中国科学: 信息科学 2022 年 第 52 卷 第 5 期: 713–741
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
评述

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*]

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 999077
* 通信作者. E-mail: panweike@szu.edu.cn, qyang@cse.ust.hk, mingz@szu.edu.cn
†同等贡献

收稿日期: 2021–10–08; 修回日期: 2021–11–23; 接受日期: 2021–12–01; 网络出版日期: 2022–05–12

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

摘要 随着互联网和移动计算等技术的发展, 人们的在线行为产生了越来越多的数据, 想要从海量数据中挑选出用户可能喜欢的物品, 推荐系统不可或缺. 然而传统的推荐算法需要将用户数据收集到服务端才能构建模型, 这会泄露用户隐私. 最近, 谷歌针对机器学习任务中需要收集用户数据才能进行建模的问题, 提出了一种新的学习范式 —— 联邦学习. 联邦学习与推荐系统相结合, 使得联邦推荐算法能够在模型构建过程中, 始终将用户数据保留在客户端本地, 从而保护了用户隐私. 本文主要对联邦学习与推荐系统相结合的研究工作进行综述, 并从架构设计、系统的联邦化和隐私保护技术的应用 3 个角度重点分析联邦推荐算法的研究进展. 最后, 对基于联邦学习的推荐系统可研究的方向进行展望.

关键词 推荐系统, 联邦学习, 隐私保护, 联邦推荐, 协同过滤

1 引言

在当今互联网大数据的背景下, 推荐系统能够利用海量的数据解决信息过载问题, 给用户带来便利的同时也给企业带来经济效益, 进而实现用户和企业的双赢. 许多企业将推荐系统应用在了各自的业务场景中, 例如, 淘宝的 “猜你喜欢”、网易云音乐的 “每日推荐”、腾讯视频的 “今日热门” 等, 类似的服务在人们日常的互联网生活中随处可见, 这些商业服务的建立离不开推荐算法.

随着通用数据保护条例 (general data protection regulation, GDPR) [1] 等隐私和数据保护法律法规的颁布, 以及人们隐私保护意识的提高, 用户数据中的隐私安全愈发受到重视. GDPR 等法律法规要求, 在未经用户同意的情况下, 任何组织和机构不得收集数据主体的个人数据. 然而传统的机器学习算法在没有获取足够多的用户数据的情况下, 往往难以通过训练得到一个有效的模型. 为了解决用户数据的隐私问题, 以及在不直接获取用户原始数据的前提下得到一个有效的模型, 谷歌 (Google) 提

引用格式: 梁锋, 羊恩跃, 潘微科, 等. 基于联邦学习的推荐系统综述. 中国科学: 信息科学, 2022, 52: 713–741, doi: 10.1360/SSI-2021-0329
Liang F, Yang E Y, Pan W K, et al. Survey of recommender systems based on federated learning (in Chinese). Sci Sin Inform, 2022, 52: 713–741, doi: 10.1360/SSI-2021-0329

出了联邦学习范式[2,3]. 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. 此外, 谷歌还将联邦学习应用在 Gboard 产品上, 用于表情符号预测[4] 和下一个单词的预测[5], 并且取得了不错的效果. Yang 等[1] 进一步将联邦学习分为横向联邦学习、纵向联邦学习和联邦迁移学习. 横向联邦学习是指在参与联合训练的多方中, 特征重叠较多, 样本重叠较少; 纵向联邦学习是指在参与联合训练的多方中, 特征重叠较少, 样本重叠较多; 而联邦迁移学习是指在参与联合训练的多方中, 特征重叠和样本重叠都较少. 目前对联邦学习的研究大多是基于横向联邦学习和纵向联邦学习, 而对联邦迁移学习的研究相对较少.

在推荐系统中, 用户的数据通常是指用户对物品的交互行为和用户的个人信息. 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. 为了解决这一问题, 一些研究工作[6,7] 将联邦学习应用于推荐算法的设计中, 使得用户在不上传自己的原始数据的前提下仍能得到良好的个性化服务. 近年来, 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. 在 2019 年的神经信息处理系统大会 (NeurIPS) 上, 微众银行以联邦推荐为主题介绍了他们的多个应用场景, 同时还基于自主研发的企业级联邦学习平台 FATE (federated AI technology enabler)[8] 提出了联邦矩阵分解和联邦因子分解机等算法, 引起了众多研究人员的关注. 目前, 对联邦推荐的研究仍处于起步阶段, 大多数联邦推荐算法通过设计不同的联邦训练策略对传统的推荐模型进行联邦化, 从而保护用户的隐私, 这也是本文论述的一个重点. 值得注意的是, 联邦学习领域中的一些重要问题, 如通信成本、计算效率和激励机制等, 在联邦推荐算法的设计中还较少涉及, 但它们在模型的训练和部署等方面有较大影响, 这也是本文关注的另一个重点.

本文主要对基于联邦学习的推荐系统的研究进行综述. 第 2 节首先简要介绍经典的和前沿的推荐算法, 其次从模型的架构、模型的联邦化、模型的优化和隐私保护技术的应用 4 个角度介绍联邦学习技术, 最后概述联邦推荐技术. 第 3~5 节分别从架构设计、系统的联邦化和隐私保护技术的应用 3 个角度重点分析基于联邦学习的推荐系统的研究进展. 第 6 节展望基于联邦学习的推荐算法的研究趋势. 第 7 节是结束语.

2 概述

2.1 推荐系统概述

传统的推荐方法主要包括基于内容的推荐、基于协同过滤 (collaborative filtering, CF) 的推荐和混合推荐. 基于内容的推荐算法的核心思想是给用户推荐与其历史交互过的物品相似的物品, 它能够解决物品的冷启动问题. 其中物品特征的提取较为关键, 只要能构建出新物品的特征描述, 该新物品就有可能被推荐给用户. 由于推荐的物品通常是与用户交互过的物品较为相似的物品, 因此基于内容的推荐算法难以推荐一些新颖的物品. 基于协同过滤的推荐算法的核心思想是给用户推荐与其历史偏好相似的用户群体交互过的物品, 其主要包括基于邻域的推荐算法和基于模型的推荐算法. 其中, 基于邻域的推荐算法主要分为两大类: 基于用户的协同过滤推荐算法[9] 和基于物品的协同过滤推荐算法[10]. 矩阵分解 (matrix factorization, MF)[11] 是协同过滤推荐算法中最受欢迎的算法之一, 其以高维的 (用户, 物品) 评分矩阵为输入, 输出一个低维的用户特征矩阵和一个低维的物品特征矩阵, 通过

用户特征矩阵和物品特征矩阵的内积计算得到用户对物品的评分矩阵. 与基于内容的推荐算法相比, 基于协同过滤的推荐算法考虑了不同用户偏好之间的关系, 但存在用户和物品的冷启动问题. 混合推荐算法将多种推荐算法以一定的方式组合起来, 以解决单一推荐算法存在的问题. 例如, 将基于内容的推荐算法和基于协同过滤的推荐算法结合起来的混合推荐算法, 能够解决物品的冷启动问题, 同时考虑了用户之间的偏好关系, 从而构建一个更好的推荐模型.

近年来, 随着深度学习在计算机视觉、语音识别和自然语言处理等领域的快速发展, 深度学习也成为推荐系统领域的一项重要技术. 与传统的推荐算法相比, 基于深度学习的推荐算法表达能力更强, 能够更好地挖掘数据的潜在特征, 获取深层次的用户和物品的特征描述. 基于深度学习的推荐算法主要利用一些深度学习技术, 如: 自编码器 [12]、受限玻尔兹曼机 (restricted Boltzmann machine, RBM) [13]、卷积神经网络 (convolutional neural network, CNN) [14] 和循环神经网络 (recurrent neural network, RNN) [15] 等, 来构建推荐模型. AutoRec [12] 是较为简单的基于深度学习的推荐算法, 其将自编码器技术应用到协同过滤中, 输入是某个用户对所有物品的评分构成的向量或所有用户对某个物品的评分构成的向量, 通过一个包含单隐层的神经网络, 让输出向量尽可能逼近输入向量, 从而预测输入向量中的缺失值, 进而实现对物品的排序和推荐. 但是 AutoRec [12] 没有很好地解决特征交叉问题, 模型的表达能力有一定的局限. Deep crossing [16] 设计了包含 embedding 层、stacking 层、multiple residual units 层和 scoring 层的网络结构, 通过多层残差网络对特征向量进行多次特征交叉, 从而捕捉更多非线性的特征信息. NCF (neural collaborative filtering) [17] 使用多层神经网络来代替矩阵分解中的内积操作, 使得用户特征向量和物品特征向量之间的交互更加丰富, 从而提高模型的表达能力. Wide&Deep [18] 和 Deep&Cross [19] 等通过组合不同特性的神经网络来提高模型的综合能力. DIN (deep interest network) [20] 等将注意力机制与基于深度学习的推荐算法结合, 使得模型能更好地捕捉用户的兴趣点. BERT4Rec [21] 将基于 Transformer 的双向编码器表征应用在序列推荐中, 用于捕捉用户行为序列上下文的关系, 以此来预测用户可能会喜欢的下一物品. NGCF (neural graph collaborative filtering) [22] 将 (用户, 物品) 表示为二部图, 将图神经网络 (graph neural network, GNN) 应用到协同过滤算法中, 并对 (用户, 物品) 的高阶交互历史行为进行建模.

上述推荐算法是基于集中式架构设计的, 其中客户端 (即用户) 仅充当数据产生者和数据传输者的角色, 而数据处理和模型构建的过程由服务端来实现. 由于客户端需要将用户的原始数据上传到服务端, 因此存在用户隐私泄露的风险. 同时, 为了充分利用数据的价值, 挖掘更高维的潜在特征, 服务端构建的推荐模型越来越复杂. 此外, 当用户数据增长到一定的数量级, 传统的集中式推荐系统通常难以满足越来越高的存储成本和计算成本的要求. 分布式推荐系统将用户数据或模型参数分布在各个数据节点或者计算节点中, 通过使用分布式计算和并行计算等技术来加快模型的训练, 从而支持更大规模的数据的处理和更复杂的推荐模型的构建 [23]. 需要说明的是, 隐私保护不是设计分布式推荐系统时首要关注的问题, 因而服务端通常可以收集各个节点的原始数据和模型参数.

在推荐系统的应用场景中, 可以将原始数据划分为用户个人信息、物品属性信息和用户与物品之间的交互信息. 对用户而言, 隐私信息包括用户的个人信息 (例如, 性别、年龄和地理位置等)、用户对物品的显式反馈 (例如, 用户对物品的评分等) 和用户对物品的隐式反馈 (例如, 用户对物品的点击、收藏和购买等) 等. 一般认为, 同一组织内部的物品属性信息是共享的, 不属于用户的个人隐私. 而对不同组织, 物品属性信息以及模型参数可能涉及公司的商业机密, 因此通常不能直接与其他组织共享.

2.2 联邦学习概述

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

表 1 联邦学习算法的分类

Table 1 Classification of federated learning algorithms

	Categories	Features or classical algorithms
Architectures of models	Client-server architecture	It can make full use of the server-side resources, but it has a single point of failure.
	Decentralized architecture	It can provide users with anonymity, and it has no single point of failure.
Federalization of models	Machine learning	Linear regression [1], tree boosting [25], clustering via matrix factorization [26], ...
	Deep learning	GNN [27], BERT [28], CNN [29], LSTM [30], ...
	Transfer learning	Refs. [31, 32]
	Reinforcement learning	Ref. [33]
	Meta learning	Refs. [34, 35]
Optimization of models	Model compression	Refs. [2, 3]
	Communication strategies	Refs. [3, 36∼40]
	Incentive mechanism	Refs. [41∼43]
	Sampling strategies for clients	Refs. [44∼48]
Privacy-preserving technology	Homomorphic encryption	It supports arithmetic operations on ciphertexts, but it is of high computation cost [49, 50].
	Differential privacy	It sacrifices model performance to enhance the strength of privacy protection [51, 52].
	Local differential privacy	The data is added with noise before it is collected by the servers [53].
	Secure multi-party computation	It includes techniques such as secret sharing, homomorphic encryption and oblivious transfer [54].

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 [24]. 需要说明的是, 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. 因此, 服务端在训练过程中需要满足各个参与方不同程度的隐私保护的要求. 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, 见表 1 [1∼3, 25∼54]. 其中, 模型的架构取决于不同的部署环境, 不同的架构在对模型进行联邦化时需要设计不同的训练流程. 对不同模型的联邦化的研究是联邦学习的研究重点, 而隐私保护技术是在模型联邦化过程中需要使用的重要技术手段. 对于联邦化后的模型, 考虑到不同的业务需求, 例如, 提高通信效率和模型性能等, 可以设计不同的模型优化策略.

2.2.1 模型的架构

通常, 在联邦学习中使用的架构可以分为客户端 – 服务端架构和去中心化架构. 如图 1 所示, 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以及从服务端接收到的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. 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更新本地的模型参数; (3) 客

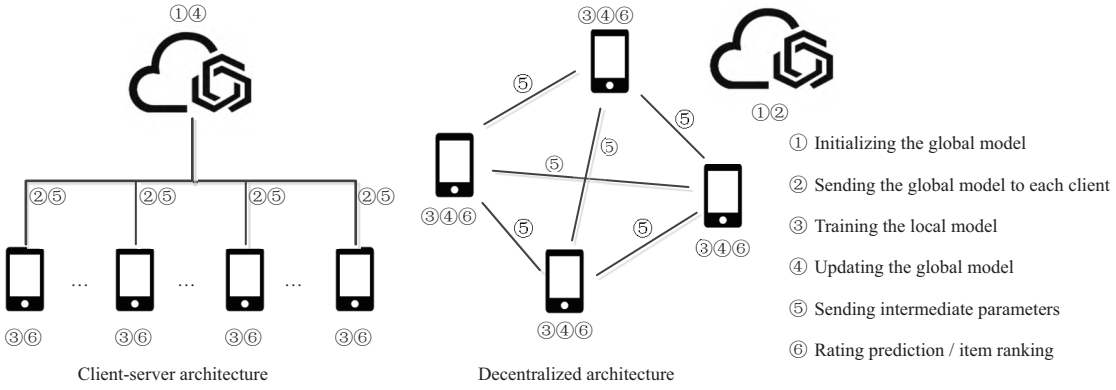

图 1 联邦学习的模型架构示意图

Figure 1 Diagram of model architectures of federated learning

户端选取一些其他客户端, 发送本地的中间参数, 同时接收其他客户端的中间参数, 并更新本地的模型; (4) 重复步骤 (2) 和 (3), 直到模型收敛. 需要说明的是, 不同组织之间的联邦应用场景, 例如, 纵向联邦学习和联邦迁移学习, 可以看作特殊的去中心化架构. 在这些场景中, 若引入第三方服务器, 则又可视为特殊的客户端 – 服务端架构.

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, 但容易发生单点故障. 同时, 对于好奇的服务端, 其可能根据客户端上传的中间参数推断客户端的隐私信息, 从而泄露客户端的隐私. 相比客户端 – 服务端架构, 去中心化架构不使用服务端或者服务端仅提供初始化模型参数和协助客户端之间通信的功能, 而不对模型进行更新. 去中心化架构的主要优势包括以下 3 个方面. (1) 匿名性 [55]. 在模型训练过程中, 客户端能以匿名的方式发送中间参数给其他客户端, 从而解决客户端之间的隐私泄露问题. (2) 节省服务端的资源. 服务端仅需初始化模型参数, 将模型参数分发给各个客户端, 不需要参与模型的更新. (3) 高可用性. 不存在单点故障, 即不会因为服务端的某一个部件出错而导致整个联邦学习系统中止训练.

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. 在实际应用中, 考虑到不同模型的优化需求, 使用这两种架构时的训练流程会有所不同, 例如, 为了减少通信成本, 一些基于客户端 – 服务端架构的联邦学习算法会采用在客户端多次训练后再将中间参数上传给服务端的训练方式 [3,36,37,56]. 我们将在 2.2.3 小节关于模型的优化中, 介绍一些对训练流程进行改进的方法.

2.2.2 模型的联邦化

为了保护各个参与方的隐私, 联邦学习采用原始数据不离开本地的建模方式, 因此, 在仅依赖传递加密的或不包含任何隐私信息的中间参数的前提下, 研究传统的机器学习算法能否联邦化, 是目前联邦学习研究的其中一个重点. 本小节将围绕这个主题介绍多种经典的和前沿的机器学习算法的联邦化方法.

对于传统的机器学习算法, Yang 等 [1] 将线性回归模型联邦化. 该模型引入了第三方服务器来辅助计算共享的损失函数和各个参与方的梯度. 为了不泄露任何信息给第三方服务器, 该模型还使用了同态加密技术对上传给第三方服务器的参数进行加密. Cheng 等 [25] 提出了安全联邦提升树, 在保护参与方原始数据中的隐私的前提下对齐各个参与方的样本, 并协同训练得到一个共享的梯度提升树模型.

Wang 等 [57] 通过对文档主题的联邦化, 提出了联邦隐含狄利克雷分布模型 (federated latent Dirichlet allocation, FedLDA), 其通过对筛选出的候选值进行扰动来保护数据隐私. Wang 等 [26] 首次将基于矩阵分解的聚类算法联邦化, 分别基于模型平均方法 [3] 和梯度共享方法提出了 FedCAvg 和 FedCGds 这两个联邦聚类算法. Wang 等 [58] 提出了一个基于草图 (sketch) 数据结构和差分隐私技术的联邦排序学习方法 (cross-silo federated learning to rank, CS-F-LTR), 有效地打通了组织之间的数据孤岛. 在 CS-F-LTR 中, 他们设计了一个通用的基于差分隐私的跨组织词频特征生成方法. 首先, 各个组织使用相同的哈希 (Hash) 函数在本地构建草图, 以便不同组织的数据之间相互查询. 其次, 为保证其他组织无法推断出需要查询的单词, 某一组织想要得到某个单词在另一组织的词频时, 使用带混淆的哈希函数对该单词进行哈希运算, 并将得到的向量发送给提供查询服务的组织. 然后, 提供查询服务的组织需要对查询结果进行扰动, 防止其他组织通过查询一些敏感的单词来推断本地的文档词频分布. 在对深度学习模型联邦化的研究中, He 等 [27] 设计了一个基于图神经网络 (GNN) 的联邦学习系统, 以促进基于 GNN 的联邦学习的研究. Liu 等 [28] 通过对双向表征编码器 (bidirectional encoder representations from Transformers, BERT) 模型的联邦化, 解决了在传输多个医疗机构的原始数据时存在的隐私问题. 在预训练阶段, 各个客户端首先使用自己的原始数据来训练本地模型, 然后服务器收集所有客户端的模型并以各个客户端中的样本数量为权重进行模型平均, 最后将更新后的模型发送给各个客户端. 经过周期性的预训练后, 每个客户端再针对特定的任务使用自己的原始数据进行模型微调, 从而得到一个效果较好的个性化联邦模型. Wang 等 [29] 提出了联邦浅层卷积神经网络 (shallow-CNN) 识别框架 (Fed-SCNN). 首先, 各个客户端通过深度神经网络 (deep neural networks, DNN) 和 shallow-CNN 构建本地的混合模型, 用以识别车内图像数据, 并以加密的方式上传中间参数给服务端. 其次, 服务端聚合收集到的加密参数, 构建一个全局的云模型. 最后, 客户端根据全局的云模型, 更新 DNN 并进一步优化混合模型. 重复上述步骤, 直到模型收敛. Fed-SCNN [29] 是一个基于动态学习的联邦框架, 其与现有的机器学习算法相比, 准确性和效率都有较大的优势. Chen 等 [30] 基于字符级的长短时间记忆神经网络 (long short-term memory, LSTM) 模型, 在不上传敏感的文本信息给服务端的情况下训练模型, 并通过从中提取的高频词来学习词汇外单词 (out-of-vocabulary, OOV), 从而达到扩展智能手机虚拟键盘词汇表的目的.

对于迁移学习模型, Liu 等 [31] 提出了一个安全联邦迁移学习框架. 该框架在协同多方优化目标函数时, 使用随机掩码和同态加密技术, 防止在交换模型损失和模型参数梯度的过程中泄露参与方的隐私信息. 考虑到同态加密带来的计算复杂度 [31], Sharma 等 [32] 使用秘密共享技术, 提出了一个更高效的联邦迁移学习框架. 对于强化学习模型, Liu 等 [33] 提出了一个终身联邦强化学习框架, 用于机器人学习导航, 使得机器人能够快速适应新环境. 首先, 服务端初始化模型参数. 然后处于不同环境中的机器人下载该模型, 使用强化学习技术学习导航, 并将训练好的模型上传给服务端. 最后, 基于生成网络的融合算法, 服务端融合各个机器人的模型. 融合后的模型能够应用在新环境中机器人的导航学习. 对于元学习模型, Chen 等 [34] 将元学习算法与联邦学习相结合, 以共享参数化的算法的方式, 提出了一个联邦元学习框架 (federated meta-learning, FedMeta). 同时, 他们在 MAML (model-agnostic meta-learning) [59] 和 Meta-SGD (meta-learner acts like stochastic gradient descent) [60] 上验证了该框架的有效性. 其中, MAML 只需学习参数 θ, 而 Meta-SGD 需要学习参数 θ 和内部学习速率 γ. 实验结果表明, FedMeta 训练得到的模型能够较快地适应新任务.

2.2.3 模型的优化

与传统的机器学习算法相比, 联邦学习的训练过程中存在以下问题. (1) 客户端资源受限问题. 客

户端通常是一些移动设备, 其存储能力、计算能力和通信带宽有限. 在模型训练过程中, 如果接收的数据包过大, 则会占用客户端本地过多的存储资源; 发送的数据包过大, 则会占用客户端过多的通信资源, 造成通信时延过长, 影响模型训练时间. (2) 贡献与回报不平等问题. 由于各个客户端的本地数据以及模型的质量不同, 且在联邦训练过程中, 不可避免会消耗各个客户端的资源. 如果没有得到与其贡献等价的收益, 客户端通常不愿意参与到训练过程中. (3) 客户端的在线率低. 由于网络带宽等原因, 在实际应用场景中, 客户端不可能时刻在线, 因此在联邦推荐算法的训练过程中, 想让所有客户端同时在线参与训练, 通常是比较困难的.

我们总结了以下几种能够解决或缓解上述问题的优化方法: 模型压缩、通信策略的改进、激励机制和客户端采样.

(1) 模型压缩. Konečný 等 [2] 提出了结构化更新算法 (structure update) 和草图更新算法 (sketch update), 用于降低客户端上传模型参数到服务端时的通信成本. 结构化更新算法分为低秩算法和随机掩码算法, 其中低秩算法将客户端要上传给服务端的模型参数分解成两个低秩的矩阵, 固定其中一个低秩矩阵, 训练另一个矩阵, 然后将训练好的矩阵发送给服务端. 随机掩码算法则将客户端要上传的模型参数转化为稀疏矩阵, 然后再上传到服务端. 草图更新算法分为子采样算法和概率量化算法, 其中, 子采样算法只随机采样部分模型参数上传到服务端, 而概率量化算法将模型参数的取值范围量化为两个或多个值, 以此来降低模型参数所占用的字节. Konečný 等 [2] 还提出了结构化随机旋转算法, 用于减少概率量化算法存在的误差. Xu 等 [61] 提出了基于三元量化压缩的联邦学习算法, 来降低客户端上传模型参数到服务端时的通信成本. 此外, 他们还提出了三元联邦学习协议, 降低客户端从服务端下载模型参数时的通信成本.

(2) 通信策略的改进. Lu 等 [36]、Liu 等 [56]、Reisizadeh 等 [37] 和 McMahan 等 [3] 通过在客户端本地执行多次迭代训练的方式来减少客户端与服务端之间的通信次数, 从而降低通信成本. 值得一提的是, Reisizadeh 等 [37] 还只挑选部分客户端进行模型训练, 并且使用低精度量化方法来压缩客户端要上传给服务端的模型参数. Wang 等 [38] 通过判断本地更新与上一次迭代训练时的全局更新是否相关来决定是否上传这部分本地更新的参数给服务端, 以此来提高联邦学习中的通信效率. Goetz 等 [39] 为了减少客户端上传和下载模型参数时的通信成本, 提出了一个主动联邦学习框架 (active federated learning, AFL). 在该框架中, 每个客户端执行一个价值评估函数 (例如, 损失函数), 然后将计算得到的价值上传给服务端, 服务端根据客户端上传的价值计算得到该客户端被挑选参与下一次模型训练的概率. 此外, 为了避免某些客户端永远没有被挑选到, AFL [39] 还从剩下的没有被挑选到的客户端中随机挑选部分客户端参与模型训练. Cao 等 [40] 提出了一个用于隐私保护和并行训练的分布式深度学习框架. 该框架基于客户端数据集的大小和损失值定义了一个优度函数 (goodness function), 每个客户端上传优度函数的输出值给服务端, 通过服务端的选择, 优度值较大的客户端将上传模型参数, 同时, 服务端将从剩余的客户端中获取一个表示模型更新方向的三元组用于模型的更新. 以三元组的方式上传模型参数, 既保护了客户端的隐私, 又降低了客户端的通信成本.

(3) 激励机制. 考虑到在现有联邦学习算法中不能解决用户贡献与奖励相匹配的问题, Yu 等 [41] 提出了联邦激励方案 (federated learning incentive, FLI). 该方案以用户贡献作为输入, 利用模型成本 (用户因贡献给联盟而产生的成本)、模型遗憾 (模型成本与用户应获奖励之差的累加和) 和模型时间遗憾信息, 在尽可能保证公平的同时, 给予一些贡献较大但是长时间没有获得足够多奖励的用户更多的奖励. Khan 等 [42] 基于斯塔克尔伯格博弈 (Stackelberg game) 设计了一个用于边缘网络的联邦学习激励机制. 该机制首先在基站设置一个回报率, 每个客户端根据回报率返回其认为最优的 CPU 频率给基站, 基站根据客户端返回的 CPU 频率继续调整回报率, 通过客户端和基站的交互, 在客户端获得尽可

能多的收益的同时, 基站也能够尽可能使得模型效果最好和模型训练时间最短. Kang 等 [43] 基于契约理论提出了一个激励机制, 吸引具有高质量数据的用户参与联邦学习的模型训练. 该机制根据用户所拥有数据的质量, 将用户划分为不同的类型, 基站 (任务发布者) 根据用户的类型为其提供契约 (包含不同的回报方案). 用户可以选择任意的契约进行签署, 并且需要完成对应的训练任务. 如果任务无法完成, 那么该用户将无法获得回报.

(4) 客户端采样. 考虑到在现有的联邦学习算法的训练过程中没有验证参与方的数据质量的问题, Zhao 等 [44] 基于杰卡德 (Jaccard) 相似度提出了一种安全的成员选择策略 (secure member selection strategy, SMSS). SMSS 使得参与联邦学习的成员能够通过公共渠道来相互验证并确认他们的公共实体 ID, 只有在成员通过了验证, 且公共实体 ID 的数量大于某个阈值时, 该成员才能参与联邦学习的训练. 此外, SMSS 在获取公共实体 ID 时, 使用了秘密的集合交集 (pirvate set intersection, PSI) 和 Shamir 的秘密共享等技术来避免用户隐私的泄露. Nishio 等 [45] 提出了一个联邦客户端选择协议 (federated client selection, FedCS). 在模型训练之前, 服务端会根据客户端的数据量、计算能力和无线信道的条件来估算服务端分发模型参数、客户端本地更新和客户端上传模型参数到服务端的时间. FedCS 通过基于贪心策略的启发式算法, 利用这些时间信息选择进行模型参数更新并上传到服务端所需的时间最少的客户端, 在指定时间内尽可能多的聚合客户端的模型参数. 为了消除在联邦学习的模型训练过程中一些对模型更新无用的客户端模型, Wang 等 [46] 提出了一种信誉评分方法. 该方法通过将客户端本地模型的测试效果, 与 (1) 每次迭代的本地模型测试效果的平均值, (2) 经过进一步训练但是没有聚合到全局模型中的局部模型的测试效果, 以及 (3) 上一次迭代的全局模型的测试效果分别相减, 再将得到的 3 个差值相加, 进而计算出每个客户端的信誉评分. 需要说明的是, 它们的差可以有不同的权重. 根据信誉评分, 服务端可以挑选出对模型更新有用的客户端本地模型, 以此来提高模型的准确率. 为了在最小化客户端与服务端的模型交换时间 (包括模型分发、模型训练和模型上传的时间) 的同时保证公平性, Huang 等 [47] 提出了基于信誉的公平客户端选择算法 (reputation based client selection with fairness, RBCS-F). 该算法首先使用李雅普诺夫 (Lyapunov) 优化框架将离线的客户端选择问题转换为在线问题, 然后使用上下文组合多臂赌博机 (contextual combinatorial multi-arm bandit, CC-MAB) 技术, 利用客户端的历史性能 (又称为信誉) 估计客户端与服务端模型交换的时间. RBCS-F 根据获取到的客户端的可用性 (即客户端是否愿意参与模型训练) 和模型交换时间等信息来选取一些客户端, 并将模型参数发送给这些客户端. 最后, 被选到的客户端使用本地数据进行模型训练, 然后将训练好的模型参数上传给服务端, 服务端统计模型交换时间并使用接收到的模型参数来更新模型. Cho 等 [48] 提出了一个有偏的客户端选择策略: 选择幂 (power-of-choice). 在该策略中, 服务端首先以特定的概率选择 n 个客户端作为客户端子集, 然后将全局模型发送给这些客户端, 这些客户端使用本地数据计算出局部损失并将其发送给服务端, 服务端选择损失最大的 n_1 ($n_1 < n$) 个客户端参与模型训练. 与随机采样客户端相比, 选择幂策略大大加快了收敛速度并提高了模型的效果.

2.2.4 隐私保护技术的应用

常用的隐私保护技术包括同态加密、差分隐私、本地差分隐私和安全多方计算等.

(1) 同态加密. 同态加密技术 (homomorphic encryption, HE) [49, 50] 支持密文之间的运算, 而不需要解密后再运算, 即解密后的密文运算结果与明文的运算结果相等. HE 常用的加密算法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. 加法同态加密是指密文 $E(x)$ 和 $E(x_1)$ 在经过算法 $\oplus$ 运算以后, 再将结果进行解密, 得到的结果与明文 x 和 x_1 相加的结果相等, 即 $D(E(x) \oplus E(x_1)) = x + x_1$.

类似的, 乘法同态加密有 $D(E(x)\otimes E(x_1))=xx_1$, 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.

(2) 差分隐私. 差分隐私技术 (differential privacy, DP) [51, 52] 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. 差分隐私技术在联邦学习中的应用较为广泛. 对主题模型进行联邦化时, 可以使用差分隐私技术来提供隐私保护 [62, 63]. 给定任何两个相邻数据集 $D_1, D_2\in\mathcal{D}$, 它们最多只有一条数据记录不同. 存在一个随机算法 A, 其所有可能的输出的任一子集为 S_A, 如果存在如下不等式, 则称算法 A 满足 ϵ–差分隐私:

$$\Pr[A(D_1)\in S_A]\leqslant e^{\epsilon}\Pr[A(D_2)\in S_A], \tag{1}$$

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. 值得说明的是, 噪声的引入使得攻击者不能轻易通过生成的输出 S_A 来推断输入的数据集是 D_1 还是 D_2. 例如, 对于包含某一个用户的隐私信息的数据集 D_1 和没有包含这一用户的隐私信息的数据集 D_2, 由于随机算法 A 使它们得到相同的输出结果的概率接近, 因此较难通过查询输出结果来推断数据集中是否包含该用户的隐私信息.

(3) 本地差分隐私. 差分隐私 [51] 需要将用户数据收集到服务端, 再使用随机响应 (randomized response) [64] 等技术进行数据的扰动处理, 而在本地差分隐私技术 (local differential privacy, LDP) [53] 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. 对于随机算法 A, 如果存在如下不等式, 则称其满足 ϵ–本地差分隐私:

$$\Pr[A(D_1^u)\in S_A]\leqslant e^{\epsilon}\Pr[A(D_2^u)\in S_A]. \tag{2}$$

值得说明的是, 随机算法 A 使得攻击者 (即服务端) 较难通过上传的输出值来推断用户的原始数据是 D_1^u 还是 D_2^u, 从而保护了用户的隐私.

(4) 安全多方计算. 安全多方计算技术 (secure multi-party computation, SMPC) [54] 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. SMPC 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, 通过这种方式, 用户得以安全地进行协同计算. 对于通信的双方, 不经意传输能够保证发送方不知道接收方收到哪一部分数据, 而接收方不能接收除特定数据以外的其他任何数据.

我们将在第 5 节中重点讨论这些隐私保护技术在联邦推荐系统中的应用.

2.3 联邦推荐系统概述

随着联邦学习在各个领域的应用, 对基于联邦学习的推荐系统的研究也受到了关注. 推荐系统通常需要通过用户的历史行为来学习用户的偏好. 此外, 为了训练得到更好的推荐模型, 通常还会结合用户的个人信息等数据. 用户的历史行为数据包括用户对物品的评分等显式反馈, 用户对物品的点击、收藏和购买等隐式反馈, 以及用户在物品上的浏览时间等其他信息. 用户的个人信息包括用户的性别、年龄、社交关系和地理位置等信息. 对用户而言, 这些都属于较为敏感的隐私数据, 用户通常不愿意提供给服务端. 除此之外, 不同组织之间的数据和模型可能涉及商业机密, 通常也不能直接共享, 进而导致组织之间的数据孤岛问题. 联邦学习和推荐系统的结合旨在保护用户隐私和商业机密的前提下, 为用户提供精准的个性化服务.

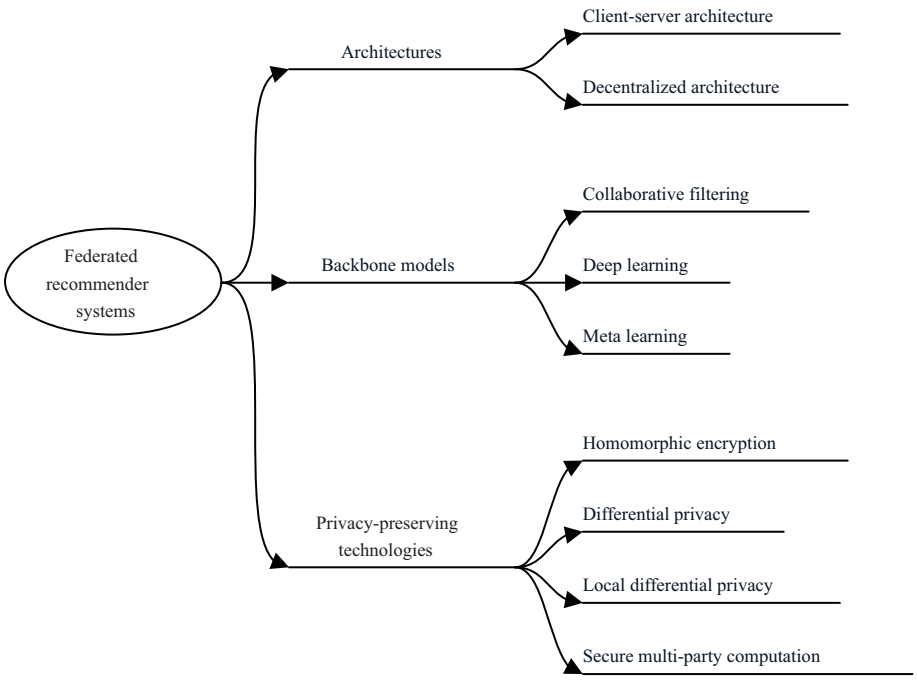

图 2　联邦推荐系统的分类

Figure 2　Categorization of federated recommender systems

联邦推荐系统是联邦学习领域的一个重要应用场景, 在这个场景中, 一个客户端可以是一个用户或一个组织, 客户端需在不共享数据的前提下联合建模. 与联邦学习的分类类似, 我们将从架构设计、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. 我们在图 2 中展示了上述的 3 个研究角度. 需要说明的是, 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, 我们将在第 6 节的展望部分进行讨论.

3　联邦推荐系统的架构设计

3.1　客户端 – 服务端架构

目前, 在大多数联邦推荐算法的研究中, 都使用了客户端 – 服务端架构. 我们将以 FCF (federated collaborative filtering) [7] 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. 概率矩阵分解算法 (probabilistic matrix factorization, PMF) [65] 是推荐算法中最经典的算法之一, 它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

$$\hat{r}_{ui} = U_{u\cdot} V_{i\cdot}^{\mathrm{T}}, \tag{3}$$

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. 在联邦学习的范式中, 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, 一旦上传给服务端, 服务端便能通过预测式 (3) 获得用户对物品的评分, 因此每个客户端 u 的用户特征向量 $U_{u\cdot}$ 也需要保留在客户端本地. 首先, 服务端初始化物品特征矩阵 V 并发送给每个客户端. 然后, 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

$$U_{u\cdot} = \frac{\sum_{i=1}^{m} y_{ui} V_{i\cdot}(1+\lambda y_{ui})}{\sum_{i=1}^{m}(V_{i\cdot}^{\mathrm{T}} V_{i\cdot} + \lambda y_{ui} V_{i\cdot}^{\mathrm{T}} V_{i\cdot} + \alpha I)}, \tag{4}$$

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. 进一步, 客户端计算并上传所有物品特征向量的梯度给服务端. 最后, 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. 需要说明的是, 由于基于最小二乘法的矩阵分解在计算 $V_{i\cdot}$ 的解析解时需要用户特征矩阵 U, 因此 FCF 在对 $V_{i\cdot}$ 的更新时采用梯度下降的方式. 在客户端上传计算好的物品特征向量的梯度后, 服务端聚合物品特征向量的梯度, 并更新物品特征向量. 重复多轮的迭代训练, 直到模型收敛.

3.2 去中心化架构

Chen 等 [66] 针对兴趣点 (point-of-interest, POI) 推荐中的物品排序问题, 提出了一个去中心化的分布式矩阵分解框架 (decentralized distributed MF, DMF). DMF 首先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 [67] 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、本地物品特征向量的梯度和全局物品特征向量的梯度. 其中, 用户特征向量的梯度和本地物品特征向量的梯度分别用于本地更新用户特征向量 $U_{u\cdot}$ 和本地物品特征向量 $V_{i\cdot}^{\mathrm{lcl},u}$, 全局的物品特征向量的梯度则发送给邻居用户 u' 用于更新全局的物品特征向量 $V_{i\cdot}^{\mathrm{glb},u'}$. DMF 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 [11] 和 BPR (Bayesian personalized ranking) [68]. 但是 DMF 在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. Duriakova 等 [55] 提出了一个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 (privacy-enhanced DMF for recommendation, PDMFRec), 解决了 DMF 在构建用户邻接图时暴露用户地理位置的问题, 与 DMF 相比, PDMFRec 能够达到更好的隐私保护效果. 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. 为了实现不同的隐私保护等级, PDMFRec 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. 此外, 除了在构建用户邻接图时能隐藏用户数据, 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. PDMFRec 区别于中心化的联邦推荐算法 [6,7,69] 的一个重要特性是, 客户端之间能够直接传递信息, 且客户端具有匿名性. Hegedüs 等 [70] 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, 而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.

4 推荐系统的联邦化

推荐模型的联邦化具有一定的共性, 一个联邦推荐模型的训练框架通常适用于具有相同训练方式的其他模型. 然而考虑到不同场景中的隐私保护级别可能不同以及不同模型参数可能带来的不同隐私问题, 不同推荐模型在联邦化的过程中存在一定的差异. 对于模型的联邦化, 可以划分为基于协同过滤

表 2 一些联邦推荐算法的对比

Table 2 Comparison of some federated recommendation algorithms

	Algorithms	Backbone models	Intermediate parameters	Features
Collaborative filtering	FCF [7]	MF	Gradients of items	It protects the users' original ratings, users' latent vectors and users' rating behaviors.
	FedRec [69]	PMF, SVD++	Gradients of items	It uses the hybrid filling strategy and the way of sampling some un-interacted items.
	FederatedMF [71]	MF	Latent feature vectors of items	It uses data anonymization measure and differential privacy.
	FedMF [6]	MF	Ciphertext of items' gradients	It uses additive homomorphic encryption.
	SharedMF [72]	MF	Ciphertext of items' gradients	It uses secret sharing technology.
	FPL [73]	BPR	Gradients of items	The first federated pairwise learning method based on matrix factorization.
	FedRecSys [74]	Wide&Deep, SVD, FM	Model parameters	It uses homomorphic encryption and secret sharing.
	FRecLSH [75]	LSH-based ANN	Hash signature	It uses a locality sensitive hashing function based on differential privacy.
	PP-NMF [76]	NMF	User group latent vectors	It uses anonymity and k-means methods, and models group preferences.
	FED-MNMF [77]	MVMF	Gradients	It introduces the third-party server, and uses items' feature data and users' feature data.
	PPRSF [78]	CF, NN	Model parameters	It reduces the communication cost in the recall layer.
Deep learning	JointRec [79]	CNN	Weight parameters	It compresses the weight parameters.
	SFSL [80]	DIN	Gradients of items	It introduces the sub-model methods, and uses doubly randomized response technology.
	FedFast [81]	GMF	Model parameters	It uses an aggregation method to speed up training.
	FL-MV-DSSM [82]	DSSM	Gradients	It solves the cold-start problem of DSSM, and uses multiple views of users' features and differential privacy.
	DeepRec [83]	GRU4Rec	None	It assumes that the business data can be collected.
	FedGNN [84]	GNN	Gradients	It introduces the third-party server, hides items' IDs from it, uses the strategy of sampling some fake interacted items, and uses local differential privacy.
Meta learning	SEFR [85]	Reptile meta learning	Model parameters	It fine-tunes the global model to fit each individual client and build a personalized federated model.
	MetaMF [35]	MF	Gradients	It combines collaborative filtering and meta learning.
	Fed4Rec [86]	MAML	Model parameters	It solves the scenario where only a few users share data, while others share parameters.

的推荐算法的联邦化、基于深度学习的推荐算法的联邦化和基于元学习的推荐算法的联邦化 3 个类别. 表 2 [6, 7, 35, 69, 71~86] 展示了一些推荐模型的联邦化的例子及其特点.

表 3 联邦协同过滤推荐算法解决的隐私问题

Table 3 Privacy issues solved by federated collaborative filtering recommendation algorithms

Privacy issues	Algorithms
Leakage of users' original data	FCF [7], FederatedMF [71], FedMF [6], SharedMF [72], FPL [73], FedRec [69], PPRSF [78], FRecLSH [75]
Leakage of users' rating behaviors	FCF [7], FPL [73], SharedMF [72], FedRec [69]
Leakage of users' preference implied by users' latent feature vectors	FCF [7], FederatedMF [71], FedMF [6], FPL [73], FedRec [69]
Leakage of users' rating scores implied by the gradients of items' latent feature vectors	FedMF [6], SharedMF [72], FedRec [69]

4.1 协同过滤推荐算法的联邦化

本小节主要介绍基于协同过滤的联邦推荐算法, 并在表 3 [6,7,69,71~73,75,78] 中总结了部分联邦协同过滤算法解决的隐私问题.

Ammad-ud-din 等 [7] 提出了第 1 个联邦协同过滤推荐算法 (FCF). 他们针对基于 ALS (alternating least square) 的协同过滤算法 (CF) [87] 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, 将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, 然后将物品特征向量的梯度上传到服务端进行物品特征向量的更新, 在保护用户的隐私的同时, FCF 能达到和 CF 一样的推荐性能. 虽然 FCF 在物品排序问题中能够较好地保护用户的原始评分信息, 但是在将其扩展到评分预测问题时, 所有未评分物品的评分被置为 0, 模型会产生偏差, 并且将所有物品特征向量的梯度都上传到服务端的方式将导致客户端通信成本的增加. 因此, Lin 等 [69] 提出了一个面向显式反馈的联邦协同过滤推荐算法 (federated recommendation, FedRec). 他们提出了混合填充方法: (1) 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; (2) 客户端 u 对随机采样的物品填充虚假的评分值. 在模型训练的前 t 次迭代中, 客户端 u 使用已评分物品的分值的平均值给未评分的物品进行分值填充, 在第 t 次迭代以后客户端 u 使用未评分物品的预测评分进行填充; (3) 最后, 利用这些虚假的评分来计算得到未评分物品的梯度, 并将客户端 u 的已评分物品和虚假采样的未评分物品的特征向量的梯度一起上传到服务端, 从而避免服务端得知客户端 u 评过分的物品. Lin 等在 PMF [65] 和 SVD++ (singular value decomposition with implicit feedback) [88] 上验证了混合填充算法的有效性. 需要说明的是, FedRec 中客户端与服务端的交互流程与 FCF 一致, 但是在 FedRec 中, 每个客户端仅上传已评分物品的梯度和虚假采样物品的特征向量的梯度.

Dolui 等 [71] 针对传统矩阵分解算法需要在服务端收集用户和物品特征矩阵的问题, 提出了一个联邦矩阵分解算法 (FederatedMF), 其将每个用户的 (用户, 物品) 评分向量存储在客户端本地, 并在本地进行用户特征向量 $U_{u\cdot}$ 和物品特征向量 $V_{i\cdot}$ 的更新, 然后将物品特征矩阵发送给服务端. 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 Doliu 等建议使用数据匿名化和差分隐私技术 [89] 对用户特征向量进行处理, 再发送给服务端. FederatedMF 通过将矩阵分解算法和联邦学习相结合, 不仅保护了用户的评分数据, 还节省了服务端的计算成本. 但是, 一旦将客户端上传的物品特征向量与更新前的物品特征向量进行对比, 服务端就能够推断出用户对哪些物品评过分, 从而泄露用户的评分行为. Chai 等 [6] 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. 为了解决上述问题, Chai 等提出了一个安全的联邦矩阵分解框架 (FedMF). FedMF 使用加法同态加密技术 [90] 对客户端将要上传到服务端的物品特征向量的梯度做加密处理, 从而保护了用户的评分信息. 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. 但是, FedMF 仍存在泄露用户评分行为的问题 (即用户对哪个物品评过分). 为了避免服务端在两次迭代训练过程中通过客户端连续上传的同一物品的特征向量的梯度来推断客户端对该物品的评分, 以及解决 FederatedMF [71] 和 FedMF 中存在的评分行为泄露问题, Ying 等 [72] 基于秘密共享技术 [91], 提出了共享矩阵分解方法 (SharedMF). 与使用加法同态加密技术的算法相比, SharedMF 的计算复杂度较低, 从而能够适用于较大规模的推荐场景. SharedMF 使用秘密共享技术对物品梯度的处理方法如下:

$$\nabla V_{i\cdot} = \nabla V_{i\cdot}^{(1)} + \nabla V_{i\cdot}^{(2)} + \cdots + \nabla V_{i\cdot}^{(n)}, \tag{5}$$

其中, n 表示客户端的数量, $\nabla V_{i\cdot}$ 表示物品 i 的特征向量梯度. 每个客户端 u 在其本地使用秘密共享技术 [91] 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, 保留一份在本地, 然后将剩下的 $n-1$ 份发送给其他客户端. 同时每个客户端 u 将会接收到来自其他客户端的物品特征向量的梯度分片. 然后客户端 u 将这些分片与本地保留的梯度分片进行求和运算, 最后将求和运算后得到的物品特征向量的梯度发送给服务端. 由于服务端从客户端 u 获取到的物品特征向量的梯度包含了其他客户端的物品特征向量的梯度信息, 所以服务端无法反推出客户端 u 对物品的真实评分, 从而保护了用户的评分行为.

Anelli 等 [73] 基于 BPR 算法 [68], 提出了一个联邦成对学习算法 (federated pairwise learning, FPL). 在 FPL 中, 客户端通过上传用户较不敏感的信息 (即用户未交互过物品的特征向量的梯度) 来进行模型参数的更新, 以达到保护用户评分行为的目的, 并且 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和模型效果. FPL 是第 1 个将成对学习应用于联邦学习的研究工作. FPL 的目标函数如下所示:

$$\min_{\Theta} \sum_{u\in\mathcal{U}} \sum_{i\in\mathcal{I}_u} \sum_{j\in\mathcal{I}\setminus\mathcal{I}_u} f_{uij}, \tag{6}$$

其中, $\Theta = \{U, V, b\}$ 表示待训练的模型参数, $f_{uij} = -\ln\sigma(\hat{r}_{uij} + \frac{\alpha}{2}(||U_{u\cdot}||^2 + ||V_{i\cdot}||^2 + ||V_{j\cdot}||^2 + ||b_j||^2 + ||b_i||^2))$, $\sigma(\hat{r}_{uij}) = \frac{1}{1+\mathrm{e}^{-\hat{r}_{uij}}}$, $\hat{r}_{uij} = \hat{r}_{ui} - \hat{r}_{uj}$. 参数 Θ 对应的梯度计算公式如下所示:

$$\nabla U_{u\cdot} = \frac{\partial f_{uij}}{\partial U_{u\cdot}} = -\sigma(-\hat{r}_{uij})(V_{i\cdot} - V_{j\cdot}) + \alpha U_{u\cdot}, \tag{7}$$

$$\nabla V_{i\cdot} = \frac{\partial f_{uij}}{\partial V_{i\cdot}} = -\sigma(-\hat{r}_{uij})U_{u\cdot} + \alpha V_{i\cdot}, \tag{8}$$

$$\nabla V_{j\cdot} = \frac{\partial f_{uij}}{\partial V_{j\cdot}} = -\sigma(-\hat{r}_{uij})(-U_{u\cdot}) + \alpha V_{j\cdot}, \tag{9}$$

$$\nabla b_{i\cdot} = \frac{\partial f_{uij}}{\partial b_{i\cdot}} = -\sigma(-\hat{r}_{uij}) + \alpha b_{i\cdot}, \tag{10}$$

$$\nabla b_{j\cdot} = \frac{\partial f_{uij}}{\partial b_{j\cdot}} = -\sigma(-\hat{r}_{uij})(-1) + \alpha b_{j\cdot}, \tag{11}$$

其中, 式 (7) 中的用户 u 的梯度 $\nabla U_{u\cdot}$ 保留在客戶端本地, 用于用户特征向量 $U_{u\cdot}$ 的更新. 需要说明的是, 用户特征向量 $U_{u\cdot}$ 包含了用户的敏感信息 (即用户对物品的偏好信息), 因此不能在服务端进行更新. Anelli 等发现, 通过观察式 (8) 和 (9), 或者观察式 (10) 和 (11), 在不包含正则化项时, $\nabla V_{i\cdot}$ 和 $\nabla V_{j\cdot}$,

以及 ∇b_i 和 ∇b_j 互为相反数. 因此服务端可以通过分析式 (8) 中物品 i 的特征向量的梯度 ∇V_i. 和式 (10) 中物品 i 的偏差梯度 ∇b_i 中的正负号, 来判断物品 i 是否是用户 u 评过分的物品, 从而重构出用户的评分行为. 为了解决这个问题, FPL [73] 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 π 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, 防止服务端重构出用户的评分行为. 在较好地保护了用户隐私的同时, FPL 的推荐性能也与传统的 BPR 算法 [68] 相当.

Tan 等 [74] 基于 FATE 平台建立了一个在线的联邦推荐系统 (FedRecSys), 他们使用同态加密 [90] 和秘密共享 [91] 技术, 实现了一些比较经典的推荐算法 (例如, 矩阵分解算法 [11]、分解机算法 [92] 和基于广度 &深度学习的推荐算法 [18] (Wide&Deep) 等). Tan 等 [74] 还在 2020 年推荐系统大会 (RecSys) 上公开演示了其系统[1]. Hu 等 [75] 针对已有的位置敏感哈希算法 (locality sensitive Hashing, LSH) [93] 难以量化隐私保护预算的问题, 提出了一种基于位置敏感哈希的联邦推荐算法 (federated locality sensitive Hashing, FRecLSH). 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) 使用本地差分隐私技术 [53] 处理哈希值 S_u, 得到扰乱后的哈希值 S'_u; (3) 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. FRecLSH [75] 通过本地差分隐私技术 [53], 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. Wang 等 [76] 为了保护 POI 推荐中用户的地理位置等隐私信息, 提出了一个基于非负矩阵分解 (nonnegative matrix factorization, NMF) 的 POI 推荐框架. 首先, 服务端挑选一批志愿者对一些地点进行签到; 其次, 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. 值得一提的是, 在整个模型的构建过程中, 用户的原始数据始终保留在本地, 达到了保护用户数据中的隐私的目的.

Flanagan 等 [77] 提出了第 1 个联邦多视图矩阵分解算法 (federated multi-view matrix factorization, FED-MVMF), 其通过集成来自多个数据源的信息来解决冷启动问题. 在 FED-MVMF 中, 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). 其中, 每个客户端有两个矩阵, 分别是 (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. 其中, 物品潜在因子向量的梯度需发送给联邦服务器; 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. 在 FED-MVMF 的训练过程中, 用户的原始数据和较为敏感的模型参数始终保留在本地. 同时, 其使用了多视图矩阵分解的方法, 有效地利用了用户特征和物品特征数据, 从而提高了模型的推荐效果.

Gao 等 [94] 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. 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

1) https://ad.webank.com/fedrecdemo/index.html?type=en.

到全局的用户特征向量和全局的物品特征向量. 模型平均的公式如下所示:

$$U_{u\cdot}^{\mathrm{glb}} = \frac{(U_{u\cdot}^{\mathrm{A}} + U_{u\cdot}^{\mathrm{B}})}{2}, \tag{12}$$

$$V_{i\cdot}^{\mathrm{glb}} = \frac{(V_{i\cdot}^{\mathrm{A}} + V_{i\cdot}^{\mathrm{B}})}{2}. \tag{13}$$

但是这一过程中仍存在隐私泄露的风险. 以 A 方为例, 在聚合过程中, 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 $\nabla V_{i\cdot}^{\mathrm{B}}$. 同理, A 方也会向 B 方泄露相同的信息. 因此, Gao 等建议使用同态加密 [49, 50] 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. 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, 但是在对齐用户 ID 时, 会泄露 B 方的用户特征信息. 因此, Gao 等建议 B 方应当对用户特征信息进行加密再发送给 A 方. 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 方同样能够计算出 B 方的物品特征向量的梯度, 甚至通过 B 方连续几次迭代传过来的物品梯度来反推出用户特征向量 $U_{u\cdot}^{\mathrm{B}}$ [6], 进而反推出 B 方的用户 u 对物品的真实评分. 但是由于 A 方和 B 方的用户不需要进行对齐, 即使发送了评分数据和用户特征向量, 用户 ID 仍处于匿名的状态. 因此, Gao 等建议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.

Qin 等 [78] 针对推荐系统中的物品排序问题, 提出了一个适用于基于内容的推荐算法模型 [95]、基于协同过滤的推荐算法模型 [11] 和基于神经网络的推荐算法模型 [18] 的框架, 即隐私保护的推荐系统框架 (privacy-preserved recommender system framework, PPRSF). PPRSF [78] 框架分为 4 层, 分别是召回层、排序层、重排层和服务层. (1) 召回层处于服务端, 其以用户的公共数据和物品信息为输入, 通过召回模型为每个客户端生成召回物品 (物品子集); (2) 排序层处于客户端, 其以用户的本地数据和服务端生成的召回物品为输入, 通过本地排序模型来生成有序的候选物品列表; (3) 重排层以客户端的候选物品列表为输入, 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; (4) 服务层处于客户端, 其展示最终的推荐结果, 并收集用户对物品的交互行为. PPRSF 通过召回层的处理, 减少了发送物品列表时的通信成本. 此外, 服务层也较好地保护了用户的隐私.

4.2 深度学习推荐算法的联邦化

Duan 等 [79] 提出了一个基于深度学习的联邦云视频推荐框架 (JointRec), 让多个拥有非独立同分布数据的云服务器进行联合训练, 从而为用户推荐更符合其需求的视频, 还能大大减少多个云服务器协同训练时的通信成本. JointRec 首先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 [65] 中来预测用户对视频的评分, 进而为用户推荐视频. 为了能够在多个云服务器之间协同训练用户和视频的特征向量, JointRec 将每个云服务器的权重参数发送到聚合器中进行聚合, 聚合完毕后再将其发送给每个云服务器, 用于更新用户和视频的特征向量. 更进一步, 为了减少多个云服务器之间协同训练时的通信成本, Duan 等 [79] 还提出了一个权重参数压缩算法, 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. 实验结果表明该算法在 12.83 的压缩比下, JointRec 仍能达到近似无损的推荐性能. JointRec 较好地解决了云服务器之间的数据孤岛问题, 同时也大大减少了云服务器之间的通信成本, 但是其将用户的原始数据保存在云服务器, 而非客户端本地. 此外, JointRec 也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隐私问题.

在传统的协同过滤推荐算法的联邦化过程中, 服务端通常将整个物品特征矩阵发送给客户端. 而当扩展到深度学习模型时, 物品特征矩阵通常非常庞大. 以淘宝平台为例, 其部署的推荐系统约有 20 亿个物品, 其物品特征矩阵大概需要 135 GB [80]. 然而, 客户端通常都是一些小型的移动设备, 如智能手机等. 客户端的通信能力和存储能力不足以下载整个物品特征矩阵, 且在实际应用中客户端只与其中的一小部分物品有交互. 为了减少客户端的通信成本, 服务端只需要将用户已评分物品的特征向量发送给特定的客户端, 同时客户端也只需上传已评分物品的梯度到服务端. 然而下载或者上传与物品 i 有关的参数代表用户对物品 i 评过分, 且服务端可以从梯度中推断出用户对物品的真实评分 [6]. 为了解决这些问题, Niu 等 [80] 结合随机响应、安全聚合和布隆过滤器等技术提出了一个安全的联邦子模型学习框架 (secure federated submodel learning, SFSL). 在每轮训练过程中, SFSL [80] 首先随机采样 n 个客户端参与模型训练, 在这些客户端中使用布隆过滤器来表示已评分物品的索引, 结合安全聚合技术, 在客户端能够保护自己评分行为 (即隐藏自己已评过分的物品的集合) 的前提下, 服务端获取所有客户端的物品索引的并集. 然后, 服务端将物品索引的并集发送给 n 个参与模型训练的客户端, 每个客户端使用满足本地差分隐私 (LDP) [53] 的随机响应技术来扰乱用户已评过分的物品和未评过分的物品, 从而保护了用户的评分行为. 需要说明的是, 为了防止在多次随机应答后, 服务端能根据在多轮迭代训练过程中每个物品出现的概率来推测随机响应的概率参数并重构客户端的评分行为, Niu 等改进了二次随机响应方法 [96], 使得在多次随机应答后, 服务端仍无法推测出客户端真实的评分行为.

Muhammad 等 [81] 提出了 FedFast 算法, 该算法将基于深度学习的推荐算法 GMF (generalized matrix factorization) [17] 和联邦学习进行结合. 首先, FedFast 算法使用客户端采样技术采样部分客户端来参与模型的训练, 然后对这些客户端上传的模型参数进行安全聚合. FedFast 算法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. 实验结果表明, FedFast 的推荐效果和模型收敛速度都优于基于 FedAvg [97] 的 GMF [17]. 在使用客户端采样技术之前, 服务端使用 k–均值 (k-means) 算法, 根据用户嵌入对用户进行聚类, 然后再执行客户端采样技术, 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. FedFast 算法在使用客户端采样技术时, 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. 服务端使用安全聚合技术将从客户端 A 接收到的模型参数发送给与客户端 A 处于同一群的其他客户端, 这样其他客户端也能够利用客户端 A 的模型参数来加速自己的模型训练.

Huang 等 [82] 基于深度结构化语义模型 (deep structured semantic models, DSSM) 提出了一个通用的基于内容的联邦多视图框架 (federated multi-view DSSM, FL-MV-DSSM), 其不仅解决了冷启动的问题, 还联合学习了多个视图的用户特征, 进一步提高了推荐效果. 在 FL-MV-DSSM 中, 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). 因为通用数据保护条例 (GDPR) [1] 等隐私和数据保护法律法规的限制, 不同应用程序的原始数据不能直接进行共享. 因此, 在 FL-MV-DSSM 中, 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.

Han 等 [83] 基于 GRU4Rec [98] 模型, 提出了一个通用的联邦序列推荐模型 (DeepRec). 他们认为一些商业数据 (例如, 用户的购买记录), 即使属于用户的隐私, 但为了完成订单, 服务端仍需要收集该数据. 同时, 他们假定在 GDPR 条例颁布前, 服务端仍保存有以往收集到的数据. 服务端首先使用 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.

DeepRec 的优点是客户端不需要上传任何中间参数给服务端, 避免隐私泄露的风险. 然而, 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. 同时, 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.

Wu 等 [84] 提出了一个通用的 GNN 联邦推荐学习框架 (FedGNN), 该框架引入第三方服务器, 在对第三方服务器使用同态加密隐藏物品 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.

需要说明的是, 上述提到的基于深度学习的联邦推荐模型都使用了客户端 – 服务端架构. 因此, 在训练过程中, 大多数模型都采用相似的训练方式, 即各个客户端从服务端接收全局模型, 同时各个客户端共享中间参数. 其中, 中间参数可以是权重参数 [79]、模型参数 [81] 或者梯度 [80, 82, 84] (见表 2). 然而, Han 等 [83] 认为, 即使对上传的中间参数进行加密或扰动, 其仍有可能泄露用户的隐私. 因此, 在 DeepRec 模型中, 各个客户端接收到预训练好的全局模型后, 仅使用本地数据对模型进行微调, 而不再发送任何参数给服务端.

4.3 元学习推荐算法的联邦化

元学习旨在利用以往的经验来指导新任务的学习, 能够在少量样本中快速学习出个性化的模型. 这种特性与联邦推荐的结合, 能够实现在客户端本地使用较少数据的情况下, 构建一个个性化的联邦推荐模型. 因此, 我们单独介绍基于元学习的联邦推荐方面的相关工作.

Jalalirad 等 [85] 提出了基于 Reptile 元学习算法 [99] 的联邦推荐框架, 用于解决推荐系统中的评分预测问题. 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. 虽然 Jalalirad 等 [85] 提出的模型能较好地保护用户的原始评分信息, 但是其上传的物品嵌入 (embedding) 泄露了用户的评分行为. Lin 等 [35] 为了解决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, 提出了一个基于联邦学习的元矩阵分解框架 (MetaMF), 其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 (collaborative memory, CM) 模块和元推荐 (meta recommender, MR) 模块都部署在服务端, 评分预测 (rating prediction, 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. MetaMF 模型的推荐效果优于目前一些较为先进的方法, 例如, NCF [17] 和 FedMeta [34]. Zhao 等 [86] 将联邦学习和与模型无关的元学习算法 (MAML) [59] 相结合, 提出了一个基于元学习的联邦推荐框架 (Fed4Rec), 其主要用于解决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. 在 Fed4Rec 中, 服务端首先初始化模型参数, 然后将模型参数发送给参与模型训练的客户端, 这些客户端使用本地数据来训练模型参数, 然后将更新后的参数发送到服务端, 服务端使用 MAML 元学习算法 [59], 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, 然后再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. Fed4Rec 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, 但是 Fed4Rec 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.

表 4 联邦推荐中的隐私保护技术

Table 4 Privacy protection technology in federated recommendation

Technologies	Advantages	Disadvantages	Scenarios
Homomorphic encryption	It is lossless and highly secure.	It is of high computation cost.	To protect user/item profiles [100], to protect users' bahaviors [100], to protect users' ratings [100∼103]
Differential privacy	It does not depend on background knowledge and its privacy budget can be managed.	It sacrifices model performance.	To protect implicit feedback of users [104]
Local differential privacy	It prevents differential attacks from an untrusted server.	It sacrifices model performance.	To protect sensitive information implied by gradients [105], to protect sensitive statistical information of users' action data [106]
Secret sharing	It is lossless and is of low computation cost.	It is of high communication cost.	To protect users' information from being accessed by other parties in multi-party collaborative computing [100, 106∼108]

5 隐私保护技术在联邦推荐系统中的应用

基于不同的隐私保护技术, 联邦推荐算法可以分为基于同态加密的联邦推荐算法、基于差分隐私的联邦推荐算法、基于本地差分隐私的联邦推荐算法和基于安全多方计算的联邦推荐算法. 如表 4 [100∼108] 所示, 我们总结了一些隐私保护技术在联邦推荐算法设计中的应用.

5.1 基于同态加密的推荐算法

考虑到直接将用户偏好数据存储在不可信的云服务器上会泄露用户的隐私, Soni 等 [102] 设计的算法在客户端使用同态加密技术对用户的偏好数据进行加密并上传到云服务器后, 再使用服务器对用户的加密数据进行分析. 为保护用户的原始评分数据, Wang 等 [101] 提出了一个基于隐私保护的推荐算法 (CryptoRec). 他们使用同态加密算法对用户的原始评分数据进行加密, 然后将加密后的用户评分数据上传到服务端, 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, 服务端进行评分预测, 然后返回对应的预测评分给用户. 此外, 为了进一步提高模型的推荐效果, CryptoRec 还在服务端计算模型梯度之前使用用户的加密数据对模型进行微调. 更进一步, 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 (sparse quantization reuse) 算法, 该算法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, 例如, 有两个加密后的数据 $E(x)$ 和 $E(x_1)$, 已计算它们的乘法结果, 如果有另外两个加密数据 $E(x_2)$ 和 $E(x_3)$ 分别与 $E(x)$ 和 $E(x_1)$ 相等, 那么直接复用 $E(x)$ 和 $E(x_1)$ 的乘法结果.

Lyu 等 [103] 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. 该框架主要包括 3 大部分: 提供隐私保护推荐的服务器 (privacy-preserving recommendation on server, PPRS), 提供公钥和私钥的隐私服务提供方 (privacy service provider, PSP), 加密的数据库 (encrypted database, 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加密后的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.

Kim 等 [100] 首次将全同态加密技术应用于矩阵分解算法中, 提出了一个对模型性能无损的基于虚假评分的推荐算法, 达到了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的目的. 首先, 该算法使用加法同态加密算法加密用户的真实评分数据和虚假评分数据, 并将其上传到服务端. 然后服务端在密文中加上随机掩码以保护用户的评分数据不被加密服务提供方 (crypto-service provider, CSP) 获取. CSP 将密文解密, 并使用定点算法处理, 然后将处理结果加密并发送给服务端. 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. 需要说明的是, 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.

5.2 基于差分隐私的推荐算法

针对现有一些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, Gao 等 [104] 提出了一个基于差分隐私的本地协同过滤算法 (differentially private local collaborative filtering, DPLCF), 其主要包括 3 个计算步骤: (1) 对每个客户端的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, 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) 将翻转后的隐式反馈数据上传到服务端, 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 (distributed cardinality estimation) [109] 能较为准确地计算得到 $|\mathcal{I}_u^{\text{flip}} \cap \mathcal{I}_{u_1}^{\text{flip}}|$ 和 $|\mathcal{I}_u^{\text{flip}} \cup \mathcal{I}_{u_1}^{\text{flip}}|$, 进而计算得到较为准确的杰卡德物品相似度. 其中, I_u^{flip} 和 $I_{u_1}^{\text{flip}}$ 分别表示客户端 u 和 u_1 经过翻转后的已评分物品的集合; (3) 将物品相似度矩阵发送给每个客户端, 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 [10] 来进行物品推荐. DPLCF 较好地保护了用户的隐式反馈数据和推荐结果, 同时实验结果表明模型的推荐效果优于一些较为先进的算法, 例如 BPR [68] 和 GMF [17].

5.3 基于本地差分隐私的推荐算法

Chen 等 [106] 面向 POI 推荐场景, 提出了一个隐私保护的推荐框架 (privacy preserving POI recommendation, PriRec), 其将一些公共的数据 (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. 需要说明的是, 这部分数据是所有用户共享的, 与用户的隐私无关. 此外, PriRec 将一些敏感的数据 (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. 在建模过程中, 服务端需要构建一些 POI 的动态特征, 如 POI 的访问量、POI 的平均消费等, 这可能会泄露客户端对 POI 的交互行为. 为了解决这个问题, PriRec 使用本地差分隐私技术 (LDP) [53], 使得用户的原始数据在被服务端收集之前, 由客户端自主添加干扰噪声, 从而保护所上传的数据中潜在的用户隐私信息, 同时服务端收集到的 POI 访问量能接近真实的访问量.

Qi 等 [105] 将新闻推荐与联邦学习相结合, 提出了 FedNewsRec 框架. 每个客户端在服务端中存储新闻推荐模型的副本, 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, 而服务端利用客户端上传的模型梯度进行模型的更新. 需要说明的是, 模型梯度中可能包含一些用户的敏感信息, 所以在上传裁剪后的模型梯度之前, 他们使用 LDP 技术往模型梯度中加入

随机噪声, 以此来保护用户的隐私, 同时模型的推荐效果也只受到了轻微的影响.

5.4 基于安全多方计算的推荐算法

5.3 小节中所介绍的 PriRec 框架 [106] 除了使用 LDP 技术保护用户对 POI 的交互行为外, 还使用了秘密共享技术 [91], 在使用去中心化梯度下降算法 [110] 学习线性模型时, 用于保护用户的偏好隐私. 在 PriRec 中, 每个用户 u 都需要对其邻居用户 u' 的线性模型进行求和, 求和过程中需要获取用户邻居 u' 的模型 $W_{u'}, u' \in \mathcal{N}(u)$, 而模型中包含的用户偏好信息会泄露邻居用户的隐私. 其中, $\mathcal{N}(u)$ 代表用户 u 的所有邻居. 为了解决这个问题, PriRec 首先在每个邻居用户本地 u' 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. 然后, 使用秘密共享技术将每个邻居用户 $u' \in \mathcal{N}(u)$ 的权重线性模型 $S_{uu'}W_{u'}, u' \in \mathcal{N}(u)$ 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. 每个邻居用户 $u' \in \mathcal{N}(u)$ 接收并汇总来自其他邻居用户的权重线性模型, 最后再将其发送给用户 u. 用户 u 接收来自其他邻居用户的权重线性模型, 用于更新模型 W_u. Chen 等 [107] 提出了一个安全的社交推荐 (secure social recommendation, SeSoRec) 框架, 其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. 同时, 他们提出了基于秘密共享的矩阵乘法 (secret sharing based matrix multiplication, SSMM), 使得 SeSoRec 在进行矩阵相乘操作时不泄露社交平台的隐私信息. Li 等 [108] 针对基于同态加密的协同过滤算法 [111] 的计算效率较低和基于随机扰乱的协同过滤算法 [112] 的推荐效果较差的问题, 使用秘密共享技术来计算物品之间的相似度, 在相似度计算过程中保证用户的评分信息不向服务端泄露. Li 等基于余弦相似度和皮尔逊相似度, 分别提出了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). PrivateCosine 算法首先在每个客户端 u 本地计算得到 $r_{ui}r_{uj}$, r_{ui}^2 和 r_{uj}^2, 然后使用秘密共享技术分别将它们随机分割成 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 $k_u \geqslant 3$. 同时, 客户端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, 然后再发送给服务端进行聚合, 并由服务端计算得到物品之间的相似度. PrivatePearson 算法与 PrivateCosine 算法类似, 区别在于 PrivatePearson 算法还需要利用秘密共享技术计算物品的平均评分.

Kaur 等 [113] 为了解决在基于用户的协同过滤推荐算法 [9] 计算用户之间相似度时泄露用户的评分和评分行为的问题, 提出了一个基于隐私保护的余弦相似度算法 (privacy preserving cosine similarity computation, PPCSC). 该算法首先扰乱目标用户对已评分物品和未评分物品的评分, 然后再将其发送给其他参与计算的用户. 其他参与计算的用户在接收到目标用户的扰乱评分后, 利用目标用户的扰乱评分和自己的扰乱评分计算得到一个扰乱值, 再将之发送给目标用户. 目标用户从接收到的扰乱值中提取出其与其他参与计算的用户之间的相似度, 从而在计算用户之间的相似度时保护用户的评分和评分行为. 实验结果表明, PPCSC 方法不会影响模型的推荐效果.

6 未来研究展望

最近, 十三届全国人大常委会第二十九次会议通过了《中华人民共和国数据安全法》[114], 对企业收集和使用公民个人信息等问题作出规制. 联邦学习通过不上传原始数据的学习范式, 结合多种隐私计算技术, 能在相关法律法规的要求下发挥数据的价值, 因此在推荐系统的应用中受到了学术界和工业界越来越多的关注. 然而, 目前联邦学习在推荐系统中的应用仍处于起步阶段, 在未来有很多值得尝试和探索的研究方向. 以下总结了 3 个值得探索的研究方向.

6.1 推荐系统的联邦化

在对传统的推荐模型进行联邦化方面, 目前已有不少的研究工作, 虽然它们都将原始数据保存在客户端本地, 但仍存在其他的隐私问题. 例如, 一些工作 [6, 71] 泄露了用户的评分行为, 即用户评过哪些物品. 以 FederatedMF [71] 为例, 服务端只要对比更新前后的物品特征向量, 就可以知道哪些物品的特征向量被更新过, 从而知道上传该特征向量的用户对哪些物品评过分. 再者, 一些工作 [7, 69] 直接上传物品特征向量的梯度给服务端, Chai 等 [6] 证明了连续两次上传同一个物品的梯度给服务端时, 服务端能够反推出用户对物品的评分. 此外, 为了获取更丰富的信息, 以 SVD++ [88], MF-MPC [115] 等算法为例, 他们使用了一些和评分值相关的模型参数. 例如, 在 MF-MPC 中, 不同的评分值 r 都有一个对应的模型参数 $M_{i\cdot}^r$. 当用户 u 更新物品 i 的 $M_{i\cdot}^r$ 时, 会直接暴露用户 u 对物品 i 的评分值. 虽然目前已有相关的研究, 使用如同态加密 [6, 74, 94]、虚假采样 [69, 73, 116]、差分隐私 [89] 和秘密共享 [72, 74] 等技术, 能较好地解决这些隐私问题, 但这些技术会带来如通信成本增加、计算复杂度增大和推荐性能下降等新的问题. 此外, 一些经典的推荐算法 (例如, PMF [65] 和 BPR [68] 等) 以 SGD 作为优化方法时, 其每次只采样一个 (用户, 物品) 对, 然后计算用户特征向量的梯度和物品特征向量的梯度, 并用于更新对应的用户特征向量和物品特征向量. 在联邦学习范式中, 以分布式学习的方式进行模型训练时, 每次只采样一个 (用户, 物品) 对的训练方式会导致算法的训练效率较低. 一个提高效率的训练方式是让客户端并行地进行模型训练 [97], 再对上传的物品特征向量的梯度进行平均, 然而这样的做法与非联邦版本的对应算法相比, 得到的效果往往会有所下降. 在对推荐模型进行联邦化时, 如何在训练方式与非联邦版本等价的同时, 保证算法的训练效率, 也是联邦推荐值得关注的一个问题.

目前对于基于深度学习的推荐算法的联邦化的研究相对较少. 主要挑战在于, 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. DeepRec [83] 采用模型参数较少的 RNN 作为主干模型, 然而对于更大规模的神经网络, 客户端的存储资源会比较受限. Niu 等 [80] 使用随机响应技术, 使得客户端能以子模型的方式来下载和上传模型. 然而这种方式仅支持物品的特征向量能按行表示的模型, 模型的通用性有一定的限制. 将模型参数和计算过程交给边缘设备的边缘计算 [117], 以及从学习能力强的教师模型中提炼出参数较少的学生模型的知识蒸馏 [118], 是两个解决客户端资源受限的研究思路.

除此之外, 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. 在保护隐私的前提下, 运用序列信息和多行为等数据, 构建一个性能更好的联邦推荐模型, 也是一个值得研究的问题.

6.2 联邦推荐系统的优化

在 2.2.3 小节中介绍了 4 种适用于联邦学习的优化方法, 即模型压缩、通信策略的改进、激励机制和客户端采样. 这些优化方法如何在联邦推荐模型中应用, 以及如何为特定的推荐模型设计更有效的优化算法, 值得深入研究. 现有的部分研究工作或能给予一定的启发. 如 Yang 等 [119] 提出的 FCMF (federated collective matrix factorization), 针对纵向联邦推荐问题, 设计了一个有效的通信策略: 辅助方先充分训练好物品特征矩阵, 加密后发送给目标方. 在目标方训练过程中, 只有少数的中间参数需要回传给辅助方解密. Minto 等 [120] 发现在 FCF 框架中对物品特征向量的梯度使用本地差分隐私技术进行处理时, 训练得到的模型性能较差. 因此, 对于每一个要上传给服务端的梯度, 他们仅对其随机的某一维度添加噪声, 在满足差分隐私的条件下, 提高了模型的性能.

6.3 联邦推荐场景中的隐私安全问题

在较早的研究工作中, 原始数据和能表征用户偏好的模型参数被视为用户的隐私. 因此, 在保留原始数据和用户特征向量的情况下, FCF [7] 上传物品特征向量的梯度, 用于构建全局的物品特征矩阵. 在文献 [6] 中, 研究人员证明了物品特征向量的梯度会泄露用户的评分信息. 为了解决这个问题, SharedMF [72] 使用秘密共享技术, FedMF [6] 使用同态加密技术. 然而, 在训练过程中, 仅有与用户交互过的物品需要上传梯度, 因而在上传某个物品特征向量的梯度时, 在保护了梯度信息的情况下, 通过分析物品特征向量的 ID, 仍能推导出用户的评分行为. 因此在已有的研究工作中, FPL [73] 和 FedRec [69] 采用虚假采样的方式, 混淆评过分的物品. 此外, 在最近的研究工作中, DeepRec [83] 认为, 一些商业数据的收集并不违反 GDPR 等法律法规 [1]. 例如, 用户购买一个商品时, 需要在付款后将购买行为告知服务端, 否则该订单无法完成. 因此, 这些必要的商业数据能够被服务端收集, 而其他隐私数据, 例如在完成订单前对商品的点击、浏览等行为, 以及在完成订单后对商品的评分、评论等行为, 则不能直接被服务端收集. 未来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, 是一个非常有价值的研究问题.

除此之外, 大部分联邦场景都假设服务端和客户端是诚实且好奇的. 未来的研究工作可假设更复杂的真实环境, 即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. 在这种环境下, 在一个联邦推荐模型中设计一个能辨别数据源的可靠性的算法, 是一个值得研究的问题. 例如, 服务端可对上传的模型参数质量进行评估 [121], 从而筛选出恶意的或低质量的模型参数, 也可以通过将主成分分析技术 (principal component analysis, PCA) 和数据复杂度相结合 [122], 使用检测托攻击算法来解决客户端伪造虚假评分, 还可以通过客户端之间梯度的差异来检测恶意的客户端 [123]. 此外, 在去中心化的架构中通常采用匿名的方式传递参数, 这给恶意的客户端提供了攻击的机会. 例如, 攻击者很容易通过匿名的方式, 将精心制作的参数传递给其他客户端, 以操控训练数据分布 [124]. 因此, 客户端如何运用模型投毒防御 [124] 和对抗攻击防御 [125] 等防御手段来保护自己模型的安全性和有效性, 也是一个值得研究的问题.

7 结束语

在大数据时代, 安全与隐私问题日益受到重视, 对与用户隐私保护问题息息相关的联邦推荐算法的研究, 将成为基于用户行为数据建模的推荐算法中不可或缺的一部分. 如何更好地设计和优化联邦推荐模型, 在保护用户隐私的同时, 实现个性化推荐, 是一个十分重要的研究问题. 本文通过对推荐系统和联邦学习等的介绍, 从 4 个角度阐述联邦学习的研究方向, 分析基于联邦学习的推荐系统的研究进展, 并讨论联邦推荐中可尝试和可探索的研究方向, 希望对工业界和学术界相关领域的研究工作者们带来一定的帮助和思考.

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 Konečný J, McMahan H B, Yu F X, et al. Federated learning: strategies for improving communication efficiency. 2016. ArXiv:1610.05492

3 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

4 Ramaswamy S, Mathews R, Rao K, et al. Federated learning for emoji prediction in a mobile keyboard. 2019. ArXiv:1906.04329
5 Yang T, Andrew G, Eichner H, et al. Applied federated learning: improving Google keyboard query suggestions. 2018. ArXiv:1812.02903
6 Chai D, Wang L Y, Chen K, et al. Secure federated matrix factorization. IEEE Intell Syst, 2021, 36: 11–20
7 Ammad-ud-din M, Ivannikova E, Khan S A, et al. Federated collaborative filtering for privacy-preserving personalized recommendation system. 2019. ArXiv:1901.09888
8 Liu Y, Fan T, Chen T J, et al. FATE: an industrial grade platform for collaborative learning with data protection. J Mach Learn Res, 2021, 22: 1–6
9 Zhao Z D, Shang M S. User-based collaborative-filtering recommendation algorithms on Hadoop. In: Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, Phuket, 2010. 478–481
10 Sarwar B M, Karypis G, Konstan J A, et al. Item-based collaborative filtering recommendation algorithms. In: Proceedings of the 10th International Conference on World Wide Web, Hong Kong, 2001. 285–295
11 Koren Y, Bell R, Volinsky C. Matrix factorization techniques for recommender systems. Computer, 2009, 42: 30–37
12 Sedhain S, Menon A K, Sanner S, et al. AutoRec: autoencoders meet collaborative filtering. In: Proceedings of the 24th International Conference on World Wide Web, Florence, 2015. 111–112
13 Biswal A, Borah M D, Hussain Z. Music recommender system using restricted Boltzmann machine with implicit feedback. Adv Comput, 2021, 122: 367–402
14 Cheng J, Wang P S, Li G, et al. Recent advances in efficient computation of deep convolutional neural networks. Front Inf Technol Electron Eng, 2018, 19: 64–77
15 Huang L W, Jiang B T, Lv S Y, et al. Survey on deep learning based recommender systems. Chin J Comput, 2018, 41: 1619–1647 [黄立威, 江碧涛, 吕守业, 等. 基于深度学习的推荐系统研究综述. 计算机学报, 2018, 41: 1619–1647]
16 Ying S, Hoens T R, Jian J, et al. Deep crossing: web-scale modeling without manually crafted combinatorial features. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, 2016. 225–262
17 He X N, Liao L Z, Zhang H W, et al. Neural collaborative filtering. In: Proceedings of the 26th International Conference on World Wide Web, Perth, 2017. 173–182
18 Cheng H T, Koc L, Harmsen J, et al. Wide & deep learning for recommender systems. In: Proceedings of the 1st Workshop on Deep Learning for Recommender Systems, Boston, 2016. 7–10
19 Wang R X, Fu B, Fu G, et al. Deep & cross network for ad click predictions. In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, 2017
20 Zhou G R, Zhu X Q, Song C R, et al. Deep interest network for click-through rate prediction. In: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, London, 2018. 1059–1068
21 Sun F, Liu J, Wu J, et al. BERT4Rec: sequential recommendation with bidirectional encoder representations from transformer. In: Proceedings of the 28th ACM International Conference on Information and Knowledge Management, Beijing, 2019. 1441–1450
22 Wang X, He X N, Wang M, et al. Neural graph collaborative filtering. In: Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval, Paris, 2019. 165–174
23 Karydi E, Margaritis K. Parallel and distributed collaborative filtering: a survey. ACM Comput Surv, 2016, 49: 1–41
24 Kairouz P, McMahan H B, Avent B, et al. Advances and open problems in federated learning. Found Trends Mach Learn, 2021, 14: 1–210
25 Cheng K W, Fan T, Jin Y L, et al. SecureBoost: a lossless federated learning framework. 2018. ArXiv:1901.08755
26 Wang S, Chang T H. Federated clustering via matrix factorization models: from model averaging to gradient sharing. 2020. ArXiv:2002.04930
27 He C Y, Balasubramanian K, Ceyani E, et al. FedGraphNN: a federated learning system and benchmark for graph neural networks. 2021. ArXiv:2104.07145
28 Liu D B, Miller T A. Federated pretraining and fine tuning of BERT using clinical notes from multiple silos. 2020. ArXiv:2002.08562
29 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

30 Chen M Q, Mathews R, Ouyang T, et al. Federated learning of out-of-vocabulary words. 2019. ArXiv:1903.10635
31 Liu Y, Kang Y, Xing C P, et al. A secure federated transfer learning framework. IEEE Intell Syst, 2020, 35: 70–82
32 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
33 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
34 Chen F, Dong Z H, Li Z G, et al. Federated meta-learning for recommendation. 2018. ArXiv:1802.07876
35 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
36 Lu S T, Zhang Y W, Wang Y L, et al. Learn electronic health records by fully decentralized federated learning. 2019. ArXiv:1912.01792
37 Reisizadeh A, Mokhtari A, Hassani H, et al. FedPAQ: a communication-efficient federated learning method with periodic averaging and quantization. 2019. ArXiv:1909.13014
38 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
39 Goetz J, Malik K, Bui D, et al. Active federated learning. 2019. ArXiv:1909.12641
40 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
41 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
42 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
43 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
44 Zhao K, Xi W, Wang Z, et al. SMSS: secure member selection strategy in federated learning. IEEE Intell Syst, 2020, 35: 37–49
45 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
46 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
47 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
48 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
49 Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, Prague, 1999. 223–238
50 Craig G, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. In: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, 2011. 129–148
51 Li T, Song L Q, Fragouli C. Federated recommendation system via differential privacy. In: Proceedings of IEEE International Symposium on Information Theory, Los Angeles, 2020. 2592–2597
52 Li X G, Li H, Li F H, et al. A survey on differential privacy. J Cyber Secur, 2018, 3: 92–104 [李效光, 李晖, 李凤华, 等. 差分隐私综述. 信息安全学报, 2018, 3: 92–104]
53 Cormode G, Jha S, Kulkarni T, et al. Privacy at scale: local differential privacy in practice. In: Proceedings of International Conference on Management of Data, Houston, 2018. 1655–1658
54 Evans D, Kolesnikov V, Rosulek M. A pragmatic introduction to secure multi-party computation. FNT Priv Secur, 2017, 2: 70–246
55 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

56 Liu Y, Kang Y, Zhang X W, et al. A communication efficient vertical federated learning framework. 2019. ArXiv:1912.11187

57 Wang Y S, Tong Y X, Shi D Y. Federated latent Dirichlet allocation: a local differential privacy based framework. In: Proceedings of the 34th AAAI Conference on Artificial Intelligence, New York, 2020. 6283–6290

58 Wang Y S, Tong Y X, Shi D Y, et al. An efficient approach for cross-silo federated learning to rank. In: Proceedings of the 37th IEEE International Conference on Data Engineerin, Chania, 2021. 1128–1139

59 Finn C, Abbeel P, Levine S. Model-agnostic meta-learning for fast adaptation of deep networks. In: Proceedings of the 34th International Conference on Machine Learning, Sydney, 2017. 1126–1135

60 Li Z G, Zhou F W, Chen F, et al. Meta-SGD: learning to learn quickly for few shot learning. 2017. ArXiv:1707.09835

61 Xu J J, Du W L, Cheng R, et al. Ternary compression for communication-efficient federated learning. 2020. ArXiv:2003.03564

62 Shi Y X, Tong Y X, Su Z Y, et al. Federated topic discovery: a semantic consistent approach. IEEE Intell Syst, 2020, 35: 96–103

63 Jiang D, Tong Y X, Song Y F, et al. Industrial federated topic modeling. ACM Trans Intell Syst Technol, 2021, 12: 1–22

64 Jiang J Y, Li C T, Lin S D. Towards a more reliable privacy-preserving recommender system. Inf Sci, 2019, 482: 248–265

65 Salakhutdinov R, Mnih A. Probabilistic matrix factorization. In: Proceedings of the 21st International Conference on Neural Information Processing Systems, Vancouver, 2007. 1257–1264

66 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

67 Jamali M, Ester M. Trustwalker: a random walk model for combining trust-based and item-based recommendation. In: Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Paris, 2009. 397–406

68 Rendle S, Freudenthaler C, Gantner Z, et al. BPR: Bayesian personalized ranking from implicit feedback. In: Proceedings of the 25th Conference on Uncertainty in Artificial Intelligence, Montreal, 2009. 452–461

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

70 Hegedüs 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, Würzburg, 2019. 317–332

71 Dolui 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

72 Ying S C. Shared MF: a privacy-preserving recommendation system. 2020. ArXiv:2008.07759

73 Anelli 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

74 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

75 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

76 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

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

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

79 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

80 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

81 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

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

83 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

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

85 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

86 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

87 Hu Y F, Koren Y, Volinsky C. Collaborative filtering for implicit feedback datasets. In: Proceedings of the 8th IEEE International Conference on Data Mining, Pisa, 2008. 263–272

88 Koren Y. Factorization meets the neighborhood: a multifaceted collaborative filtering model. In: Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Las Vegas, 2008. 426–434

89 McMahan H B, Ramage D, Talwar K, et al. Learning differentially private recurrent language models. In: Proceedings of the 6th International Conference on Learning Representations, Vancouver, 2018

90 Acar A, Aksu H, Uluagac A S, et al. A survey on homomorphic encryption schemes: theory and implementation. ACM Comput Surv, 2018, 51: 79

91 Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security, Dallas, 2017. 1175–1191

92 Rendle S. Factorization machines with libFM. ACM Trans Intell Syst Technol, 2012, 3: 57

93 Qi L Y, Zhang X Y, Dou W C, et al. A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data. IEEE J Sel Areas Commun, 2017, 35: 2616–2624

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

95 Basu C, Hirsh H, Cohen W W. Recommendation as classification: using social and content-based information in recommendation. In: Proceedings of the 15th National Conference on Artificial Intelligence and the 10th Innovative Applications of Artificial Intelligence Conference, Madison, 1998. 714–720

96 Erlingsson Ú, Pihur V, Korolova A. RAPPOR: randomized aggregatable privacy-preserving ordinal response. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, 2014. 1054–1067

97 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

98 Hidasi B, Karatzoglou A, Baltrunas L, et al. Session-based recommendations with recurrent neural networks. In: Proceedings of the 4th International Conference on Learning Representations, San Juan, 2016

99 Nichol A, Achiam J, Schulman J. On first-order meta-learning algorithms. 2018. ArXiv:1803.02999

100 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

101 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

102 Soni K, Panchal G. Data security in recommendation system using homomorphic encryption. In: Proceedings of the 2nd Information Conference on Information and Communication Technology for Intelligent Systems, 2017. 308–313

103 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

104 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
105 Qi T, Wu F Z, Wu C H, et al. Privacy-preserving news recommendation model training via federated learning. 2020. ArXiv:2003.09592
106 Chen C C, Wu B Z, Fang W J, et al. Practical privacy preserving POI recommendation. 2020. ArXiv:2003.02834
107 Chen C C, Li L, Wu B Z, et al. Secure social recommendation based on secret sharing. 2020. ArXiv:2002.02088
108 Li 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
109 Stanojevic R, Nabeel M, Ting Y. Distributed cardinality estimation of set operations with differential privacy. In: Proceedings of IEEE Symposium on Privacy-Aware Computing, Washington, 2017. 37–48
110 Yuan K, Ling Q, Yin W T. On the convergence of decentralized gradient descent. SIAM J Optim, 2016, 26: 1835–1854
111 Kikuchi H, Kizawa H, Tada M. Privacy-preserving collaborative filtering schemes. In: Proceedings of the 4th International Conference on Availability, Reliability and Security, Fukuoka, 2009. 911–916
112 Polat H, Du W L. Privacy-preserving collaborative filtering using randomized perturbation techniques. In: Proceedings of the 3rd IEEE International Conference on Data Mining, Melbourne, 2003. 625–628
113 Kaur H, Kumar N, Obaidat M S. Multi-party secure collaborative filtering for recommendation generation. In: Proceedings of IEEE Global Communications Conference, Waikoloa, 2019. 1–6
114 Data Security Law of the People's Republic of China. Gazette of the Standing Committee of the National People's Congress of the People's Republic of China, 2021, 5: 951–956 [中华人民共和国数据安全法. 中华人民共和国全国人民代表大会常务委员会公报, 2021, 5: 951–956]
115 Pan W K, Ming Z. Collaborative recommendation with multiclass preference context. IEEE Intell Syst, 2017, 32: 45–51
116 Lin Z H, Pan W K, Ming Z. FR-FMSS: federated recommendation via fake marks and secret sharing. In: Proceedings of the 15th ACM Conference on Recommender Systems, Amsterdam, 2021. 668–673
117 Zeng Q S, Du Y Q, Huang K B, et al. Energy-efficient radio resource allocation for federated edge learning. In: Proceedings of IEEE International Conference on Communications Workshops, Dublin, 2020. 1–6
118 Zhu Z D, Hong J Y, Zhou J Y. Data-free knowledge distillation for heterogeneous federated learning. In: Proceedings of the 38th International Conference on Machine Learning, 2021. 12878–12889
119 Yang E Y, Huang Y F, Liang F, et al. FCMF: federated collective matrix factorization for heterogeneous collaborative filtering. Knowl-Based Syst, 2021, 220: 106946
120 Minto L, Haller M, Haddadi H, et al. Stronger privacy for federated collaborative filtering with implicit feedback. In: Proceedings of the 15th ACM Conference on Recommender Systems, Amsterdam, 2021. 342–350
121 Zhao L C, Wang Q, Zou Q, et al. Privacy-preserving collaborative deep learning with unreliable participants. IEEE Trans Inform Forensic Secur, 2020, 15: 1486–1500
122 Zhang F, Deng Z J, He Z M, et al. Detection of shilling attack in collaborative filtering recommender system by PCA and data complexity. In: Proceedings of International Conference on Machine Learning and Cybernetics, Chengdu, 2018. 673–678
123 Chen C, Zhang J F, Tung A K H, et al. Robust federated recommendation system. 2020. ArXiv:2006.08259
124 Tolpegin V, Truex S, Gursoy M E, et al. Data poisoning attacks against federated learning systems. In: Proceedings of the 25th European Symposium on Research in Computer Security, Guildford, 2020. 480–501
125 Fang M H, Cao X Y, Jia J Y, et al. Local model poisoning attacks to byzantine-robust federated learning. In: Proceedings of the 29th USENIX Security Symposium, 2019

Survey of recommender systems based on federated learning

Feng LIANG[1†], Enyue YANG[1†], Weike PAN[1*], Qiang YANG[2*] & Zhong MING[1*]

1. *College of Computer Science and Software Engineering, Shenzhen University, Shenzhen* 518060*, China*;
2. *Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong* 999077*, China*
* Corresponding author. E-mail: panweike@szu.edu.cn, qyang@cse.ust.hk, mingz@szu.edu.cn
† Equal contribution

Abstract With the development of the Internet and mobile computing, people's online behaviors have generated increasing amounts of data. In order to select items that users may like from massive data, recommender systems are indispensable. However, traditional recommendation algorithms need to collect user data to the server to build the model, which will leak user privacy. Recently, Google has proposed a new learning paradigm called federated learning for machine learning problems that require user data to be collected for modeling. The combination of federated learning and recommender systems enables federated recommendation algorithms to always keep user data in clients during the modeling process, so as to protect user privacy. In this study, the research works on the combination of federated learning with recommendation algorithms are surveyed. Then, the research development on federated recommendation algorithms is analyzed from three perspectives, namely, design of architectures, federalization of models, and application of privacy-preserving technology. Finally, some research directions and prospects for recommender systems based on federated learning are discussed.

Keywords recommender systems, federated learning, privacy protection, federated recommendation, collaborative filtering