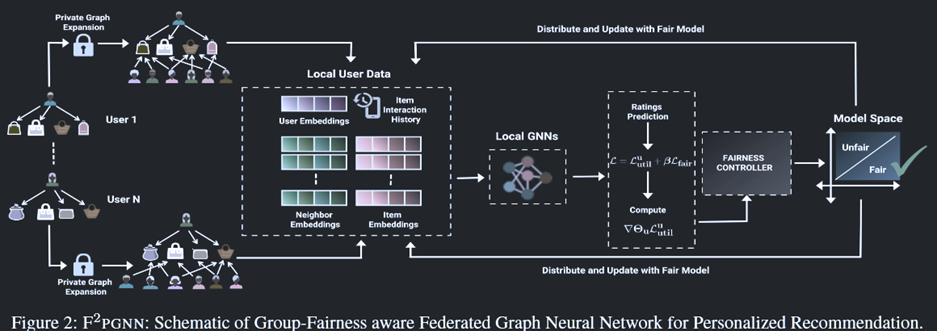
**2024AAAI-No Prejudice! Fair Federated Graph Neural Networks for Personalized Recommendation**

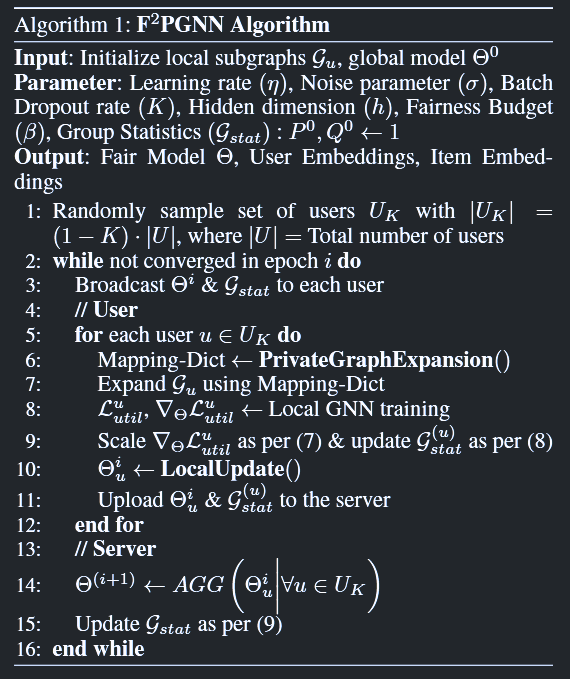
**Abstract**

由于推荐系统（RSs）在个性化医疗、金融和电子商务等应用中的日益普及，确保其在不同人口统计群体间的公平性变得至关重要。基于图的推荐系统（RSs）在捕捉实体间复杂的高阶交互方面发挥着关键作用。然而，将这些图模型集成到具有公平性约束的联邦学习（FL）范式中面临着巨大的挑战，因为这需要在中央服务器端访问完整的交互图和敏感用户信息（如性别、年龄等）。本文解决了在基于图的模型的联邦学习（FL）环境中，不同人口统计群体在RSs中存在固有偏差的普遍问题，同时不损害敏感用户属性的隐私。为了解决群体偏差，本文提出了F²PGNN（公平联邦个性化图神经网络），这是一个新颖的框架，它利用了个性化图神经网络（GNN）的能力并结合了公平性考虑。此外，还使用差分隐私技术来加强隐私保护。在三个公开数据集上的实验评估表明，与最先进的方法相比，F²PGNN在保护隐私和保持效用的同时，能够将群体不公平性降低47%∼99%。

**Algorithm**

算法流程始于服务器初始化全局模型并广播给部分客户端。每个被选中的客户端首先运行隐私保护的归纳图扩展算法：将其交互过的物品ID加密后上传服务器，服务器匹配有共同交互的匿名用户并将其嵌入信息返回，客户端借此扩展本地子图以纳入高阶交互信息。接着，客户端使用图注意力网络（GAT） 在扩展后的子图上进行本地训练，计算效用损失和梯度。然后，算法引入公平性调节机制：客户端根据服务器广播的全局群体性能统计量，计算一个缩放因子来动态调整其本地梯度，从而在更新模型时对表现较差的群体给予更多关注。在上传前，为保护隐私，客户端对模型更新进行梯度裁剪并添加拉普拉斯噪声（满足局部差分隐私-LDP），同时对需要上传的群体统计信息也添加噪声以隐藏其真实群体隶属关系。最后，服务器聚合所有客户端上传的、经过隐私处理的模型更新和群体统计信息，更新全局模型和全局群体统计量，并开启新一轮的广播与训练，如此迭代直至模型收敛，最终得到一个在保护隐私的同时兼具推荐效用和群体公平性的联邦图神经网络模型。





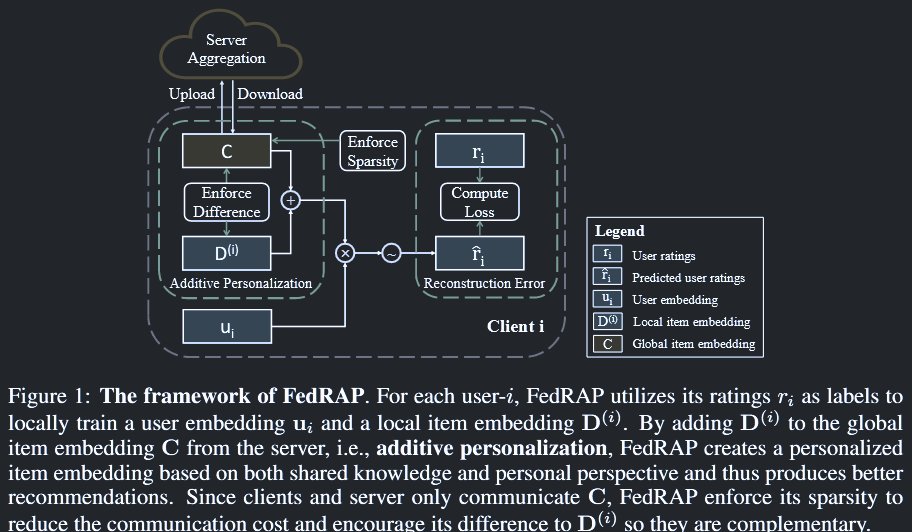
**2024ICLR-FEDERATED RECOMMENDATION WITH ADDITIVE PERSONALIZATION**

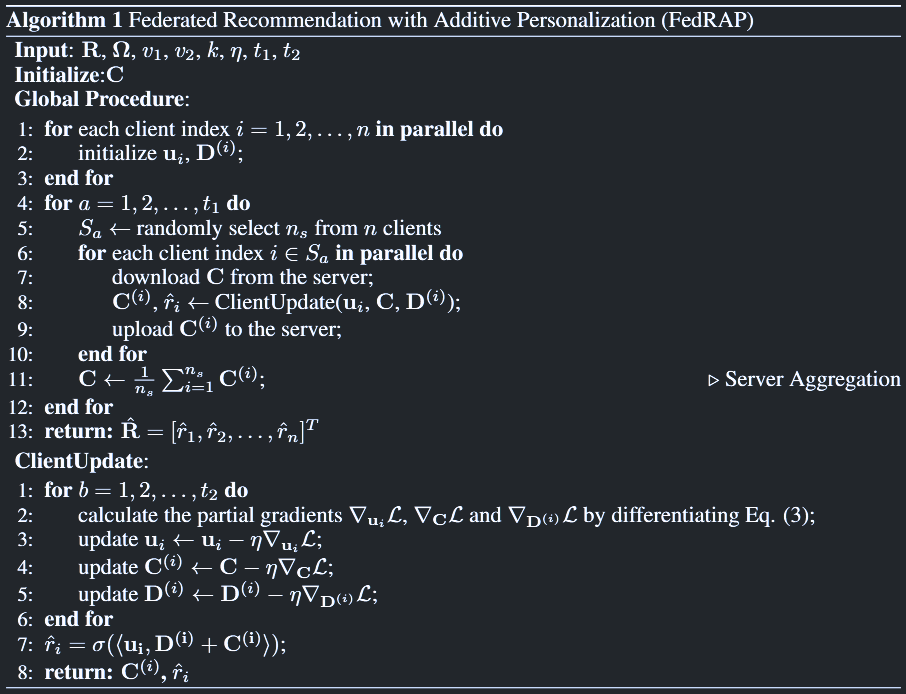
**Abstract**

通过联邦学习（FL）构建推荐系统是下一代互联网服务面临的一个新兴挑战。现有的联邦学习模型在客户端之间共享物品嵌入，同时将用户嵌入保持私有并本地存储在客户端。然而，相同的物品嵌入无法捕捉用户对同一物品感知的个体差异，可能导致个性化效果不佳。此外，联邦学习中的密集物品嵌入会导致昂贵的通信成本和延迟。为了应对这些挑战，我们提出了 基于加法个性化的联邦推荐（FedRAP），该方法通过联邦学习学习物品的全局视图，并在每个用户本地学习个性化视图。FedRAP鼓励稀疏的全局视图以节省联邦学习的通信成本，并通过两个正则化器确保两个视图互补。我们提出了一种有效的课程学习策略，通过逐渐增加正则化权重来逐步学习局部和全局视图。为了给用户生成推荐，FedRAP将两个视图相加以获得个性化的物品嵌入。FedRAP在多个基准测试的联邦学习设置中取得了最佳性能，其表现优于近期的联邦推荐方法以及多个消融研究的基线模型。

**Algorithm**

FedRAP算法首先由服务器初始化全局物品嵌入C，各客户端初始化其用户嵌入u\_i和本地物品嵌入D⁽ⁱ⁾。在每轮训练中，服务器选择部分客户端，分发当前的C。各客户端在本地基于其评分数据，通过优化一个结合了预测损失、促使D⁽ⁱ⁾与C差异化的正则项（其权重随训练递增）以及促使C稀疏化的正则项（其权重亦递增）的目标函数，来更新u\_i、D⁽ⁱ⁾和C的本地副本C⁽ⁱ⁾。随后，客户端将更新后的C⁽ⁱ⁾上传至服务器，由服务器聚合（平均）这些更新以生成新的全局C。最终，通过将学习到的全局视图C与本地个性化视图D⁽ⁱ⁾相加，形成每个用户独有的个性化物品嵌入，用于生成推荐。该过程通过课程学习策略平滑过渡到完整的加法个性化，并利用C的稀疏化有效降低了通信开销。





首先在服务器上初始化 C，在各自的客户端上初始化 ui 和 D（i）（i = 1， 2， . . . ， n）。假定每个客户端代表一个用户。对于每一轮，服务器随机选择以 Sa 为代表的客户端子集来参与训练。客户端最初从服务器接收嵌入 C 的稀疏全局项。然后调用函数 ClientUpdate 以根据学习率η相应地更新其参数。客户端将更新的 C（i）上传到服务器进行聚合。然后，服务器在下一轮训练中使用聚合的 C。训练过程完成后，FedRAP 会输出预测评级 Rˆ 以指导建议。FedRAP 通过在客户端上保留特定于用户的潜在嵌入，并且仅将更新的稀疏全局项目嵌入上传到服务器来维护用户隐私。这种方法显着降低了隐私风险和通信成本。此外，FedRAP 通过在客户端本地学习特定于用户的个性化模型来适应用户行为异质性。因此，即使用户数据因个人偏好而异，FedRAP 也能确保用户内的数据符合独立同分布假设。

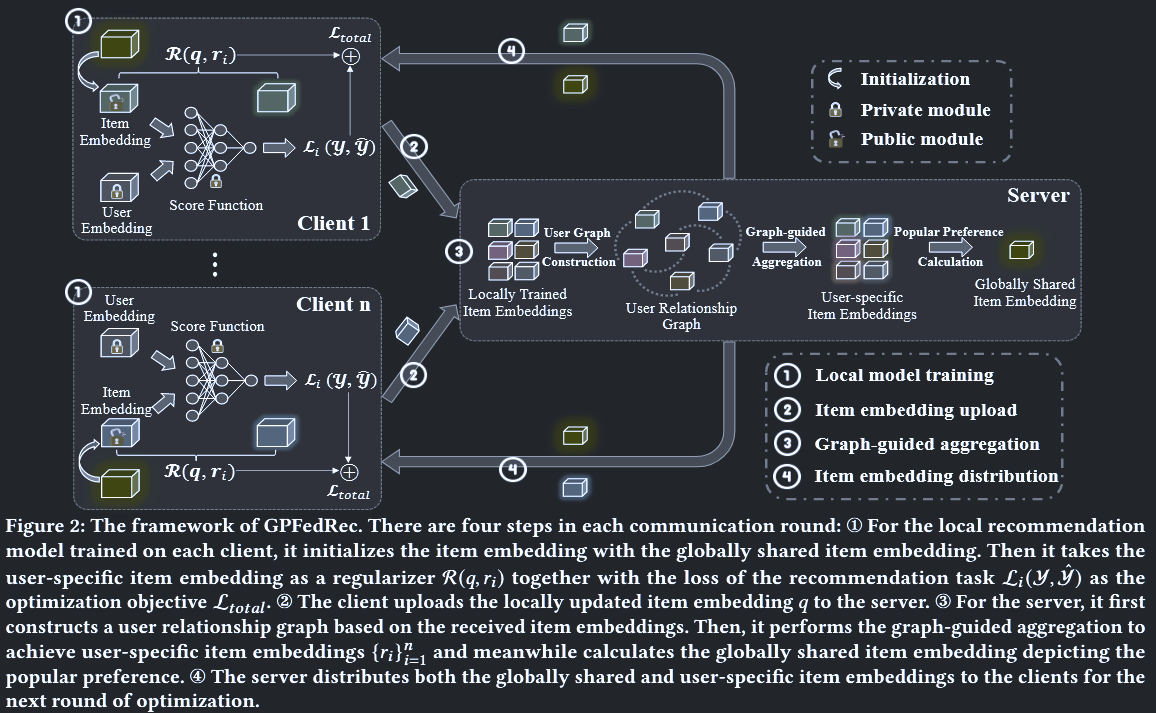
**2024KDD-GPFedRec: Graph-Guided Personalization for Federated Recommendation**

**Abstract**

联邦推荐系统是一种新兴的人工智能服务架构，旨在以保护隐私的方式提供推荐服务。利用用户关系图来增强联邦推荐是一个前景广阔的研究方向。然而，如何在联邦设置中构建用户关系图，同时保持基于数据本地性的隐私保护，仍然是一个开放的挑战。受一个简单动机的启发——相似的用户对同一组物品共享相似的视角（嵌入），本文提出了一种新颖的图引导个性化联邦推荐方法（GPFedRec）。该方法在服务器端利用用户特定的个性化物品嵌入来构建用户关系图，而无需访问用户的交互记录。个性化物品嵌入在每个设备上本地进行微调，然后通过衡量客户端特定物品嵌入之间的相似性来构建用户关系图。由于无需访问用户的历史交互记录，我们体现了原始联邦学习基于数据本地性的隐私保护。此外，还设计了一种图引导的聚合机制，以同时利用用户关系图和联邦优化框架。在五个基准数据集上进行的大量实验证明了GPFedRec的卓越性能。深入的研究验证了GPFedRec可以作为一种插件普遍改进现有的联邦推荐方法，同时保持用户隐私安全。代码已开源。

**Algorithm**

GPFedRec算法通过多轮服务器-客户端交互实现联邦推荐。每轮开始时，客户端使用服务器下发的全局共享物品嵌入初始化本地模型，并结合本地交互数据及服务器提供的用户特定物品嵌入（作为正则化项）进行本地训练，之后上传更新后的本地物品嵌入至服务器。服务器收集这些嵌入后，计算用户间相似度并构建用户关系图，进而通过图卷积聚合相似用户信息，为每个用户生成个性化的用户特定物品嵌入，同时聚合所有用户特定嵌入得到新的全局共享物品嵌入。最后，服务器将这两类嵌入下发给客户端用于下一轮训练，如此迭代直至模型收敛，从而在保护隐私的前提下利用用户间相似性提升推荐性能。



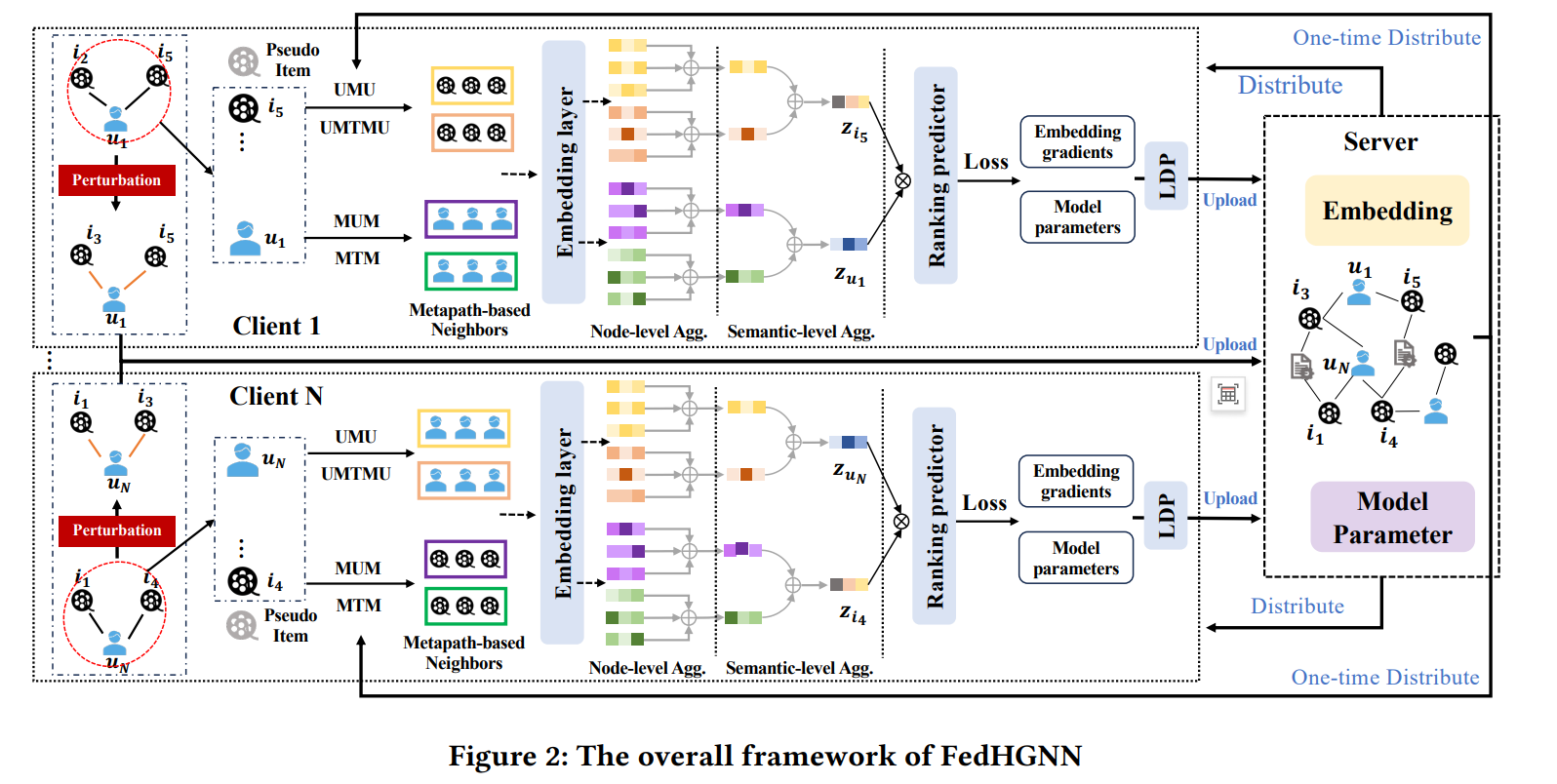
**2024WWW-Federated Heterogeneous Graph Neural Network for Privacy-preserving Recommendation**

**Abstract**

包含由元路径描述的丰富语义的异构信息网络（HIN），已成为缓解推荐系统中数据稀疏性的有力工具。现有的基于HIN的推荐系统在集中式存储和模型训练的假设下运行。然而，现实世界中的数据由于隐私问题通常是分布式的，这导致HIN中的语义断裂问题，进而导致集中式基于HIN的推荐失败。在本文中，我们建议将HIN划分为存储在客户端的私有HIN和存储在服务器上的共享HIN。基于此设置，我们提出了一个基于联邦异构图神经网络（FedHGNN）的框架，该框架利用分布式HIN进行推荐模型的协同训练，同时保护用户隐私。具体来说，我们首先根据差分隐私为基于HIN的联邦推荐（FedRec）形式化隐私定义，目标是保护私有HIN内的用户-物品交互以及来自共享HIN的用户高阶模式。为了恢复断裂的基于元路径的语义并确保所提出的隐私措施，我们精心设计了一种语义保留的用户交互发布方法，该方法在本地扰动用户的高阶模式及相关用户-物品交互以供发布。随后，我们引入了一个用于推荐的HGNN模型，该模型执行节点级和语义级聚合以捕获恢复的语义。在四个数据集上的大量实验表明，在合理的隐私预算下，我们的模型显著优于现有方法（HR@10提升高达34%，NDCG@10提升高达42%）。

**Algorithm**

FedHGNN算法首先进行初始化，将异构信息网络划分为客户端存储的私有HIN和服务器存储的共享HIN。随后，每个客户端一次性执行两阶段语义保留扰动：首先使用指数机制扰动用户关联的共享HIN列表以保护高阶模式隐私，接着在筛选出的语义引导物品集上应用度保持随机响应（DPRR）扰动用户-物品交互以保护交互隐私；扰动后的交互数据被上传至服务器。服务器根据所有客户端上传的数据重构全局扰动图，并计算每个用户基于各元路径的邻居集合，然后将这些邻居信息分发给相应用户。此后进入迭代式联邦训练阶段：每轮通信中，服务器抽样部分客户端并分发当前全局模型参数；各客户端基于收到的参数和邻居信息，利用异构GNN模型（包含节点级和语义级的注意力聚合）进行本地训练，计算梯度（并可选择应用LDP扰动和伪物品采样以增强隐私），并将梯度上传；服务器聚合梯度并更新全局模型，直至模型收敛。



**2024WWW-Prompt-enhanced Federated Content Representation Learning for Cross-domain Recommendation**

**Abstract**

**Algorithm**

