一种基于联邦学习的高效隐私保护的服务质量预测方法

张 逍 杨 士 唐 静 赵美利
（滁州城市职业学院，安徽 滁州 239000）

摘要：云计算提供了许多服务资源，使得由服务组成的大规模云应用在许多关键领域得到广泛的应用。服务质量通常作为服务选择和组合的指标，以确保云应用的质量。为了促进服务的选择和组合，以往的研究使用协同过滤技术预测未知的服务质量值。然而，协同过滤技术在实际服务质量预测中存在着隐私泄漏的问题，用户可能不愿意通过共享数据进行协作。因此，解决隐私威胁成为实现服务质量预测方法的关键。本文从保护用户隐私的角度出发，提出了一种基于联邦学习的隐私保护的服务质量预测方法，且进一步提出改进技术，以显著降低系统的开销效率，使预测模型能够快速地，及时地提供预测结果。

关键词：服务质量；联邦学习；隐私保护

一、背景介绍

云计算提供许多支持大规模云应用的服务资源，这些云应用为全球的数百万用户提供服务。随着服务市场的快速增长，用户可以公开地访问部署在云环境中的大量服务，面向服务体系结构也成为构建云应用的主要范式。云应用以松散耦合的方式运行，在许多关键领域被广泛应用。

为了让更多的用户安全地参与到协同过滤模型构建中，保护用户隐私的服务质量预测方法是迫切需要的。在最近的研究中，保护用户隐私的方法被提出，这些方法与利用原始数据建立预测模型的协同过滤方法不同。在这些方法中，研究者用加密、模糊处理、匿名化和其他数据转换技术来预测服务质量。虽然这些方法可以提供一定程度的隐私保护，但仍面临以下限制，本文提出基于联邦学习的高效服务质量预测方法，以保护用户的隐私。

二 、问题描述

一般情况下，一个用户可以调用一组服务，并且服务可以被不同的用户调用。由于大量服务存在许多功能相同或功能相似的情况，所以用户可以选择质量更好的服务。每个用户调用服务生成的质量值，在用户端被记录。其表示该用户当时体验的个性化服务性能。通过协作共享机制收集所有用户的数据，从而形成一个全局服务质量矩阵。在矩阵中，每一个条目代表用户调用相应服务的质量值，空的条目表示用户没有调用该服务。实际生活中，用户只调用少量服务，不可能调用所有服务。因此服务质量矩阵中的大多数条目都是未知的。本文研究如何在保护用户隐私的同时，通过共享机制更有效、更准确地预测未知的服务质量值？本文提出了利用联邦学习技术对未知服务质量值进行预测的方法，以保护用户的隐私。用户和服务器以分布式协作的方式，共同训练一个全局服务质量预测模型。在这种模式下，用户不需要发送大量的本地数据，而只需要向中央服务器发送少量的本地模型参数，从而达到保护用户隐私的目的。为了提高联邦预测模型的效率，本文从减少计算开销、减小传输信息的大小、和减少通信次数等方面，提出改进技术以实现高效的服务质量预测。

三 、基于联邦学习的隐私保护的服务质量预测方法

（一）数据预处理

1. 数据预处理

实际上，服务质量数据的分布具有很大的偏差，且变化较大，不同的服务质量属性也有不同的取值范围（例如，吞吐量为0~7000kbps，可用性为0~100%）。因此，本文采用 BoX–CoX 变换对数据进行处理。BoX–CoX 是一种数据转换技术，在数据分析中被广泛地使用。BoX–CoX 变换是一种将非正态变量转换为正态分布的方法，如式（3.1）所示：

$$b(x)=\begin{cases}\dfrac{x^{a}-1}{a}, ifa\neq 0\\ \log(x), ifa=0\end{cases} \quad (3.1)$$

式（3.1）中，α 表示控制转换的程度，$q_{\max}$ 表示服务质量值的上界，$q_{\min}$ 表示服务质量值的下界，$b(x)$ 是单调非递减函数，$b(q_{\max})$ 和 $b(q_{\min})$ 是转换后的服务质量上下界。服务质量值可以通过以下公式被映射到 [0，1] 范围，如式（3.2）所示：

$$\hat{q}_{ij}=\frac{b\left(q_{ij}\right)-b\left(q_{\min}\right)}{b\left(q_{\max}\right)-b\left(q_{\min}\right)} \quad (3.2)$$

因此，预测结果 p_{ij} 可以通过 Sigmoid 函数被映射到 [0，1] 范围，如式（3.3）所示：

$$\hat{p}_{ij}=\frac{1}{1+e^{-p_{ij}}} \quad (3.3)$$

（二）隐私保护矩阵分解

尽管传统的矩阵分解模型具有很高的预测精度，但很难应用于实际。当他们向第三方提供数据时，用户担心其隐私会受到损害，因此协同过滤方法很难有效地发挥作用。本文提出基于联邦学习的隐私保护的服务质量预测方法，以解决这一问题。

当应用运行时，用户可以在本地记录观察的服务质量数据，并且这些数据不需要传输到中央服务器。矩阵分解的部分过程在用户站点进行，并通过联邦学习技术在中央服务器上再次集成。更具体地说，用户潜在因子在用户端被学习，服务潜在因子在服务器端被学习。预测模型在多轮（即时间片）中连续被训练和更新。在每一轮（即时间片）中，用户从中央服务器接收最新的全局服务潜在矩阵。然后，每个用户用新观察的服务质量值来更新本地服务质量矩阵，只需将更新后的服务潜在矩阵发送到中央服务器，并将原始服务质量数据和用户潜在向量保存在本站点中。最后，中央服务器收集所有用户更新的信息并对其进行组合，确定该轮对全局服务潜在矩阵的更新，并将更新后的全局服务潜在矩阵提供给下一轮的用户。每个用户都可以利用本地用户潜在向量和全局服务潜在矩阵快速预未知的服务质量值。

四、 高效的联邦学习

虽然联邦服务质量预测方法可以保护用户的隐私，但是仍需

要进一步地改进，以适应用户设备的多样性。本文从减少计算开销、减少数据传输量和减少通信次数三个方面提出提高模型效率的技术。

（一）减少每轮用户端计算的开销

每一个用户都需要学习用户潜在因子 ui，并在几轮迭代过程中更新服务潜在矩阵 S。在迭代过程中，从随机初始化到收敛是需要时间的。由于用户潜在因子在两个连续轮之间变化不大，因此，使用前一轮的用户潜在因子来初始化每一轮，而不是使用随机值来初始化每一轮，以减少学习时间。因此，本文只需要计算每轮的增量更新，然后使用随机梯度下降算法 SGD，以训练预测模型。

（二）减少每轮传输信息的大小

在实践中，大量用户会在联邦服务质量预测时使用各种设备（如台式机、笔记本电脑、平板电脑、智能手机、车载系统等）。并且，互联网上的通信比本地计算慢了许多数量级。互联网速度的不对称性，（即上行链路速度通常比下行链路速度慢很多），使得通信成为联邦服务质量预测的瓶颈。因此，降低成本是非常有必要的，尤其是上行通信成本。本文采用以下优化措施来减少数据传输量。

五、实验结果与分析

（一）数据集说明

本文在一个常用的真实数据集上进行实验，对一些服务质量预测方法进行评估。该数据集包含两个重要的服务质量属性，它们分别是响应时间（RT）和吞吐量（TP），它们表示了服务的非功能属性。RT 是指服务响应用户请求所需的时间。TP 是指用户调用服务时，数据传输的速率。在不损失通用性的前提下，本文的方法很容易扩展到其他服务质量属性。

（二）评估指标

本文使用平均绝对误差（MAE）来评估服务质量预测方法的准确性。其公式如下：

$$MAE = \frac{1}{N}\sum_{I_{ij}=0}\left|q_{ij} - p_{ij}\right| \quad (5.1)$$

其中，qij 表示实际的服务质量值，pij 表示预测的服务质量值，N 表示实验中预测的条目总数。MAE 是一种应用广泛的评估预测模型精度的指标。一般来说，MAE 值越低，模型的性能越好，预测精度越高。

（三）预测精度

本文比较了EFMF方法与其他一些经典预测方法的预测精度。其中，有些预测方法没有保护用户隐私。

UIPCC：该方法利用相似用户和相似服务的历史服务质量数据，预测未知的服务质量值。它是一种协同过滤方法，没有任何隐私保护机制。

PMF：这是一种协同过滤方法，该方法采用矩阵分解技术进行服务质量预测，也没有隐私保护机制。

P–PMF：此方法与 PMF 方法类似，区别在于它使用数据模糊处理技术集成了隐私保护机制。

FMF：它是具有隐私保护机制的服务质量预测方法。

EFMF：该方法通过本文第四部分提出的效率改进技术进一步扩展了 FMF 方法。

本文随机地将一些条目指定为未观察到的条目，并将它们从服务质量矩阵中删除。将剩下条目的百分比从 10% 调整到 30%，步长为 5%。在 EFMF 实验中，l=10，r=20%，b=8，δ 调整到最佳值，并相应地优化了实验参数。对每个密度的数据随机初始化 20 次，以平均精度为最终结果。结果表明，FMF 和 EFMF 比 UIPCC 和 P–PMF 具有更高的精度。P–PMF 使用的数据比较混乱，会给模型带来噪声。FMF 和 EFMF 使用原始的服务质量数据，因此比 P–PMF 更精准。所有的方法都会随着数据密集而更加准确，因为更多的训练数据意味着信息更加的全面化。实验表明，本文提出的隐私保护的服务质量预测方法是有效的。

（四）预测效率

本文比较了不同方法的收敛时间来评估预测效率。与其他方法相比，FMF 和 EFMF 需要更少的收敛时间来预测未知的服务质量值。联邦预测模型是以分布式方式训练的，包括局部模型和全局模型。用户在本地处理少量数据以更新本地模型。另一方面，中央服务器可以通过简单地处理用户收集的新数据，来更新全局模型。相比之下，其他方法则要求中央服务器处理大量数据，并需要对模型进行长时间的训练，所以本文提出的改进技术使得 EFMF 比 FMF 更有效。

（五）扩展性分析

本文进一步分析了 EFMF 方法的可扩展性，通过改变用户数量和服务数量，比较各方法的中值收敛时间。由于实际数据集的规模有限，本文只有利用重复数据生成大规模的合成数据集，这对于测量收敛时间是合理的。FMF 和 EFMF 的收敛时间增长非常缓慢，而其他方法的收敛时间却大大增加。这是因为 FMF 和 EFMF 的计算任务是分配给用户的。此外，EFMF 采用在线预测技术对数据进行增量更新，而其他方法则需要在每个时间片上进行迭代。这些结果表明 EFMF 可以很容易地扩展以处理来自用户和服务的大规模的数据。

六、 总结

为了构建高质量的云应用，隐私保护是提高服务质量预测精度的关键。本章提出了基于联邦学习的，保护用户隐私的服务质量预测方法。该方法采用联邦学习技术，以分散的方式训练服务质量预测模型。用户可以安全地将数据保存在本地站点，而不必担心数据泄露。然后，进一步采取一些改进技术，以提高服务质量预测模型的效率。实验表明，本文的方法是有效和高效的，同时有效地防止了隐私泄露。

参考文献：

[1] 张韶峰，单进勇 .“一种基于 PSI 技术保护联邦学习预测阶段隐私的方法 .”，CN202010046301.3.2022.

[2] 张泽辉等 . 面向船联网的高效隐私保护联邦学习方法 [J]. 中国舰船研究，2022，17（6）：11.

课题信息：省级大数据技术专业中国特色学徒制：2022tsxtz044；校企合作与产教融合双驱动的高职大数据专业课程实践教学体系构建：AZCJ2023171；Java 程序设计课程思政示范课程：2022sfk09；计算机文化基础课程思政优秀教学团队：2022szjxtd06；省级大数据技术专业创新团队，编号：2022jxtd02