工程科学学报, 第 47 卷, 第 9 期: 1825−1840, 2025 年 9 月
Chinese Journal of Engineering, Vol. 47, No. 9: 1825−1840, September 2025
https://doi.org/10.13374/j.issn2095-9389.2024.12.24.001; http://cje.ustb.edu.cn

面向医疗健康领域的联邦学习综述: 应用、挑战及未来发展方向

张　畅, 李　卫✉

国家工业信息安全发展研究中心, 北京 100040
✉通信作者, E-mail: ai4cics@126.com

摘　要　本文综述了联邦学习(Federated learning, FL)在医疗健康领域的应用现状和面临的挑战. FL 作为一种去中心化的机器学习范式, 能够在不共享原始数据的前提下实现多方协作建模, 特别适用于对隐私和安全性要求极高的医疗健康数据处理. 首先介绍了 FL 的定义和训练过程, 重点探讨了其在医疗健康领域的主要应用, 包括基于分类任务(如疾病诊断)、分割任务(如医学影像分割)以及其他任务(如电子健康记录分析)中的具体实践. 还深入分析了 FL 在医疗健康领域应用中面临的关键挑战: 第一, 数据异质性问题, 不同医疗机构的数据分布差异显著, 导致模型性能不稳定; 第二, 隐私保护问题, 如何在训练和聚合过程中保障数据和模型的安全; 第三, 通信成本问题, 特别是在大规模数据和多客户端场景下, 通信开销较高. 针对上述挑战, 本文提出了未来发展方向, 包括个性化医疗与精准医疗的算法优化、疾病预测与早期干预的深度学习模型创新, 以及医疗数据安全与隐私保护的强化. 总结了 FL 在医疗健康领域的潜在价值与关键问题, 为未来相关技术的研究与应用提供重要参考.

关键词　联邦学习; 医疗健康; 数据异质; 隐私安全; 应用
分类号　TP309.2

Survey of federated learning in healthcare: Applications, challenges, and future directions

ZHANG Chang, *LI Wei*✉

China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China
✉Corresponding author, E-mail: ai4cics@126.com

ABSTRACT　This paper provides an extensive review of federated learning (FL) applications and challenges in the healthcare domain, with emphasis on its transformative role in enabling collaborative learning while addressing critical privacy and security concerns. FL, as a decentralized machine-learning paradigm, allows multiple clients, such as hospitals or medical institutions, to collaboratively train models without sharing raw data. This renders FL particularly suitable for the healthcare sector, where sensitive patient information is governed by stringent privacy regulations and ethical considerations. This paper first introduces the fundamental concepts of FL, including its definition, architecture, and training process. How FL differs from conventional centralized learning by maintaining data localization while enabling a global model to benefit from diverse datasets is explained. This characteristic is particularly valuable in healthcare, where data are typically siloed across institutions and regions owing to legal and operational constraints. The applications of FL in healthcare are categorized into three primary areas: classification tasks, segmentation tasks, and other specialized use cases. In classification tasks, FL has been employed for disease-diagnosis models, such as for predicting diabetes risk, detecting Alzheimer's disease, and identifying cancers. These applications demonstrate FL's ability in leveraging distributed data for improving diagnostic

收稿日期: 2024−12−24

accuracy. For segmentation tasks, FL is applied in medical-image analysis, including tumor-boundary delineation in MRI scans and lung-nodule detection in CT scans. Additionally, FL enables the integration and analysis of electronic health records (EHRs) across institutions, thus enhancing data utility while ensuring compliance with privacy standards. However, the deployment of FL in healthcare presents some challenges. One major issue is data heterogeneity, where variations in data distributions across institutions can adversely affect model performance and convergence. Privacy and security concerns remain significant, as FL must ensure the confidentiality of local data and the security of model updates during training and aggregation processes. Another critical challenge is the high communication cost, particularly in scenarios involving large-scale, multi-institutional collaborations. Frequent communication between clients and the central server or aggregators can introduce latency and increase resource demands. Hence, this study aims to identify innovative solutions and propose future research directions. Techniques such as personalized FL algorithms and transfer-learning approaches are proposed to address data heterogeneity. Privacy-preserving mechanisms, including differential privacy, secure multiparty computation, and homomorphic encryption, are highlighted to ensure robust data protection. Communication efficiency can be improved using advanced aggregation methods such as hierarchical FL and compression techniques. These innovations are expected to reduce communication overhead and enhance scalability in practical implementations. Results from existing studies indicate the effectiveness of FL in improving healthcare outcomes. For example, FL resulted in highly accurate multisite breast-cancer classification, improved disease-prediction models, and enabled the secure integration of EHR data. These advancements showcase FL's potential in revolutionizing medical research and practice by fostering cross-institutional collaboration while maintaining patient confidentiality. In conclusion, this review emphasizes FL's pivotal role in addressing critical challenges in healthcare data analysis and collaborative modeling. By leveraging its unique features and addressing its limitations, FL is well-positioned to propel significant advancements in disease diagnosis, personalized treatments, and large-scale medical research. This study serves as a foundation for future studies and advocates for continued innovation to satisfy the evolving demands of the healthcare industry.

KEY WORDS federated learning; healthcare; data heterogeneity; privacy and security; applications

人工智能(Artificial intelligence, AI)、物联网(Internet of things, IoT)、以及元宇宙[1]、数字孪生[2]等新生技术的快速发展为医疗健康领域带来了新的机遇,尤其是在实时监控、老年护理和高危患者识别等医疗服务中展现出了巨大潜力[3]. 深度学习(Deep learning, DL)作为 AI 的核心技术,已成为医疗数据智能化分析的关键手段,为精准诊断和个性化治疗开辟了新路径[4]. 然而,DL 的高效性能依赖于大规模高质量数据,这些数据主要由医疗设备和 IoT 节点生成. 由于医疗数据的敏感性,传统集中式学习方法在隐私保护和数据共享方面存在严重的局限性,阻碍了 DL 在医疗场景中的大规模应用. 联邦学习(Federated learning, FL)[5]作为一种新兴的分布式学习范式,通过模型参数而非原始数据的共享,有效地缓解了隐私风险. 自 2016 年提出 FL 概念以来[6], FL 因其在保护数据隐私的同时实现高效分布式协作的能力,成为医疗健康领域的研究热点. 近年来,FL 在医学图像分割、电子健康记录分析和实时健康监测等领域得到了广泛应用[7]. 然而,FL 在医疗领域的实际推广仍面临一系列技术和应用挑战,包括数据异质性、通信成本以及隐私与安全风险等.

目前已有文献总结了 FL 在医疗领域的典型应用及其核心挑战,并提出针对性的解决方案. 例如,文献 [8] 在医疗健康领域应用中使用 FL 的当前研究进行了系统性文献综述但是只针对电子健康记录数据. 文献 [9] 系统性归纳了 FL 在医疗场景中针对数据异质性、隐私保护和 IoT 节点通信安全的解决策略,但是没有讨论应用场景. 文献 [10] 则剖析了 FL 在数据分布不均、基准数据集缺乏以及数据保护技术瓶颈方面的困难,并指明了解决方案的研究方向. 文献 [11] 从《通用数据保护条例》(General data protection regulation, GDPR)视角探讨了隐私保护策略的重要性,通过总结过往研究成果,提出了多项关键策略以缓解用户隐私威胁. 文献 [12] 总结了 FL 架构的关键问题,但是只探讨了 FL 在分类任务中医疗健康的应用. 文献 [13] 介绍了 FL 模型在医疗健康领域的应用,包括常用的评估指标和公开数据集,但是对于应用领域以及在医疗健康领域应用的挑战分析较少.

虽然以上综述文献对 FL 在医疗健康领域的应用和挑战进行了讨论,但本综述的特点在于本文基于 FL 在医疗健康领域的多样化应用,将其应用场景划分为三大类别:分类、分割及其他. 此分类方式旨在帮助研究者对现有研究的主要方向和内容有更清晰的理解. 本文在梳理典型应用的基

础上, 总结了 FL 在医疗健康领域所面临的挑战以及对应的解决方案, 例如数据异质性、隐私保护和通信效率等问题, 同时综述了领域内相关问题的最新研究成果, 并对现有解决方案进行分类与评估, 以便研究者全面了解当前技术的优劣及其适用性, 为研究者提供剖析这些挑战的参考框架, 推动 FL 技术在医疗健康领域的进一步发展.

1　联邦学习介绍

1.1　FL 的定义

FL[14] 作为一种分布式机器学习框架, 旨在实现多个参与方在无需迁移本地数据的前提下, 协同进行模型训练的目标. 具体而言, 各参与方在本地环境中执行模型训练任务, 并仅将模型参数的更新或梯度信息上传至中央服务器进行集中聚合处理. 这一机制增强了数据隐私与安全性保护, 有效利用了广泛分布于不同机构或设备中的数据资源.

1.2　FL 训练过程

FL 学习的过程主要分为以下几个阶段[5], 如图 1 所示(其中 n 表示第 n 个参与方, 在医疗健康领域中, 表示第 n 个参与的医疗机构), 即: ①模型初始化阶段、②本地模型训练阶段、③模型更新上传阶段、④全局模型聚合阶段、⑤更新后的模型下载阶段.

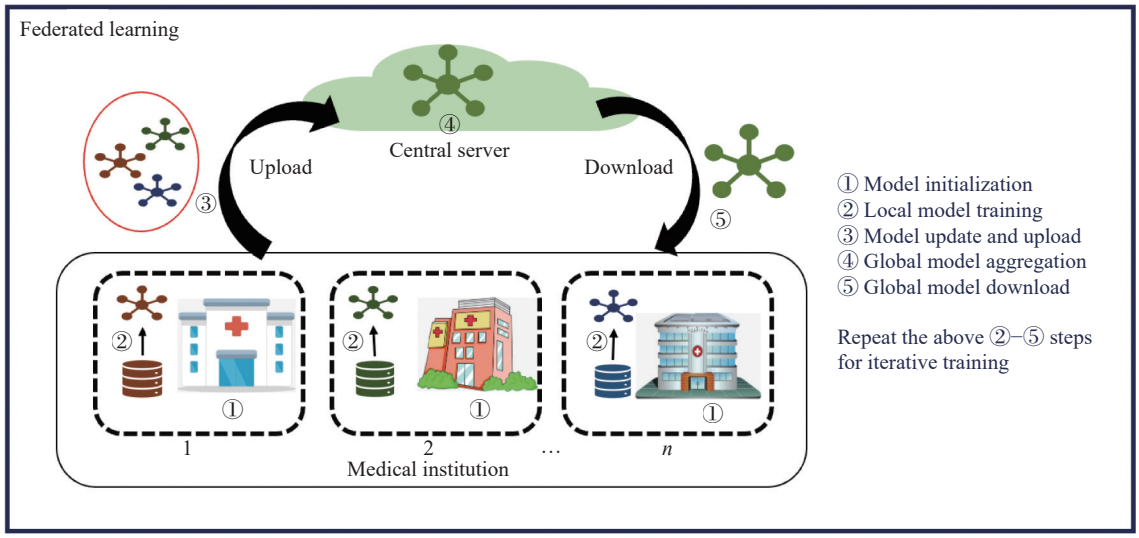

图 1　联邦学习

Fig.1　Federated learning

其中, 模型初始化阶段, 中央服务器扮演重要的角色, 要将预先设定的初始模型参数分发给所有参与方. 这一步骤为后续分布式训练奠定了基础, 确保了所有参与方在训练开始时拥有相同的模型起点. 本地模型训练阶段, 各参与方在接收到初始模型后, 利用各自持有的本地数据集进行独立的模型训练. 通过应用适当的优化算法, 参与方对模型参数进行迭代更新, 以期在本地数据上达到更好的拟合效果. 模型更新上传阶段, 完成本地训练后, 参与方并不直接传输其持有的原始数据, 而是将训练过程中得到的模型更新信息(如梯度或参数变化量)上传至中央服务器. 这一做法有效保护了数据隐私, 避免了敏感信息的泄露. 全局模型聚合阶段, 中央服务器接收到来自各方的模型更新后, 采用特定的聚合策略(如加权平均法)对这些更新进行合并处理, 从而生成一个新的全局模型. 这一步骤是 FL 框架的核心所在, 实现了模型知识的跨参与方共享与整合. 更新后的模型下载阶段, 主要将在中心服务器更新好的模型下载到本地进行训练. 重复以上步骤, 对模型进行迭代训练, 直到达到模型的最大训练时间或者模型的收敛为止.

1.3　FL 的技术分类

1.3.1　横向联邦学习

横向联邦学习(Horizontal federated learning, HFL)适用于参与方之间数据特征空间和标签空间相同, 但样本不同的场景. 例如, 不同地区的医疗机构可能拥有相同的医疗检查项目(特征), 但患者群体不同(样本). 在这种情况下, 各参与方通过联合训练提升模型性能. HFL 适用于各参与方数据特征空间和标签空间相同但样本不同的场景, 例如不同医院的医疗影像分类任务. 其需求在于解

决数据分布的非独立同分布问题, 并在保护隐私的前提下通过多中心协作提升模型的泛化能力, 常用于影像诊断[15] 和疾病预测[16] 等任务.

1.3.2　纵向联邦学习

纵向联邦学习(Vertical federated learning, VFL)适用于参与方之间样本相同, 但数据特征空间和标签空间不同的场景. 例如, 银行和电商平台可能拥有相同的用户群体(样本), 但数据特征不同. 在这种场景下, 各参与方通过特征互补提升模型性能. VFL 适用于各参与方样本相同但特征空间和标签空间不同的场景, 例如结合电子病历和影像数据进行疾病诊断. 其需求在于解决特征空间的异构性问题, 并在不共享原始数据的情况下实现特征融合和模型训练, 常用于多模态数据融合[17] 和电子病历[18] 联合分析.

1.3.3　联邦迁移学习

联邦迁移学习(Federated transfer learning, FTL)适用于参与方之间样本和数据特征空间均不重叠的场景. 例如, 不同国家的医疗机构可能在患者群体和检查项目上均无交集. 在这种情况下, 通过迁移学习技术, 利用预训练模型的知识来适应新的数据分布. FTL 适用于各参与方样本和特征空间均不重叠的场景, 例如不同医院的患者群体和检查项目完全不同. 其需求在于解决跨机构的数据异构性问题, 并通过预训练模型的知识快速适应本地数据, 常用于医疗影像领域的跨机构协作[19] 和小样本学习任务[20].

2　联邦学习在医疗健康领域的应用

研究 FL 在医疗健康领域的应用具有重要学术价值和现实意义[8]. 医疗健康数据具有高度敏感性和异质性, 受限于隐私保护法规及数据孤岛现象的影响, 传统集中式机器学习模型在数据共享和整合方面面临挑战. FL 的分布式训练框架能够在数据不离开本地的情况下, 整合跨机构、多地域的数据资源, 促进全局模型的优化, 同时保障数据隐私和安全. FL 在医疗健康领域的应用过程可以分为以下步骤: 首先, 明确参与 FL 的各方, 如多家医疗机构; 其次, 初始化全局模型, 选择一个基础模型作为全局模型的起点, 这个模型可以是预训练的, 也可以是从零开始训练的; 然后, 本地模型训练, 各参与方在本地使用自己的数据集对全局模型进行训练, 生成本地模型更新; 之后, 参数聚合, 各参与方将本地模型更新上传至中心服务器(或某个指定的参与方), 中心服务器对这些更新进行聚合, 生成新的全局模型, 将更新后的全局模型分发回各参与方, 用于下一轮的本地训练; 最后, 经过多轮迭代, 重复以上步骤, 直到全局模型达到预定的性能标准或收敛. 相关伪代码如表 1, 其中, global_healthcare_model 表示全局医疗健康模型, hospital_list 是参与 FL 的医疗机构列表, 每个医疗机构都拥有自己的加密患者数据集 hospital.encrypted_patient_data, num_federated_rounds 表示预定的 FL 轮次.

表 1　FL 在医疗健康领域应用的伪代码

Table 1　Pseudocode for applying federated learning in healthcare

Algorithm 1: Application of FL in the field of healthcare
1: initialize_global_healthcare_model(global_model)
2: for round in range(num_federated_rounds):
3:　　local_model_updates = []
4:　for hospital in hospital_list:
5:　　securely_send_global_model_to_hospital(hospital, global_model)#
6:　　local_update = hospital.train_and_update_disease_risk_model(global_model)
7:　　local_model_updates.append(local_update)
8:　aggregate_local_updates_to_global_model(global_model, local_model_updates)
9:　# evaluate_global_model_on_validation_set(global_model)
10: return global_model
11: def hospital_train_and_update_disease_risk_model(hospital, global_model):
12:　　local_model = copy_global_model(global_model)
13:　train_local_model_on_encrypted_data(local_model, hospital.encrypted_patient_data)
14:　　local_update = compute_model_difference(local_model, global_model)
15:　return securely_transmit_local_update(local_update)

2.1　基于医疗健康分类任务的 FL 应用

分类任务的目标是将数据划分为预定义的类别, 通常涉及全局特征提取, 模型结构相对简单. FL 在医疗健康领域的分类任务中, 具有数据异构性、隐私保护要求高和模型泛化能力需求强等特点. 它面临的挑战包括数据分布不均衡、通信开销高和隐私易泄漏等问题. 然而, FL 相较于传统方法, 具有显著的优越性: 它通过分布式训练保护数据隐私, 打破数据孤岛, 提升模型性能和泛化能力, 尤其在多中心协作下表现出更高的准确率, 为医疗数据的高效利用和隐私保护提供了新的解决方案. 分类(检测/预测)是 FL 中常见的问题, 鉴于医疗健康数据的复杂性及敏感性, 使用 FL 检测或预测医疗健康领域中的某些场景, 能够有效缓解病人数据被泄露的风险. 目前, 在医疗健康领域, FL 已经在医疗健康中的分类任务中进行了相关的应用, 主要包括癌症诊断, 人类活动识别, 重度抑郁症的诊断, 自闭症谱系障碍预测, 手术阶段识别, 以及 COVID-19 检测和肺炎诊断, 癫痫发作检测.

2.1.1　联邦学习在癌症诊断中的应用

FL 通过多机构协作无需共享原始患者数据的特性, 为癌症诊断提供了隐私合规的解决方案[21]. 癌症诊断依赖于整合医学影像、病理切片和基因组数据等多模态信息, 但不同机构间的数据异质性可能导致模型收敛困难, 且专家标注标准不一致会引入标签噪声. FL 通过分布式聚合多样化数据集, 在保护隐私的前提下增强模型对不同人群的泛化能力, 同时缓解单一机构标注样本不足的问题, 推动可扩展诊断工具的开发. 目前, Heidari 等[22] 结合区块链技术, 通过数据归一化与分类优化, 训练出高性能的全局模型, 并在多个数据集上验证了该方法在肺癌检测中的有效性. Tomczak 等[23] 基于癌症基因组图谱数据集的实验表明, FL 能有效保护患者隐私, 在性能上优于传统的非 FL 模型. 还有研究着眼于提升 FL 在多癌种诊断任务中的表现, Rehman 等[24] 提出了一种基于 FL 和生成对抗网络优化的临床癌症诊断框架 FedCSCD–GAN, 通过利用分布式数据源提高癌症诊断准确性, 同时确保敏感患者数据的安全性, 通过分布式数据源的协同学习, 实现了肺癌、前列腺癌和乳腺癌的高精度诊断. 针对皮肤癌相关诊断, 文献 [25] 采用自监督预训练策略, 改善了模型的诊断性能, 但客户端数量有限的问题仍有待解决. 为进一步提升 FL 的稳定性与一致性, 有些研究提出了创新的优化方法, 文献 [26] 设计了一种记忆感知课程学习方法, 通过惩罚预测不一致的样本, 增强了本地模型的一致性. 在三个临床数据集上的实验表明, 该方法相较传统 FL 设置, 精确率和召回率分别提升了约 5% 和 6%. 总体来看, FL 在提升数据隐私保护与诊断性能方面展现了巨大的应用潜力, 但同时也面临诸如数据异质性和客户端限制等挑战, 需要进一步研究与优化.

2.1.2　联邦学习在 COVID-19 检测与肺炎诊断中的应用

COVID-19 的全球快速传播要求跨地区协作建模, FL 成为实现实时知识共享的关键技术. 其支持从 X 光、CT 到便携超声设备的异构数据联合训练, 但地域感染率差异和病毒变种演化可能导致数据分布偏移, 而联邦通信开销可能影响疫情动态模型的实时更新. 尽管如此, FL 仍能通过轻量化模型部署和自适应区域特征优化, 在满足数据本地化法规的同时提升诊断准确性, FL 在 COVID-19 检测和肺炎诊断中的应用具有重要意义[27]. Zhang 等[15] 提出动态融合 FL 框架, 通过实时评估各客户端本地模型的分类准确率和收敛状态, 筛选高贡献度客户端参与全局聚合, 减少无效通信. 引入优先级队列管理客户端参与频率, 避免低质量模型拖累全局性能. 根据客户端计算资源预估其本地训练耗时, 动态调整模型融合时间窗口, 解决异构设备导致的同步延迟问题. 采用加权聚合策略, 权重由客户端数据量、模型性能及历史贡献度综合确定. 其结果表明, 该方法在模型性能、通信效率和容错性方面均优于传统 FL 设置, 具有较强的实用性. 针对个性化医疗, Lu 等[28] 通提出双路径优化框架. 通过批量归一化层的统计特征构建客户端间表征相似性矩阵, 实现知识迁移的领域自适应; 在全局模型共享参数的基础上, 允许各客户端维护个性化参数以适配本地数据分布, 并在 COVID-19 数据集上表现出良好的性能和快速收敛特性. Qayyum 等[29] 提出基于边缘计算与集群联邦学习的协同优化框架, 通过该框架将 X 光、超声等多模态数据分布处理于边缘节点, 降低云端传输延迟; 基于客户端数据特征相似性自适应构建联邦集群, 实现模态特异性模型的并行训练, 缓解非独立同分布影响; 在边缘端部署压缩模型, 通过知识蒸馏技术平衡诊断精度与计算资源约束. 实验验证表明, 该框架在保持数据本地化隐私优势的同时, 显著提升跨模态诊断性能, 可用于自动 COVID-19 诊断, 并通过两个基准数据集验证了其有效性. Zhang 等[30] 采用轻量级时空变换器网络, 通过雾节点本

地聚合和贪婪选择协调节点, 减少对中央服务器的依赖. 实验表明, 该框架在检测性能、资源效率、稳定性和可扩展性方面表现优异. 在隐私保护方面, 一些研究探索了生成对抗网络与 FL 的结合, 以减轻数据隐私泄露的风险[31]. 这一方向的研究为解决医疗数据共享与隐私保护的难题提供了新的思路. 总之, FL 在应对 COVID-19 及其他健康领域的挑战中, 展示了其在提升诊断效率和保护隐私方面的潜力, 但目前仍需通过优化通信成本和提升模型的通用性来克服现存瓶颈.

2.1.3　联邦学习在癫痫发作检测中应用

基于脑电图等时序数据的癫痫检测面临正样本稀疏与设备采样率差异导致的时序对齐难题, 且可穿戴设备的计算资源限制复杂模型部署. FL 通过跨机构数据互补提升罕见发作模式的识别能力, 并采用联邦蒸馏技术压缩模型以适应边缘设备. 该方法在避免原始脑电数据传输的同时, 支持个性化阈值设定以应对患者特异性发作模式. Ding 等[32] 提出了一种隐私保护的 FL 框架, 专为基于雾计算的物联网医疗技术设计, 该框架通过利用地理位置相关的雾节点作为本地聚合器, 支持基于位置的 EEG 信号共享, 并在检测性能、资源效率、稳定性和可扩展性方面表现出色. 在去中心化模型的探索中, Baghersalimi 等[33] 设计了一种结合自适应集成学习和知识蒸馏的去中心化 FL 框架, 该框架训练阶段采用自适应集成学习, 动态融合多医院模型生成定制化本地模型, 缓解数据异构性; 在部署阶段通过知识蒸馏压缩模型, 来适配可穿戴设备资源. 在公开癫痫数据集和边缘计算平台上的实验表明, 该方法性能优越. Baghersalimi 等[34] 提出了一种基于深度神经网络的实时个性化 FL 框架, 用于移动平台上的癫痫发作检测, 尽管其应用效果较好, 但模型的敏感性有待进一步优化, 其实验也仅限于少量客户端. Suryakala 等[35] 开发了一种基于 FL 式癫痫发作检测方法, 通过整合分布式数据源, 提升了模型对病例异质性的适应能力. 实验结果显示, 该模型在 EEG 信号检测中的敏感性、特异性和准确性, 表明了其有较好的应用效果. FL 在癫痫发作检测领域展现出保护患者隐私与提升检测性能的双重优势, 但实现更高的敏感性、更广泛的客户端覆盖以及更强的系统适应性仍需进一步研究与优化.

2.1.4　联邦学习在人类活动识别中的应用

人类活动识别(Human activity recognize, HAR)需融合智能手机、惯性传感器等多源设备数据, 但传感器异构性与用户标注成本高昂构成挑战. FL 通过元学习框架快速适配新用户行为模式, 利用分布式数据覆盖多样化活动场景, 并通过本地数据处理规避敏感行为数据的传输风险, 实现隐私与用户体验的平衡. 物联网技术的迅速发展推动了 HAR 在医疗诊断中的应用, FL 的引入, 保护了 HAR 中 IoT 设备中数据的隐私[36]. Zhou 等[37] 提出了一个二维 FL 框架, 针对不同用户和设备的 HAR 应用, 利用两个公开数据集进行了实验. 结果显示, 该模型在加快和优化收敛速度的同时, 有效提升了精确度、召回率和 F1 分数. Zhang 等[38] 通过引入自然语言标签指定共享数据以确保隐私合规性, 并在 HAR 数据集上取得了优于传统 FL 方法的分类效果. 在增强隐私保护方面, 一些研究结合新兴技术取得了进展, 例如, 基于雾–物联网网络的 FL 平台[39] 通过整合区块链技术提升了数据隐私保护能力, 并在智能手机数据的 HAR 任务中表现出良好的性能. Xiao 等[40] 设计了一种感知提取网络作为用户特征提取器. 该网络由卷积块构成的特征网络和结合长短期记忆与注意力机制的关系网络组成, 分别负责提取局部特征与发掘全局关系. 在四个常用的数据集上进行的实验表明, 与现有的特征提取结构相比, 该方法在 HAR 中表现出更优的性能. 尽管上述研究取得了较好的研究成果, 但现有研究通常基于有限数量的客户端进行实验, 可能难以完全反映现实场景中的复杂性和广泛适用性. 综上, FL 在 HAR 任务中展现了提升模型性能与保护数据隐私的潜力, 但进一步扩大客户端覆盖范围与优化模型适应性仍是未来研究的重要方向.

2.1.5　联邦学习在重度抑郁障碍诊断中的应用

重度抑郁障碍(Major depressive disorder, MDD)诊断需整合语音、文本与生理信号等多模态数据, 但非结构化数据处理复杂性与医生评估标准差异导致标签噪声问题突出. FL 支持构建分布式循环模型析症状时序演化, 并通过跨机构多模态融合提升诊断精度. 其增量学习机制可持续更新患者状态模型, 支持长期病程追踪. MDD 是一种全球普遍且代价高昂的精神疾病. FL 的引入为 MDD 诊断提供了一个能提高诊断精度又能缓解患者隐私泄露风险的解决方案. Kuang 等 [41] 使用 FL 整合个体、家庭和学校三方面的心理数据, 涵盖 11 种心理现象, 以全面评估抑郁症状状态. Liu 等[42] 开发了一种联邦联合估计器, 通过多层贝叶斯网络在静息态功能磁共振成像数据上检测功能连接生物标志物, 其结果显示了较高的精确度和优越的

性能. FL 在 MDD 诊断中的应用提升了分析的全面性与精准度, 展示了有效保护患者隐私的潜力, 但在更大规模数据和多样化客户端环境下的表现仍需进一步探索.

2.1.6　联邦学习在 ASD 预测中的应用

孤独症谱系障碍(Autism spectrum disorder, ASD)是一种对精神健康和社会行为产生重大影响的神经发育障碍. ASD 早期筛查依赖眼动追踪、行为视频等多模态数据, 但患者数据稀缺与跨模态对齐带来挑战. FL 通过跨国协作覆盖遗传多样性, 并采用小样本学习技术提升罕见亚型预测能力. 该方法在遵守 GDPR 等伦理规范的前提下, 减少单中心数据集偏差, 增强模型公平性, FL 在 ASD 预测中的应用中保护了病人的隐私数据. Lakhan 等[43]提出了一种结合卷积神经网络和长短期记忆网络的 FL 框架, 利用多模态数据进行儿童 ASD 的检测. 结果表明, 该框架在多数据集中的检测准确率较高, 优于现有的 ASD 检测方法. 然而, 传统的 CNN 和 RNN 架构在忽视个体之间的关系上存在局限性. 为解决这一问题, 最新研究引入了图神经网络, 结合图生成对抗网络[16]以弥补局部网络中的数据缺失, 并在两个神经影像数据集上验证了其有效性. 目前的研究尽管 FL 在 ASD 预测中的表现较好, 但其在应对更多客户端、异质性数据和复杂现实场景中的表现仍需深入研究, 以进一步提升其适用性和鲁棒性.

2.2　基于分割任务的 FL 在医疗健康中应用

分割任务侧重于像素级或体素级的划分, 处理高分辨率的多模态数据, 模型复杂且参数量大. 在医疗健康领域的分割任务中, FL 面临多模态数据融合需求、模型复杂性以及隐私保护与数据共享限制等特点. 其主要挑战包括多模态数据处理复杂性、通信开销与计算资源需求, 以及隐私保护与数据合规性问题. FL 相较于其他方法, 展现出显著的优越性: 通过分布式训练满足隐私法规要求, 减少数据共享风险; 在多模态磁共振成像(Magnetic resonance imaging, MRI)分割等任务中, 通过优化模型结构和多中心数据训练, 显著提升了分割精度和泛化能力, 为医疗影像分割任务提供了高效且合规的解决方案. 分割任务是 FL 在医疗健康领域的常见的情景, 这些任务涉及对前列腺疾病、大脑肿瘤、乳腺癌、皮肤疾病或肝脏中肿瘤及其他病灶进行精确勾画.

2.2.1　联邦学习在前列腺癌分割中的应用

前列腺癌分割主要基于多参数 MRI 影像, 其应用需克服不同医疗机构间影像参数差异及前列腺复杂解剖边界的精准界定. 由于多模态数据空间分辨率不一致、放射科医师标注标准差异显著, 以及各向异性分辨率导致的 3D 重建误差, 模型泛化能力常受限制. FL 通过聚合多中心数据提升对微小临床显著性癌灶的检测敏感性, 并采用动态加权聚合策略缓解扫描协议差异引起的域偏移问题, 同时避免敏感影像数据的直接共享, 在保护隐私的前提下实现跨机构协同优化. 在磁共振成像中, 前列腺区域的精准分割是医学影像分析中的关键步骤, 广泛用于前列腺癌的检测、侵袭性表征、复发预测及治疗效果评估[44]. 文献 [45] 提出了一种具有双重个性化功能的新型 FL 方案, 从特征和预测两个层面改进了模型个性化效果, 实验显示其分割性能优于其他方法. Chen 等[46]进一步提出了一种个性化 FL 范式, 利用联合原型对齐损失函数解决标签分布不平衡的问题, 实验结果表明性能显著优于其他方法. 然而, 该方法因本地训练时间较长, 可能在边缘设备环境下增加通信负担. 尽管取得一定进展, 但其在前列腺癌分割任务中的实际优势需通过进一步研究验证. FL 在前列腺癌分割中的应用展示了提升性能和隐私保护的潜力, 但在性能对比、客户端优化及实际场景应用方面仍需进一步探索.

2.2.2　联邦学习在乳腺肿瘤分割中的应用

乳腺癌是女性中最常见的癌症类型, 其早期检测对于降低死亡率具有重要意义. 乳腺肿瘤分割依赖于乳腺 MRI 或数字乳腺断层合成影像, 需应对肿瘤形态多样性及腺体密度异质性带来的挑战. 数据分布不平衡、影像伪影及多中心数据中乳腺压缩力度差异, 均可能影响分割精度. FL 通过整合多机构数据增强模型对异质性肿瘤的鲁棒性, 结合个性化 FL 算法并在边缘设备上实现术中实时分割, 为精准诊疗提供技术支持. 文献 [47] 出了一种基于联邦迁移学习的方案, 通过迁移学习从图像中的感兴趣区域提取特征, 并使用合成少数类过采样技术优化数据分类以提高模型性能. 实验结果表明, 该方案在乳腺肿瘤分割任务中优于其他传统模型. 文献 [48] 介绍了一种专为乳腺癌分割设计的 FL 框架, 使用随机感兴趣区域和双线性插值以解决异构数据分布问题, 同时通过高斯混合模型提高分割质量. 该方法在五个公开乳腺癌数据集上进行实验, 结果表明其分割性能优于最先进的模型. 从目前的研究成果, 可以总结, FL 在乳腺癌分割任务中展示了优越的适用性, 但其

在不同医疗机构间的大规模部署效果仍需进一步验证.

2.2.3 联邦学习在脑肿瘤分割中的应用

在脑肿瘤的临床治疗中, 精准分割医学图像中的肿瘤区域是制定有效治疗方案的关键步骤[49]. 脑肿瘤分割需融合多模态 MRI 序列, 其核心难点在于肿瘤异质性、跨机构影像协议差异及复杂亚区标注. FL 通过跨中心协作提升对罕见亚型的识别能力, 并借助联邦蒸馏技术将高精度 3D 分割模型压缩为轻量版本, 适配术中 MRI 等边缘计算场景, 在保护数据隐私的同时满足临床实时性需求. 文献 [50] 提出了一种基于消息队列遥测传输协议的实时 FL 分布式网络框架. 该框架结合了改进版 U-Net 模型, 并通过日常临床实践数据进行训练, 显著提高了模型的实用性和准确性. 实验结果表明, 基于 MQTT 协议的框架在可靠性、带宽效率和可扩展性方面表现优越. 针对 Non-IID 数据和隐私保护需求, 文献 [51] 提出了一种基于 FL 的创新框架, 该框架通过未标注的公共数据进行离线单向知识蒸馏, 充分提取本地知识, 同时确保隐私安全. 实验结果表明, 该方法在脑肿瘤分割任务中表现出高度竞争性的性能, 并显著增强了隐私保护. 文献 [52] 设计了联邦解耦学习方法, 通过全局形状参数与局部外观参数的解耦设计, 实现跨机构健康脑部 MRI 的无监督协同建模, 支撑异常分割. 该方法在多种脑部病变分割中显著优于本地模型, 验证了其在保护隐私前提下整合多中心健康数据的有效性, 该方法在脑肿瘤分割任务中表现出良好的性能. 然而, 研究中客户端数量有限, 需进一步扩大客户端规模以验证其实用性. 总结来看, FL 在脑肿瘤分割任务中展现了隐私保护与性能提升的双重优势, 但其在大规模真实场景中的适应性仍有待深入研究.

2.2.4 联邦学习在肝脏肿瘤分割中的应用

肝脏肿瘤分割多基于 CT 或超声影像, 面临肝脏呼吸运动伪影、病灶边界模糊及多期相 CT 数据跨中心对齐困难等挑战. 超声影像的低对比度与斑点噪声进一步增加特征提取难度, 部分机构仅提供非增强 CT 数据则导致模态缺失问题. FL 通过联合多模态数据提升模型泛化性, 利用联邦迁移学习解决小样本机构的冷启动问题, 并在介入治疗中支持超声引导下的实时病灶定位, 为肝脏肿瘤精准介入提供技术保障. 肝癌以其高致死率成为临床诊断的重要研究方向, 而基于计算机断层扫描的肝脏肿瘤分割在诊断中发挥了关键作用[20], 研究者提出了一种 FL 算法, 通过修复网络和差异检测网络, 将图像级标注转化为像素级监督, 实现高效的肿瘤分割, 减少标注工作量. 实验表明, 该方法在分布式、异构数据集上的表现优越, 为利用碎片化数据构建统一的分割模型提供了理论依据. 总之, FL 在肝脏肿瘤分割中的应用为复杂场景下的多任务分割提供了重要支撑, 但其稳定性与广泛适用性仍需改进.

2.2.5 联邦学习在气胸分割中的应用

气胸分割依赖胸部 X 光或 CT 影像, 需应对紧急诊断场景下的低对比度影像分割及跨区域病因差异导致的数据分布偏移. FL 支持跨区域医院快速协作构建高精度模型, 通过动态客户端选择优先聚合高质量数据节点, 并结合轻量化分割网络实现床旁设备的低延迟推理, 显著提升气胸急诊诊断效率. 文献 [53] 提出了一种基于补丁排列的创新方法, 将排列组合引入补丁嵌入层, 并采用 Vision Transformer(ViT)作为核心组件, 形成多任务 FL 框架. 实验结果表明, 该方法在气胸分割任务中取得了较高的平均 Dice 分数, 性能优于集中式模型, 凸显了 FL 在该领域的应用潜力. 然而, 该研究中客户端数量有限, 限制了其结果的普适性. FL 在气胸分割任务中的表现良好, 但需进一步扩展客户端规模和多样性, 以验证其在实际应用中的广泛适用性.

2.3 医疗健康领域的其他应用

2.3.1 联邦学习在 MRI 重建中的应用

磁共振成像(MRI)扫描时间较长的问题对患者和医生的诊断造成了不良影响, 激发了对高质量 MRI 重建技术的需求[54]. 然而, 传统基于条件模型的 MRI 重建方法在泛化能力方面存在局限性, 难以适应不同的加速比率. 为应对此挑战, 文献 [55] 提出了一种基于无条件生成对抗网络的 FL 重建方法, 通过跨站点学习生成图像, 并引入映射器子网络利用站点特定的潜在表示保持图像特异性. 实验表明, 该方法在多个机构数据集上的性能显著提升, 同时计算和推理时间有所降低. 尽管其优越性已在一定范围内得到验证, 但解剖学准确性需在更广泛的患者群体中进一步评估. 在平衡全局泛化与局部特异性方面, 文献 [56] 提出了一种结合全局编码器与客户端特定解码器的 FL 算法, 采用权重对比正则化增强训练效果. 实验显示, 该方法在 fastMRI 数据集上的性能优于主流方法, 展现了更强的稳定性. 文献 [57] 进一步开发了一种联邦一致正则化约束特征解纠缠方法, 通过有效

利用重叠样本和解决不同模态引起的域偏移问题, 提升了 MRI 重建效果. 在两个经典 MRI 数据集上的实验表明, 该方法的性能优于现有最先进的 MRI 重建方法. 针对 MRI 重建数据的异质性问题, 文献 [58] 提出了一种用于加速磁共振成像的可泛化联邦神经架构搜索框架, 实现了来自不同中心 MR 图像的高效神经网络表征学习. 实验表明, 该框架在性能和泛化能力方面优于七种先进 FL 方法, 且模型更加轻量化, 是 MR 图像重建任务的高效选择. 为解决 FL 在 MRI 重建应用中通信成本高的问题, 文献 [59] 提出了一种基于自监督学习的联邦框架, 通过客户端基于物理的对比重建网络, 在未完全采样数据的情况下实现跨站点协同训练. 大量实验结果表明, 该框架能够以低通信成本从多家机构的欠采样数据中重建出高精度的 MRI 图像. 总结来说, FL 在 MRI 重建中的应用展示了显著的性能提升和数据隐私保护能力, 但进一步研究仍需针对更大规模患者群体、复杂场景的泛化性能以及通信效率进行优化, 以满足实际临床需求.

2.3.2　联邦学习在医疗关系提取中的应用

关系提取作为人工智能知识获取的重要方式, 在医疗领域具有重要应用[17]. 然而, 不同医疗机构间的文本数据异质性对 FL 提出了巨大挑战. 文献 [60] 提出了一种名为 PF–BRE 的个性化 FL 框架, 专为生物医学文档级关系抽取设计, 使多个客户端能够在不共享原始数据的情况下协同训练出稳健的模型. 研究通过对现有生物医学文档级关系抽取数据集进行处理, 创建不同的客户端以实现个性化联邦训练. 实验结果表明, 与集中式训练相比, PF-BRE 框架不仅在性能上表现优异, 还有效保护了各客户端的数据隐私. 为进一步处理客户端之间标签分布的异质性问题, 文献 [61] 提出了一种名为 FedCMC 的算法, 该算法通过对比主要分类器向量来限制局部模型的更新, 从而避免模型因局部标签分布过拟合. 实验结果显示, FedCMC 在三个医疗关系抽取数据集上的表现显著优于其他最先进的 FL 算法. 总之, FL 为医疗关系提取任务提供了隐私保护与性能优化的有效解决方案, 但在处理更大规模异构数据以及跨语言和跨领域的扩展应用中仍需进一步研究.

2.3.3　联邦学习在死亡率预测中的应用

电子病历中标记数据不足和分布式数据特性为高性能模型的训练带来了显著挑战[18]. 为应对此问题, 研究者提出了一个改进的 Reptile 元学习算法框架, 通过引入动态神经图和半监督学习, 将标记和未标记数据整合到训练阶段. 实验结果显示, 该方法的性能与集中式模型相当, 但其收敛速度较慢, 训练耗时较长. 文献 [62] 通过在各医院的本地数据上训练带有 L1 正则化/最小绝对收缩和选择算子的逻辑回归模型及多层感知器模型, 开发了一个综合模型. 实验结果表明, 该综合模型在死亡率预测任务中优于其他模型. 针对 FL 在带宽消耗昂贵的问题, 文献 [63] 一种基于差分隐私的带宽高效 FL 框架, 可在适度降低预测准确率的同时, 实现可证明的患者级隐私保护, 实验基于包含约一百万患者电子健康记录的真实数据集, 验证了其在院内死亡率预测中的有效性. 通过包含约一百万名患者电子健康记录的真实数据集进行实验, 结果显示该框架在仅适度损失预测精度的情况下实现了强大且可证明的隐私保护. 与此同时, 针对数据分布非独立同分布(Non-independent and identically distributed, Non-IID)及不平衡特性对 FL 性能的影响, 文献 [19] 设计了一种个性化联邦学习(Personalized federated learning, PFL)方法. 采用一次性两步流程, 为每个参与机构生成高性能的个性化模型. 实验结果显示, 与其他方法相比, 该方法不仅提高了预测性能, 还显著减少了通信轮次, 其通用性和可扩展性也表明其有潜力应用于其他跨领域 FL 场景. 总之, FL 在死亡率预测中的应用展现了隐私保护和性能提升的良好前景, 但在通信效率提升、模型收敛速度优化以及跨机构协作激励机制方面仍有进一步研究的空间.

2.3.4　联邦学习在心理健康检测中的应用

技术的飞速发展为包括心理健康在内的多个医学领域带来了提升诊断、治疗和患者护理效率的机会. 在心理健康领域, FL 有望通过整合来自可穿戴设备、智能手机应用程序、电子健康记录和社交媒体等来源的数据, 实现精神疾病的检测、诊断和治疗, 同时保护患者隐私并防止数据被用于未经授权的目的[64–65] 文献 [66] 提出了一种基于 FL 的心理健康检测模型, 结合超图和情感词汇方法以保留语义相关性, 同时利用注意力位移机制优化检测过程. 实验结果表明, 该方法效果较好, 但在某些类别的预测表现不佳, 并且未考虑社会文化因素等潜在变量. 此外, 缺乏与集中式模型的直接比较限制了研究的广泛应用性. 文献 [67] 展示了 FL 如何利用智能手机的传感能力预测抑郁症严重程度, 开发的深度神经网络模型验证了 FL 在性能优化和隐私保护方面的潜力, 为传统机

器学习提供了替代方案. 文献 [68] 提出一种基于差分隐私的联邦迁移学习框架, 通过参数噪声注入和预训练模型迁移, 解决心理健康监测中数据隐私、不平衡和不足问题. 该方法利用纵向研究中的生理和情境数据, 实现了 10% 的准确率提升和 21% 的召回率提升, 同时确保了数据隐私. 目前相关的研究表明, FL 在心理健康领域展现出改善精神疾病检测和隐私保护的潜力, 但优化针对不同人群的适应性和跨文化通用性方面仍需进一步研究.

3 联邦学习在医疗健康领域中应用的挑战

通过上述 FL 在医疗健康领域的应用研究, 可系统梳理其在实践过程中所面临的多重挑战, 包括数据异质性、隐私与安全保障以及资源限制等关键问题. 本章节分析了上述挑战在医疗健康场景中产生的原因, 并对现有应对策略进行了全面综述, 以期为未来研究提供详细且具有指导意义的参考框架.

3.1 联邦学习在医疗健康领域应用中数据异质性的挑战

在医疗健康领域, 数据的分布特性对模型构建与预测性能具有至关重要的影响[69]. 通常, 医疗健康数据可划分为独立同分布(Independent and identically distributed, IID)和 Non-IID 两种类型. 理想情况下, 数据应遵循 IID 假设, 即数据样本彼此独立且来自相同分布. 然而, 在实际应用中, 由于数据量、特征或标签的不平衡, 常常出现 Non-IID 情况. 这种数据异质性在医疗健康领域尤为显著, 因为不同医疗健康机构的数据来源于多种医疗设备、患者人群和诊疗流程[70]. 例如, 专注于肿瘤研究的医院可能收集乳腺癌患者的基因表达数据和临床信息, 依赖高通量测序技术获取关于基因变异、表达水平等详细信息. 由于乳腺癌的高度异质性, 不同患者之间的基因表达模式可能显著不同, 导致数据呈现出高度的 Non-IID 特性. 相比之下, 更多关注心血管疾病的医疗机构则处理心电图、血压监测和血液生化指标等数据, 这些数据来源于不同类型的设备, 且受患者年龄、性别、生活习惯等多重因素影响, 同样具有 Non-IID 特性. 在 FL 框架下处理这些医疗数据时, 每个客户端(即医疗机构)的数据分布差异显著, 数据异质性带来的挑战尤为严峻. 为应对这一问题, 研究者提出了多种策略. 例如, 部分方法通过引入额外的正则化项限制模型复杂度, 提高泛化能力[71−72]; 另一些方法通过调整模型结构或优化算法, 适应数据分布的差异[73−74]. 此外, 迁移学习与域适应策略也被广泛研究, 以利用不同客户端之间的相似性促进模型学习[75−76]. 这些方法在实践中取得了一定成效, 并为 FL 在医疗健康领域提供了潜在的解决方案. 在表 2 中总结了相关方法的优缺点, 以便于研究人员后期能够灵活的应用. 总结来说, FL 在应对医疗数据异质性方面已取得积极进展, 但进一步提高模型适应性与稳定性, 尤其是在大规模 Non-IID 数据场景下的应用, 仍是未来的重要研究方向.

3.2 联邦学习在医疗健康领域的应用中隐私保的挑战

在医疗健康领域, 数据的隐私性被视为至关重要的核心要素, 因此, FL 的安全与隐私保护技术成为该领域研究的重点[95]. 由于医疗数据直接关联患者的个人隐私, 其敏感程度极高, 如何在确

表 2 FL 在医疗健康领域面临数据异质性的解决方法总结

Table 2 Summary of solutions to data heterogeneity confronted by federated learning in healthcare field.

Method	Principle	Advantages	Disadvantages	Fields and references
Client-data resampling and weighting	Weights model updates based on data distributions and individual client contributions.	Facilitates the development of a more robust global model; particularly suitable for heterogeneous datasets.	Complex weighting strategies; improper weights may degrade performance.	Skin diseases[77], medical information mart for intensive care[78], and COVID-19[79]
Personalized FL	Trains personalized models for each client based on the global model.	Improved model accuracy and generalization; suitable for heterogeneous data.	Additional training and adjustment required; performance affected by local-data quality.	Home health monitoring[80], electronic health records[81], skin diseases[82−83], eye retinopathy detection, diabetes monitoring, maternal health, and HAR[72, 84]
Data augmentation and adversarial training	Enriches training data and uses adversarial samples to enhance model robustness.	Improved data diversity and model robustness.	Effectiveness limited by data quality; additional computational resources required.	COVID-19[85 -87], intensive care[88], cancer detection, and MRI[89]
Feature transformation	Converts data from different sources into a unified format.	Facilitates processing and analysis; improves model accuracy.	Complex process; improper transformation may cause data loss.	Breast cancer[90], activity tracker, and heart-rate monitor[91]
Improved aggregation methods	Enhance aggregation algorithms to tolerate client model diversity	Adapts to client heterogeneity; no significant client-side changes.	Increased aggregation complexity; limited for extreme heterogeneity.	Intensive care[92], activity monitoring[93], and respiratory diseases[94]

保数据充分利用的同时, 有效防止隐私泄露, 已成为亟待解决的问题. 在表 3 中总结了 FL 在医疗健康领域面临隐私泄漏问题解决方法的优缺点, 以便于研究人员后期能够灵活的应用.

表 3　FL 在医疗健康领域中隐私保护的方法总结

Table 3　Summary of FL's methods for privacy protection in healthcare field.

Method	Principle	Advantages	Disadvantages	Fields and references
Differential privacy	Adds randomness to data to protect individual privacy. A single record's addition/removal should minimally affect query results' statistical properties.	Provides strong privacy protection; allows data analysis and mining while protecting privacy.	Requires adding noise, which may affect query accuracy; implementation requires complex algorithms and resources.	The Cancer Genome Atlas[96], blood disorders[97], and healthcare monitoring[98]
Homomorphic encryption	Allows computation on encrypted data without decryption. The result of computing on encrypted data matches encryption result of computing on original data.	Provides strong data privacy protection; allows direct computation on encrypted data.	Algorithms are complex and require high computational resources; may be susceptible to specific attacks such as quantum attacks.	Skin diseases[99], blindness detection[100], and COVID-19[101−102]
Secure multiparty computation	Allows multiple participants to jointly compute a function in a mutually untrusted environment, thus ensuring the privacy of inputs and outputs.	Provides strong privacy protection; allows multiparty computation in a mutually untrusted environment.	Requires complex cryptographic algorithms and protocols; may be susceptible to attacks such as collusion attacks.	Electrocardiogram, heart beat, categorization[103], heart monitoring[104], and Pima Indian Diabetes[105]

差分隐私技术应运而生, 为数据的安全传输与存储提供了有力保障. 差分隐私技术的核心思想是在数据传输前添加噪声, 使得单个数据点难以被准确识别和推断, 从而降低数据被滥用的风险[106]. 文献 [107] 证明, 差分隐私在有效保护隐私的同时, 对模型性能的负面影响可以控制在可接受范围内. 然而, 差分隐私方法面临如何在隐私保护与模型精度之间找到最佳平衡点的挑战, 尤其是在噪声水平的选择和调整上. 为优化差分隐私技术, 文献 [108] 提出了一种动态差分隐私方法, 该方法可根据训练过程中的实际情况动态调整噪声水平, 在保护隐私的同时尽量减少模型精度的损失. 在医疗健康数据的疾病预测等实际场景中, 该方法展现了较强的隐私保护效果, 并降低了推断攻击的成功率. 此外, 安全多方计算和同态加密等新型隐私保护技术也逐渐在 FL 中得到应用. 安全多方计算[109] 通过对模型参数进行加密计算, 确保数据传输过程中的安全性, 但其较高的计算开销限制了在医疗健康领域的应用. 同态加密技术[110] 则允许在加密数据上直接进行计算, 进一步提升了数据的安全性. 基于同态加密的 FL 方案不仅提高了数据安全性, 还增强了模型更新的透明性, 为 FL 在医疗健康领域的应用提供了更加可靠的技术支持. 然而, 这些隐私保护技术在实际应用中仍面临计算成本高、延迟大等问题. 尽管差分隐私、同态加密和安全多方计算等技术在 FL 中的应用展现了显著的隐私保护能力, 但进一步优化这些技术以平衡安全性与计算效率, 仍是推动其广泛应用的关键方向. 表 3 总结了相关方法的优缺点, 为研究人员的应用提供了参考.

3.3　联邦学习在医疗健康领域的应用中昂贵通信的挑战

FL 作为一种分布式机器学习技术, 在医疗健康领域的应用中逐渐展现出处理大规模医疗数据、保护数据隐私以及提升模型泛化能力的巨大潜力. 然而, 在实际应用中, FL 面临着显著的通信挑战, 主要源于频繁的模型更新和参数传输. 传统 FL 架构要求参与方(如医疗机构、个人设备等)反复与中心服务器交换模型参数, 通信频率高且数据量大. 这在医疗数据量庞大、设备计算资源有限的场景中尤为突出, 导致了通信负担和计算压力[111]. 为解决这一问题, 研究者提出了多种通信优化方法, 包括量化、剪枝和模型稀疏化等, 旨在降低数据传输的频率和规模, 从而缓解通信压力[112]. 这些技术通过减少模型参数的浮点精度或删除冗余参数, 有效减少了通信量, 同时保持了模型的性能[113]. 例如, FedAvg-GP[114] 等方法利用剪枝技术大幅减少了模型参数量和通信频率, 从而降低了传输带宽需求. 这些优化策略在医疗影像分析和健康数据分类等应用中表现出色, 不仅通信成本能够降低, 同时还保持高精度和准确性. 模型压缩和剪枝技术的优势在于显著减少模型参数量, 降低通信带宽需求, 加快模型更新速度, 并提升系统整体性能. 在保证模型性能的前提下, 这些技术还节省了存储和计算资源, 特别适用于资源受限的医疗设备. 然而, 这些技术在高压缩比例下可能导致模型精度的下降, 需要额外的调优和验证步骤以确保其在实际应用中的有效性和可靠性[115−116]. 优化通

信的压缩技术为 FL 在医疗健康领域的应用提供了重要支持, 但未来需要更高效且可自适应的通信优化策略, 以进一步平衡模型精度、通信成本和系统性能.

4　联邦学习在医疗健康领域应用中未来发展方向

4.1　个性化医疗与精准医疗的算法优化

针对数据异质性, 开发基于元学习的特征映射和跨模态融合策略, 探索联邦迁移学习实现知识迁移. 未来的研究将着重开发更加高效的 FL 算法, 例如基于深度学习的 FL 模型, 以更好地挖掘和利用跨机构的医疗健康数据. 特别是需要探索如何有效融合不同来源、不同格式的医疗健康数据, 包括基因组学、蛋白质组学、临床病历以及医学影像数据, 以构建更加全面和准确的个性化医疗模型. 这一过程涉及复杂的数据预处理、特征提取和模型训练, 需要跨学科合作与技术创新, 为个性化医疗提供可靠的技术支持.

4.2　医疗数据安全与隐私保护的强化

在医疗健康领域, 数据安全和隐私保护始终是至关重要的考量. 虽然 FL 通过本地数据处理方式降低了数据泄露的风险, 但随着技术的进步和攻击手段的复杂化, 仍需进一步强化数据安全与隐私保护. 在隐私保护方面, 构建差分隐私、同态加密与安全多方计算的协同防护体系, 并结合区块链审计机制和细粒度访问控制. 未来的研究将致力于将 FL 与先进的加密技术相结合, 包括同态加密、差分隐私以及 FL 中的安全多方计算, 以实现更加安全的医疗数据共享与分析. 此外, 区块链技术的引入将为 FL 平台提供不可篡改性和可追溯性, 从而显著提升医疗数据的安全性与隐私保护水平.

4.3　高效通信与资源优化的技术创新

针对通信效率挑战, 开发基于重要度采样的梯度更新策略和高效模型量化方法, 探索异步通信机制实现资源优化. FL 在医疗健康领域的广泛应用受限于高昂的通信成本. 为突破这一瓶颈, 未来的研究将着重开发更加智能的通信优化技术, 例如基于自适应压缩的模型更新机制, 以显著降低分布式训练过程中的通信开销. 特别是需要探索如何在保证模型性能的前提下, 实现梯度更新、模型参数和中间结果的智能压缩与选择性传输, 同时设计鲁棒的异步通信协议来协调异构设备的参与. 这一过程涉及通信–计算–存储的协同优化, 需要建立跨层优化框架来平衡系统效率与模型精度.

4.4　疾病预测与早期干预的深度学习模型创新

在疾病预测和早期干预中, FL 的应用依赖于先进的深度学习模型. 未来, 将探索如何构建更加准确且鲁棒的疾病预测模型, 对医学影像数据和时序数据进行高效分析和预测. 研究还将聚焦于引入如注意力机制、自注意力机制和图神经网络等前沿技术, 以增强模型对复杂疾病模式的识别能力. 这些创新不仅有助于提高疾病的早期预测能力, 还能在干预时提供更加精准的建议, 从而改善患者的生活质量和生存率.

5　总结

本文综述了 FL 在医疗健康领域的应用进展, FL 作为一种创新的分布式学习范式, 通过仅共享模型参数而非敏感原始数据, 有效缓解了医疗数据隐私泄露和共享障碍, 从而成为该领域的研究热点. FL 已被广泛应用于医学图像分割、电子健康记录分析及药物研发等多个关键场景, 展现出巨大的应用潜力. 然而, FL 在医疗健康领域的实际应用仍面临数据异质性、隐私安全、以及高昂的通信成本等多重挑战. 本文回顾了 FL 在该领域的应用现状, 剖析了这些核心挑战及其现有解决方案, 并进一步探讨了 FL 未来发展方向, 以期为 FL 技在医疗健康领域的未来发展提供相关的参考.

参　考　文　献

[1] Wang W X, Zhou F, Wan Y L, et al. A survey of metaverse technology. *Chin J Eng*, 2022, 44(4): 744
(王文喜, 周芳, 万月亮, 等. 元宇宙技术综述. 工程科学学报, 2022, 44(4): 744)

[2] Lin Y J, Chen L M, Ali A, et al. Human digital twin: A survey. *J Cloud Comput*, 2024, 13(1): 131

[3] Baker S, Xiang W. Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities. *IEEE Commun Surv Tutor*, 2023, 25(2): 1261

[4] Chakraborty C, Bhattacharya M, Pal S, et al. From machine learning to deep learning: Advances of the recent data-driven paradigm shift in medicine and healthcare. *Curr Res Biotechnol*, 2024, 7: 100164

[5] Kairouz P, McMahan H B, Avent B, et al. Advances and open problems in federated learning. *FNT Machine Learning*, 2021, 14(1−2): 1

[6] Konečný J, McMahan H B, Yu F X, et al. Federated learning: Strategies for improving communication efficiency [J/OL]. *arXiv preprint* (2016−10−18) [2024−12−24]. https://arxiv.org/abs/1610.05492

[7] Nguyen D C, Pham Q V, Pathirana P N, et al. Federated learning for smart healthcare: A survey. *ACM Comput Surv*, 2023, 55(3): 1

[8] Antunes R S, André da Costa C, Küderle A, et al. Federated learning for healthcare: Systematic review and architecture proposal. *ACM Trans Intell Syst Technol*, 2022, 13(4): 1

[9] Xu J, Glicksberg B S, Su C, et al. Federated learning for healthcare informatics. *J Healthc Inform Res*, 2021, 5(1): 1

[10] Paragliola G, Ribino P. Exploring heterogeneous data distribution issues in e-health federated systems. *Biomed Signal Process Contr*, 2024, 92: 106039

[11] Lieftink N, Ribeiro C D S, Kroon M, et al. The potential of federated learning for public health purposes: A qualitative analysis of GDPR compliance, Europe, 2021. *Euro Surveill*, 2024, 29(38): 2300695

[12] Li H, Li C C, Wang J, et al. Review on security of federated learning and its application in healthcare. *Future Gener Comput Syst*, 2023, 144: 271

[13] Chaddad A, Wu Y H, Desrosiers C. Federated learning for healthcare applications. *IEEE Internet Things J*, 2024, 11(5): 7339

[14] Yang Q. AI and data privacy protection: The way to federated learning. *J Inf Secur Res*, 2019, 5(11): 961
(杨强. AI 与数据隐私保护：联邦学习的破解之道. 信息安全研究, 2019, 5(11)：961)

[15] Zhang W S, Zhou T, Lu Q H, et al. Dynamic-fusion-based federated learning for COVID-19 detection. *IEEE Internet Things J*, 2021, 8(21): 15884

[16] Peng L, Wang N, Dvornek N, et al. FedNI: Federated graph learning with network inpainting for population-based disease prediction. *IEEE Trans Med Imag*, 2023, 42(7): 2032

[17] Wang H L, Qin K, Zakari R Y, et al. Deep neural network-based relation extraction: An overview. *Neural Comput Appl*, 2022, 34(6): 4781

[18] Thakur A, Sharma P, Clifton D A. Dynamic neural graphs based federated reptile for semi-supervised multi-tasking in healthcare applications. *IEEE J Biomed Health Inform*, 2022, 26(4): 1761

[19] Deng T, Hamdan H, Yaakob R, et al. Personalized federated learning for in-hospital mortality prediction of multi-center ICU. *IEEE Access*, 2023, 11: 11652

[20] Lyu F, Ma A J, Yip T C, et al. Weakly supervised liver tumor segmentation using couinaud segment annotation. *IEEE Trans Med Imag*, 2022, 41(5): 1138

[21] Kulkarni P, Kanhere A, Paul H Y, et al. Surgical aggregation: A federated learning framework for harmonizing distributed datasets with diverse tasks [J/OL]. *arXiv preprint* (2023−01−17) [2024−12−24]. https://arxiv.org/abs/2301.06683v2

[22] Heidari A, Javaheri D, Toumaj S, et al. A new lung cancer detection method based on the chest CT images using Federated Learning and blockchain systems. *Artif Intell Med*, 2023, 141: 102572

[23] Tomczak K, Czerwińska P, Wiznerowicz M. Review the cancer genome atlas (TCGA): An immeasurable source of knowledge. *Contemp Oncol (Pozn)*, 2015, 19(1A): 68

[24] Rehman A, Xing H L, Feng L, et al. FedCSCD-GAN: A secure and collaborative framework for clinical cancer diagnosis *via* optimized federated learning and GAN. *Biomed Signal Process Contr*, 2024, 89: 105893

[25] Yan R, Qu L Q, Wei Q Y, et al. Label-efficient self-supervised federated learning for tackling data heterogeneity in medical imaging. *IEEE Trans Med Imag*, 2023, 42(7): 1932

[26] Jiménez-Sánchez A, Tardy M, González Ballester M A, et al. Memory-aware curriculum federated learning for breast cancer classification. *Comput Meth Programs Biomed*, 2023, 229: 107318

[27] Zhou J X, Zhou L X, Wang D, et al. Personalized and privacy-preserving federated heterogeneous medical image analysis with PPPML-HMI. *Comput Biol Med*, 2024, 169: 107861

[28] Lu W, Wang J D, Chen Y Q, et al. Personalized federated learning with adaptive batchnorm for healthcare. *IEEE Trans Big Data*, 2024, 10(6): 915

[29] Qayyum A, Ahmad K, Ahsan M A, et al. Collaborative federated learning for healthcare: Multi-modal COVID-19 diagnosis at the edge. *IEEE Open J Comput Soc*, 2022, 3: 172

[30] Zhang K, Liu X H, Shen J, et al. Clinically applicable AI system for accurate diagnosis, quantitative measurements, and prognosis of COVID-19 pneumonia using computed tomography. *Cell*, 2020, 181(6): 1423

[31] Nguyen D C, Ding M, Pathirana P N, et al. Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet Things J*, 2021, 9(12): 10257

[32] Ding W P, Abdel-Basset M, Hawash H, et al. Fed-ESD: Federated learning for efficient epileptic seizure detection in the fog-assisted Internet of medical things. *Inf Sci*, 2023, 630: 403

[33] Baghersalimi S, Teijeiro T, Aminifar A, et al. Decentralized federated learning for epileptic seizures detection in low-power wearable systems. *IEEE Trans Mob Comput*, 2023, 23(5): 6392

[34] Baghersalimi S, Teijeiro T, Atienza D, et al. Personalized real-time federated learning for epileptic seizure detection. *IEEE J Biomed Health Inform*, 2022, 26(2): 898

[35] Suryakala S V, Sree Vidya T R, Ramakrishnans S H. Federated machine learning for epileptic seizure detection using EEG. *Int J Adv Comput Sci Appl*, 2024, 15(4): 1048

[36] Zhang C, Ren X R, Zhu T, et al. Federated Markov Logic Network for indoor activity recognition in Internet of Things. *Knowl Based Syst*, 2022, 253: 109553

[37] Zhou X K, Liang W, Ma J H, et al. 2D federated learning for personalized human activity recognition in cyber-physical-social systems. *IEEE Trans Netw Sci Eng*, 2022, 9(6): 3934

[38] Zhang J, Zhang X, Zhang X, et al. Federated learning with client-exclusive classes [J/OL]. *arXiv preprint* (2023−01−01) [2024−12−24]. https://arxiv.org/abs/2301.00489v1

[39] Baucas M J, Spachos P, Plataniotis K N. Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Trans Comput Soc Syst*, 2023, 10(4): 1732

[40] Xiao Z W, Xu X, Xing H L, et al. A federated learning system with enhanced feature extraction for human activity recognition. *Knowl Based Syst*, 2021, 229: 107338

[41] Kuang Y L, Liao X, Jiang Z K, et al. Federated learning-based prediction of depression among adolescents across multiple districts in China. *J Affect Disord*, 2025, 369: 625

[42] Liu S, Guo X, Qi S, et al. Learning personalized brain functional connectivity of MDD patients from multiple sites *via* federated Bayesian networks [J/OL]. *arXiv preprint* (2023−01−06) [2024−12−24]. https://arxiv.org/abs/2301.02423

[43] Lakhan A, Abed Mohammed M, Abdulkareem K H, et al. Autism Spectrum Disorder detection framework for children based on federated learning integrated CNN–LSTM. *Comput Biol Med*, 2023, 166: 107539

[44] Zaridis D I, Mylona E, Tachos N, et al. Region-adaptive magnetic resonance image enhancement for improving CNN-based segmentation of the prostate and prostatic zones. *Sci Rep*, 2023, 13(1): 714

[45] Rajagopal A, Redekop E, Kemisetti A, et al. Federated learning with research prototypes: Application to multi-center MRI-based detection of prostate cancer with diverse histopathology. *Acad Radiol*, 2023, 30(4): 644

[46] Chen Z, Yang C, Zhu M L, et al. Personalized retrogress-resilient federated learning toward imbalanced medical data. *IEEE Trans Med Imag*, 2022, 41(12): 3663

[47] Tan Y N, Tinh V P, Lam P D, et al. A transfer learning approach to breast cancer classification in a federated learning framework. *IEEE Access*, 2023, 11: 27462

[48] Nguyen Tan Y, Lam P D, Tinh V P, et al. Joint federated learning using deep segmentation and the Gaussian mixture model for breast cancer tumors. *IEEE Access*, 2024, 12: 94231

[49] Caroprese L, Ruga T, Vocaturo E, et al. Federated learning applications for breast cancer // 2023 *IEEE International Conference on Bioinformatics and Biomedicine* (*BIBM*). Istanbu, 2023: 4029

[50] Camajori Tedeschini B, Savazzi S, Stoklasa R, et al. Decentralized federated learning for healthcare networks: A case study on tumor segmentation. *IEEE Access*, 2022, 10: 8693

[51] Gong X, Song L C, Vedula R, et al. Federated learning with privacy-preserving ensemble attention distillation. *IEEE Trans Med Imag*, 2023, 42(7): 2057

[52] Bercea C I, Wiestler B, Rueckert D, et al. Federated disentangled representation learning for unsupervised brain anomaly detection. *Nat Mach Intell*, 2022, 4(8): 685

[53] Wang Y P, Wang K, Peng X Q, et al. DeepSDM: Boundary-aware pneumothorax segmentation in chest X-ray images. *Neurocomputing*, 2021, 454: 201

[54] Zhou B, Dey N, Schlemper J, et al. DSFormer: A dual-domain self-supervised transformer for accelerated multi-contrast MRI reconstruction // 2023 *IEEE/CVF Winter Conference on Applications of Computer Vision* (*WACV*). Waikoloa, 2023: 4955

[55] Elmas G, Dar S U H, Korkmaz Y, et al. Federated learning of generative image priors for MRI reconstruction. *IEEE Trans Med Imag*, 2023, 42(7): 1996

[56] Feng C M, Yan Y L, Wang S S, et al. Specificity-preserving federated learning for MR image reconstruction. *IEEE Trans Med Imag*, 2023, 42(7): 2010

[57] Yan Y L, Wang H, Huang Y W, et al. Cross-modal vertical federated learning for MRI reconstruction. *IEEE J Biomed Health Inform*, 2024, 28(11): 6384

[58] Wu R Y, Li C, Zou J, et al. Generalizable reconstruction for accelerating MR imaging via federated learning with neural architecture search. *IEEE Transactions on Medical Imaging*, 2024, 44(1): 106

[59] Zou J, Pei T R, Li C, et al. Self-supervised federated learning for fast MR imaging. *IEEE Trans Instrum Meas*, 2023, 73: 2502911

[60] Xiao Y, Jin Y C, Zhang H Y, et al. A personalized federated framework for document-level biomedical relation extraction // 2024 6*th International Conference on Data-driven Optimization of Complex Systems* (*DOCS*). Hangzhou, 2024: 457

[61] Du C H, He H, Jin Y H. Contrast with major classifier vectors for federated medical relation extraction with heterogeneous label distribution. *Appl Intell*, 2023, 53(23): 28895

[62] Vaid A, Jaladanki S K, Xu J, et al. Federated learning of electronic health records to improve mortality prediction in hospitalized patients with COVID-19: Machine learning approach. *JMIR Med Inform*, 2021, 9(1): e24207

[63] Kerkouche R, Ács G, Castelluccia C, et al. Privacy-preserving and bandwidth-efficient federated learning: An application to in-hospital mortality prediction // *Proceedings of the Conference on Health, Inference, and Learning*. Online, 2021: 25

[64] Khalil S S, Tawfik N S, Spruit M. Exploring the potential of federated learning in mental health research: A systematic literature review. *Appl Intell*, 2024, 54(2): 1619

[65] Farnaz N, Guru S, Prakash A, et al. A smart federated learning approach for mental health detection // *Proceedings of Fifth Doctoral Symposium on Computational Intelligence*. Singapore, 2024: 467

[66] Ahmed U, Lin J C, Srivastava G. Hyper-graph attention based federated learning methods for use in mental health detection. *IEEE J Biomed Health Inform*, 2023, 27(2): 768

[67] Tabassum N, Ahmed M, Shorna N J, et al. Depression detection through smartphone sensing: A federated learning approach. *Int J Interact Mob Technol*, 2023, 17(1): 40

[68] Wang Z Y, Yang Z Q, Azimi I, et al. Differential private federated transfer learning for mental health monitoring in everyday settings: A case study on stress detection [J/OL]. *arXiv preprint* (2024−02−16) [2024−12−24]. https://arxiv.org/abs/2402.

10862

[69] Ye M, Fang X W, Du B, et al. Heterogeneous federated learning: State-of-the-art and research challenges. *ACM Comput Surv*, 2024, 56(3): 1

[70] Wen J, Zhang Z X, Lan Y, et al. A survey on federated learning: Challenges and applications. *Int J Mach Learn Cybern*, 2023, 14(2): 513

[71] Ahmad Madni H, Umer R M, Foresti G L. Federated Learning for Data and Model Heterogeneity in Medical Imaging // *International Conference on Image Analysis and Processing*. Cham: Springer Nature Switzerland, 2023: 167

[72] Zhang C, Meng X Z, Liu Q, et al. FedBrain: A robust multi-site brain network analysis framework based on federated learning for brain disease diagnosis. *Neurocomputing*, 2023, 559: 126791

[73] Sachin D N, Annappa B, Hegde S, et al. FedCure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in IoMT environments. *IEEE Access*, 2024, 12: 15867

[74] Milasheuski U, Barbieri L, Tedeschini B C, et al. On the impact of data heterogeneity in federated learning environments with application to healthcare networks [J/OL]. *arXiv preprint* (2024−04−29) [2024−12−24]. https://export.arxiv.org/abs/2404.18519

[75] Chaddad A, Lu Q Z, Li J L, et al. Explainable, domain-adaptive, and federated artificial intelligence in medicine. *IEEE/CAA J Autom Sin*, 2023, 10(4): 859

[76] Li X, Zhang C, Li X, et al. Federated transfer learning in fault diagnosis under data privacy with target self-adaptation. *J Manuf Syst*, 2023, 68: 523

[77] Elayan H, Aloqaily M, Guizani M. Sustainability of healthcare data analysis IoT-based systems using deep federated learning. *IEEE Internet Things J*, 2022, 9(10): 7338

[78] Abaoud M, Almuqrin M A, Khan M F. Advancing federated learning through novel mechanism for privacy preservation in healthcare applications. *IEEE Access*, 2023, 11: 83562

[79] Alsulaimawi Z. Meta-FL: A novel meta-learning framework for optimizing heterogeneous model aggregation in federated learning [J/OL]. *arXiv preprint* (2024−06−23) [2024−12−24]. https://arxiv.org/abs/2406.16035

[80] Wu Q, Chen X, Zhou Z, et al. FedHome: Cloud-edge based personalized federated learning for in-home health monitoring. *IEEE Trans Mob Comput*, 2022, 21(8): 2818

[81] Wang T N, Zhang K, Cai J N, et al. Analyzing the impact of personalization on fairness in federated learning for healthcare // 2023 *IEEE 11th International Conference on Healthcare Informatics* (*ICHI*). Houston, 2023: 701

[82] Chen Z Q, Du J, Hou X W, et al. Channel adaptive and sparsity personalized federated learning for privacy protection in smart healthcare systems. *IEEE J Biomed Health Inform*, 2024, 28(6): 3248

[83] Selvaraj A K, Prathiba S B, Kumar A D, et al. Co-training-based personalized federated learning with generative adversarial networks for enhanced mobile smart healthcarediagnosis. *IEEE Transactions on Consumer Electronics*, 2024, 70(3): 6131

[84] Chen Y Q, Lu W, Qin X, et al. MetaFed: Federated learning among federations with cyclic knowledge distillation for personalized healthcare. *IEEE Trans Neural Netw Learn Syst*, 2024, 35(11): 16671

[85] Li S, Hu L, Sun C Y, et al. Federated edge learning for medical image augmentation. *Appl Intell*, 2024, 55(1): 56

[86] Murmu A, Kumar P, Rao Moparthi N, et al. Reliable federated learning with GAN model for robust and resilient future healthcare system. *IEEE Trans Netw Serv Manag*, 2024, 21(5): 5335

[87] He T Y, Han P Y, Duan S M, et al. Generative data augmentation with differential privacy for non-IID problem in decentralized clinical machine learning. *Future Gener Comput Syst*, 2024, 160: 171

[88] Yin Z L, Wang H Y, Chen B, et al. Federated semi-supervised representation augmentation with cross-institutional knowledge transfer for healthcare collaboration. *Knowl Based Syst*, 2024, 300: 112208

[89] Darzi E, Sijtsema N M, van Ooijen P M A. Fed-safe: Securing federated learning in healthcare against adversarial attacks [J/OL]. *arXiv preprint* (2023−10−12) [2024−12−24]. https://arxiv.org/abs/2310.08681

[90] Almufareh M F, Tariq N, Humayun M, et al. A federated learning approach to breast cancer prediction in a collaborative learning framework. *Healthcare*, 2023, 11(24): 3185

[91] Raza A, Tran K P, Koehl L, et al. AnoFed: Adaptive anomaly detection for digital health using transformer-based federated learning and support vector data description. *Eng Appl Artif Intell*, 2023, 121: 106051

[92] Qi P, Chiaro D, Guzzo A, et al. Model aggregation techniques in federated learning: A comprehensive survey. *Future Gener Comput Syst*, 2024, 150: 272

[93] Houssein E H, Sayed A. Boosted federated learning based on improved Particle Swarm Optimization for healthcare IoT devices. *Comput Biol Med*, 2023, 163: 107195

[94] Abdul Sattar Shaikh A, Bhargavi M S, Kumar C P. Weighted aggregation through probability based ranking: An optimized federated learning architecture to classify respiratory diseases. *Comput Meth Programs Biomed*, 2023, 242: 107821

[95] Zhang C, Yang S K, Mao L F, et al. Anomaly detection and defense techniques in federated learning: A comprehensive review. *Artif Intell Rev*, 2024, 57(6): 150

[96] Adnan M, Kalra S, Cresswell J C, et al. Federated learning and differential privacy for medical image analysis. *Sci Rep*, 2022, 12(1): 1953

[97] Fares M H, Saad A M S E. Towards privacy-preserving medical imaging: Federated learning with differential privacy and secure aggregation using a modified ResNet architecture [J/OL]. *arXiv preprint* (2024−12−01) [2024−12−23]. https://arxiv.org/abs/2412.00687

[98] Barnawi A, Chhikara P, Tekchandani R, et al. A differentially privacy assisted federated learning scheme to preserve data privacy for IoMT applications. *IEEE Trans Netw Serv Manag*, 2024, 21(4): 4686

[99] Zhang L, Xu J B, Vijayakumar P, et al. Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. *IEEE Trans Netw Sci Eng*, 2023, 10(5): 2864

[100] Wang B, Li H T, Guo Y N, et al. PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data. *Appl Soft Comput*, 2023, 146: 110677

[101] Wibawa F, Catak F O, Kuzlu M, et al. Homomorphic encryption and federated learning based privacy-preserving CNN training: COVID-19 detection use-case // *EICC* 2022: *Proccedings of the European Interdisciplinary Cybersecurity Conference*. Barcelona, 2022: 85

[102] Mantey E A, Zhou C H, Anajemba J H, et al. Federated learning approach for secured medical recommendation in Internet of medical things using homomorphic encryption. *IEEE J Biomed Health Inform*, 2024, 28(6): 3329

[103] Muazu T, Mao Y C, Muhammad A U, et al. A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing. *Comput Commun*, 2024, 216: 168

[104] Şahinbaş K, Catak F O. Secure multi-party computation based privacy preserving data analysis in healthcare IoT systems[J/OL]. *arXiv preprint*（2021−09−29）[2024−12−24]. https://arxiv.org/abs/2109.14334

[105] Su Y F, Huang C W, Zhu W W, et al. Multi-party Diabetes Mellitus risk prediction based on secure federated learning. *Biomed Signal Process Contr*, 2023, 85: 104881

[106] Dwork C. Differential privacy [Z/OL]. *Springer Nature*（2011）[2024−12−24]. https://doi.org/10.1007/978-1-4419-5906-5_752

[107] Yang X, Huang W, Ye M. Dynamic personalized federated learning with adaptive differential privacy. *Adv Neural Inform Process Syst*, 2023, 36: 72181

[108] Li J C, Meng Y, Ma L C, et al. A federated learning based privacy-preserving smart healthcare system. *IEEE Trans Ind Inform*, 2022, 18(3): 2021

[109] Liu F X, Zheng Z M, Shi Y X, et al. A survey on federated learning: a perspective from multi-party computation. *Front Comput Sci*. 2024 18(1): 181336.

[110] Hijazi N M, Aloqaily M, Guizani M, et al. Secure federated learning with fully homomorphic encryption for IoT communications. *IEEE Internet Things J*, 2024, 11(3): 4289

[111] Almanifi O R A, Chow C O, Tham M L, et al. Communication and computation efficiency in federated learning: A survey. *Internet Things*, 2023, 22: 100742

[112] Prakash P, Ding J H, Chen R, et al. IoT device friendly and communication-efficient federated learning *via* joint model pruning and quantization. *IEEE Internet Things J*, 2022, 9(15): 13638

[113] Liu X N, Ratnarajah T, Sellathurai M, et al. Adaptive model pruning and personalization for federated learning over wireless networks. *IEEE Trans Signal Process*, 2024, 72: 4395

[114] lglesias Jr C, de Outeiro S A, de Farias C M, et al. Two Students: Enabling Uncertainty Quantification in Federated Learning Clients // *NeurIPS* 2024 *Workshop on Bayesian Decision-making and Uncertainty*. Vancouver, 2024: 119

[115] Dubey P, Kumar M. Quantization Strategies in Federated Learning: Comparative Assessment of Methods and Challenges [J/OL]. *TechRxiv*（2024−08−30）[2024−12−24]. https://d197for5662m48.cloudfront.net/documents/publicationstatus/220952/preprint_pdf/50235c0c304a9abd8703591d0de3465c.pdf

[116] Herzog A, Southam R, Mavromatis I, et al. FedMap: Iterative magnitude-based pruning for communication-efficient federated learning [J/OL]. *arXiv preprint*（2024−06−27）[2024−12−24]. https://arxiv.org/abs/2406.19050