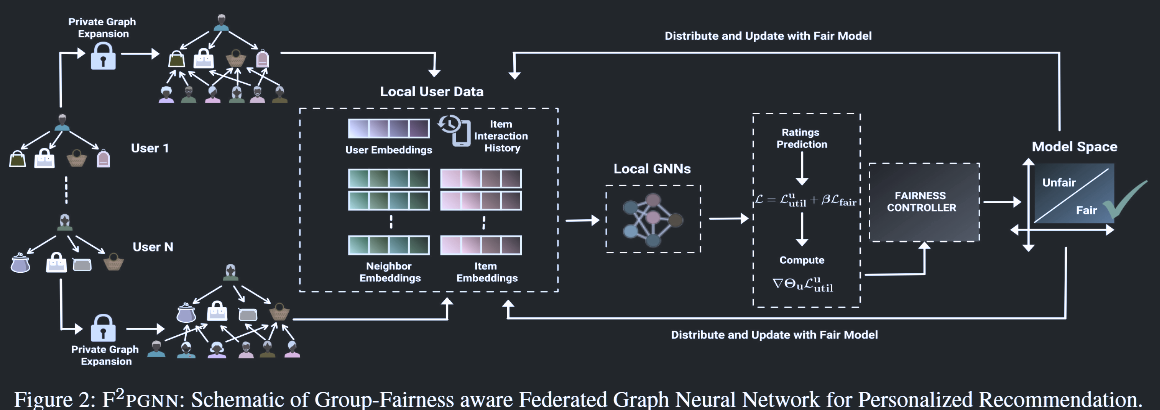
**2024AAAI-No Prejudice! Fair Federated Graph Neural Networks for Personalized Recommendation**

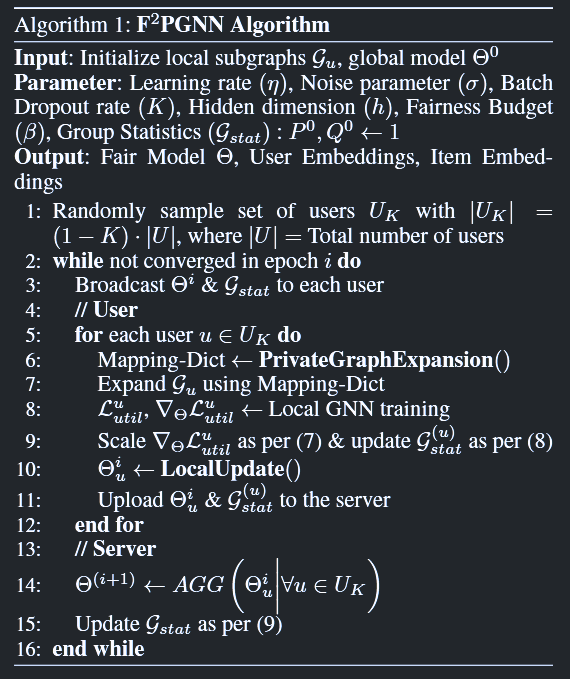
公平、隐私保护、个性化

引入了具有隐私保护功能的归纳图扩展算法，该算法最大限度地减少了通信开销，同时有效地从分布式用户数据中捕获了高阶交互。

增加了一个本地差分隐私模块用于模型更新，同时保护了模型更新的隐私。

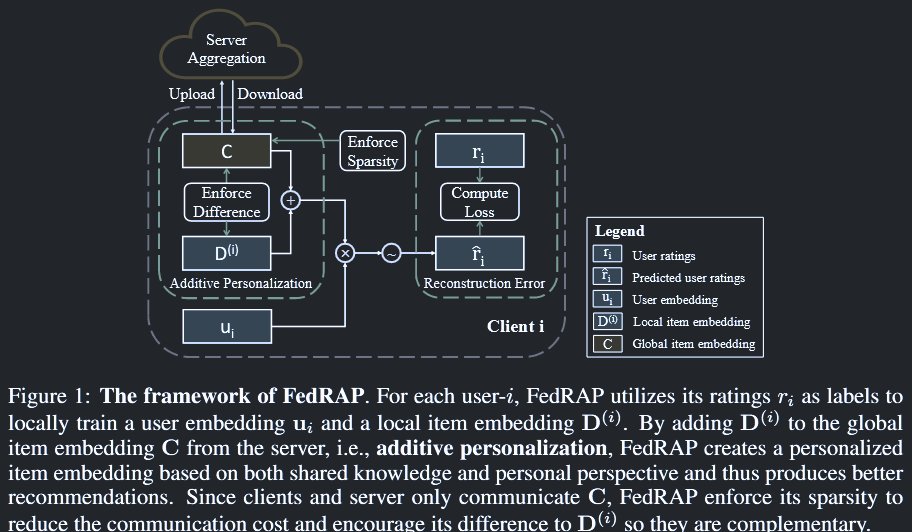


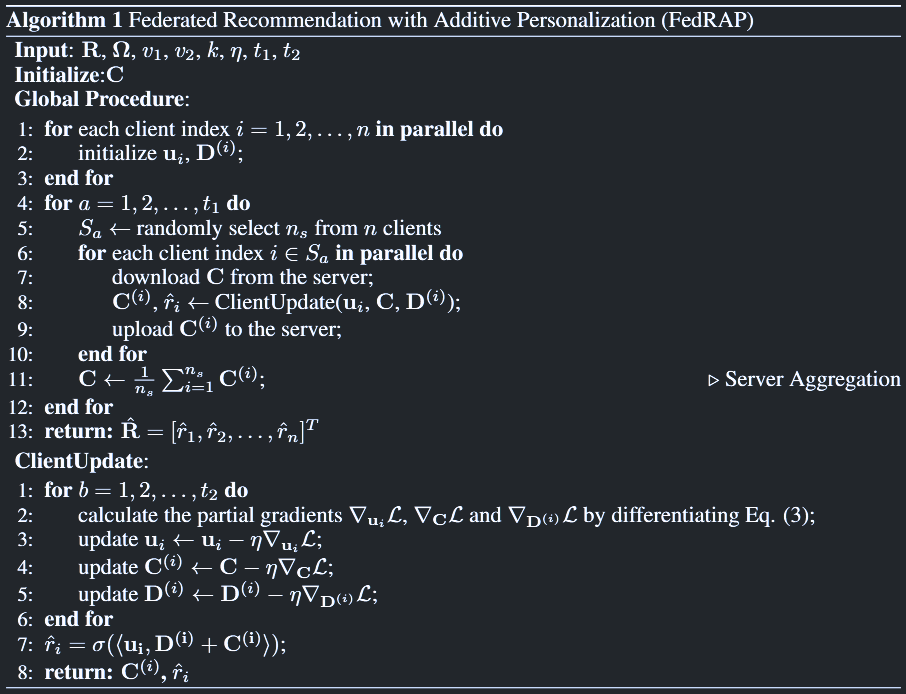
每个用户都存储其用户-项目交互历史以构成一个本地子图。为了训练个性化的 GNN，首先，每个用户使用归纳私有图扩展算法扩展局部子图，以合并高阶交互。通过匹配加密项目并分发匿名用户嵌入，扩展图包括每个用户与共交互项目的邻居。接下来，使用 GAT 模型根据局部子图更新这些嵌入。然后，对于每个用户 ui，用GAT模型的输出表示出推荐过程的损失，该损失用于获取模型的局部梯度和每个用户的性能。



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

挑战：现有的 FL 模型跨客户端共享项目嵌入，同时在客户端保持用户嵌入的私有和本地。然而，相同的项目嵌入无法捕捉用户感知同一项目的个体差异，并可能导致个性化不佳。此外，FL 中的密集项目嵌入会导致昂贵的通信成本和延迟。



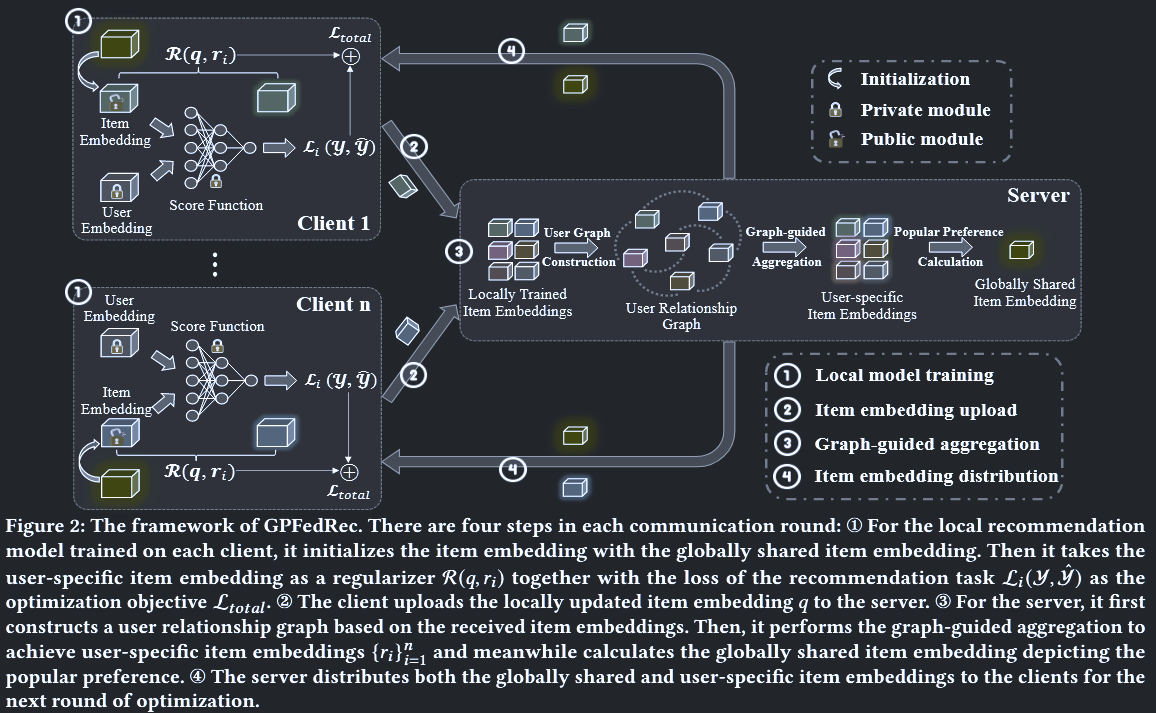


首先在服务器上初始化 C，在各自的客户端上初始化 ui 和 D（i）（i = 1， 2， . . . ， n）。假定每个客户端代表一个用户。对于每一轮，服务器随机选择以 Sa 为代表的客户端子集来参与训练。客户端最初从服务器接收嵌入 C 的稀疏全局项。然后调用函数 ClientUpdate 以根据学习率η相应地更新其参数。客户端将更新的 C（i）上传到服务器进行聚合。然后，服务器在下一轮训练中使用聚合的 C。训练过程完成后，FedRAP 会输出预测评级 Rˆ 以指导建议。FedRAP 通过在客户端上保留特定于用户的潜在嵌入，并且仅将更新的稀疏全局项目嵌入上传到服务器来维护用户隐私。这种方法显着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**

现有的联邦推荐研究通常将用户视为个体来训练全局模型，而忽略了他们之间的相关性。在推荐场景中，用户通常具有多种联系。例如，购买相同商品的用户表现出共同的兴趣，也可能更喜欢其他相同的产品。这些相关性可以用图结构来有效地描述。在推荐系统中使用它可以丰富表示学习，促进用户偏好建模，这已成为一种流行的范式，并在集中式环境中取得了出色的性能。因此，开发用户关系图增强的联合推荐系统有可能提供更好的隐私保护推荐服务。

贡献：提出了一种在联合推荐设置中识别用户之间相关性的新方法，该方法使用共享项目嵌入构建用户关系图，而无需暴露隐私。引入了一种图形引导的聚合机制，可以学习用户特定的项目嵌入，从而促进用户个性化建模。整体算法可以制定为统一的联邦优化框架GPFedRec。

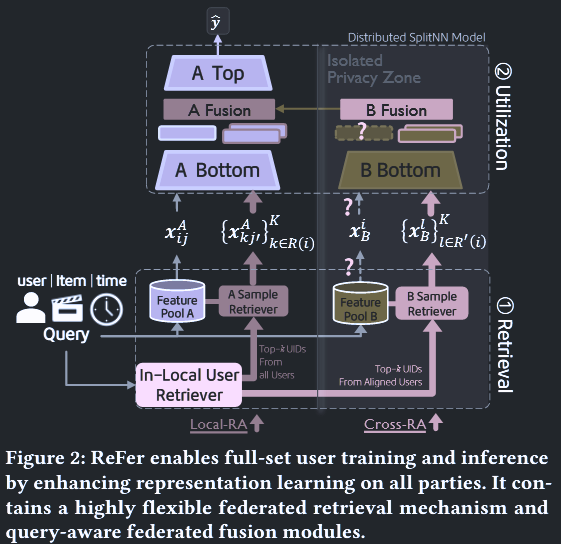


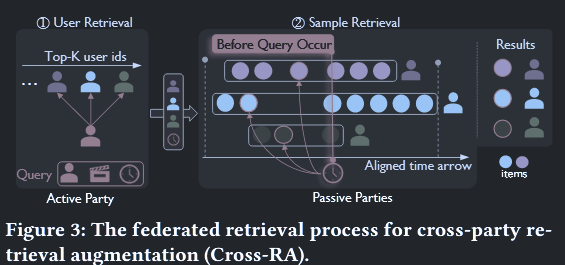
**2024SIGIR-ReFer: Retrieval-Enhanced Vertical Federated Recommendation for Full Set User Benefit**

有点复杂，没看懂

在典型的VFL过程中，参与者首先执行私有集交集以获得对齐（即重叠）的数据集，然后进行分布式训练。这实质上限制了模型仅对齐用户进行训练和推断。

贡献：提出了第一个基于检索的垂直联邦学习算法，以实现全用户集建模和增强表示学习；提出了一个通用有效的“检索融合”框架，以实现局部侧RA（检索增强）和跨侧RA，系统地增强各方的代表性，促进更好的预测。





**2024SIGIR-Revisit Targeted Model Poisoning on Federated Recommendation: Optimize via Multi-objective Transport**

做安全方面的工作（中毒攻击）