融合分析说明文档

1. 算法的主要模块：
2. 数据融合分析模块：此部分以联邦学习机制为基础。在每个轮次开始前，服务端随机选取参与方并下发一个统一的全局模型到每个数据源拥有者，各数据源拥有者根据服务端的选取情况再进行随机响应以实现服务端无法追溯具体客户端的参与情况。然后，通过在每个数据源本地使用私有数据训练模型，在每个轮次通信阶段，由服务端整合各参与方所交付的模型参数更新值从而完成全局模型的更新。不断重复训练直至达到隐私边界。
3. 差分隐私模块：此部分主要为了解决联邦学习过程中，恶意攻击者或服务端可能根据中间传递的模型参数来推断原始数据。在每个参与方返回模型更新参数前，在本地通过高斯机制实现差分隐私保护。同时，在每个轮次训练结束，计算隐私损失，如达到隐私边界（隐私边界设置为1/|BN|，B为批次数量，N为参与客户端数量）则停止训练。
4. 算法的测试方法：
5. 为了尽可能模拟真实场景下多数据源的非独立同分布数据，将数据拆分为不同数量的各个部分来模拟各参与方的数据，同时要保持每个参与方数据尽可能包含不同标签的数据，从而在单一数据源数据上训练得到的模型无法拥有较好表现，使得数据融合分析是有必要且效果显著的；
6. 在每一轮训练结束，输出依次为“当前训练轮次、训练参与方数量、训练时间、当前的隐私参数、模型损失、模型精确度”。观察发现，模型精确度逐轮提升，当隐私参数delta达到边界1/|BN|时，训练停止，满足隐私要求。
7. 对应指标：

支持自有和外部数据融合分析场景的隐私保护：基于联邦学习的多源数据融合分析机制

敏感数据脱敏方法一种：基于差分隐私的本地更新保护机制