

分布式用户隐私保护可调节的云服务个性化 QoS 预测模型

许建龙, 林健, 黎宇森, 熊智

(汕头大学工学院, 广东 汕头 515063)

摘要: 个性化服务质量 (QoS, quality of service) 预测是构建高质量云服务系统的重要环节, 传统基于协同过滤方法采用集中式的训练模式难以保护用户隐私, 为了在获取高准确预测效果的同时有效保护用户隐私, 提出分布式用户隐私保护可调节的云服务个性化 QoS 预测模型 (DUPPA)。该模型采用“服务器-多用户”架构, 服务器协调多个用户, 处理多用户上传模型梯度和下载全局模型的请求并维护全局模型参数。为进一步保护用户隐私, 提出用户隐私程度调节策略, 通过调节本地模型参数初始化比例、梯度上传比例以平衡隐私程度和预测精度。在本地模型初始化阶段, 用户计算本地模型与全局模型的差值矩阵, 并选择差值矩阵中数值较大元素所对应的全局模型参数初始化本地模型参数; 在梯度上传阶段, 用户可选择部分重要的梯度上传至服务器来满足不同应用场景对隐私保护的需求。为了评估 DUPPA 的隐私程度, 提出针对分布式矩阵分解模型梯度共享方案的数据重构攻击方法。实验结果表明, 当 DUPPA 在梯度上传比例为 0.1、本地模型参数初始化比例为 0.5 时, 预测的平均绝对误差 (MAE, mean absolute error) 和均方根误差 (RMSE, root mean square error) 较传统的集中式矩阵分解模型分别降低了 1.20% 和 0.91%; 当 DUPPA 的梯度上传比例为 0.1 时, 隐私程度至少是梯度上传比例为 1 时的 5 倍; 当 DUPPA 的本地模型参数初始化比例为 0.5 时, 隐私程度至少是本地模型参数初始化比例为 1 时的 3.44 倍。

关键词: 云服务; 隐私保护; 分布式矩阵分解; 服务质量预测

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023022

Distributed user privacy preserving adjustable personalized QoS prediction model for cloud services

XU Jianlong, LIN Jian, LI Yusen, XIONG Zhi

School of Engineering, Shantou University, Shantou 515063, China

收稿日期: 2022-04-19; 修回日期: 2023-02-21

通信作者: 许建龙, xujianlong@stu.edu.cn

基金项目: 国家自然科学基金 (61702318); 广东省基础与应用基础研究基金 (2023A1515010707, 2021A1515012527); 广东省科技专项资金 (“大专项+任务清单”) 项目 (STKJ2021201); 广东省普通高校重点领域专项 (2022ZDZX1008)

Foundation Items: The National Natural Science Foundation of China (61702318), Guangdong Province Basic and Applied Basic Research Fund (2023A1515010707, 2021A1515012527), Guangdong Science and Technology Special Fund Project (“Major Project + Task List”) (STKJ2021201), Special Projects in Key Fields of Guangdong Universities (2022ZDZX1008)

引用格式: 许建龙, 林健, 黎宇森, 等. 分布式用户隐私保护可调节的云服务个性化 QoS 预测模型[J]. 网络与信息安全学报, 2023, 9(2): 70-80.

Citation Format: XU J L, LIN J, LI Y S, et al. Distributed user privacy preserving adjustable personalized QoS prediction model for cloud services[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 70-80.

Abstract: Personalized quality of service (QoS) prediction is crucial for developing high-quality cloud service system. However, the traditional collaborative filtering method, based on centralized training, presents challenges in protecting user privacy. In order to effectively protect user privacy while obtaining highly accurate prediction effect, a distributed user privacy adjustable personalized QoS prediction model for cloud services (DUPPA) was proposed. The model adopted a “server-multi-user” architecture, in which the server coordinated multiple users, handled multiple users’ requests for uploading model gradients and downloading global model, and maintained global model parameters. To further protect user privacy, a user privacy adjustment strategy was proposed to balance privacy and prediction accuracy by adjusting the initialization proportion of local model parameters and gradient upload proportion. In the local model initialization stage, the user calculated the difference matrix between the local model and the global model, and selected the global model parameters corresponding to the larger elements in the difference matrix to initialize the local model parameters. In the gradient upload stage, the user can select some important gradients to upload to the server to meet the privacy protection requirements of different application scenarios. To evaluate the privacy degree of DUPPA, a data reconstruction attack method was proposed for the distributed matrix factorization model gradient sharing scheme. The experimental results show that when DUPPA sets the gradient upload proportion to 0.1 and the local model parameter initialization proportion to 0.5, the predicted MAE and RMSE are reduced by 1.27% and 0.91%, respectively, compared with the traditional centralized matrix factorization model. Besides, when DUPPA sets the gradient upload proportion to 0.1, the privacy degree is 5 times higher than when the gradient upload proportion is 1. And when DUPPA sets the local model parameter initialization proportion to 0.5, the privacy degree is 3.44 times higher than when the local model parameter initialization proportion is 1.

Keywords: cloud service, privacy protection, distributed matrix factorization, quality of service prediction

0 引言

随着云计算技术发展, 互联网上出现了越来越多的云服务, 用户可根据需要调用这些云服务来构建高质量云计算应用系统, 随着云服务数量呈指数级增长, 大量等价或类似功能的候选服务应运而生, 如谷歌、亚马逊等互联网公司通过云平台为开发者提供数以万计的云服务^[1-2]。为了从众多候选服务中选择最合适服务以满足用户个性化需求, 云服务的非功能性属性——服务质量 (QoS) 成为主要关注的指标^[3]。用户可通过调用云服务来获得其 QoS 值 (包括吞吐量、响应时间、可靠性等) 从而判断云服务质量的优劣, 以此来筛选合适的云服务。然而, 用户如果每次都调用所有服务再通过排序其 QoS 值来选择出最优 QoS 值, 将付出大量代价。解决这个问题有效方法是收集大量用户调用云服务的历史 QoS 值, 在此基础上对未知云服务的 QoS 值进行预测^[4]。目前, 众多学者采用以协同过滤为主的 QoS 预测方法^[5], 为了获取更准确的 QoS

值, 很多学者在传统方法的基础上融合了地理位置^[6]、时间信息^[7]、上下文信息^[8]等因素, 构建更加优越的预测模型。

尽管这些方法能较准确预测出未知服务的 QoS 值, 但仍然存在以下主要问题。① 传统的集中式训练方法需要较高存储成本^[9], 因为集中式训练方法需要中心云服务器收集分散的用户原始数据并进行建模, 但用户和云服务数量激增所产生的数以百万计的 QoS 值将加重云中心数据存储压力。② 集中式存储原始数据具有高隐私风险^[10], 因为第三方可能利用收集到的用户数据推断个人信息或将用户数据转售给其他企业以谋取利益。③ 相关法律, 如通用数据保护条例^[11] (GDPR, general data protection regulation) 对收集和使用用户数据有严格的规定, 要求企业或组织只能为特定目的收集和处理最低数量个人信息, 这无疑给集中式存储数据带来了挑战。此外, 对于分布式用户来说, 在训练预测模型过程中, 若共享原始数据, 则存在较高的隐私泄露风险; 若共享模型权重或梯度则可降低风险, 但难以权衡分享参数

与预测精度,因此模型需要具备在不同场景下对隐私程度进行调节的能力。

针对以上问题,本文提出分布式用户隐私保护可调节的云服务个性化 QoS 预测模型(DUPPA)。该模型采用分布式训练模式,即用户数据和模型训练都在本地,用户间无须共享原始数据,只需用户间共享模型梯度来学习个性化 QoS 预测模型。由于不同数据共享对隐私的影响不一样,相比共享原始数据,共享模型权重或梯度将使得第三方推断用户敏感信息更加困难,从而降低隐私泄露的等级。为进一步保护用户隐私,该模型允许用户通过用户隐私调节策略平衡隐私程度和预测精度,包括在本地模型初始化阶段调节本地模型参数初始化比例和在梯度共享阶段调节梯度交换数量。此外,为了评估 DUPPA 的隐私程度,本文提出了针对分布式矩阵分解模型梯度共享方案的数据重构攻击方法,本文主要贡献如下。

1) 提出 DUPPA,可有效解决集中式模型训练方法的用户隐私泄露问题。

2) 提出用户隐私程度调节策略,该策略允许用户调节本地模型参数初始化比例和梯度上传比例以平衡用户隐私程度和预测精度。

3) 提出针对分布式矩阵分解梯度分享方案的数据重构攻击方法。

4) 在真实数据集中通过大量实验来验证所提方法的有效性。

1 相关工作

1.1 基于协同过滤的 QoS 预测方法

协同过滤方法是目前常用的 QoS 预测方法,分为基于内存的协同过滤^[12-14]和基于模型的协同过滤^[2,15-16]。基于内存的协同过滤方法利用用户感知服务的 QoS 值来计算用户和服务间的相似性。典型的例子包括基于相似用户的协同过滤^[12]、基于相似服务的协同过滤^[13]和基于相似用户-服务的混合协同过滤^[14]。尽管基于内存的协同过滤方法实现简单,但该方法在数据稀疏情况下的 QoS 预测准确性较低,难以给出可靠的云服务推荐。基于模型的协同过滤方法有效缓解了这个问题。矩阵分解^[15-16]是一种普遍应用在服务推荐领域的

基于模型协同过滤的技术,其原理是将用户-服务交互矩阵分解成两个低维的矩阵乘积。Zheng 等^[15]提出一种融合了基于邻域协同过滤并结合矩阵分解的方法为用户提供个性化的 QoS 预测。Zhang 等^[16]提出一种在云环境下基于矩阵分解的可行在线 QoS 预测方法。

1.2 隐私保护

尽管协同过滤技术可以给用户带来许多好处,但用户敏感数据的收集会导致越来越多的用户不愿意提供自己的历史数据。因此,在为用户推荐高质量服务的同时保护用户隐私成为一个重要的问题。针对隐私保护,诸多解决方案被提出,如利用混淆数据方法^[1,17-18]、密码学方法^[19-21]、匿名化技术^[22]、局部敏感哈希技术^[23]或者采用联邦学习技术^[24]。Zhu 等^[1]提出了一种应用数据混淆技术的隐私保护方法,该方法通过给每个用户观察到的 QoS 值添加一个随机的噪声,然后利用基于协同过滤的方法进行预测未知的 QoS 值。Badsha 等^[19]提出了一种利用同态加密技术保护用户的 QoS 值和用户位置的协议,该协议允许第三方在加密后的数据上进行计算并通过协同过滤技术预测 QoS 值。Qi 等^[23]提出一种考虑时间、空间上下文的 QoS 隐私保护方法,该方法首先通过局部敏感哈希技术哈希原来的数据,然后通过基于内存的协同过滤方法处理哈希后的 QoS 数据。然而以上这些方法采用集中式的训练方法,集中式训练需要存储大量用户相关的数据(如加密或混淆后的 QoS 值),这会产生昂贵的存储费用。Zhang 等^[24]提出了将联邦学习应用到矩阵分解方法中,这是一种分布式训练方法,该方法允许用户不暴露原始数据,而是通过共享模型参数协同训练一个全局模型。尽管该方法没有直接泄露隐私,但完整传递模型参数给第三方是存在风险的^[25],因为第三方可以从共享的模型参数中推断出用户的原始数据。

2 模型

2.1 模型概述

分布式用户隐私保护可调节的云服务个性化 QoS 预测模型示意如图 1 所示,其中包括一个参数服务器和多个用户。参数服务器负责协调用户

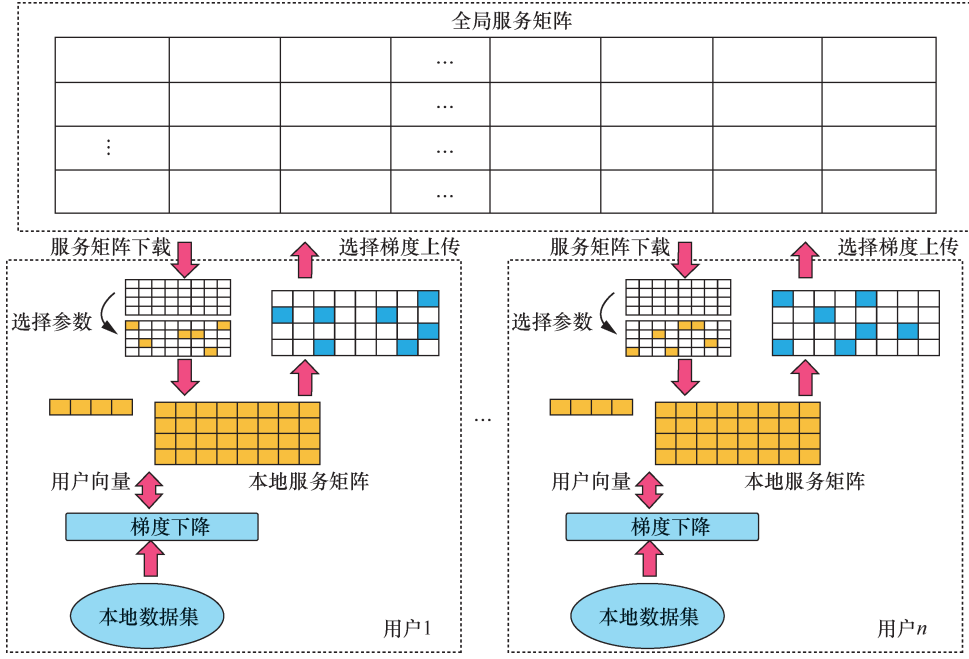


图 1 分布式用户隐私保护可调节的云服务个性化 QoS 预测模型

Figure 1 Distributed user privacy preserving adjustable personalized QoS prediction model for cloud services

参与模型训练并维护全局服务矩阵参数。用户负责利用持有的本地数据集更新本地模型并通过上传本地服务矩阵梯度的方式与其他用户协同训练全局服务矩阵。用户参与协同训练的过程分为以下 3 个步骤：① 用户下载最新的全局服务矩阵并选取一定比例的全局服务矩阵参数初始化本地服务矩阵；② 用户利用本地数据对用户向量和初始化后的本地服务矩阵采用梯度下降方法进行更新；③ 本地模型完成更新后将一定比例的服务矩阵梯度上传至参数服务器。

可以看出，整个协同训练过程中，用户无须共享原始数据至参数服务器，只需上传本地服务矩阵梯度至参数服务器，这将有效保护用户隐私。一方面，用户不需要上传全部梯度；另一方面，若上传梯度，其上传比例是可以调节的。这样做是为了提高恶意攻击者（本文假设参数服务器是恶意攻击者）从上传的梯度中推断用户原始数据的难度。此外，该模型可以通过调节本地服务矩阵初始化的比例进一步保护用户隐私。

2.2 参数服务器协调策略

参数服务器主要有 3 个任务：① 协调用户参与模型训练；② 处理用户上传本地服务矩阵梯度和下载全局服务矩阵的请求；③ 维护全局服务矩阵。

在每一轮训练开始前，参数服务器从所有用户中随机选择比例为 C 的用户参与该轮模型训练（记被选中参与训练用户组成的集合为 Set ）并发送最新的全局服务矩阵 $\mathbf{S}^{\text{global}}$ 至被选中的用户。当用户 i 完成本地模型训练并上传梯度 $\mathbf{g}^i$ 时，参数服务器利用用户上传的梯度更新全局服务矩阵，公式如下。

$$\mathbf{S}^{\text{global}} = \mathbf{S}^{\text{global}} - \eta \sum_{i \in \text{Set}} \mathbf{g}^i \quad (1)$$

其中， η 为学习率，控制每一轮全局服务矩阵的变化。在参数服务器完成本轮全局服务矩阵更新后，参数服务器协调用户参与下一轮的模型训练，直至模型收敛。DUPPA 在参数服务器的执行算法如算法 1 所述。

算法 1 DUPPA 在参数服务器的执行算法

初始化 全局服务矩阵 $\mathbf{S}^{\text{global}}$

输入 用户的本地服务矩阵梯度 $\mathbf{g}^i$, $i \in \text{Set}$

输出 更新后的全局服务矩阵 $\mathbf{S}^{\text{global}}$

1) 聚合用户的服务矩阵梯度 $\mathbf{g}^i$, $i \in \text{Set}$

2) $\mathbf{S}^{\text{global}} = \mathbf{S}^{\text{global}} - \eta \sum_{i \in \text{Set}} \mathbf{g}^i$ // 利用梯度更新全局服务矩阵

局服务矩阵

3) 如果模型收敛，则训练结束，否则参数服务器协调用户进入下一轮模型训练，即重新从所

有用户中随机选择比例为 C 的用户参与模型训练并发送最新的全局服务矩阵 $\mathbf{S}^{\text{global}}$ 。

2.3 用户隐私程度调节策略

假设在 DUPPA 中有 n 个用户, m 个服务, 由于每个用户的训练过程都是一样的, 不失一般性, 本文选取用户 i 为例。用户 i 存储了本地 QoS 矩阵 $\mathbf{R}_i$ 以及本地矩阵分解模型 (本地模型参数包括用户向量 $\mathbf{U}_i$ 和本地服务矩阵 $\mathbf{S}^i$), 于是用户 i 可以利用用户向量 $\mathbf{U}_i$ 和本地服务矩阵 $\mathbf{S}^i$ 来拟合 QoS 矩阵 $\mathbf{R}_i$ 。

$$\mathbf{R}_i \approx (\mathbf{U}_i)^\top \mathbf{S}^i \quad (2)$$

其中, $\mathbf{R}_i \in \mathbb{R}^{1 \times m}$, $\mathbf{U}_i \in \mathbb{R}^{d \times 1}$, $\mathbf{S}^i \in \mathbb{R}^{d \times m}$ 。在每一轮本地训练开始前, 用户需要初始化本地服务矩阵 $\mathbf{S}^i$ 。本地服务矩阵初始化需要完成两个步骤:

① 下载来自参数服务器最新的全局服务矩阵 $\mathbf{S}^{\text{global}}$; ② 用户可自由调节重写本地服务矩阵比例 θ_o 以控制隐私程度并利用比例 θ_o 的全局服务矩阵元素重写本地服务矩阵。

本文通过二进制掩码矩阵 $\mathbf{Mask}_o^i$ 为每个用户选择满足重写条件的全局服务矩阵元素, 步骤如下。① 用全局服务矩阵 $\mathbf{S}^{\text{global}}$ 减去本地服务矩阵 $\mathbf{S}^i$ 得到差值矩阵 $\mathbf{d}^i$, 并对矩阵 $\mathbf{d}^i$ 求绝对值, 得到矩阵 $\mathbf{D}^i$, 公式如下。

$$\mathbf{D}^i = |\mathbf{S}^{\text{global}} - \mathbf{S}^i| \quad (3)$$

② 将矩阵 $\mathbf{D}^i$ 的元素从大到小排列, 并优先记录比较大的元素的索引 (元素的行和列的位置), 直至比例满足 θ_o 。③ 将索引对应的二进制掩码矩阵 $\mathbf{Mask}_o^i$ 元素赋值为 1, 其他元素为 0。④ 将赋值后的掩码矩阵 $\mathbf{Mask}_o^i$ 和全局矩阵对应元素相乘得到满足重写条件的全局服务矩阵元素, 全局服务矩阵被选取的元素可以用式子 $\mathbf{Mask}_o^i \odot \mathbf{S}^{\text{global}}$ 表示, 其中 $\odot$ 表示元素乘法。假设 $\mathbf{ONE} \in \mathbb{R}^{d \times m}$ 为元素全为 1 的矩阵, 重写后的本地服务矩阵表示为

$$\mathbf{S}^i = (\mathbf{ONE} - \mathbf{Mask}_o^i) \odot \mathbf{S}^i + \mathbf{Mask}_o^i \odot \mathbf{S}^{\text{global}} \quad (4)$$

特别指出的是, 重写比例 θ_o 是可以调节的, 一般来说, 重写比例越高, 预测精度越高, 但同时用户隐私泄露的风险越大, 所以需要平衡用户隐私程度和预测精度。通过以上步骤就完成了本

地模型的初始化。

在本地模型初始化后, 用户利用本地数据 (即 QoS 矩阵) 训练保存在本地的用户向量 $\mathbf{U}_i$ 和被重写后的本地服务矩阵 $\mathbf{S}^i$ 。由于本地矩阵分解模型的优化目标是缩小式(2)中不等式两边的误差, 同时为了避免过拟合, 需要加入正则项, 于是用户 i 本地矩阵分解模型的损失函数表示为

$$L_i = \frac{1}{2} \sum_{j=1}^m I_{ij} (\mathbf{R}_{ij} - (\mathbf{U}_i)^\top \mathbf{S}_j^i)^2 + \frac{\lambda_u}{2} \|\mathbf{U}_i\|_F^2 + \frac{\lambda_s}{2} \|\mathbf{S}^i\|_F^2 \quad (5)$$

其中, I_{ij} 表示该 QoS 值是否被观察到, 如果 $I_{ij} = 1$ 表示该 QoS 值被观察到, 如果 $I_{ij} = 0$ 表示该 QoS 值没有被观察到, λ_u 、 λ_s 表示正则化的程度。本文采用梯度下降方法^[26]来训练本地模型。如式(6)和式(7)所示。

$$\mathbf{U}_i = \mathbf{U}_i - \eta \frac{\partial L_i}{\partial \mathbf{U}_i} \quad (6)$$

$$\mathbf{S}^i = \mathbf{S}^i - \eta \frac{\partial L_i}{\partial \mathbf{S}^i} \quad (7)$$

本地训练结束后, 需要上传本地服务矩阵梯度 $\frac{\partial L_i}{\partial \mathbf{S}^i}$ 至参数服务器。用户可自由调节梯度上传比例 θ_u 以控制隐私保护程度。本文通过二进制掩码矩阵 $\mathbf{Mask}_u^i$ 为每个用户选择满足上传条件的服务矩阵梯度, 步骤如下。① 计算梯度 $\frac{\partial L_i}{\partial \mathbf{S}^i}$ 的绝对值 $\mathbf{G}^i$ 。② 将矩阵 $\mathbf{G}^i$ 的元素从大到小排列, 优先记录比较大元素的索引 (元素的行和列的位置), 直至比例满足 θ_u 。③ 将索引对应的二进制掩码矩阵 $\mathbf{Mask}_u^i$ 元素赋值为 1, 其他元素为 0。④ 将赋值后的掩码矩阵 $\mathbf{Mask}_u^i$ 和梯度矩阵对应元素相乘得到满足上传条件梯度, 如式(8)所示。

$$\mathbf{g}^i = \mathbf{Mask}_u^i \odot \frac{\partial L_i}{\partial \mathbf{S}^i} \quad (8)$$

用户隐私程度调节算法如算法 2 所示。

算法 2 用户隐私程度调节算法

初始化 本地服务矩阵重写比例 θ_o , 梯度上传比例 θ_u

输入 全局服务矩阵 $\mathbf{S}^{\text{global}}$

输出 上传的服务矩阵梯度 $\mathbf{g}^i$

- 1) $\mathbf{d}^i = \mathbf{S}^{\text{global}} - \mathbf{S}^i$ //差值矩阵 $\mathbf{d}^i$ ，全局服务矩阵 $\mathbf{S}^{\text{global}}$ ，本地服务矩阵 $\mathbf{S}^i$
- 2) $\mathbf{D}^i = |\mathbf{d}^i|$ //对矩阵 $\mathbf{d}^i$ 取绝对值
- 3) 对矩阵 $\mathbf{D}^i$ 的元素从大到小排列
- 4) 优先记录比较大的元素的索引（元素的行和列的位置），直至比例满足 θ_o
- 5) 将索引对应的二进制掩码矩阵 $\mathbf{Mask}_o^i$ 元素赋值为 1，其他元素为 0
- 6) 重写本地服务矩阵
- 7) 用户利用本地数据通过梯度下降法更新本地服务矩阵和本地用户向量
- 8) $\mathbf{G}^i = \left| \frac{\partial L_i}{\partial \mathbf{S}^i} \right|$ //对本地服务矩阵梯度取绝对值
- 9) 优先记录比较大的元素的索引（元素的行和列的位置），直至比例满足 θ_u
- 10) 将索引对应的二进制掩码矩阵 $\mathbf{Mask}_u^i$ 元素赋值为 1，其他元素为 0
- 11) $\mathbf{g}^i = \mathbf{Mask}_u^i \odot \mathbf{G}^i$ // $\mathbf{g}^i$ 为要上传的梯度

3 数据重构攻击方法

数据重构攻击^[26]指的是恶意攻击者（本文指参数服务器）能够从用户在分布式机器学习模型训练过程中分享的梯度推理出其原始数据，为了评估 DUPPA 的隐私程度，本文提出了针对分布式矩阵分解模型梯度分享方案的数据重构攻击方法。假设用户 i 的训练数据集为 $\mathbf{R}_i$ ，用户向量为 $\mathbf{U}_i$ ，用户在任意连续两轮训练中分享的梯度为 $\mathbf{g}^{i,t}$ 、 $\mathbf{g}^{i,t+1}$ ，虚拟数据集为 $\mathbf{R}'_i$ ，虚拟用户向量为 $\mathbf{U}'_i$ ，虚拟梯度为 $(\mathbf{g}^{i,t})'$ 、 $(\mathbf{g}^{i,t+1})'$ 。数据重构攻击的目标是从用户分享的梯度 $\mathbf{g}^{i,t}$ 、 $\mathbf{g}^{i,t+1}$ 重构用户训练数据集 $\mathbf{R}_i$ 。值得注意的是，第 t 轮、第 $t+1$ 轮的全局服务矩阵 $\mathbf{S}^t$ 、 $\mathbf{S}^{t+1}$ 是公开的。

为了从梯度中重构用户数据，本文执行以下 3 个步骤。① 随机初始化 $\mathbf{R}'_i$ 和 $\mathbf{U}'_i$ 。② 利用 $\mathbf{U}'_i$ 和 $\mathbf{S}$ 初始化矩阵分解模型，并计算初始化后的模型在 $\mathbf{R}'_i$ 上的损失函数 $(L_i)'$ 和梯度 $(\mathbf{g}^i)'$ 。 $(L_i)'$ 可表示为

$$(L_i)' = \frac{1}{2} \sum_{j=1}^m L_{ij} (\mathbf{R}'_{ij} - (\mathbf{U}'_i)^T \mathbf{S}_j)^2 + \frac{\lambda_u}{2} \|\mathbf{U}'_i\|_F^2 + \frac{\lambda_s}{2} \|\mathbf{S}\|_F^2 \quad (9)$$

$(\mathbf{g}^{i,t})'$ 可由第 t 轮的损失函数 $(L_i)'$ 计算得到。

$$(\mathbf{g}^{i,t})' = \frac{\partial (L_i)'}{\partial \mathbf{S}^t} \quad (10)$$

可根据 $(L_i)'$ 更新 $\mathbf{U}'_i$ ，如式(11)所示。

$$\mathbf{U}'_i = \mathbf{U}'_i - \eta \frac{\partial (L_i)'}{\partial \mathbf{U}'_i} \quad (11)$$

然后计算 $(\mathbf{g}^{i,t+1})'$ 。

$$(\mathbf{g}^{i,t+1})' = \frac{\partial (L_i^{t+1})'}{\partial \mathbf{S}^{t+1}} \quad (12)$$

③ 通过最小化 $\mathbf{g}^i$ 和 $(\mathbf{g}^i)'$ 之间的距离使 $\mathbf{R}'_i$ 和 $\mathbf{U}'_i$ 逼近真实的 QoS 数据 $\mathbf{R}_i$ 和真实的用户向量 $\mathbf{U}_i$ ，得到近似真实用户训练数据 $\mathbf{R}_i^*$ 和近似用户向量 $\mathbf{U}_i^*$ ， $\mathbf{R}_i^*$ 和 $\mathbf{U}_i^*$ 的计算式为

$$(\mathbf{R}_i^*, \mathbf{U}_i^*) = \arg \min_{(\mathbf{R}_i^*, \mathbf{U}_i^*)} (\|(\mathbf{g}^{i,t})' - \mathbf{g}^{i,t}\|^2 + \|(\mathbf{g}^{i,t+1})' - \mathbf{g}^{i,t+1}\|^2) \quad (13)$$

在式(13)中，本文采用标准的基于梯度的算法^[27]对目标函数进行优化，值得注意的是，由于优化结果 $\mathbf{R}_i^*$ 可能会出现负数，但在实际场景下的 QoS 值都为正数，所以需要对优化结果 $\mathbf{R}_i^*$ 取绝对值以提高数据重构质量，如式(14)所示。

$$\mathbf{R}_i^* = |\mathbf{R}_i^*| \quad (14)$$

4 实验

本节通过实验来验证所提方法的有效性，重点关注以下几个问题。

问题 1：如何平衡模型预测精度和用户隐私程度的关系？

问题 2：相比传统集中式的矩阵分解，本文提出的模型的预测精度如何？

问题 3：相比传统集中式矩阵分解，本文模型的收敛效率如何？

问题 4：增加每轮参与训练的用户数量是否能加快本文模型收敛效率？

4.1 数据集

本文采用由 Zheng 等^[28]维护的 WS-DREAM 数据集进行实验，该数据集包括来自 339 个用户（分布于 31 个国家）调用 5 825 个服务（分布于 79 个国家）的 QoS 记录。本文采用响应时间 (RT, response time) 的子数据集包含 1 974 675 条 QoS

记录, 属性的范围为 0~20 s。

4.2 评估指标

本文从预测精度和隐私程度两方面来评估所提模型的性能。

预测精度采用平均绝对误差 (MAE, mean absolute error) 和均方根误差 (RMSE, root mean square error) 两个评估指标来衡量。

$$\text{MAE} = \frac{\sum_{I_{ij}=0} |\hat{R}_{ij} - R_{ij}|}{N} \quad (15)$$

$$\text{RMSE} = \sqrt{\frac{\sum_{I_{ij}=0} (\hat{R}_{ij} - R_{ij})^2}{N}} \quad (16)$$

其中, N 为数据集中 $I_{ij}=0$ 的数量, $\hat{R}_{ij}$ 为第 i 个用户感知第 j 个服务的预测 QoS 值, R_{ij} 为第 i 个用户感知第 j 个服务的真实 QoS 值。MAE 通常被用来表示 QoS 预测模型的平均预测精度。RMSE 通常被用来衡量模型的稳定性。

隐私程度采用数据重构质量^[29]来衡量, 用重构 QoS 值与原始 QoS 值之间的均方误差 (MSE, mean square error) 表示。

$$\text{MSE} = \frac{\sum_{I_{ij}=1} (R'_{ij} - R_{ij})^2}{M} \quad (17)$$

其中, M 为数据集中 $I_{ij}=1$ 的数量, R'_{ij} 为第 i 个用户感知第 j 个服务的重构 QoS 值, R_{ij} 为第 i 个用户感知第 j 个服务的真实 QoS 值。式(17)中, MSE 越小, 数据重构质量越高, 隐私程度越低。

4.3 参数设置

实验中, 将集中式矩阵分解模型^[30] (CMF, centralized matrix factorization model) 与本文提出的 DUPPA 做比较。DUPPA 和 CMF 的学习率

$\eta=0.003$, 正则化程度 $\lambda_u, \lambda_s=0.1$, 隐含特征维度 $d=10$ 。此外, 本文设置 DUPPA 的梯度上传比例 $\theta_u=0.1$, 本地服务矩阵重写比例 $\theta_o=0.5$, 参与模型训练的用户比例 $C=1$ 。在实际场景下, 由于单个用户调用云服务占总云服务比例很小, 为了模拟实际场景, 本文设置矩阵密度 (MD, matrix density) = {2.5%, 5%, 7.5%, 10%}。MD=10% 表示从原始数据集中随机选择 10% 的 QoS 记录作为训练集用以预测剩余 90% 的 QoS 记录。MD=10% 数据集的选取分为两个步骤: ① 从原数据集中随机抽取占总样本数量的 10%; ② 由于每个数据是由 (用户, 服务, QoS) 三元组组成, 故本文将用户元素相同的元组放在同一个用户数据集中, 剩余 90% 数据集样本作为测试集用来验证模型性能。

此外, 对于数据重构攻击方法, 本文将该方法的基于梯度的优化算法设置为 L-BFGS^[27], 学习率为 1。本文随机选择 1 个用户作为攻击目标。

4.4 调整梯度上传和本地服务矩阵重写比例 (问题 1)

为了平衡预测精度和用户隐私程度, 本文实验分别调整梯度上传比例 θ_u 和本地服务矩阵重写比例 θ_o , 并讨论 DUPPA 在不同参数下对预测精度和隐私程度的影响。为了讨论梯度上传比例 θ_u 对 DUPPA 预测精度和隐私程度的影响, 本文实验设置梯度上传比例 $\theta_u=\{1, 0.1, 0.01, 0.001\}$, 本地服务矩阵重写比例 $\theta_o=1$ 。表 1 为在固定服务矩阵重写比例 θ_o 的情况下, 不同梯度上传比例在 RT 上的预测精度和隐私程度。从表 1 可看出, 当 $\theta_u=0.1$ 时, MSE 至少是 $\theta_u=1$ 时的 5 倍, 但 MAE 与 RMSE 均与 $\theta_u=1$ 时的值特别接近。此外, 当 θ_u 小于 0.1 时, 随着 θ_u 变小, MSE 在变大,

表 1 不同梯度上传比例在 RT 上的预测精度和隐私程度
Table 1 Prediction accuracy and privacy degree for different gradient upload proportions on RT

上传比例	MD = 2.5%		MD = 5.0%		MD = 7.5%		MD = 10.0%	
	MAE/RMSE	MSE	MAE/RMSE	MSE	MAE/RMSE	MSE	MAE/RMSE	MSE
1	0.634/1.609	0.000 1	0.550/1.40	0.000 1	0.512/1.301	0.000 1	0.500/1.290	0.002
0.1	0.650/1.633	0.000 5	0.577/1.422	0.001	0.520/1.296	0.002	0.504/1.278	0.124
0.01	0.694/1.723	0.090	0.615/1.477	0.712	0.531/1.302	2.806	0.532/1.280	2.067
0.001	0.835/1.948	6.402	0.715/1.621	9.556	0.650/1.406	14.052	0.650/1.396	14.185

MAE 与 RMSE 也在变大。该实验结果说明: 用户间共享部分梯度和共享全部梯度的预测精度是很接近的, 但在共享部分梯度时能够有效提高用户的隐私程度。因此, 在同时考虑用户隐私、预测精度和计算效率的情况下, 将梯度上传比例 θ_u 设为 0.1。

为了讨论本地服务矩阵重写比例 θ_o 对 DUPPA 预测精度和隐私程度的影响, 本文实验设置本地服务矩阵的重写比例 $\theta_o = \{1, 0.5, 0.1, 0.05\}$, 梯度上传比例 $\theta_u = 0.1$ 。表 2 为在固定梯度上传比例 θ_u 的情况下, 不同本地服务矩阵重写比例在 RT 上的预测精度和隐私程度。从表 2 可看出, 当 $\theta_o = 0.5$ 时, MSE 至少是 $\theta_o = 1$ 时的 3.44 倍, 但 MAE 与 RMSE 的值均与 $\theta_o = 1$ 时的值特别接近 (相差约 0.03)。此外, 随着 θ_o 变小, MSE 变大, MAE 与 RMSE 也在变大。该实验结果说明: 用户重写部分本地服务矩阵参数和重写全部本地服务矩阵参数的预测精度是很接近的, 但在重写部分本地服务矩阵参数时能够有效提高用户的隐私程度。因此, 在同时考虑用户隐私、预测精度和计算效率的情况下, 接下来的实验将本地服务矩阵重写比例 θ_o 设为 0.5。

为了讨论梯度上传比例 θ_u 与本地服务矩阵重写比例 θ_o 对 DUPPA 预测精度和隐私程度的影

响, 本文实验设置 MD=10%, 梯度上传比例 $\theta_u = \{1, 0.1, 0.01, 0.001\}$, 本地服务矩阵重写比例 $\theta_o = \{1, 0.5, 0.1, 0.05\}$ 。表 3 为梯度上传比例和本地服务矩阵重写比例对 RT 的预测精度和隐私程度的影响。从表 3 可看出, 当 $\theta_u = 0.01$ 、 $\theta_o = 0.1$ 时, MSE 是 $\theta_u = 0.01$ 、 $\theta_o = 1$ 时的 4.8 倍, 是 $\theta_u = 1$ 、 $\theta_o = 0.1$ 时的 14.56 倍; MAE 与 RMSE 较 $\theta_u = 0.01$ 、 $\theta_o = 1$ 分别约 0.02、0.02, 较 $\theta_u = 1$ 、 $\theta_o = 0.1$ 时分别增大约 0.05、0.03。该实验结果说明: 相比只调节梯度上传比例或本地服务矩阵重写比例, 同时调节梯度上传比例和本地服务矩阵重写比例对模型的隐私程度和预测精度影响更大。

4.5 预测精度 (问题 2)

本节通过实验比较本文模型 DUPPA 与集中式矩阵分解模型 CMF 的预测精度。表 4 为不同模型在 RT 上的预测精度比较。从表 4 可看出, DUPPA 与 CMF 模型相比, DUPPA 在 MD={5%, 7.5%, 10%} 时的 MAE、RMSE 都优于 CMF 模型。这可能是由于用户间共享部分关键梯度和用户重写部分关键模型参数起到正则化的效果, 使协同训练的模型在少量训练数据的情况下能避免过拟合现象。因此, 与传统矩阵分解模型相比, DUPPA 可在提高预测精度的情况下保障用户隐私。

表 2 不同本地服务矩阵重写比例在 RT 上的预测精度和隐私程度

Table 2 Prediction accuracy and privacy degree for different local service matrix overwrite proportions on RT

重写比例	MD = 2.5%		MD = 5.0%		MD = 7.5%		MD = 10.0%	
	MAE/RMSE	MSE	MAE/RMSE	MSE	MAE/RMSE	MSE	MAE/RMSE	MSE
1	0.650/1.633	0.000 5	0.577/1.422	0.001	0.520/1.296	0.002	0.504/1.278	0.124
0.5	0.652/1.642	0.043	0.573/1.414	0.193	0.528/1.322	0.095	0.500/1.265	0.426
0.1	0.654/1.660	1.847	0.588/1.454	3.757	0.536/1.332	1.271	0.515/1.281	1.660
0.05	0.672/1.679	4.393	0.630/1.549	7.454	0.594/1.432	5.146	0.586/1.335	2.615

表 3 梯度上传比例和本地服务矩阵重写比例对 RT 的预测精度和隐私程度的影响

Table 3 Impact of gradient upload proportions and local service matrix overwrite proportions on prediction accuracy and privacy degree for RT

上传比例	$\theta_o = 1$		$\theta_o = 0.5$		$\theta_o = 0.1$		$\theta_o = 0.05$	
	MAE/RMSE	MSE	MAE/RMSE	MSE	MAE/RMSE	MSE	MAE/RMSE	MSE
1	0.500/1.290	0.002	0.496/1.275	0.071	0.507/1.278	0.682	0.564/1.320	2.761
0.1	0.504/1.278	0.124	0.500/1.265	0.426	0.515/1.281	1.660	0.586/1.335	2.615
0.01	0.532/1.280	2.067	0.539/1.267	2.810	0.556/1.304	9.929	0.583/1.346	8.294
0.001	0.650/1.396	14.185	0.654/1.373	13.553	0.647/1.376	16.118	0.689/1.490	27.348

表 4 不同模型在 RT 上的预测精度比较
Table 4 Comparison table of prediction accuracy of different models on RT

模型	MD = 2.5%		MD = 5.0%		MD = 7.5%		MD = 10.0%	
	MAE	RMSE	MAE	RMSE	MAE	RMSE	MAE	RMSE
CMF	0.652 3	1.650 2	0.580 4	1.427 5	0.528 3	1.321 3	0.500 9	1.268 2
DUPPA	0.652 9	1.642 7	0.573 0	1.414 5	0.528 0	1.322 5	0.500 8	1.265 2
增益	-0.09%	0.45%	1.27%	0.91%	0.05%	-0.09%	0.01%	0.23%

4.6 模型收敛效率（问题 3）

本节通过调整不同梯度上传比例和服务矩阵重写比例讨论模型收敛效率受影响情况，并采用模型的误差到达预期误差所需最小训练轮数（Round）作为衡量模型收敛效率的指标。

1) 不同梯度上传比例 θ_u 对模型收敛效率的影响。实验设置梯度上传比例 $\theta_u = \{1, 0.1, 0.01, 0.001\}$ ，本地服务矩阵重写比例 $\theta_o = 1$ ，MD=10%，预期误差 MAE=0.6，RMSE=1.4。图 2 为不同梯度上传比例在 RT 上的收敛效率。从图 2 可看出，随着训练轮数增加，CMF 模型和 DUPPA 的 MAE 和 RMSE 均呈下降趋势，CMF 模型和 DUPPA (θ_u 为 1 和 0.1) 到达预期误差所需的训练轮数约为 20，并且在训练轮数大于 16 后，它们的变化曲线基本重合（相差约 0.02）。这说明本文提出的模型收敛效率和集中式梯度下降的矩阵分解模型的收敛效率基本相同。

2) 不同服务矩阵重写比例 θ_o 对 DUPPA 收敛效率的影响。实验设置本地服务矩阵重写比例 $\theta_o = \{1, 0.5, 0.1, 0.05\}$ ，梯度上传比例 $\theta_u = 0.1$ ，MD=10%，预期误差 MAE=0.6，RMSE=1.4。图 3 为不同的本地服务矩阵重写比例在 RT 上的收敛效率。从图 3 可看出，随着训练轮数的增加，CMF 模型和 DUPPA 的 MAE 和 RMSE 均呈下降趋势，CMF 模型和 DUPPA (θ_o 为 1 和 0.5) 到达预期误差所需的训练轮数约为 20 轮，并且它们的变化曲线基本重合（相差约 0.03）。当服务矩阵重写比例为 0.05 时，DUPPA 模型到达预期误差的训练轮数增加到 24。这说明随着 DUPPA 服务矩阵重写比例 θ_o 降低，模型的收敛效率也降低。

4.7 参与训练的用户数量（问题 4）

本节通过调整参与训练用户比例讨论模型收

敛效率受影响情况，并采用模型的误差到达预期误差所需最小训练轮数（Round）作为衡量模型收敛效率的指标^[31]，Round 越小，收敛效率越好。

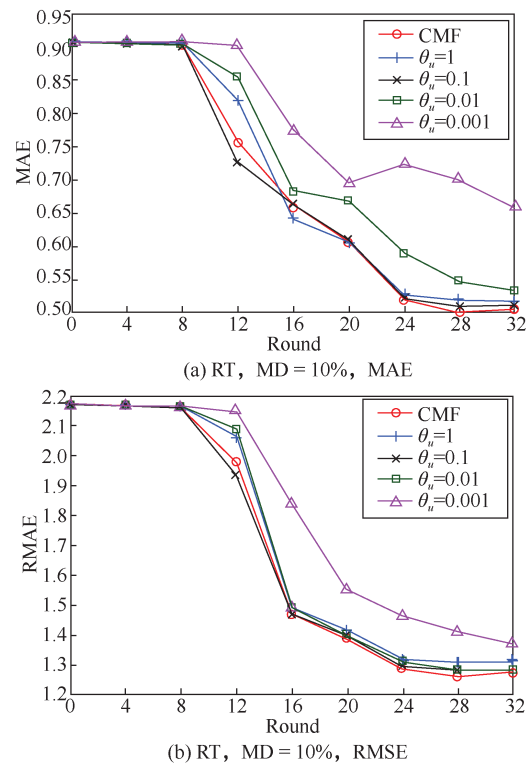


图 2 不同梯度上传比例在 RT 上的收敛效率
Figure 2 Convergence efficiency of different gradient upload proportions on RT

实验设置参与训练用户比例 $C = \{1, 0.5, 0.2, 0.1\}$ ，并将不同矩阵密度下用户比例 $C=1$ 时模型收敛的误差作为预期误差。表 5 为不同参与训练用户比例在 RT 上的收敛效率。从表 5 可看出，随着用户比例的减少，DUPPA 收敛所需的轮数均呈上升趋势。具体来说，当用户比例为 0.1 时，收敛所需的轮数大约为用户比例为 1 时的 10 倍；当用户比例为 0.2 时，收敛所需的轮数大约为用户比例为 1 时的 5 倍；当用户比例为 0.5

时, 收敛所需的轮数大约为用户比例为 1 时的 2 倍。可见, 用户比例和模型收敛所需的轮数成反比。因此, 在实际场景中, 应在每一轮挑选尽量多的用户参与模型训练以降低收敛所需的轮数, 从而加快模型收敛的速度。

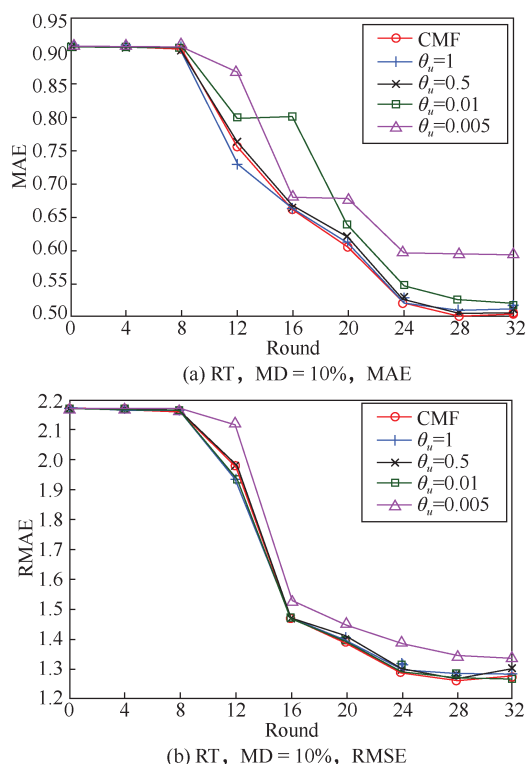


图 3 不同的本地服务矩阵重写比例在 RT 上的收敛效率
Figure 3 Convergence efficiency of different local service matrix overwrite proportions on RT

5 结束语

本文针对云服务个性化 QoS 预测中用户的隐私保护问题, 提出 DUPPA, 通过用户间共享模型参数来学习个性化的预测模型, 从而保护用户隐私。模型中, 本文提出了用户隐私程度调节策略, 即用户可通过调节本地服务矩阵初始化比例、梯

度上传比例以平衡隐私程度和预测精度。此外, 为了衡量 DUPPA 的隐私程度, 本文提出了针对分布式矩阵分解模型梯度分享方案的数据重构攻击方法。在真实数据集中进行的大量实验结果表明, 该模型在保障用户隐私的同时较传统的集中式矩阵分解模型更能提高 QoS 预测精度, 证明本文方法的有效性。在未来工作中, 将探索通过同态加密、差分隐私等技术加强隐私保护程度, 此外, 还将考虑在线情况下的用户隐私保护问题, 构建在线环境下具有用户隐私保护的预测模型。

参考文献:

- [1] ZHU J, HE P, ZHENG Z, et al. A privacy-preserving qos prediction framework for web service recommendation[C]//Proceedings of 2015 IEEE International Conference on Web Services. 2015: 241-248.
- [2] CHEN Z, SUN Y, YOU D, et al. An accurate and efficient web service QoS prediction model with wide-range awareness[J]. Future Generation Computer Systems, 2020, 109: 275-292.
- [3] ZHANG Y, PAN J, QI L, et al. Privacy-preserving quality prediction for edge-based IoT services[J]. Future Generation Computer Systems, 2021, 114: 336-348.
- [4] LIU J, CHEN Y. A personalized clustering-based and reliable trust-aware QoS prediction approach for cloud service recommendation in cloud manufacturing[J]. Knowledge-Based Systems, 2019, 174: 43-56.
- [5] WU D, HE Q, LUO X, et al. A posterior-neighborhood-regularized latent factor model for highly accurate web service QoS prediction[J]. IEEE Transactions on Services Computing, 2019.
- [6] YANG Y, ZHENG Z, NIU X, et al. A location-based factorization machine model for Web service QoS prediction[J]. IEEE Transactions on Services Computing, 2018, 14(5): 1264-1277.
- [7] LI J, WANG J, SUN Q, et al. Temporal influences-aware collaborative filtering for QoS-based service recommendation[C]//Proceedings of 2017 IEEE International Conference on Services Computing (SCC). 2017: 471-474.
- [8] WU H, YUE K, LI B, et al. Collaborative QoS prediction with context-sensitive matrix factorization[J]. Future Generation Com-

表 5 不同参与训练用户比例在 RT 上的收敛效率

Table 5 Convergence efficiency of different proportions of users participating in training on RT

用户比例	MD = 2.5%	MD = 5.0%	MD = 7.5%	MD = 10.0%
1	56	42	35	28
0.5	112	86	71	54
0.2	354	226	164	139
0.1	568	548	398	282

- puter Systems, 2018, 82: 669-678.
- [9] CHEN C, LIU Z, ZHAO P, et al. Privacy preserving point-of-interest recommendation using decentralized matrix factorization[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2018, 32(1).
- [10] 牛犇, 李凤华, 华佳烽, 等. 移动网络中场景关联的隐私保护机制研究[J]. 网络与信息安全学报, 2015, 1(1): 31-42.
- NIU B, LI F H, HUA J F, et al. Research on scenario-based mechanism in privacy-aware mobile networks [J]. Chinese Journal of Network and Information Security. 2015, 1(01): 31-42.
- [11] VOIGT P, VON DEM BUSSCHE A. The eu general data protection regulation (gdpr)[M]. A Practical Guide (1st Ed). Cham: Springer International Publishing, 2017, 10(3152676): 10.5555.
- [12] SHAO L, ZHANG J, WEI Y, et al. Personalized QoS prediction for web services via collaborative filtering[C]//Proceedings of IEEE International Conference on Web Services (ICWS 2007). 2007: 439-446.
- [13] SARWAR B, KARYPIS G, KONSTAN J, et al. Item-based collaborative filtering recommendation algorithms[C]//Proceedings of the 10th international conference on World Wide Web. 2001: 285-295.
- [14] ZHENG Z, MA H, LYU M R, et al. QoS-aware web service recommendation by collaborative filtering[J]. IEEE Transactions on services computing, 2010, 4(2): 140-152.
- [15] ZHENG Z, MA H, LYU M R, et al. Collaborative web service QoS prediction via neighborhood integrated matrix factorization[J]. IEEE Transactions on Services Computing, 2012, 6(3): 289-299.
- [16] ZHANG Y, ZHANG X, ZHANG P, et al. Credible and online qos prediction for services in unreliable cloud environment[C]//Proceedings of 2020 IEEE International Conference on Services Computing (SCC). 2020: 272-279.
- [17] ZHU X, JING X Y, WU D, et al. Similarity-maintaining privacy preservation and location-aware low-rank matrix factorization for QoS prediction based web service recommendation[J]. IEEE Transactions on Services Computing, 2018.
- [18] 张鹏程, 金惠颖. 一种移动边缘环境下面向隐私保护 QoS 预测方法[J]. 计算机学报, 2020, 43(8): 1555-1571.
- ZHANG P C, JIN H Y. A forward privacy-preserving QoS prediction method for mobile edge environments [J]. Chinese Journal of Computers. 2020, 43(8): 1555-1571.
- [19] BADSHA S, YI X, KHALIL I, et al. Privacy preserving location-aware personalized web service recommendations[J]. IEEE Transactions on Services Computing, 2018.
- [20] BADSHA S, YI X, KHALIL I, et al. Privacy preserving user based web service recommendations[J]. IEEE Access, 2018, 6: 56647-56657.
- [21] RAHMAN M S, KHALIL I, ALABDULATIF A, et al. Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform[J]. Knowledge-Based Systems, 2019, 180: 104-115.
- [22] ZHANG S, LIU Q, LIN Y. Anonymizing popularity in online social networks with full utility[J]. Future Generation Computer Systems, 2017, 72: 227-238.
- [23] QI L, ZHANG X, LI S, et al. Spatial-temporal data-driven service recommendation with privacy-preservation[J]. Information Sciences, 2020, 515: 91-102.
- [24] ZHANG Y, ZHANG P, LUO Y, et al. Efficient and privacy-preserving federated QoS prediction for cloud services[C]//Proceedings of 2020 IEEE International Conference on Web Services (ICWS). 2020: 549-553.
- [25] ZHU L, LIU Z, HAN S. Deep leakage from gradients[J]. Advances in Neural Information Processing Systems, 2019, (32).
- [26] RUDER S. An overview of gradient descent optimization algorithms[J]. arXiv preprint arXiv:1609.04747, 2016.
- [27] LIU D C., NOCEDAL J. On the limited memory BFGS method for large scale optimization[J]. Mathematical Programming, 1989, 45(1): 503-528.
- [28] ZHENG Z, ZHANG Y, LYU M R. Investigating QoS of real-world web services[J]. IEEE Transactions on Services Computing, 2012, 7(1): 32-39.
- [29] WEI W, LIU L, LOPER M, et al. A framework for evaluating gradient leakage attacks in federated learning[J]. arXiv preprint arXiv:2004.10397, 2020.
- [30] MNH A, SALAKHUTDINOV R R. Probabilistic matrix factorization[J]. Advances in Neural Information Processing Systems, 2007, 20.
- [31] MCMAHAN B, MPPRE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of Artificial Intelligence and Statistics. 2017: 1273-1282.

[作者简介]



许建龙 (1982-), 男, 广东汕头人, 汕头大学讲师, 主要研究方向为隐私计算、服务计算、区块链。



林健 (1996-), 男, 福建莆田人, 汕头大学硕士生, 主要研究方向为隐私计算、服务计算。



黎宇森 (2000-), 男, 广东佛山人, 主要研究方向为隐私计算、服务计算。



熊智 (1978-), 男, 湖北黄冈人, 汕头大学教授, 主要研究方向为信息安全、分布式计算。