似度，然后将物品相似度矩阵发送给客户端；

（3）客户端使用物品之间的相似度，通过基于物品的协同过滤算法来进行物品推荐。

基于本地差分隐私的推荐算法(1/3)

在本地差分隐私技术（local differential privacy，LDP）中，用户数据在被不可信的第三方服务端收集前，由客户端自主加入噪声。

对于客户端u，假设其任意两个输入为D_1^u和D_2^u，对于一个随机算法A，如果存在如下不等式，则称算法A满足ϵ-本地差分隐私（即很难推断出是D_1^u还是D_2^u生成了S_A）：

$$\Pr[A(D_1^u) \in S_A] \leq e^{\epsilon} \Pr[A(D_2^u)] \in S_A.$$

基于本地差分隐私的推荐算法(2/3)

在隐私保护的推荐框架（PriRec）[56]中：

- 与用户隐私无关的公共数据（例如，POI的描述信息和POI的类别信息）保存在服务端以减少客户端的存储压力；
- 敏感数据（例如，用户的配置文件、用户对某个POI的交互行为和推荐模型）保存在客户端本地；
- 在建模过程需要的POI动态特征（如POI的访问量、POI的平均消费等）通过客户端上传使用本地差分隐私技术（LDP）来添加噪声后的数据，且使得服务端计算得到的POI动态特征能接近真实的访问量。

基于本地差分隐私的推荐算法(3/3)

FedNewsRec[57]是一个基于联邦学习的新闻推荐框架。

- 客户端在服务端中存储新闻推荐模型的副本，且客户端可以利用该副本进行模型梯度的计算，然后将该梯度进行裁剪之后上传到服务端；
- 服务端利用客户端上传的模型梯度进行模型的更新。

模型梯度中可能包含用户的敏感信息，因此客户端使用本地差分隐私技术往模型梯度中加入随机噪声。

基于安全多方计算的推荐算法(1/4)

安全多方计算技术（secure multi-party computation，SMPC）使得参与计算的各方能够在协同计算的同时保护各自数据的隐私，其主要包括秘密共享、同态加密和不经意传输等技术。

- 秘密共享是指一个参与多方计算的用户将自己的数据分割成多份秘密，然后将其发送给其他用户，只有用户达到一定数量才能一起重构秘密；
- 不经意传输能够保证发送方不知道接收方收到的是哪一部分数据，而接收方不能接收除特定数据以外的其他任何数据。

基于安全多方计算的推荐算法(2/4)

在PriRec[56]框架中，用户u需要对其邻居用户$u' \in \mathcal{N}(u)$的模型$W_{u'}$进行求和，而模型中包含的用户偏好信息会泄露邻居用户的隐私。因此，PriRec使用了秘密共享技术。

- 首先，用户u的邻居用户u'在本地计算得到权重线性模型$S_{uu'}W_{u'}$，其中$S_{uu'}$是用户u与邻居用户u'之间的权重；
- 其次，基于秘密共享技术，邻居用户$u' \in \mathcal{N}(u)$的权重线性模型$S_{uu'}W_{u'}$被划分成$|\mathcal{N}(u)|$份，保留一份在邻居用户u'本地，然后将剩下的$|\mathcal{N}(u)|-1$份发送给用户u的其他邻居用户；
- 然后，邻居用户$u' \in \mathcal{N}(u)$接收并汇总来自其他邻居用户的权重线性模型，并发送给用户u；
- 最后，用户u接收来自其他邻居用户通过秘密共享后的权重线性模型，用于更新模型W_u。

基于安全多方计算的推荐算法(3/4)

安全的社交推荐框架（SeSoRec）[58]在保护社交平台和评分平台的数据的同时，利用社交平台的信息来辅助评分平台提高推荐效果。

- SeSoRec使用了基于秘密共享的矩阵乘法（SSMM），使得两个来自不同参与方的矩阵在进行矩阵相乘操作时不泄露社交平台的隐私信息。

基于安全多方计算的推荐算法(4/4)

隐私保护的余弦相似度算法（PrivateCosine）和隐私保护的皮尔逊相似度算法(PrivatePearson)[59]使用秘密共享技术来计算物品之间的相似度。以PrivateCosine算法为例：

- 首先，客户端u在本地计算得到$r_{ui}r_{uj}$，r_{ui}^2和r_{uj}^2；
- 然后，客户端u将它们随机分割成k_u个分片，并将其中的k_u-1个分片发送给随机选择的其他客户端，其中$k_u>3$。
- 同时，客户端u将其他客户端发送过来的分片与对应的本地分片进行求和运算，再发送给服务端；
- 最后，服务端对客户端上传的值进行聚合，并计算得到物品之间的相似度。

与PrivateCosine算法有所区别，PrivatePearson算法还需要利用秘密共享技术计算物品的平均评分。

隐私保护技术在推荐系统中的应用

技术	优点	缺点	应用场景
同态加密	无损；高安全	计算复杂度较高	保护用户画像或物品描述[54]，保护用户行为[54]，保护用户的评分分数[52，54]
差分隐私	不依赖背景知识；隐私预算可调	损害模型精度	保护用户的隐私反馈数据[55]
本地差分隐私	防止不可信的服务端的差分攻击	损害模型精度	保护梯度中的敏感信息[57]，保护用户行为数据中的敏感统计信息[56]
秘密共享	无损；计算复杂度较低	通信复杂度较高	在多方协同计算过程中保护用户的信息[54，56，58，59]

表 联邦推荐中的隐私保护技术

目录

推荐系统的联邦化

- 传统的推荐模型的联邦化方面的相关工作仍存在其他的隐私问题
- 在联邦推荐模型中，通过隐私保护技术来保护隐私方面会带来通信成本增加、计算复杂度增大和推荐性能下降等新的问题
- 联邦模型的训练方式与非联邦版本等价的同时，算法的训练效率较低
- 在对基于深度学习的推荐算法进行联邦化方面，客户端的存储资源和计算能力通常无法与庞大的神经网络相匹配，并且客户端自身的数据量有限，难以训练出较好的深度学习模型
  - 边缘计算和知识蒸馏是两个解决客户端资源受限的研究思路
- 目前还没有公开发表的面向序列反馈和异构反馈建模的联邦推荐方法

联邦推荐系统的优化

- 模型压缩、通信策略的改进、激励机制和客户端采样等优化方法如何在联邦推荐模型中应用
- 如何为特定的推荐模型设计更有效的优化算法

联邦推荐场景中的隐私安全问题

- 如何衡量联邦场景中的隐私安全问题，并对已有工作中存在的隐私问题，设计一个更为有效的解决方法
- 如何在可能存在恶意的客户端和服务端或者存在一些数据质量较低的客户端的环境下，设计联邦推荐模型
- 客户端如何运用模型投毒防御和对抗攻击防御等防御手段来保护自己模型的安全性和有效性

目录

致谢

感谢国家自然科学基金项目（批准号：61836005，62172283）和科技创新2030—“新一代人工智能”重大项目（批准号：2018AAA0102300）资助。

参考文献

[1] Yang Q, Liu Y, Chen T J, et al. Federated machine learning: concept and applications. ACM Trans Intell Syst Technol, 2019, 10: 1–19

[2] Cheng K W, Fan T, Jin Y L, et al. SecureBoost: a lossless federated learning framework. 2018. ArXiv:1901.08755

[3] Wang S, Chang T H. Federated clustering via matrix factorization models: from model averaging to gradient sharing. 2020. ArXiv:2002.04930

[4] He C Y, Balasubramanian K, Ceyani E, et al. FedGraphNN: a federated learning system and benchmark for graph neural networks. 2021. arXiv:2104.07145

[5] Liu D B, Miller T A. Federated pretraining and fine tuning of BERT using clinical notes from multiple silos. 2020. ArXiv:2002.08562

[6] Wang Y J, Cui X L, Gao Z Q, et al. Fed-SCNN: a federated shallow-CNN recognition framework for distracted driving. Secur Commun Netw, 2020, 2020: 6626471

[7] Chen M Q, Mathews R, Ouyang T, et al. Federated learning of out-of-vocabulary words. 2019. ArXiv:1903.10635

[8] Liu Y, Kang Y, Xing C P, et al. A secure federated transfer learning framework. IEEE Intell Syst, 2020, 35: 70–82

[9] Sharma S, Xing C P, Liu Y, et al. Secure and efficient federated transfer learning. In: Proceedings of IEEE International Conference on Big Data, Los Angeles, 2019. 2569–2576

[10] Liu B Y, Wang L J, Liu M. Lifelong federated reinforcement learning: a learning architecture for navigation in cloud robotic systems. IEEE Robot Autom Lett, 2019, 4: 4555–4562

[11] Chen F, Dong Z H, Li Z G, et al. Federated meta-learning for recommendation. 2018. ArXiv:1802.07876

[12] Lin Y J, Ren P J, Chen Z M, et al. Meta matrix factorization for federated rating redictions. In: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 2020. 981–990

[13] Koneˇcn´y J, McMahan H B, Yu F X, et al. Federated learning: strategies for improving communication efficiency. 2016. ArXiv:1610.05492

[14] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, 2017. 1273–1282

[15] Lu S T, Zhang Y W, Wang Y L, et al. Learn electronic health records by fully decentralized federated learning. 2019. ArXiv:1912.01792

[16] Reisizadeh A, Mokhtari A, Hassani H, et al. FedPAQ: a communication-efficient federated learning method with periodic averaging and quantization. 2019. ArXiv:1909.13014

[17] Wang L P, Wang W, Li B. CMFL: mitigating communication overhead for federated learning. In: Proceedings of the 39th International Conference on Distributed Computing Systems, Dallas, 2019. 954–964

[18] Goetz J, Malik K, Bui D, et al. Active federated learning. 2019. ArXiv:1909.12641

[19] Cao T D, Truong-Huu T, Tran H D, et al. A federated learning framework for privacy-preserving and parallel training. 2020. ArXiv:2001.09782

[20] Yu H, Liu Z L, Liu Y, et al. A fairness-aware incentive scheme for federated learning. In: Proceedings of AAAI/ACM Conference on AI, Ethics, and Society, New York, 2020. 393–399

[21] Khan L U, Pandey S R, Tran N H, et al. Federated learning for edge networks: resource optimization and incentive mechanism. IEEE Commun Mag, 2020, 58: 88–93

[22] Kang J W, Xiong Z H, Niyato D, et al. Incentive design for efficient federated learning in mobile networks: a contract theory approach. In: Proceedings of IEEE VTS Asia Pacific Wireless Communications Symposium, Singapore, 2019. 1–5

[23] Zhao K, Xi W, Wang Z, et al. SMSS: secure member selection strategy in federated learning. IEEE Intell Syst, 2020, 35: 37–49

[24] Nishio T, Yonetani R. Client selection for federated learning with heterogeneous resources in mobile edge. In: Proceedings of IEEE International Conference on Communications, Shanghai, 2019. 1–7

[25] Wang Y W, Kantarci B. A novel reputation-aware client selection scheme for federated learning within mobile environments. In: Proceedings of the 25th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Pisa, 2020. 1–6

[26] Huang T S, Lin W W, Wu W T, et al. An efficiency-boosting client selection scheme for federated learning with fairness guarantee. IEEE Trans Parallel Distrib Syst, 2020, 32: 1552–1564

[27] Cho J Y,Wang J Y, Joshi G. Client selection in federated learning: convergence analysis and power-of-choice selection strategies. 2020. ArXiv:2010.01243

[28] M, Ivannikova E, Khan S A, et al. Federated collaborative filtering for privacy-preserving personalized recommendation system. 2019. ArXiv:1901.09888

[29] Chen C C, Liu Z Q, Zhao P L, et al. Privacy preserving point-of-interest recommendation using decentralized matrix factorization. In: Proceedings of the 32nd AAAI Conference on Artificial Intelligence, New Orleans, 2018. 257–264

[30] Duriakova E, Tragos E Z, Smyth B, et al. PDMFRec: a decentralised matrix factorisation with tunable user-centric privacy. In: Proceedings of the 13th ACM Conference on Recommender Systems, Copenhagen, 2019. 457–461

[31] Hegedus I, Danner G, Jelasity M. Decentralized recommendation based on matrix factorization: a comparison of gossip and federated learning. In: Proceedings of Machine Learning and Knowledge Discovery in Databases International Workshops of ECML PKDD, Wurzburg, 2019. 317–332

[32] Lin G Y, Liang F, Pan W K, et al. FedRec: federated recommendation with explicit feedback. IEEE Intell Syst, 2020, 36: 21–30

[33] K, Gyllensten I C, Lowet D, et al. Towards privacy-preserving mobile applications with federated learning: the case of matrix factorization. In: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, Seoul, 2019. 624–625

[34] D, Wang L Y, Chen K, et al. Secure federated matrix factorization. IEEE Intell Syst, 2021, 36: 11–20

[35] S C. Shared MF: a privacy-preserving recommendation system. 2020. ArXiv:2008.07759

[36] V W, Deldjoo Y, Noia T D, et al. How to put users in control of their data via federated pair-wise recommendation. 2020. ArXiv:2008.07192

[37] Tan B, Liu B, Zheng W V, et al. A federated recommender system for online services. In: Proceedings of the 14th ACM Conference on Recommender Systems, 2020. 579–581

[38] Hu H S, Dobbie G, Salcic Z, et al. A locality sensitive hashing based approach for federated recommender system. In: Proceedings of the 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, Melbourne, 2020. 836–842

[39] Wang X W, Yang H, Lim K. Privacy-preserving POI recommendation using nonnegative matrix factorization. In: Proceedings of IEEE Symposium on Privacy-Aware Computing, Washington, 2018. 117–118

[40] Flanagan A, Oyomno W, Grigorievskiy A, et al. Federated multi-view matrix factorization for personalized recommendations. 2020. ArXiv:2004.04256

[41] Gao D S, Tan B, Ju C, et al. Privacy threats against federated matrix factorization. 2020. ArXiv:2007.01587

[42] Qin J C, Liu B S. A novel privacy-preserved recommender system framework based on federated learning. 2020. ArXiv:2011.05614

[43] Duan S J, Zhang D Y, Wang Y B, et al. JointRec: a deep-learning-based joint cloud video recommendation framework for mobile IoT. IEEE Int Thing J, 2020, 7: 1655–1666

[44] Niu C Y, Wu F, Tang S J. Billion-scale federated learning on mobile clients: a submodel design with tunable privacy. In: Proceedings of the 26th Annual International Conference on Mobile Computing and Networking, London, 2020

[45] Muhammad K, Wang Q Q, O'Reilly-Morgan D, et,al. FedFast: going beyond average for faster training of federated recommender systems. In: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2020. 1234–1242

[46] Huang M K, Li H, Bai B, et al. A federated multi-view deep learning framework for privacy-preserving recommendations. 2020. ArXiv:2008.10808

[47] Han J L, Ma Y, Mei Q Z, et al. DeepRec: on-device deep learning for privacy-preserving sequential recommendation in mobile commerce. In: Proceedings of the 30th International Conference on World Wide Web, 2021. 900–911

[48] Wu C H, Wu F Z, Cao Y, et al. FedGNN: federated graph neural network for privacy-preserving recommendation. 2021. ArXiv:2102.04925

[49] Jalalirad A, Scavuzzo M, Capota C, et al. A simple and efficient federated recommender system. In: Proceedings of the 6th IEEE/ACM International Conference on Big Data Computing, Auckland, 2019. 53–58

[50] Lin Y J, Ren P J, Chen Z M, et al. Meta matrix factorization for federated rating redictions. In: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 2020. 981–990

[51] Zhao S, Bharati R, Borcea C, et al. Privacy-aware federated learning for page recommendation. In: Proceedings of IEEE International Conference on Big Data, Atlanta, 2020. 1071–1080

[52] Wang J, Tang Q, Arriaga A, et al. Novel collaborative filtering recommender friendly to privacy protection. In: Proceedings of the 28th International Joint Conference on Artificial Intelligence, Macao, 2019. 4809–4815

[53] Lyu Q Y, Ishimaki Y, Yamana H. Privacy-preserving recommendation for location-based services. In: Proceedings of the 4th International Conference on Big Data Analytics, Suzhou, 2019. 98–105

[54] Kim J, Koo D, Kim Y, et al. Efficient privacy-preserving matrix factorization for recommendation via fully homomorphic encryption. ACM Trans Priv Secur, 2018, 21: 17

[55] Gao C, Huang C, Lin D S, et al. DPLCF: differentially private local collaborative filtering. In: Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval, 2020. 961–970

[56] Chen C C, Wu B Z, Fang W J, et al. Practical privacy preserving POI recommendation. 2020. ArXiv:2003.02834

[57] Qi T, Wu F Z, Wu C H, et al. Privacy-preserving news recommendation model training via federated learning. 2020. ArXiv:2003.09592

[58] Chen C C, Li L, Wu B Z, et al. Secure social recommendation based on secret sharing. 2020. ArXiv:2002.02088

[59] D S, Chen C, Lv Q, et al. An algorithm for efficient privacy-preserving item-based collaborative filtering. Future Gener Comput Syst, 2016, 55: 311–320