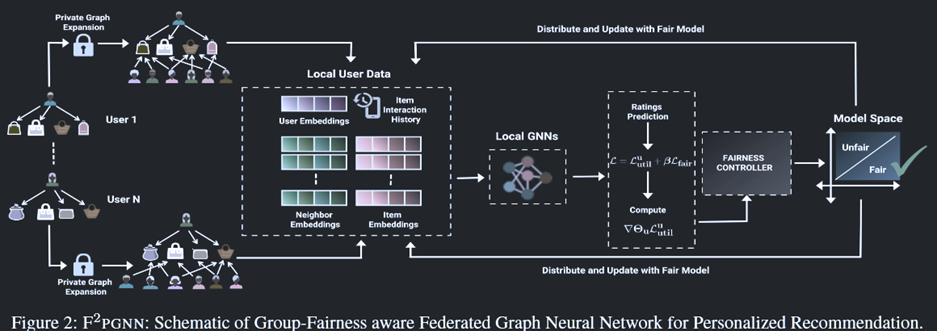
**2024AAAI-No Prejudice! Fair Federated Graph Neural Networks for Personalized Recommendation**

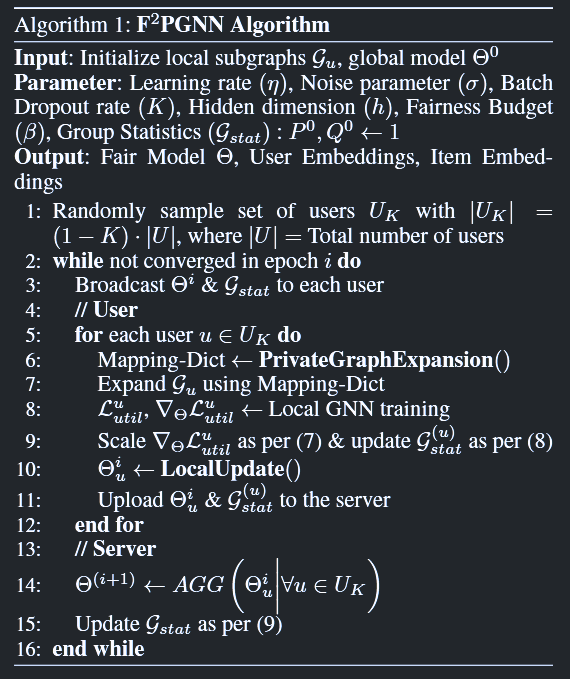
**Abstract**

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。





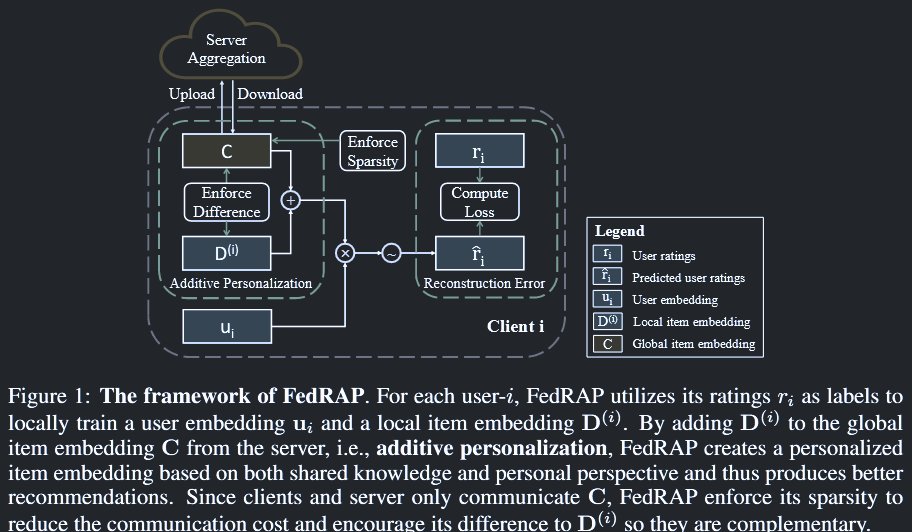
**2024ICLR-FEDERATED RECOMMENDATION WITH ADDITIVE PERSONALIZATION**

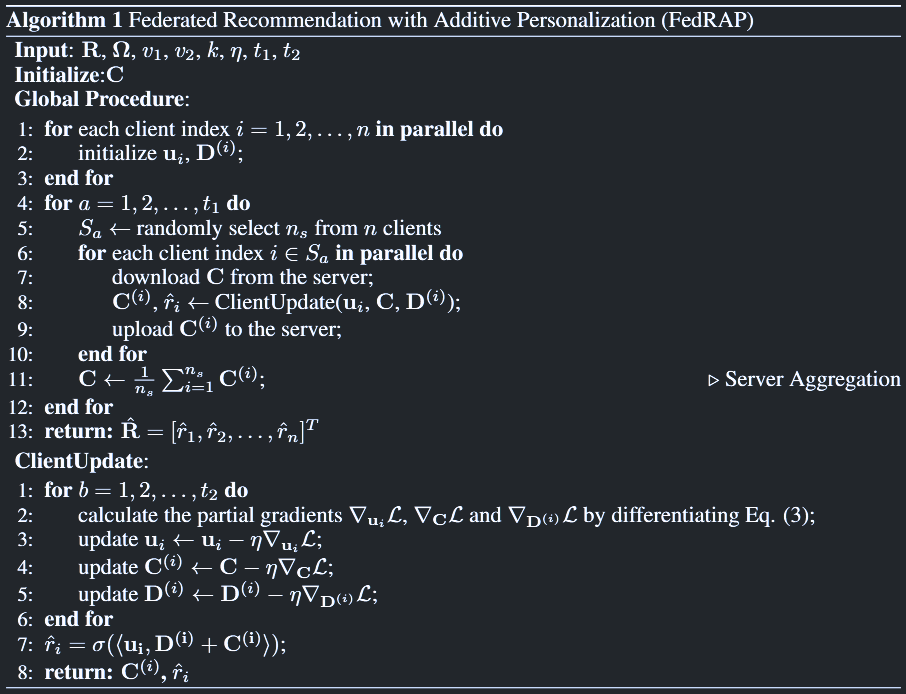
**Abstract**

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。

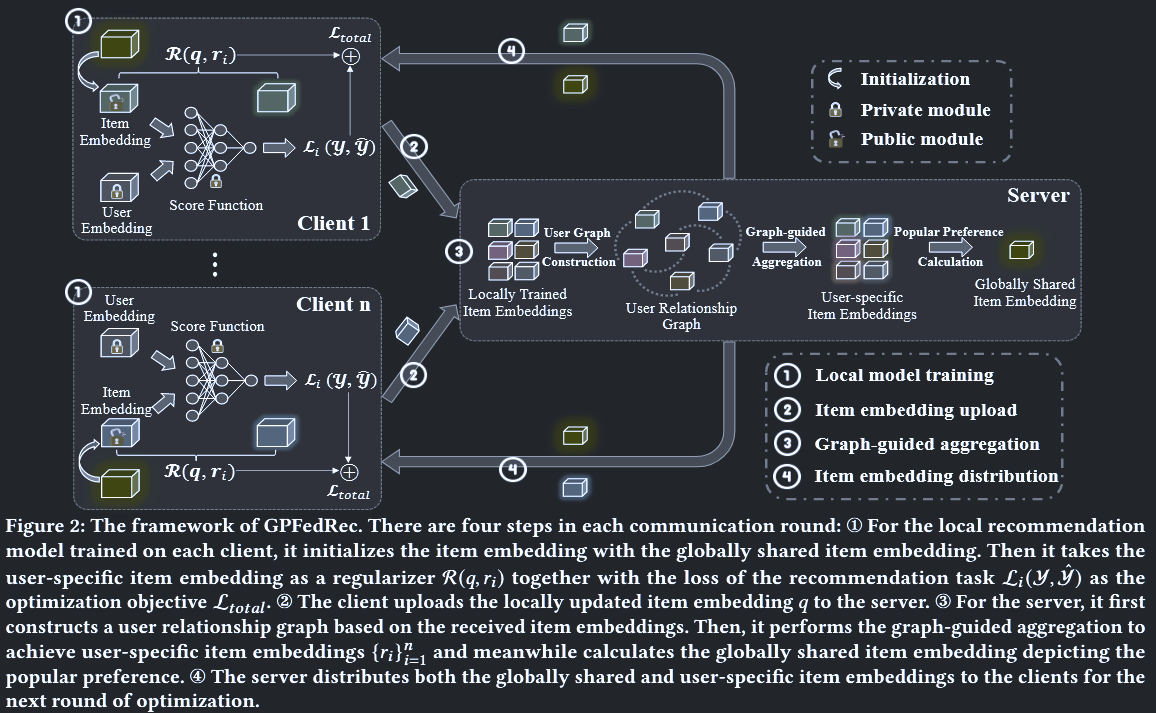
**2024KDD-GPFedRec: Graph-Guided Personalization for Federated Recommendation**

**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。



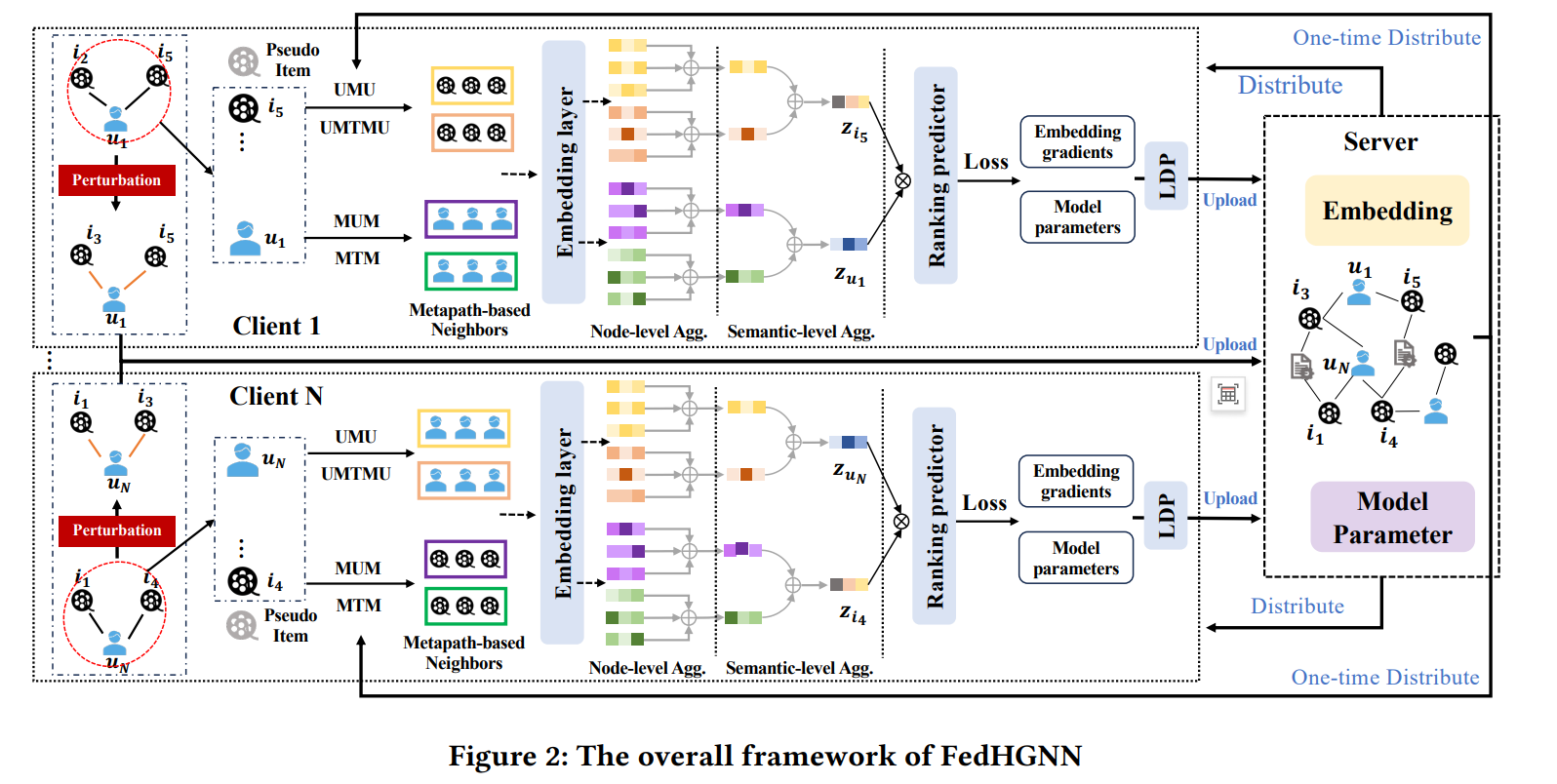
**2024WWW-Federated Heterogeneous Graph Neural Network for Privacy-preserving Recommendation**

**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。



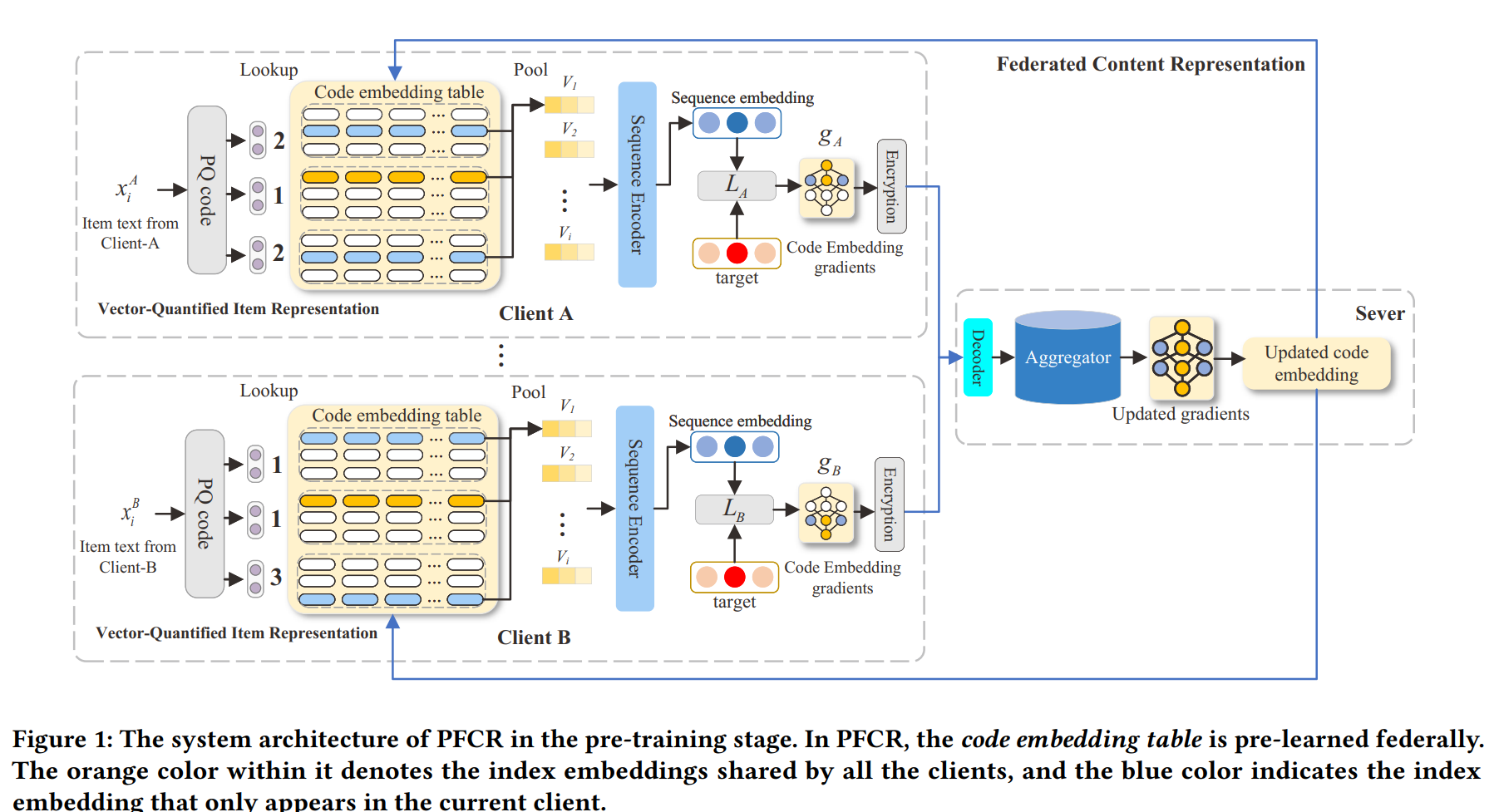
**2024WWW-Prompt-enhanced Federated Content Representation Learning for Cross-domain Recommendation**

**Abstract**

跨域推荐（CDR）作为缓解数据稀疏性问题的有效技术之一，近年来得到了广泛研究。然而，先前的工作可能导致域隐私泄露，因为它们在训练过程中需要将不同域的数据聚合到中央服务器。尽管已有一些研究通过联邦学习（FL）进行隐私保护的CDR，但它们仍存在以下局限性：1）它们需要将用户的个人信息上传到中央服务器，存在泄露用户隐私的风险。2）现有的联邦方法主要依赖原子项目ID来表示项目，这阻碍了在统一特征空间中对项目进行建模，增加了域间知识迁移的挑战。3）它们都基于已知域间重叠用户的前提，这在实际应用中是不现实的。为了解决上述局限性，我们专注于隐私保护的跨域推荐（PCDR）并提出了PFCR作为我们的解决方案。对于局限性1，我们设计了一种联邦学习方案，专门利用用户与本地客户端的交互，并设计了一种梯度加密方法。对于局限性2，我们通过项目的描述文本来在通用特征空间中表示项目。对于局限性3，我们首先学习联邦内容表示，利用自然语言的通用性来建立域间的桥梁。随后，我们设计了两种提示微调策略，使预训练模型能够适应目标域。在两个真实数据集上的大量实验证明了我们的PFCR方法相较于最先进（SOTA）方法的优越性。

**Algorithm**

PFCR算法通过两阶段流程实现隐私保护的跨域推荐。首先，在联邦预训练阶段，各域作为客户端，利用本地用户行为数据和公共项目描述文本，通过BERT和乘积量化将项目映射到共享的离散语义代码空间，并借助一个全局的代码嵌入表获得项目表示；随后使用序列编码器进行本地训练，并仅将加密后的代码嵌入表梯度上传至服务器进行联邦聚合与同步，以此学习跨域的通用内容表示而不泄露用户隐私。接着，在提示调优阶段，冻结预训练模型参数，通过引入可训练的域提示（和可选的用户提示）来适配目标域，仅微调这些提示参数，从而高效地将预训练模型的知识迁移到特定的推荐任务中。



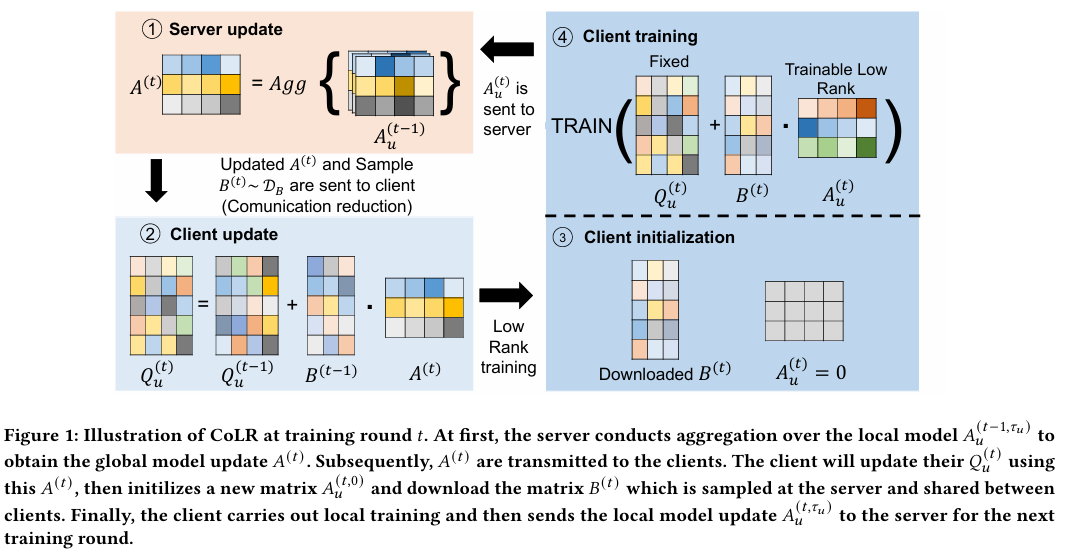
**2024WWW-Towards Efficient Communication and Secure Federated Recommendation System via Low-rank Training**

**Abstract**

联邦推荐（FedRec）系统已成为应对日益增长的监管关切、保护用户数据的一种解决方案。然而，这些系统面临的主要挑战之一在于用户设备与中央服务器之间传输神经网络模型所产生的通信成本。先前解决这些挑战的方法常常导致诸如计算开销、模型特异性限制以及与安全聚合协议兼容性等问题。为此，我们提出了一种名为相关低秩结构（Correlated Low-rank Structure, CoLR） 的新框架，该框架利用调整轻量级可训练参数同时冻结大部分参数的概念。我们的方法显著减少了通信开销，且不引入额外的计算负担。至关重要的是，我们的框架与安全聚合协议（包括同态加密的鲁棒使用）完全兼容。该方法使得有效载荷大小减少了高达93.75%，而在各数据集上的推荐性能仅下降了约8%。

**Algorithm**

在每一轮联邦训练开始时，服务器生成一个随机的共享低秩投影矩阵B并分发给选中的客户端；客户端在本地训练阶段冻结该共享矩阵B，仅优化另一个低秩矩阵A和用户嵌入参数，使得项目嵌入矩阵的更新被约束在B张成的低秩子空间内；训练完成后，客户端只需将优化后的矩阵A上传至服务器；服务器则对接收到的所有客户端的矩阵A进行加权平均（简单的加法操作），得到全局更新，并用于下一轮的初始化。这种方法通过直接在高通信效率的低秩参数空间中进行优化，避免了显式的压缩/解压缩步骤，显著减少了上下行通信量，且其加法式的聚合操作天然兼容同态加密等安全聚合协议。



**2024WWW-Towards Personalized Privacy: User-Governed Data Contribution for Federated Recommendation**

**Abstract**

联邦推荐系统（FedRecs）因其通过将用户隐私数据保留在本地、仅与服务器通信模型参数/梯度来保护用户隐私的潜力而受到广泛关注。然而，现有FedRecs架构假定所有用户都具有相同的“零隐私预算”，即不上传任何数据给服务器，从而忽略了那些对隐私不太关心、愿意上传数据以获得更好推荐服务的用户。为弥补这一差距，本文探索了一种用户主导的数据贡献联邦推荐架构，用户可以自由控制是否分享数据以及分享给服务器的数据比例。为此，本文提出了一种名为 CDCGNNFed 的云-端协同图神经网络联邦推荐模型。该模型通过对比学习，在本地训练以用户为中心的自我中心图（ego graph），并在服务器上基于用户共享的数据协同训练高阶图。此外，还利用了一种图修复策略来预测服务器端图中的缺失链接，从而充分发挥图神经网络在高阶图上的能力。在两个公共数据集上进行了大量实验，结果证明了所提方法的有效性。

**Algorithm**

本文提出的CDCGNNFed算法流程始于用户自主上传全部、部分或零数据至服务器；服务器据此构建用户-物品图并执行图修复以预测缺失链接，从而形成高阶图。随后，服务器选择部分客户端参与训练：各客户端基于本地一阶图计算嵌入（局部视图），服务器则基于修复后的高阶图计算嵌入（全局视图）。通过对比学习拉近自愿全量数据共享用户的局部与全局视图，并推远不同用户视图间的距离，以协同优化表征。客户端主要依赖BPR损失进行本地训练，服务器则结合BPR与对比损失进行更新。最终，采用FedAvg算法聚合客户端与服务器的模型参数，完成全局模型更新与分发，实现在尊重个性化隐私偏好下的高效联邦推荐。

