联邦学习在医疗信息化中的应用研究

聂文静 信 伦 李 帜

（中国移动通信有限公司研究院 北京 100053）（杭州锘崴信息科技有限公司 杭州 310053）

〔摘要〕 介绍联邦学习技术分类和特点，阐述联邦学习技术在医疗信息化领域中的典型应用场景，包括心电异常检测、罕见病研究、老年人运动健康检测、医疗影像研究等方面，分析该领域面临的挑战和未来发展趋势。

〔关键词〕 联邦学习；医疗信息化；数据共享；数据协作；联合建模

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2022.10.003

Study on the Application of Federated Learning in Medical Informatization *NIE Wenjing, XIN Lun, Research Institute of China Mobile Communications Co., Beijing 100053, China; LI Zhi, Hangzhou Nuowei Information Technology Co. Ltd., Hangzhou 310053, China*

〔**Abstract**〕 The paper introduces the classification and characteristics of federated learning technology, expounds the typical application scenarios of federated learning technology in the field of medical informatization, including electrocardiograph (ECG) abnormal detection, rare disease research, elderly exercise health detection, medical imaging research, etc., and analyzes the challenges and future development trends in this field.

〔**Keywords**〕 federated learning; medical informatization; data sharing; data collaboration; joint modeling

1 引言

人工智能（Artificial Intelligence，AI）和大数据等技术的发展进一步推动互联网医疗行业升级[1]。随着医疗行业信息化水平逐年提升，互联网技术与医疗行业场景深度融合，传统医疗服务及运营方式逐渐向移动化、信息化、数字化方向转变，医疗行业各类数据规模也逐年增加。为保障数据安全合规流通，《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国生物安全法》等相关法律法规出台。医疗行业数据种类较多且绝大部分数据都涉及用户个人隐私，敏感等级较高，如心电图、B 超等影像数据，身体指标等病例相关数据以及生物基因序列等数据。大部分医疗机构为了防止泄露，很少与其他机构互通数据，甚至机构内部部门之间数据都不能互通。医疗数据资源呈现出“数据孤岛”问题，严重影响其价值的进一步挖掘和发挥。因此如何平衡数据共享协同的需求与数据安全隐私保护的要求成为需要重点关注的问题。近几年被业界广泛关注的联邦学习（Federated Learning，FL）技术能够在保证各方数据集不出库的前提下，协助不同机构的数据集进行联合分析和建模，以共同挖掘数据潜在价值，联邦学习技术在医疗行业也得到越来越多的关注和应用。

大部分医疗行业数据集具有明显的碎片化、孤岛化特点，比较适合使用联邦学习技术来进行分析和挖掘。Xu J、Glicksberg B S 和 Su C 等[2]主要研究主从架构下纵向联邦学习在医疗行业应用的典型

〔修回日期〕 2022－10－11

〔作者简介〕 聂文静，工程师，发表论文5 篇；信伦，正高级工程师，发表论文8 篇；李帜，高级工程师。

案例，并总结应用过程中面临的问题和挑战。Guo K、Chen T 和 Ren S 等[3]为解决批量训练模型时需要消耗大量资源和增量训练导致灾难性遗忘的问题，提出一种适合医疗数据的实时联邦学习训练方法。有学者[4]提出一种群体学习训练医疗图像数据的方法，而群体学习可以理解为融合边缘学习和区块链、点对点网络架构下的一种分布式学习方法。综上所述，联邦学习技术打破了不同行业的数据壁垒，不仅可以帮助医疗行业中不同机构数据集在不出库的情况下共同构建 AI 模型，以提高医疗图像 AI 辅助诊断系统识别率，根据不同机构电子病历来预测患者健康风险，还可以将患者数据与保险等相关行业数据相结合，以提升医疗行业数据在其他行业的应用度和影响力。

2 联邦学习技术

联邦学习技术本质上是一种分布式机器学习方法，其改变了传统的集中式学习和数据共享模式，不再需要将不同计算节点的原始数据集中到一起进行模型训练，而仅需将不同计算节点本地模型的梯度或者模型参数加密后进行聚合，再返回给每个计算节点更新本地模型，经过多轮迭代，得到一个精度达到或接近传统集中式建模效果的联邦模型。根据不同数据提供方的数据集特征和标签分布情况，联邦学习可分为纵向联邦学习、横向联邦学习和联邦迁移学习 3 种类型[5]。横向联邦学习适合不同数据提供方的数据集特征相同、客户群体不同的场景，其架构分为主从式和对等式。纵向联邦学习适合不同数据提供方的数据集特征不同、客户群体相同的场景。联邦迁移学习适合不同数据提供方的数据集特征、客户群体重合度都比较低，甚至部分数据提供方数据集缺少标注信息的场景。目前联邦迁移学习在医疗领域应用较多的是基于特征的联邦迁移和基于模型的联邦迁移[6-7]，其中基于特征的联邦迁移需要在不同数据集中找到共同的特征表示，如可穿戴手势识别模型中涉及的某些特征，可以用于可穿戴步态识别模型中；基于模型的联邦迁移可以将某个预测任务中训练的模型作为另一个预测任务全部或者部分初始模型，如利用公开数据集 ImageNet 训练 AlexNet 模型参数可以作为医疗影像数据集训练卷积神经网络（Convolutional Neural Networks，CNN）的初始参数，实现医疗影像数据集的分类。

3 联邦学习在医疗行业应用场景

3.1 心电异常检测

心电图检测是临床中常见的体检项目，通过心电图机器采集、记录客户心脏活动时产生的生物电位变化。医生通过特殊位置的电位变化，判断客户是否存在心电异常的行为。为提高效率，很多学者将 AI 引入到心电异常检测项目中，将不同心电图机器历史数据汇集到同一个地方（服务器或云端等），构建心电异常检测 AI 模型，自动输出诊断结果。然而部分医疗机构由于规模等客观原因的影响，有可能采集数据量不足或者缺少部分病例数据等，导致模型不可用。因此不同机构可以采用对等式横向联邦模型技术，与其他机构共同完成 AI 模型的训练，为叙述方便该模型称为联邦心电异常检测模型。为了防止模型反演攻击[5]时利用梯度信息反推出原始数据，联邦心电异常检测模型仅交互加密的模型信息，其中可以采用差分隐私[8]的方式对共享的参数或者梯度进行加密。根据仿真实验，在心电数据独立同分布的情况下，联邦模型效果接近于集中式机器学习模型，其中集中模型指的是将所有数据汇集到一个地方。不同计算节点的心电数据呈现非独立同分布时，FedAvg 将表现不稳定[9]。为了解决数据集非独立同分布对联邦模型的影响，可以在进行联邦学习之前增加一个分组流程，即将数据分布相似的计算节点放在一起训练模型[10]。

3.2 罕见病研究

医疗机构利用疾病数据开展研究时，经常遇到样本量不足的问题，但是由于其隐私性较强，难以汇集多家医疗机构数据共同研究。鉴于以上问题，有学者[11]提出一种主从式的横向联邦学习框架，并在急性白血病治疗的造血干细胞移植后复发风险预测、分析影响前列腺活检阳性的主要因素等医疗业务场景中落地应用。整个系统分为 3 部分，见图 1。第 1 部分为联邦学习基础设施层，即由若干个计算节点构成，并将模型训练与模型预测环境进行隔

离。第 2 部分为评估设施层，即负责联邦学习训练过程中参数聚合以及评估不同计算节点的数据贡献度，根据贡献度维护计算节点的信誉分数，其中参数聚合协议不再选择 FedAvg，而是根据各个计算节点在统一的验证集上的性能，选择性能最好的计算节点聚合模型，并分配给基础设施层计算节点更新本地模型。第 3 部分为用户交互层。该系统较传统的联邦学习系统增加了评估设施层，引入激励机制，根据模型贡献度为各个计算节点分配权益以及更新信誉分数。该系统收集5 978 位患者并分析其5 年期间的前列腺癌活检的数据，从中选择 2 426 位患者数据训练模型。该系统训练的模型较之前传统方式的 LR 和 SBT 模型准确率分别提高 3.41% 和 2.22%[11]，也被应用于急性白血病治疗的造血干细胞移植后复发风险预测模型等多种罕见病研究。

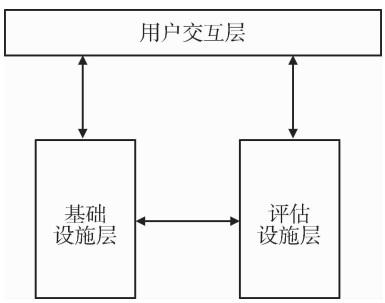

图 1 系统架构

3.3 老年人运动健康检测

目前有些学者通过在老年人家中安装摄像头、给老年人穿戴传感器等方式采集老年人日常行为数据，传递到中央服务器，构建 AI 模型，并通过 AI 模型判断老年人是否跌倒。然而，摄像头和传感器采集的数据隐私性较高，直接传输到中央服务器，容易造成数据泄露，为此需要借助联邦学习技术，在原始数据集不离开终端的前提下构建联邦 AI 模型。集中式 AI 模型需要数据集服从独立同分布且拥有足够多的质量较好样本，才能获得性能较好的模型，然而每个人的日常行为数据和身体指标数据存在差异性，导致标注成本较高，无法获得足够的标注好的样本数据训练 AI 模型，且每个终端采集的数据集也难以保证服从独立同分布，为此部分学者提出联邦迁移学习。以下以 FedHealth 框架[12]为例介绍联邦迁移学习如何训练模型。首先，FedHealth 框架的中央服务器先收集类似场景的公共数据集，并利用公共数据集训练模型，得到系统的云模型，并将该模型发送到各个终端，作为其本地模型的初始模型。其次，终端利用本地采集用户日常数据训练本地模型，并将其本地模型加密上传到中央服务器，中央服务器根据收集的本地模型更新云模型，更新后的云模型再下发给各个终端，作为下轮本地模型训练的初始参数，经过多轮迭代，直至各个终端的本地个性化模型收敛，停止迭代。研究者通过采集 30 位志愿者的 6 项活动，获得 10 299 个样本。为了模拟数据集呈现孤岛的形式，将志愿者数据分散到不同计算节点上。通过实验发现应用 FedHealth 框架训练的模型与传统深度学习模型相比，前者的准确率平均高于后者 5.3% 左右[12]。

3.4 医疗影像研究

医生通过分析患者的临床医疗影像判断其是否处于健康状态。这种人工判断方式，工作效率低。为此，医疗机构通过患者图片数据构建 AI 模型，自动判别患者的健康状态。然而，医疗影像的数据需要专业较高的医生标注，每家机构缺乏足够的标签数据训练 AI 模型。部分学者提出数据增强技术生成训练数据，但是生成的数据与真实数据存在一定差异性，模型效果可能受到这些生成数据的影响。对此有研究人员提出一种微分隐私模型[13-14]，将差分隐私技术与横向联邦学习相结合。具体流程如下：首先，中央参数服务器设置初始系统模型参数，并下发给各个计算节点。其次，各个计算节点训练本地模型，生成模型参数，并筛选出大于阈值的参数，加上噪声。再次，各个计算节点将加入噪声的参数，共享给中央参数服务器，其中为了降低共享量，加密的参数共享前需要先采用稀疏向量技术裁剪传输参数。之后中央参数服务器根据计算节点的贡献，作为系数加权对应的加密参数生成系统参数，并下发给各个计算节点。最后，计算节点更新本地模型，多轮迭代，直至系统模型稳定。微分隐私模型对 BraTS 2018 数据集的脑肿瘤分割数据进行验证，结果接近于集中模型，其中该数据集包括 285 位患者的核磁共振成像扫描数据[13-14]。

3.5 医疗保险行业应用

随着国家逐步进入老龄化社会，重大疾病保险

逐渐受到人们的关注。但是现有的保险产品定价策略存在保费偏高、个性化不足等问题。为解决该问题，研究者开始引入 AI 技术，通过分析客户数据建立个性化保险服务定价模型，其中客户的身体健康数据是影响保险产品定价的主要因素之一，而保险行业却无法直接采集客户健康数据，导致不能收集足够多的特征数据构建 AI 模型，因此保险行业需要与医疗行业合作共同构建 AI 模型。由于保险行业和医疗行业的数据涉及客户隐私，不能直接将双方数据汇集来构建 AI 模型，需要借助纵向联邦学习构建模型。传统的纵向联邦需要可信第 3 方聚合参数，但是第 3 方节点不易确定，为此可以采用基于秘密共享与同态加密的纵向联邦学习，其中秘密分享指 k 个计算节点将本地需要共享的数据随机切分为 k 份，本地仅保留 1 份，其余传输给其他计算节点，则每个计算节点依然有 k 份数据。每个计算节点计算本地 k 份数据之和，并将计算的结果传输给其他计算节点，则每个计算节点得到 k 个计算节点共享数据之和。因此不需要第 3 方节点计算 k 个计算节点共享数据之和[15]，仿真实验表明纵向联邦学习结果接近于集中模型。

4 挑战与发展方向

4.1 面临的挑战

4.1.1 通信成本高和计算复杂 联邦学习过程中需要不同的计算节点频繁交互和计算加密数据，因此其通信成本高、计算复杂。为此不少学者开始从算法角度，优化联邦学习性能，有学者[16]提出 FedAvg 和梯度压缩相结合的方法，使不同计算节点交互的数据量下降了两个数量级。但是过度降低通信成本将会导致联邦模型精度的下降。因此，在保证模型精度前提下，如何降低通信成本或者计算复杂度也是联邦学习研究热点之一。

4.1.2 安全性与模型精度之间难以平衡 医疗领域的数据和模型都属于高隐私信息，常见攻击方式包括模型攻击、数据攻击、逃避攻击等。联邦学习可以借助多方安全计算和密码学等方式防止其攻击，但是保护数据集安全性同时可能需要牺牲模型的精度或者性能。如抵御模型攻击方面，有学者提出基于差分隐私的联邦优化算法，在不良药物预测和死亡预测这两个场景验证其安全性和有效率，但是随着差分隐私保护数据力度增强，模型精度将会降低[17]。

4.1.3 数据集无法满足独立同分布 医疗机构数据集受专业性、认知不统一等因素影响，导致不同医疗机构采集的数据集无法满足独立同分布。

4.1.4 数据集个性化突出 由于患者身体体质与健康记录信息存在差异性，相同疾病或诊断结果，患者数据集可能存在较大差异。传统联邦学习是基于不同计算点的患者数据训练统一的模型，该模型可能不足以充分挖掘出不同个体差异性，尤其是穿戴传感器等个性化较突出的领域。

4.1.5 利益分配问题 联邦学习在医疗行业应用时都是假设各个医疗机构愿意无偿参与系统，实际上数据集本身是医疗机构的重要资产，共享数据集过程都需要成本。各个医疗机构借助联邦学习实现数据集对外变现的可能，自然会涉及利益分配问题。利益分配不合理将会影响医疗机构继续参与数据分享的积极性。因此，联邦学习系统在医疗行业进行商业落地时，除需要考虑系统性能、数据安全性外，还需要增加合理的利益分配策略。

4.2 发展方向

4.2.1 联邦学习与 TEE 技术相结合提高联邦学习性能 可信执行环境（Trusted Execution Enrironment，TEE）相当于在服务器中隔离出一块安全区域保证程序和数据安全性与完整性，TEE 中 SGX 可以保证数据存储时为密文，CPU 计算时为明文。在 TEE 上实现联邦学习，可以简化传统的联邦学习加密方式，降低交互频率，提高运算速率，缺点是成本比普通服务器高，且安全性是由芯片厂商保证。

4.2.2 个性化联邦学习 医疗行业不同机构的数据高度异质，传统联邦学习得到模型精度不够，因此需要构建个性化联邦学习[18]，个性化联邦学习分为两类，第 1 类是全局模型个性化，即训练流程与传统相同，但是参数初始时与更新时存在差异性，导致最终的模型存在差异性；第 2 类是个性化训练模型，即通过改变原有的参数聚合协议，建立计算节点的个性化模型。个性化联邦尤其适合不同计算节点数据呈现非独立同分布，但在数据集独立同分布的场景，模型精度并不优于传统的联邦学习。

4.2.3 基于多种加密手段的联邦学习平衡计算复杂度与模型精度 基于同态加密的联邦学习安全等级高且不会影响联邦学习精度，但是计算复杂度过高导致联邦学习性能较差，比较适合带宽受限制的环境。差分隐私计算复杂度低，但是安全等级不如同态加密，适合安全性要求不高、性能要求比较高的环境。因此两者相结合的联邦学习系统在保证安全性的同时也可以降低计算复杂度。

4.2.4 联邦学习与区块链相结合构建合理的激励机制 区块链是分布式的账本，可信度高，可以防止数据篡改，其与联邦学习有相似的应用基础，前者可以保证价值安全转移，交易记录不可被篡改，后者是实现数据价值，两者相结合，根据不同医疗机构参与联邦学习的贡献度制定利益分配方案，并将其贡献度和获得利益记录到区块链中，智能合约收到联邦学习在实际服务中产生的收益后，自动为各个医疗机构分配收益。若每个医疗机构数据异常，也可以到区块链中进行追溯。

5 结语

联邦学习打破不同行业数据壁垒，进一步加速医疗行业数据安全流通，其在医疗信息领域应用场景较广泛。尽管联邦学习在应用时会遇到一些难题，但是随着联邦学习技术的成熟，其可以衍生出多个技术路线去解决这些难题，进一步扩大联邦学习在医疗信息化领域应用场景，并推动其转型与发展。

参考文献

1 艾媒咨询. 2020—2021 中国互联网医疗行业发展白皮书 [EB/OL]. [2021 - 06 - 10]. https://www.iimedia.cn/c400/77397.html.

2 Xu J, Glicksberg B S, Su C, et al. Federated Learning for Healthcare Informatics [J]. Journal of Healthcare Informatics Research, 2021, 5 (1): 1 - 19.

3 Guo K, Chen T, Ren S, et al. Federated Learning Empowered Real - Time Medical Data Processing Method for Smart Healthcare [J]. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2022, 6 (23): 1 - 12.

4 Warnat - Herresthal S, Schultze H, Shastry K L, et al. Swarm Learning for Decentralized and Confidential Clinical Machine Learning [J]. Nature, 2021, 594 (7862): 265 - 270.

5 杨强, 刘洋, 程勇, 等. 联邦学习 [M]. 北京: 电子工业出版社, 2020.

6 吴骋, 秦婴逸, 李冬冬, 等. 迁移学习技术及其在医疗领域中的应用 [J]. 中国医疗设备, 2020, 35 (9): 161 - 164.

7 Wimmer G, Vécsei A, Uhl A. CNN Transfer Learning for the Automated Diagnosis of Celiac Disease [C]. Oulu: 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), 2016.

8 Liu Y, Liu J, Basar T. Differentially Private Gossip Gradient Descent [C]. Miami: 2018 IEEE Conference on Decision and Control (CDC), 2018.

9 张木锋. 心电异常检测场景中联邦学习算法研究 [D]. 北京: 北京邮电大学, 2021.

10 Yu L, Nie W, Xin L, et al. Clustered Federated Learning Based on Data Distribution [C]. Sanya: 2021 3rd International Conference on Advanced Information Science and System (AISS 2021), 2021.

11 Liu Z, Chen Y, Zhao Y, et al. Contribution - aware Federated Learning for Smart Healthcare [C]. Stanford: Proceedings of the 34th Annual Conference on Innovative Applications of Artificial Intelligence (IAAI - 22), 2022.

12 Chen Y, Qin X, Wang J, et al. Fedhealth: a Federated Transfer Learning Framework for Wearable Healthcare [J]. IEEE Intelligent Systems, 2020, 35 (4): 83 - 93.

13 彭南博, 王虎. 联邦学习技术及实战 [M]. 北京: 电子工业出版社, 2021.

14 网易. MICCAI 论文精选: 如何用联邦学习解决医学影像数据隐私问题 [EB/OL]. [2019 - 10 - 28]. https://www.163.com/dy/article/ESF46TLL0511DPV1.html.

15 夏家骏, 鲁颖, 张子扬, 等. 基于秘密共享与同态加密的纵向联邦学习方案研究 [J]. 信息通信技术与政策, 2021, 47 (6): 19 - 26.

16 潘明. 大数据在医疗行业的应用 [J]. 中国新通信, 2021, 23 (4): 90 - 91.

17 Choudhury O, Gkoulalas - Divanis A, Salonidis T, et al. Differential Privacy - enabled Federated Learning for Sensitive Health Data [EB/OL]. [2019 - 10 - 07]. https://arxiv.org/abs/1910.02578.

18 Tan A Z, Yu H, Cui L, et al. Towards Personalized Federated Learning [EB/OL]. [2022 - 03 - 28]. https://doi.org/10.1109/TNNLS.2022.3160699.