AI TR

2023联邦学习全球研究与应用趋势报告

智谱·AI

OpenIslands

主要发现

“中美双雄”引领全球联邦学习发展

- 中国和美国的联邦学习论文发布量遥遥领先于其他国家。六成以上高被引论文来自中美两国，中美两国论文合作数量也是全球最多；七成以上最佳论文来自中美两国。
- 联邦学习全球高被引论文领先的机构是谷歌（11 篇）、卡内基·梅隆大学（7 篇）。中国的高被引论文量较多的机构是北京邮电大学、香港科技大学、中山大学以及深圳市大数据研究院。最佳论文数量则是卡内基·梅隆大学与香港科技大学各以 3 篇而并列第一。全球高被引论文作者主要聚集在中美，美国的高被引论文作者数量是中国的 2.3 倍。
- 全球专利受理数量以中国地区最多，约占全球受理总量的七成。专利申请数量前三名机构全部是中国机构。
- 联邦学习的九成以上国家自然科学基金资助是青年科学基金项目和面上项目。
- 开源框架主要来自中美，其中 OpenMined 推出的 Pysyft 、FATE 开源社区的 FATE 热度超过 4000，居于第一梯队；FedML.AI 的 FedML、Adap 的 Flower、谷歌的 TFF 等框架的热度也较高，热度超过 2000，且 FATE 和 FedML 两个框架目前已推出 LLM 模块。

未来联邦学习研究趋势将更多与算法模型和安全隐私技术相关

- 目前联邦学习研究热点主要聚焦在机器学习方法、模型训练、隐私保护三方面。
- 未来几年研究将更多涉及算法模型和安全隐私技术，如数据隐私、差分隐私、边缘计算、物联网、同态加密等。可信联邦学习成为重要趋势，联邦大模型技术、模型产权保护（IPR）、模型定价等正在初步探索。
- 行业应用越来越成熟，应用研究方向呈现出更多与物联网、区块链、客户端、电子设备等融合的态势。

目录

人工智能之联邦学习——

《2023 联邦学习全球研究与应用趋势报告》

编写团队

顾问

李涓子　　清华大学人工智能研究院知识智能中心

唐杰　　清华大学人工智能研究院知识智能中心

编写团队

张淼　张建伟　张淳　商莹玥　孙旭东　徐洁

数据

仇瑜　赵慧军　宋健　孙尧

排版设计

边云风　韩宇　周凯杰

1. 报告说明

《联邦学习全球研究与应用趋势报告》是一个追踪联邦学习领域动态和进展的非营利性项目。2023 年度报告是本系列第三期，旨在更新展示联邦学习科研成果与技术应用的最新动态。在过去的一年里，AI 世界已经进入一个以大模型引领的新的发展阶段。人们在惊叹大模型的强大能力的同时，也在担忧其训练数据来源合规性、数据使用的偏见性等安全风险隐患；同样，在行业监管环境越来越规范化、信息安全与隐私数据越来越受重视的背景下，联邦学习研究和应用趋势也逐渐迈向可信联邦学习。

联邦学习（Federated Learning）是在进行分布式机器学习的过程中，各参与方可借助其他参与方数据进行联合建模和使用模型。参与各方无需传递和共享原始数据资源，同时保护模型参数，即在数据不出本地的情况下，进行数据联合训练、联合应用，建立合法合规的机器学习模型[1]。

联邦学习是一种新兴的人工智能基础技术，其概念于 2016 年由谷歌公司 H. Brendan Mcmahan 在论文 *Federated Learning of Deep Networks using Model Averaging*[2][3] 中最先提出，原本用于解决安卓手机终端用户在本地更新模型的问题，后来经香港科技大学与微众银行杨强教授所领导团队在 2018 年将其扩展为机构间 B2B 分布式联合建模架构，包括按样本、特征分割以及异构多方建模，同时可以建立去中心协调器的 Peer-to-Peer 架

[1] 杨强、刘洋、陈天健等：《联邦学习》，《中国计算机学会通讯》，2018 年版第 11 期，第 49-55 页.

[2] McMahan, H. B., Moore, E., Ramage, D., & y Arcas, B. A. (2016). Federated learning of deep networks using model averaging. *arXiv preprint arXiv*:1602.05629.

[3] 注：该论文后于 2017 年以 *Communication-Efficient Learning of Deep Networks from Decentralized data* 为标题发表于 AISTATS 2017。

构形式，其设计目标是在保障大数据交换时的信息安全、保护终端数据和个人数据隐私、保证合法合规的前提下，在多参与方或多计算结点之间开展高效率、安全、可靠的机器学习。联邦学习同时包括鼓励多方持续参与合作生态的激励机制，建立正向激励的数据价值交易市场机制。当下，联邦学习已经被大量应用于金融[4]、安防[5]、医疗[6]、在线推荐系统[7]等领域。联邦学习有望成为下一代人工智能协同算法、隐私计算和协作网络的基础。2023 年，美国白宫发布了《国家人工智能研发战略计划》，其中，“促进联邦机器学习方法（Federated ML）”被列为首要战略的十大优先事项之一，即列入“对基础和负责任的人工智能研究进行长期投资”战略。

《2023 联邦学习全球研究与应用趋势报告》主要从技术研究、学者画像、主流框架、行业应用，以及发展趋势几大方面，较为全面深入地介绍联邦学习自 2016 年诞生以来到 2022 年的技术研究和应用进展，并展望该技术的未来发展方向与前景。本期报告不仅将数据范围扩展到 2016-2022 年、更新了相关技术数据统计、现状进展等内容，重点突出展示了该领域具有较高技术质量、创新力的科研成果，例如，对科研实践具有较大影响力的高被引论文及其作者的分析、来自知名人工智能国际顶会的联邦学习专题研讨会最佳论文相关分析等，而且增加了联邦学习领域的国家自然科学基金获批项目分析、以及融合了大模型技术

4 https://www.fedai.org/cases/utilization-of-fate-in-anti-money-laundering-through-multiple-banks/

5 Liu, Y., Huang, A., Luo, Y., Huang, H., Liu, Y., Chen, Y., Feng, L., Chen, T., Yu, H., & Yang, Q. (2020). “FedVision: An Online Visual Object Detection Platform Powered by Federated Learning,” Proceedings of the AAAI Conference on Artificial Intelligence, 34(08), 13172-13179.

6 Li W. et al. “Privacy-Preserving Federated Brain Tumour Segmentation,” In: Suk HI., Liu M., Yan P., Lian C. (eds) Machine Learning in Medical Imaging. MLMI 2019. Lecture Notes in Computer Science, vol 11861. Springer, Cham.

7 Ben Tan, Bo Liu, Vincent Zheng, and Qiang Yang. 2020. A Federated Recommender System for Online Services. In Fourteenth ACM Conference on Recommender Systems (RecSys '20). Association for Computing Machinery, New York, NY, USA, 579–581. DOI:https://doi.org/10.1145/3383313.3411528

的联邦学习论文和专利分析，以展示更加丰富的联邦学习新方向和新探索。

1.1 数据范围

本报告研究数据范围是科技情报大数据挖掘与服务系统平台 AMiner 数据库所收录的 2016-2022 年期间与联邦学习研究主题强相关的论文数据、专利数据以及公开数据等。论文的引用量数据统计截止日期为 2023 年 3 月 31 日。

1.2 联邦学习知识树

本报告根据联邦学习的关键技术和相关技术，以及该领域高被引学术论文的研究主题，将挖掘出的全球活跃的联邦学习重要技术点表征为知识树结构，如图 1 所示。

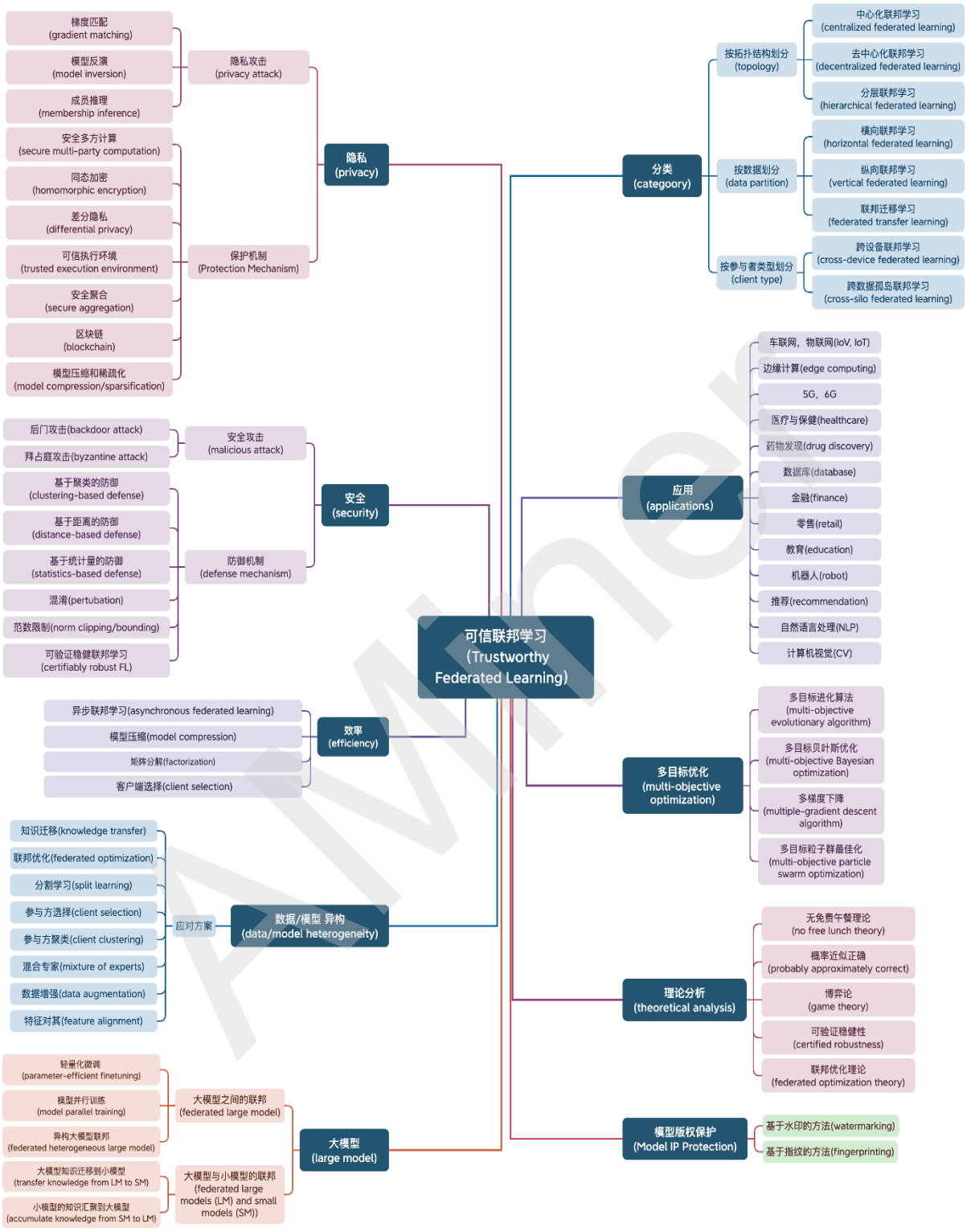

可信联邦学习
(Trustworthy Federated Learning)
隐私
(privacy)
隐私攻击
(privacy attack)
梯度匹配
(gradient matching)
模型反演
(model inversion)
成员推理
(membership inference)
保护机制
(Protection Mechanism)
安全多方计算
(secure multi-party computation)
同态加密
(homomorphic encryption)
差分隐私
(differential privacy)
可信执行环境
(trusted execution environment)
安全聚合
(secure aggregation)
区块链
(blockchain)
模型压缩和稀疏化
(model compression/sparsification)
安全
(security)
安全攻击
(malicious attack)
后门攻击(backdoor attack)
拜占庭攻击(byzantine attack)
防御机制
(defense mechanism)
基于聚类的防御
(clustering-based defense)
基于距离的防御
(distance-based defense)
基于统计量的防御
(statistics-based defense)
混淆(pertubation)
范数限制(norm clipping/bounding)
可验证稳健联邦学习
(certifiably robust FL)
效率
(efficiency)
异步联邦学习(asynchronous federated learning)
模型压缩(model compression)
矩阵分解(factorization)
客户端选择(client selection)
数据/模型 异构
(data/model heterogeneity)
应对方案
知识迁移(knowledge transfer)
联邦优化(federated optimization)
分割学习(split learning)
参与方选择(client selection)
参与方聚类(client clustering)
混合专家(mixture of experts)
数据增强(data augmentation)
特征对其(feature alignment)
大模型
(large model)
大模型之间的联邦
(federated large model)
轻量化微调
(parameter-efficient finetuning)
模型并行训练
(model parallel training)
异构大模型联邦
(federated heterogeneous large model)
大模型与小模型的联邦
(federated large models (LM) and small models (SM))
大模型知识迁移到小模型
(transfer knowledge from LM to SM)
小模型的知识汇聚到大模型
(accumulate knowledge from SM to LM)
分类
(categoory)
按拓扑结构划分
(topology)
中心化联邦学习
(centralized federated learning)
去中心化联邦学习
(decentralized federated learning)
分层联邦学习
(hierarchical federated learning)
按数据划分
(data partition)
横向联邦学习
(horizontal federated learning)
纵向联邦学习
(vertical federated learning)
联邦迁移学习
(federated transfer learning)
按参与者类型划分
(client type)
跨设备联邦学习
(cross-device federated learning)
跨数据孤岛联邦学习
(cross-silo federated learning)
应用
(applications)
车联网，物联网(IoV, IoT)
边缘计算(edge computing)
5G，6G
医疗与保健(healthcare)
药物发现(drug discovery)
数据库(database)
金融(finance)
零售(retail)
教育(education)
机器人(robot)
推荐(recommendation)
自然语言处理(NLP)
计算机视觉(CV)
多目标优化
(multi-objective optimization)
多目标进化算法
(multi-objective evolutionary algorithm)
多目标贝叶斯优化
(multi-objective Bayesian optimization)
多梯度下降
(multiple-gradient descent algorithm)
多目标粒子群最佳化
(multi-objective particle swarm optimization)
理论分析
(theoretical analysis)
无免费午餐理论
(no free lunch theory)
概率近似正确
(probably approximately correct)
博弈论
(game theory)
可验证稳健性
(certified robustness)
联邦优化理论
(federated optimization theory)
模型版权保护
(Model IP Protection)
基于水印的方法(watermarking)
基于指纹的方法(fingerprinting)

图 1 联邦学习知识树

2. 引言

人工智能未来能否可持续发展面临三大困境。

一是**数据困境**。人工智能和机器学习算法具有对数据强依赖的特性。现实中，多数行业领域存在着数据有限且质量较差的问题，并且数据以碎片化的形式分散存在，不足以支撑人工智能技术的实现。同时，数据源之间存在着难以打破的壁垒。由于行业竞争、隐私安全、行政手续复杂等问题，数据还多是以孤岛形式存在的。此外，研究界和企业界目前的情况是收集数据的一方通常不是使用数据的一方。因此，将分散在各地、各机构的数据进行整合用于机器学习所需的成本非常巨大。

二是**法律挑战**。当前，重视数据隐私和安全已经成为世界性的趋势，各国都在不断地推出和加强对数据安全和隐私保护相关法规的完善。欧盟 2018 年正式施行《通用数据保护条例》（General Data Protection Regulation, GDPR）。在中国，全国信息安全标准委员会先后于 2017 年 12 月和 2020 年 3 月发布了两版《信息安全技术个人信息安全规范》(GB/T 35273-2017、GB/T 35273-2020)，对个人信息收集、储存、使用做出了明确规定。此外，在 2017 年起实施的《中华人民共和国网络安全法》[8] 和《中华人民共和国民法总则》[9] 中也指出网络运营者不得泄露、篡改、毁坏其收集的个人信息，并且与第三方进行数据交易时需确保在合同中明确约定拟交易数据的范围和数据保护义务。2021 年陆续公布实施了《数

8 《中华人民共和国网络安全法》，中共中央网络安全和信息化委员会办公室、中华人民共和国国家互联网信息办公室，http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

9 《中华人民共和国民法总则》，中华人民共和国中央人民政府，http://www.gov.cn/xinwen/2017-03/18/content_5178585.htm#1

据安全法》[10]、《个人信息保护法》[11]、《关键信息基础设施安全保护条例》[12]，为数据安全提供了法律保护，更规范了数据的合法合规使用。

三是**算力困境**。尽管计算设备的性能不断提升，但 AI 算法的复杂性和计算需求也在同步增长。算力不足成为当前人工智能发展面临的另一个困境。分布式计算通过将计算任务分散到多个计算节点上来提高计算能力和效率，既可以减轻集中计算的压力，又可以通过动态调整计算节点的数量来适应不同的计算需求，具有可靠性和可扩展性，有助于解决人工智能发展的算力困境。

针对以上困境，“狭义”联邦机器学习的概念于 2016 年由谷歌研究人员首先提出，随后成为解决数据孤岛问题、满足隐私保护和数据安全的一个可行性解决方案[13]。联邦学习的特征是数据不出本地、各个参与者的身份和地位平等，它能够实现多个参与方在保护数据隐私、满足合法合规要求的前提下进行机器学习，协同地进行模型训练与结果预测，并且建模效果和将整个数据集放在一处建模的效果相同或相差不大（在各个数据的用户对齐（user alignment）或特征对齐（feature alignment）的条件下）[13]，从而实现企业间的数据融合建模，解决数据孤岛问题。

“广义”联邦学习的概念由香港科技大学杨强教授所领导的微众银行 AI 团队在 2018 年提出，该团队将联邦学习扩展为机构和个人间的 B2C 模式和不同机构间 B2B 分布式联合建模架构，包括按样本、按特征分割以及异构多方建模，同时可以建立去中心协调器的 Peer-

10 《中华人民共和国数据安全法》，中国人大网，2021 年 06 月 10 日，
http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

11 《中华人民共和国个人信息保护法》，中国人大网，2021 年 08 月 20 日，
http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

12 《关键信息基础设施安全保护条例》，中国政府网，2021 年 08 月 17 日
http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm

13 杨强、刘洋、陈天健等：《联邦学习》，《中国计算机学会通讯》，2018 年版第 11 期，第 49-55 页.

to-Peer 架构形式，其设计目标是在保障大数据交换时的信息安全、保护终端数据和个人数据隐私、保证合法合规的前提下，在多参与方或多计算结点之间开展高效率、安全、可靠的机器学习和模型使用。联邦学习同时包括鼓励多方持续参与合作生态的激励机制，建立正向激励的数据价值交易市场机制。

如上所述，根据孤岛数据的分布特点（用户与用户特征的重叠情况），联邦学习可以分为横向联邦学习、纵向联邦学习与联邦迁移学习 [14]。

联邦学习能够成功的一个重要根基，在于与激励机制、隐私和安全保护等技术的融合。联邦学习激励机制研究的是如何量化每个参与方对数据联邦带来的收益，公平地与参与者分享部分收益以此作为激励，从而实现数据联邦长期的可持续经营[15]。为了防止攻击者通过梯度匹配和模型反演等攻击手段复现原始数据，联邦学习通过与安全多方计算（Secure Multi-Party Computation, MPC）、同态加密（Homomorphic Encryption, HE）、差分隐私（Differential Privacy, DP）和可信执行环境（Trusted Execution Environment, TEE）等隐私计算技术相融合，进一步提升对数据的隐私保护。然而，隐私保护方法的使用往往带来联邦学习中模型性能的损失或者模型训练（或推理）效率的下降。因此联邦学习与隐私计算技术的融合通常需要在模型精度、模型训练效率和隐私（或安全）保护程度这三个维度之间进行权衡。这三个维度也是可信联邦学习中最重要的三个优化目标。如何能够在这三个维度上得到综合性的提升，是联邦学习的一个热点研究方向[16][17]。随着联邦学习的研究和应用

14 Liu Y, Chen T, Yang Q. Secure Federated Transfer Learning Framework[J]. IEEE Intelligent Systems, vol. 35, no. 4, pp. 70-82, 1 July-Aug. 2020.

15 杨强，刘洋，程勇，康焱，陈天健：《联邦学习》，电子工业出版社：北京，2020 年:99-99.

16 Girgis, Antonious M., Deepesh Data, Suhas Diggavi, Peter Kairouz, and Ananda Theertha Suresh. "Shuffled model of federated learning: Privacy, accuracy and communication trade-offs." IEEE journal on selected areas in information theory 2, no. 1 (2021): 464-478.

17 Zhang, Xiaojin, Yan Kang, Kai Chen, Lixin Fan, and Qiang Yang. "Trading off privacy, utility and efficiency in

不断深化，可信联邦学习所涉及的目标维度也在不断延伸，比如，联邦学习的模型鲁棒性[18]，公平性[19]，可解释性[20]，模型的产权保护[21]等都是支撑可信联邦学习的重要维度。

近年来，大模型（又称大型语言模型，Large Language Model，简称 LLM）进入了快速发展的时期。先进的大模型 ChatGPT [22][23] 在各种自然语言处理任务上的卓越表现，进一步激发了研究机构和各大企业对大模型进行研究和应用的热情，各种通用和垂直领域大模型层出不穷。然而，大模型在实际应用中面临诸多挑战，主要包括：1）训练大模型所需的公域数据即将耗尽；2）模型训练和使用过程中涉及数据隐私保护问题；3）所需巨额的数据、算力等资源带来的高门槛使中小型机构望而却步，不利于技术普惠。联邦学习是应对这些挑战的一个很有潜力的工具。它能够使不同规模的企业利用各自的私有领域数据共同地训练或微调一个或多个大模型，而不必担心私有领域数据的泄露。目前，联邦大模型的研究还处于早期阶段，主要集中在如何使联邦学习参与方高效地微调大模型 [24]。联邦大模型中的隐私、安全、鲁棒性等问题仍处于探索阶段。

federated learning." ACM Transactions on Intelligent Systems and Technology (2022).

18 Xie, Chulin, Minghao Chen, Pin-Yu Chen, and Bo Li. "Crfl: Certifiably robust federated learning against backdoor attacks." In International Conference on Machine Learning, pp. 11372-11382. PMLR, 2021.

19 Li, Tian, Shengyuan Hu, Ahmad Beirami, and Virginia Smith. "Ditto: Fair and robust federated learning through personalization." In International Conference on Machine Learning, pp. 6357-6368. PMLR, 2021.

20 Li, Anran, Rui Liu, Ming Hu, Luu Anh Tuan, and Han Yu. "Towards Interpretable Federated Learning." arXiv preprint arXiv:2302.13473 (2023).

21 Li, Bowen, Lixin Fan, Hanlin Gu, Jie Li, and Qiang Yang. "FedIPR: Ownership verification for federated deep neural network models." IEEE Transactions on Pattern Analysis and Machine Intelligence 45, no. 4 (2022): 4521-4536.

22 Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. "Attention is all you need." *Advances in neural information processing systems* 30 (2017).

23 Introducing ChatGPT，https://openai.com/blog/chatgpt

24 Zhang, Zhuo, Yuanhang Yang, Yong Dai, Qifan Wang, Yue Yu, Lizhen Qu, and Zenglin Xu. "FedPETuning: When Federated Learning Meets the Parameter-Efficient Tuning Methods of Pre-trained Language Models." In Findings of the Association for Computational Linguistics: ACL 2023, pp. 9963-9977. 2023.

联邦学习作为未来 AI 发展的底层技术，它依靠安全可信的数据保护措施下连接数据孤岛的模式，将不断推动全球 AI 技术的创新与飞跃。随着联邦学习在更大范围和更多行业场景中的渗透及应用，它不仅能辅助人类的工作及生活，也将逐步改变人类的认知模式，促进全社会智能化水平提升，并以“合作共赢”的模式带动跨领域的企业级数据合作，有效降低技术应用的成本和门槛，催生基于联合建模的新业态，进而推动社会经济及发展[25]。

截至目前尚没有关于联邦学习技术发展的权威统计，本报告将主要回顾其从 2016 年诞生至 2022 年的技术发展趋势，作为学者们了解该技术进展的重要渠道。未来我们将定期进行该技术的阶段性回顾。

25 微众银行人工智能部、鹏城实验室、腾讯研究院、中国信通院云大所、平安科技、招商局金融科技、电子商务与电子支付国家工程实验室(中国银联)：《联邦学习白皮书 V2.0》，深圳，2020 年，第 5-7 页.

3. 联邦学习技术研究与应用现状

3.1 技术研究现状

3.1.1 科研论文成果现状

1. 论文发表量复合年均增长率为 38.6%

基于 AMiner 系统，通过关键词组[26]在标题和摘要中检索 2016 年至 2022 年论文数据。结果显示，研究时段内联邦学习相关论文共计 6861 篇，自 2016 年被提出以来，研究论文数量逐年增多，2016-2022 年的复合年均增长率为 38.6%，相关论文趋势如图 2 所示。

26 联邦学习关键词检索式：federated machine learning OR federated optimization OR federated learning OR federation learning OR (privacy AND distributed AND data mining) OR (secure AND distributed AND data mining) OR (secure AND multiparty) OR (secure AND multi-party) OR (privacy AND multi-party) OR (privacy AND multiparty) OR (privacy AND distributed AND machine learning) OR (secure AND distributed AND machine learning) OR (privacy and joint learning) OR (secure and joint learning) OR (privacy AND distributed AND deep learning) OR (secure AND distributed AND deep learning)

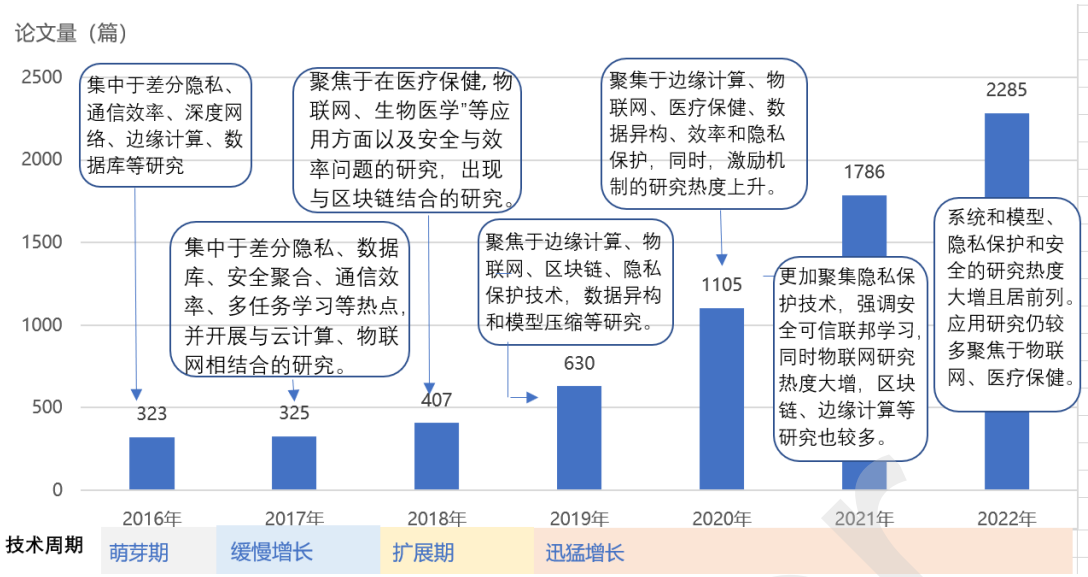


图 2 联邦学习研究论文趋势（2016–2022 年）

2. 论文发布量以中美两国为引领

根据论文作者所在机构所属国家进行排序分析，发现研究时段内联邦学习论文发布量 TOP 10 国家依次是中国、美国、英国、印度、加拿大、澳大利亚、德国、俄罗斯、日本和韩国。论文量较突出的国家是中国（2217 篇）和美国（1723 篇），详细信息如图 3 所示。

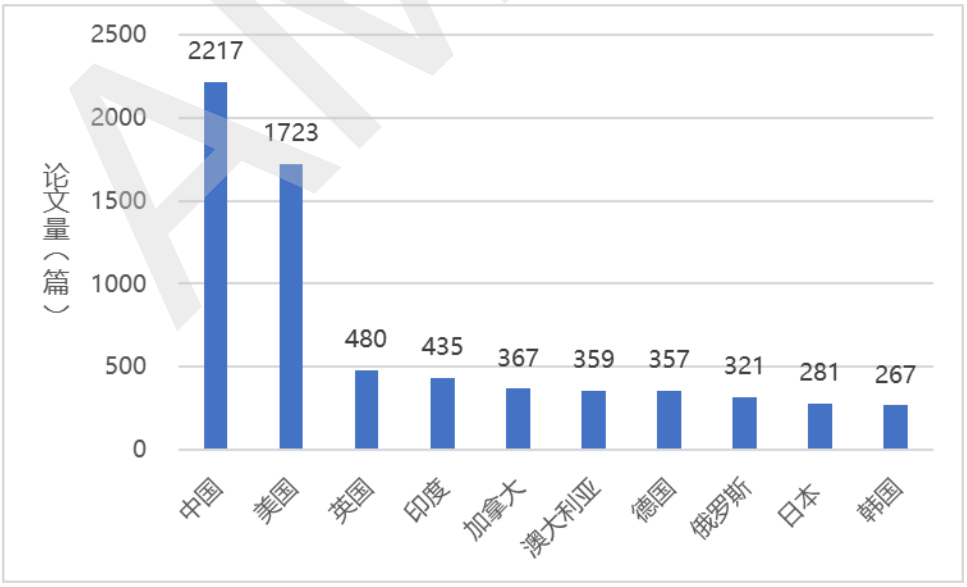


图 3 联邦学习论文发表量 TOP 10 国家（2016–2022 年）

3. 研究热点涵盖应用、系统和模型设计、安全隐私三个领域

（1）总体研究热点

总体来看，基于 AMiner 系统的论文热词分析，发现 2016-2022 年联邦学习领域的研究热点 TOP 10 按热度递减依次包括：Internet of Things（物联网）、aggregation（聚合）、optimization（优化）、blockchain（区块链）、edge computing（边缘计算）、privacy preserving（隐私保护）、differential privacy（差分隐私）、deep network（深度网络）、healthcare（医疗保健）、robustness（鲁棒性）等，如图 4 所示。可见，在研究时段内，联邦学习的主要研究热点是关于应用及相关算法模型，同时，安全[27][28][29]和

27 Xie, Chulin, Minghao Chen, Pin-Yu Chen, and Bo Li. "Crfl: Certifiably robust federated learning against backdoor attacks." In International Conference on Machine Learning, pp. 11372-11382. PMLR, 2021

28 So, Jinhyun, Başak Güler, and A. Salman Avestimehr. "Byzantine-resilient secure federated learning." IEEE Journal on Selected Areas in Communications 39, no. 7 (2020): 2168-2181.

29 Li, Bowen, Lixin Fan, Hanlin Gu, Jie Li, and Qiang Yang. "FedIPR: Ownership verification for federated deep neural network models." IEEE Transactions on Pattern Analysis and Machine Intelligence 45, no. 4 (2022): 4521-4536.

隐私[30][31][32]、效用和效率[33][34][35]，以及可信和可信赖相关的联邦学习[36][37]成为研究的关键因素。此外，reinforcement learning（强化学习）、multiparty computation（多方计算）、homomorphic encryption （同态加密）、privacy leakage（隐私泄露）、communication efficiency (沟通效率)、vehicle （车辆交互）、wireless communication（无线通信）等相关研究也较热，但在本期报告内没能进入热点 TOP 10。

30 Bonawitz, Keith, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. "Practical secure aggregation for privacy-preserving machine learning." In proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175-1191. 2017.

31 Wei, Kang, Jun Li, Ming Ding, Chuan Ma, Howard H. Yang, Farhad Farokhi, Shi Jin, Tony QS Quek, and H. Vincent Poor. "Federated learning with differential privacy: Algorithms and performance analysis." IEEE Transactions on Information Forensics and Security 15 (2020): 3454-3469.

32 Zhang, Chengliang, Suyi Li, Junzhe Xia, Wei Wang, Feng Yan, and Yang Liu. "BatchCrypt: Efficient homomorphic encryption for Cross-Silo federated learning." In 2020 USENIX annual technical conference (USENIX ATC 20), pp. 493-506. 2020.

33 McMahan, Brendan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. "Communication-efficient learning of deep networks from decentralized data." In Artificial intelligence and statistics, pp. 1273-1282. PMLR, 2017.

34 Konečný, Jakub, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. "Federated learning: Strategies for improving communication efficiency." arXiv preprint arXiv:1610.05492 (2016).

35 Liu, Yang, Xinwei Zhang, Yan Kang, Liping Li, Tianjian Chen, Mingyi Hong, and Qiang Yang. "FedBCD: A communication-efficient collaborative learning framework for distributed features." IEEE Transactions on Signal Processing 70 (2022): 4277-4290.

36 Zhang, Xiaojin, Yan Kang, Kai Chen, Lixin Fan, and Qiang Yang. "Trading off privacy, utility and efficiency in federated learning." ACM Transactions on Intelligent Systems and Technology (2022).

37 Trustworthy federated learning, Springer Cham, 2023

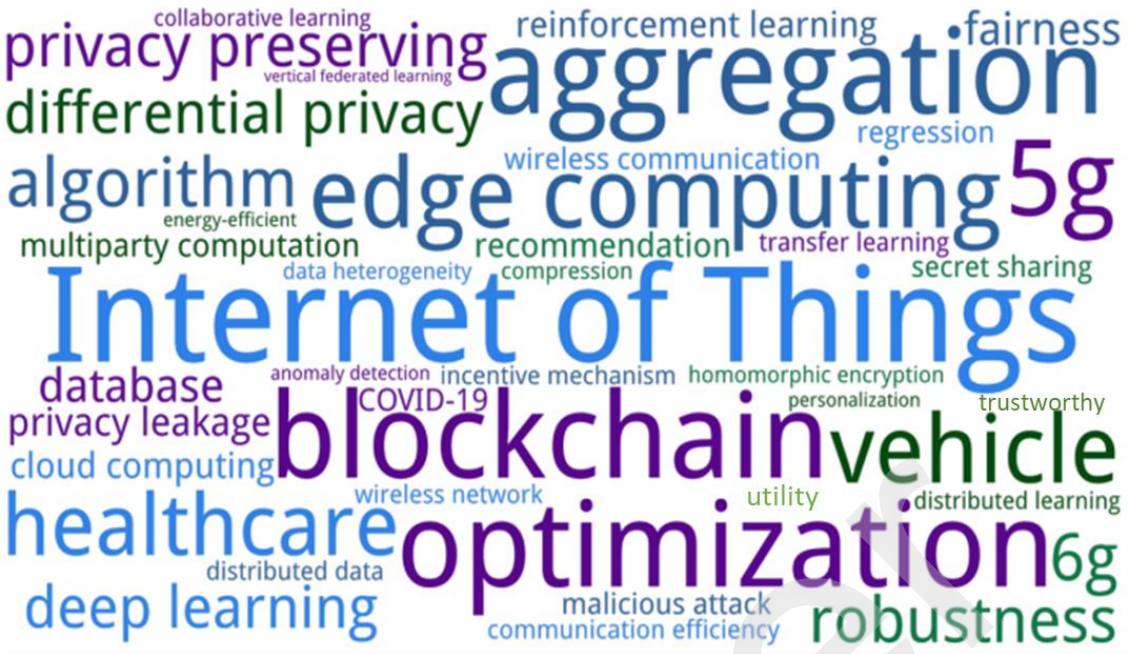
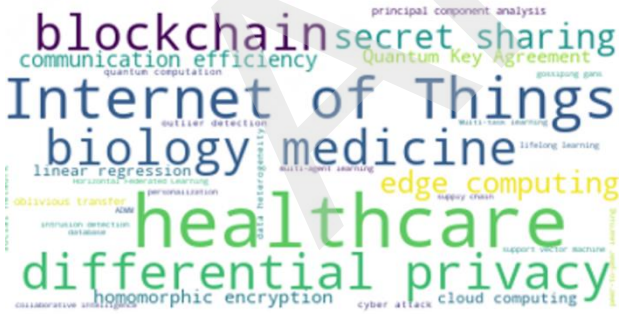
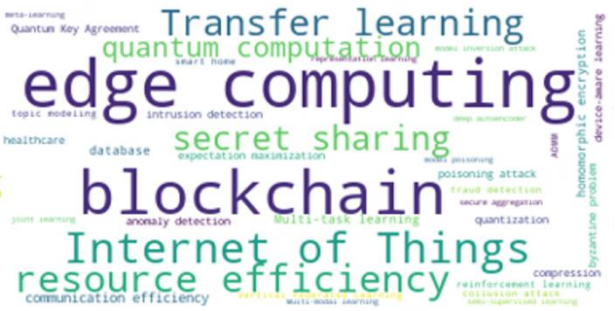
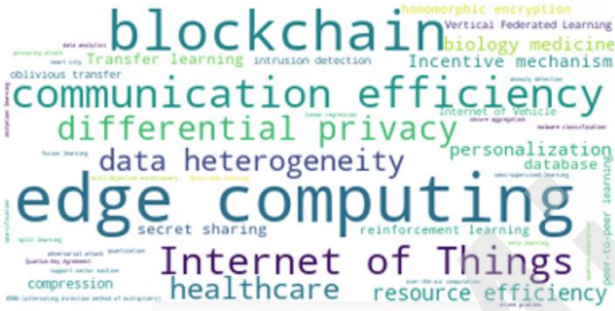
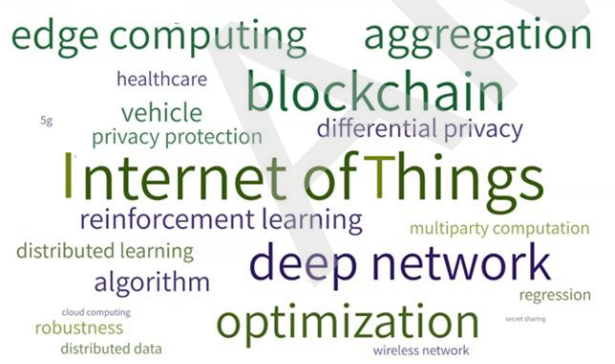


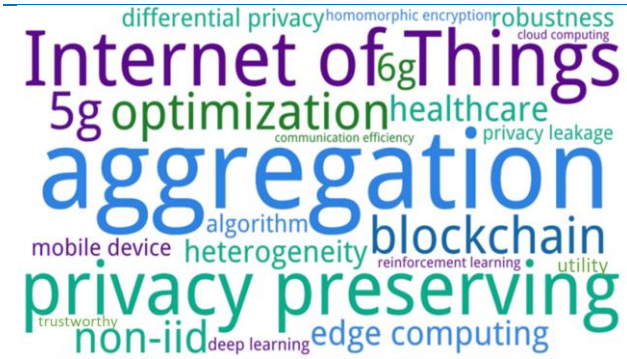
图 4 2016–2022 年联邦学习领域研究热点词云图

（2）年度研究热点

分年度来看，联邦学习研究热点从机器学习到优化、从信息统计到量子密码、从数据隐私到行业应用，学者们不断探索落地联邦学习的方法，一方面是利用交替方向乘子法（ADMM）、量化、压缩等方式进行联邦学习算法优化，另一方面是引入区块链、密码学、物联网等技术建立全局共享的数据集，并对抗恶意攻击和信息泄露。同时，学者们也对多任务学习、个性化及元学习、概率近似正确学习等方法进行广泛的研究来应对联邦学习中的数据的非独立同分布（Non-IID）问题、多目标优化问题等。各年度研究热点具体情况如下。

2016  	主要研究热点包括 differential privacy, communication efficiency，deep network，edge computing，database 等技术，关注 secret sharing, quantum signature, homomorphic encryption，secure aggregation 等安全技术问题，应用领域研究以 biology medicine，healthcare 为主。 此外，当时热点还包括 support vector machine, graph computation, vertical federated learning 等。
2017  	延续了上年的 differential privacy, database, secure aggregation, communication efficiency 等研究热点，新增出现了 multi-task learning, quantum key agreement, ADMM, anomaly detection, Bayesian learning，social network, collusion attack, quantum machine, reinforcement learning 等研究热点。在应用方面，healthcare 依然是联邦学习的热点应用方向，cloud computing 和 Internet of Things 和联邦学习的结合也成为研究热点。
2018  	2018 年联邦学习应用相关研究热度增加并居于前列，如 healthcare, Internet of Things, biology medicine, edging computing。同时，学者们依旧较关注 differential privacy, secret sharing, homomorphic encryption, Quantum Key Agreement, communication efficiency 等联邦学习安全与效率问题的研究。在这一阶段区块链 (blockchain) 技术成为热点，为联邦学习提供了保障用户隐私的新方法。

2019 	2019 年，edge computing, Internet of Things, blockchain 成为热门研究领域，homomorphic encryption，secret sharing, secure aggregation 等隐私保护技术依旧受到高度关注。2019 年加大了对数据异构和模型压缩等技术的研究力度，transfer learning, multi-task learning, quantization, compression 成为热点研究方向。如何在联邦学习中有效地利用资源也成为 2019 年研究的热点之一。
2020 	2020 年，edge computing, Internet of things, healthcare 依旧是联邦学习的应用热点。联邦学习中的效率和隐私保护技术依旧是研究热点。2020 年加大了对联邦学习数据异构方向的研究，热门的研究点包括 personalization 和 transfer learning。同时，联邦学习激励机制（incentive mechanism）的研究开始增加，以此激励更多机构加入数据联邦。
2021 	2021 年明显加大了对联邦学习技术应用的研究力度，Internet of Things 成为最热门的研究点，其次是 blockchain 和 edge computing 等应用研究。Deep network, optimization, aggregation, reinforcement learning 等相关算法技术研究依旧受到高度关注。同时，privacy protection，distributed learning, multiparty computation 等成为新的热点研究方向。
2022	2022 年系统和模型设计方面的总体研究热度明显上升且居于前列，尤其聚合技术研究热度最高。同时，privacy preserving, blockchain, differential privacy 等隐私保护和安全相关研究成果较上年显著大幅增加；可信联邦学习、安全与隐私之间的权衡、以及效用和效率等问题进一步被探索。应用研究方面，物联网 Internet of



Things、医疗保健等热度延续上升，本年度仍保持在前列。值得关注的是， 6G 等的研究热度增加较多，车辆交互等研究热度则较上年有所下降。

（3）主题热点趋势

通过 TF-IDF 算法对所研究时段内每一年的联邦学习主题相关论文数量进行计算，获取论文数量 TOP 30 的热点词，然后聚合成联邦学习的应用（application）、系统和模型设计（system and model design）和安全隐私（secure and privacy）三个主题领域的研究热点集。这三个细分主题的研究趋势呈现出如下特征。

在应用研究领域，联邦学习的研究热点按照总热度由高到低依次包括物联网（Internet of things）、边缘计算（edge computing）、医疗保健（healthcare）、车辆交互（vehicle）、无线通信（wireless communication）、5G（第 5 代移动网络）、数据库（database）、以及推荐（recommendation），详细信息如图 5 所示。联邦学习近年来在物联网、边缘计算、医疗保健、数据库、车辆交互以及推荐方面的应用研究热度逐渐上升。相比而言，数据库、医疗保健的研究热度曾在 2016 年与 2017 年的研究热度相对较高且不相上下，近年来则被其他主题的研究热度所超过，2018 年联邦学习相关的医疗保健应用研究热度明显超出其他的应用研究热度。边缘计算在 2019 年与 2020 年是联邦学习技术应用研究热度之榜首，在 2021 年与 2022 年则被物联网方面应用研究所赶超。联邦学习在物联网方面应用研究热度于 2017 年开始出现且一路上升成为当前最热，在车辆交互方面应用研究热度于 2018 年开始出现，在 5G、6G 方面应用研究热度则是分别从 2019 年、2020 年开始出现的。

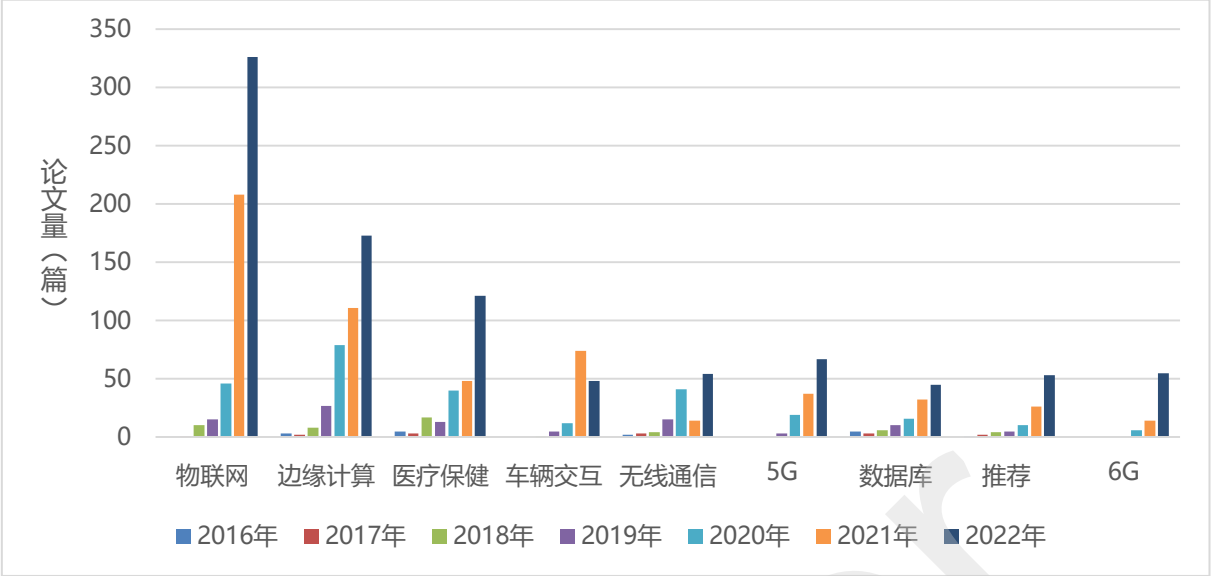


图 5 联邦学习在应用方面的研究热点趋势（2016–2022 年）

关于联邦学习在系统和模型设计方面的研究热点趋势情况如图 6 所示。由图可见，截止目前，在系统和模型设计方面研究热点依照热度递减分别是聚合（aggregation）、优化（optimization）、异构（heterogeneity）、鲁棒性（robustness）、通信效率（communication efficiency）、公平性（fairness）、激励机制（incentive mechanism）和资源效率（resource efficiency）。聚合主题曾经在 2019 年研究热度最高，经过被异构和优化等主题超越的两年之后，在 2022 年再次成为热度最高的领域研究主题。优化主题曾经在 2016 和 2017 年研究热度最高，经过 2018-2020 年的热度相对弱化后，在 2021 年再度成为最热门的研究主题。2017 年，资源效率和公平性相关主题研究开始崭露头角；2018 年通信效率相关研究占据热度榜第一；2019 年热度最高的是与聚合相关研究，同时，对联邦学习（数据和系统）异构的研究大幅提升；2020 年与异构相关研究上升为最热门，和激励机制相关的研究数量大幅提升；2021 年与优化和聚合相关主题研究上升幅度显著。从热度持续性看，聚合、优化、鲁棒性、激励机制和公平性的相关研究在研究时段内一直保持着

不同程度的热度上升。

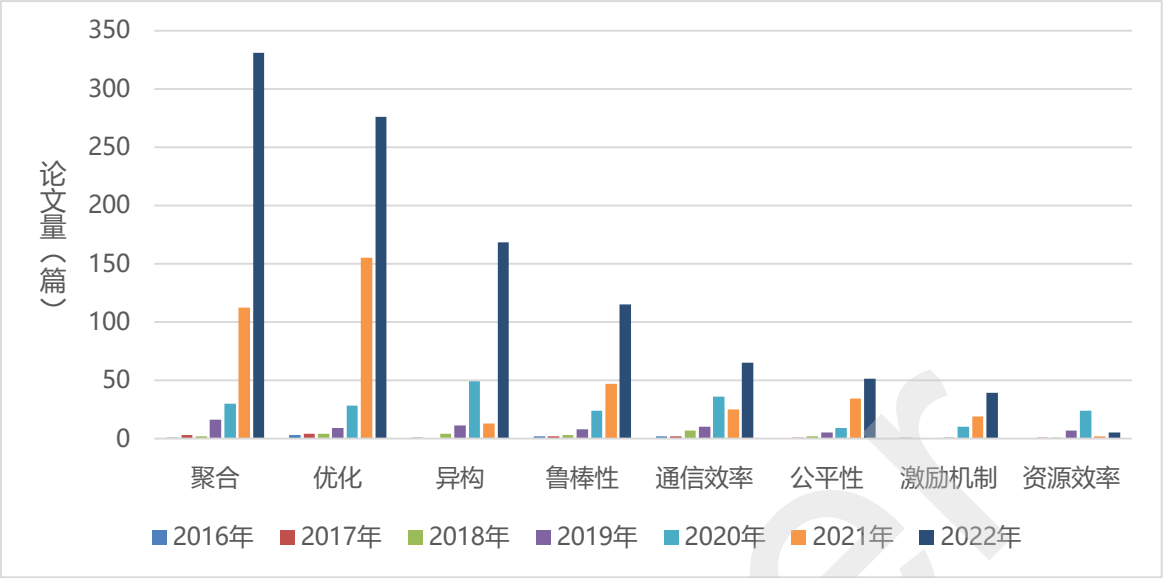


图 6 联邦学习系统和模型设计方面的研究热点趋势（2016–2022 年）

在安全隐私方面，联邦学习研究主题依据总热度递减依次包括区块链（blockchain）、差分隐私（differential privacy）、安全多方计算（multiparty computation）、隐私泄露（privacy leakage）、同态加密（homomorphic encryption）、恶意攻击（malicious attack）、网络安全（cyber security）以及容错（fault tolerance），具体热度趋势情况如图 7 所示。在研究时段内，区块链、差分隐私、恶意攻击、隐私泄露和同态加密的研究热度总体持续逐年上涨。2016 年研究最热的是对联邦学习中恶意攻击的研究，2017 年研究最热的是差分隐私，2018 年研究最热的是安全多方计算所涉及数据安全和隐私保护技术，与区块链结合的相关研究虽然于 2018 年出现但快速上升成为 2019 年至 2022 年最热的研究主题。

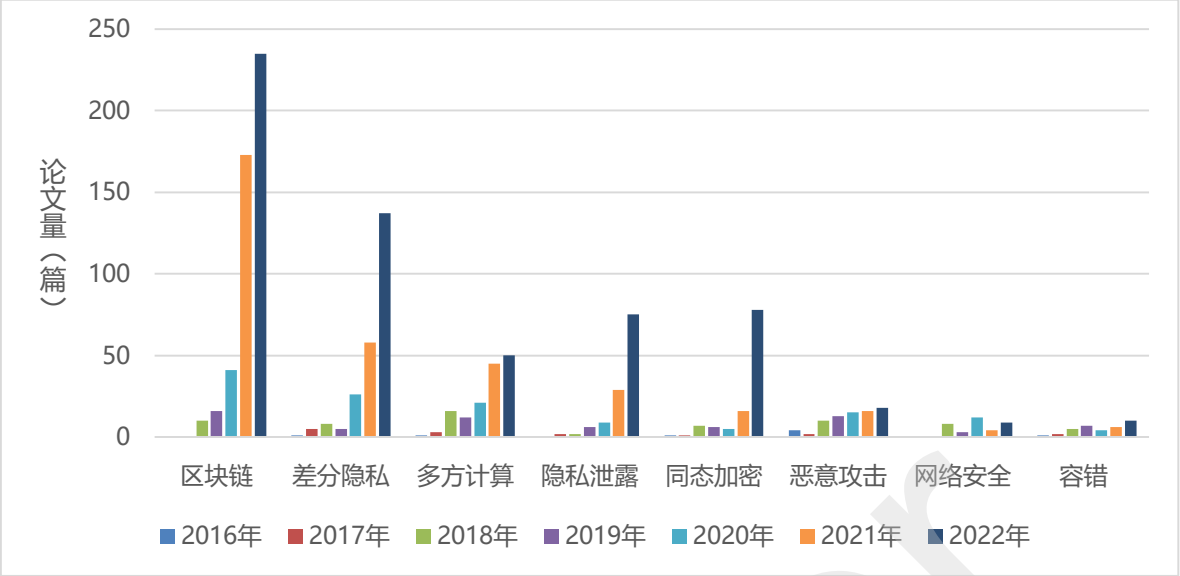


图 7 联邦学习安全隐私方面的研究热点趋势（2016–2022 年）

3.1.2 高被引论文分析

根据联邦学习领域论文被引用量进行排序，选取了排名前 3%的论文作为具有重大学术影响的高被引论文进行相关的作者及其所隶属机构与国家等特征分析。数据显示，本期联邦学习领域高被引论文的最低被引次数是 182 次，比上期高被引论文最低被引次数提升 52%，反映出该领域论文的整体学术影响力大幅提升。

考虑到在科研实践中，一篇论文通常由来自不同国家或不同机构的几名作者共同合作完成，本报告采用以第一作者所属国家和机构的方法进行统计。统计分析得到以下相关发现。

1． 六成以上高被引论文来自中美两国

根据论文第一作者所在机构的所属国家进行统计分析，发现联邦学习的近年来高被引论文发表主要是来自于美国和中国。其中，美国的高被引论文占 39.2%，较上期占比略升，保持全球首位；中国的高被引论文占 22%，虽仍居于全球第二位，但数量比上期下降了近 4 个百分点；澳大利亚、英国也拥有一定数量的高被引论文；新加坡、德国、韩国、加拿大与其

余国家所发表高被引论文的占比均低于 5%，详细信息如图 8 所示。

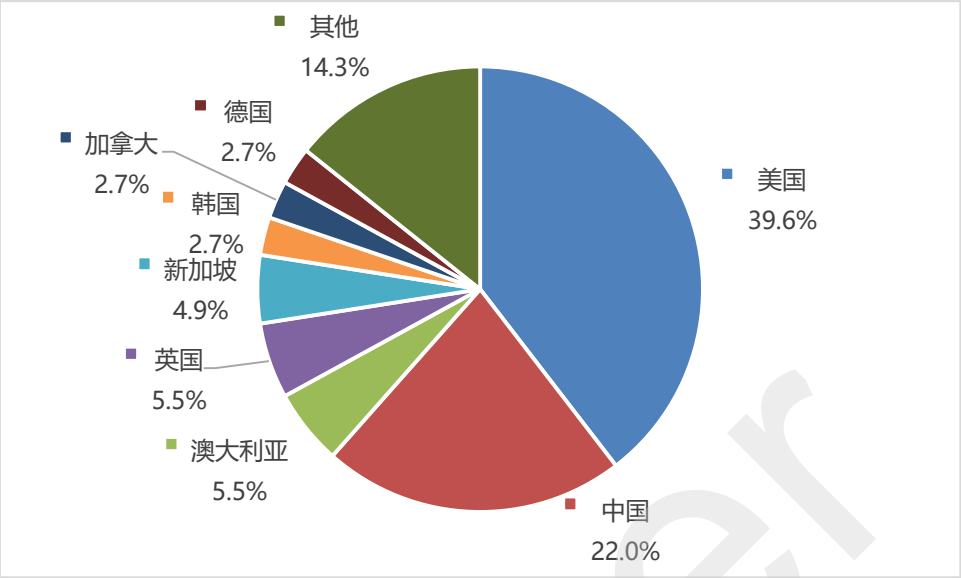


图 8 联邦学习高被论文国家分布（2016–2022 年）

2. 美国的论文被引用量全球显著领先

联邦学习相关论文总引用量 TOP 10 国家是美国、中国、德国、英国、新加坡、澳大利亚、印度、瑞士、加拿大和韩国，具体信息如图 9 所示。美国、中国已经连续三年稳居全球前两名。本期，美国的论文总被引用量仍明显高于其他国家，并较上期增长 2.3 倍，仍占据榜首；中国的论文被引用量较上期增长近 2 倍，保持第二位置。瑞士、加拿大和韩国是本期新进入前十的国家，上期居于前十的日本、以色列和波兰本期未能进入前十。

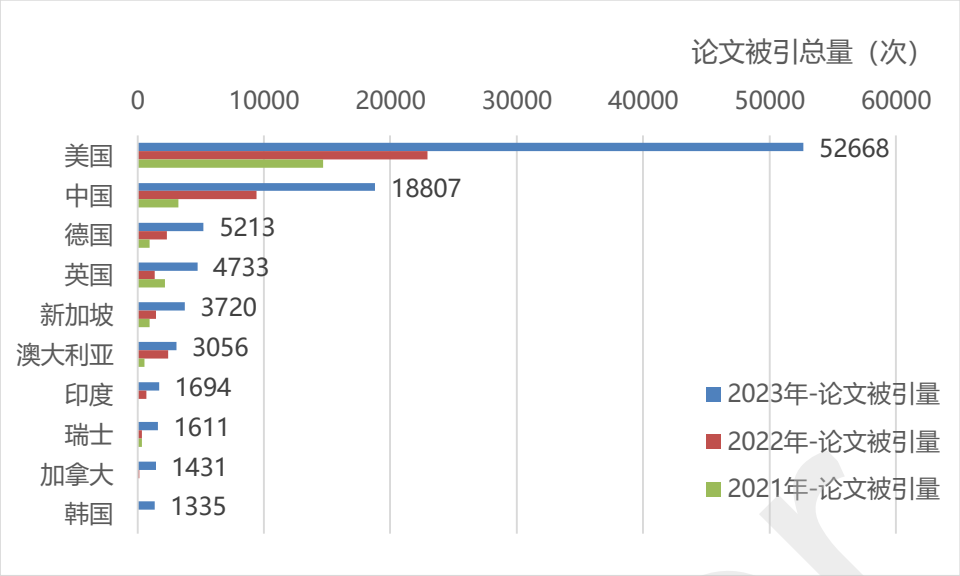


图 9 联邦学习论文引用量 TOP 10 国家（2016-2022 年）

从领先国家来看，美国联邦学习被引用量最高的论文是谷歌公司研究科学家 H. Brendan Mcmahan 作为一作发表的论文 *Communication-efficient learning of deep networks from decentralized data*[38]，该论文于 2016 年发表于 ArXiv e-prints (2016): arXiv-1602，并在 2017 年收录于 AISTATS (International Conference on Artificial Intelligence and Statistics)，目前其被引用 9226 次[39]。中国联邦学习总体论文引用量居于第二，其中被引用最高的论文是香港科技大学计算机科学与工程学系教授杨强为第一作者与微众银行 AI 部门、北京航空航天大学计算机学院的研究人员联合发表的 *Federated Machine Learning: Concept and Applications*[40]，该文被引用量 3856 次[41]。

38 McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and Statistics (pp. 1273-1282). PMLR..

39 引用量数据统计截止到 2023 年 3 月 31 日。

40 Yang, Q. , Liu, Y. , Chen, T. , & Tong, Y. . (2019). Federated Machine Learning: Concept and Applications. ACM Trans. Intell. Syst. Technol. 10, 2, Article 12, February, 2019. DOI:https://doi.org/10.1145/3298981

41 论文的被引用量数据统计截止到 2023 年 3 月 31 日。

3. 谷歌拥有最多数量的高被引论文

根据论文第一作者所属机构进行排序分析，发现从全球范围来看，联邦学习领域高被引论文来自全球 100 多家机构。入选 3 篇以上高被引论文的机构共计 11 家机构，详细分布情况如图 10 所示。其中，有两家企业、九家大学或研究所；美国机构四家，中国机构四家，另外三家分别来自澳大利亚、韩国和新加坡。其余机构的高被引论文量均在 3 篇以下。

谷歌的联邦学习高被引论文不仅入选数量最多，有 11 篇，而且相关论文的总被引用量也遥遥领先于其他机构，达 2 万多次；卡内基·梅隆大学的高被引论文数量居于第二，有 7 篇；新加坡的南洋理工大学有 6 篇，位于第三。中国的北京邮电大学、香港科技大学、中山大学以及深圳市大数据研究院也各有 3 篇以上入选。

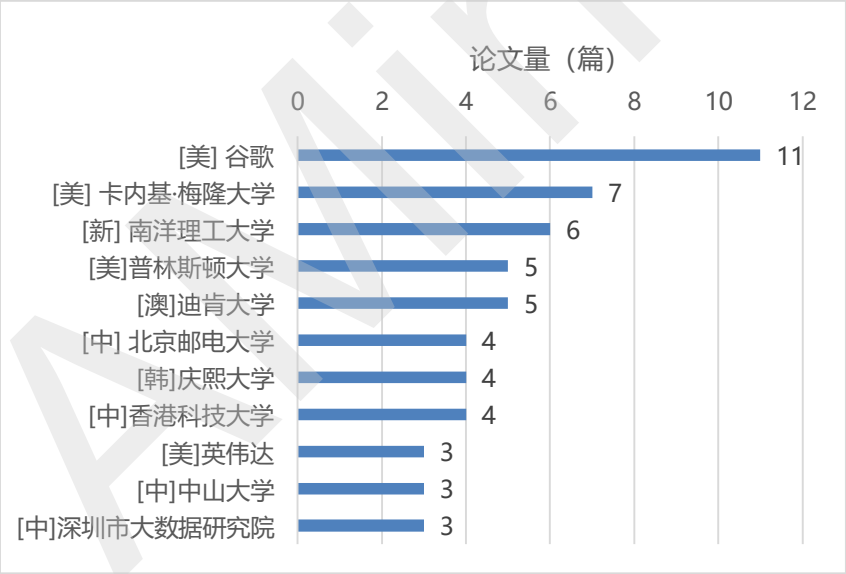


图 10 联邦学习高被引论文量 3 篇及以上的机构（2016–2022 年）

4. 联邦学习十大算法

通过对 2016 年至 2022 年底所发表的涉及联邦学习算法的论文进行引用量排序（去除

高引综述论文），选出了引用量大于 100 的前十大算法相关论文，包括 8 篇横向、2 篇纵向的联邦学习场景。这些算法及具体信息按照相关论文引用量排序显示如表 1 所示。

表 1 联邦学习十大算法

算法名	主要研究问题	联邦学习场景	论文标题	被引用量（次）
Federated Averaging（FedAvg）	Aggregation	横向联邦学习	*Communication-Efficient Learning of Deep Networks from Decentralized Data*	9226
Secure Aggregation	Security, Aggregation	横向联邦学习	*Practical Secure Aggregation for Privacy-preserving Machine Learning*	2015
Federated Stochastic Variance Reduced Gradient (FedSVRG)	Communication-efficient Data heterogeneity	横向联邦学习	*Federated Optimization: Distributed Machine Learning for On-device Intelligence*	1471
MOCHA	Communication-efficient Data heterogeneity	横向联邦学习	*Federated Multi-Task Learning*	1396
FedProx	Data heterogeneity System heterogeneity	横向联邦学习	*Federated Optimization in Heterogeneous Networks*	2357
Federated Learning with Client Selection (FedCS)	System heterogeneity	横向联邦学习	*Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge*	983

SCAFFOLD	Data heterogeneity	横向联邦学习	*SCAFFOLD: Stochastic Controlled Averaging for Federated Learning*	1232
Agnostic Federated Learning (AFL)	Data heterogeneity	横向联邦学习	*Agnostic Federated Learning*	619
Secure Logistic Regression	Security, Aggregation	纵向联邦学习	*Private Federated Learning on Vertically Partitioned Data via Entity Resolution and Additively Homomorphic Encryption*	444
Lossless Privacy-preserving Tree-boosting Algorithm (SecureBoost)	Security Aggregation	纵向联邦学习	*SecureBoost: A Lossless Federated Learning Framework*	405

注：引用量数据统计截止到 2023 年 3 月 31 日。

5. 高被引论文 TOP10 解读

通过对 2016 年至 2022 年底所发表论文的引用量进行统计和排序，得到联邦学习领域高引论文 TOP10，如表 2 所示。其中，论文的被引用量数据统计截止到 2023 年 3 月 31 日。本部分将对这些论文进行解读。

表 2 联邦学习领域高引论文 TOP 10 （2016-2022 年）

排名	论文标题	作者	发表年份	被引用量（次）
1	*Communication-Efficient Learning of Deep Networks from*	McMahan, H. Brendan; Moore, Eider; Ramage,	2016 [42]	9226

42 该文最早发表在 ArXiv e-prints (2016): arXiv-1602，后于 2017 年被 International Conference on Artificial Intelligence and Statistics (AISTATS)收录。

排名	论文标题	作者	发表年份	被引用量（次）
	Decentralized Data	Daniel; …		
2	*Federated Machine Learning: Concept and Applications*	Yang, Qiang; Liu, Yang; Chen, Tianjian; …	2019	3856
3	*Federated learning: Strategies for improving communication efficiency*	J Konečný, HB McMahan, FX Yu, P Richtárik, AT Suresh, D Bacon	2016	3577
4	*Advances and Open Problems in Federated Learning*	Kairouz Peter;McMahan H. Brendan;Avent Brendan; …	2021	3321
5	*Federated Learning: Challenges, Methods, and Future Directions*	Li, Tian; Sahu, Anit Kumar; Talwalkar, Ameet; …	2020	2709
6	*Towards federated learning at scale: System design*	K Bonawitz, H Eichner, W Grieskamp, D Huba, A Ingerman, V Ivanov, …	2019	2019
7	*Practical Secure Aggregation for Privacy-Preserving Machine Learning*	Bonawitz, Keith; Ivanov, Vladimir; Kreuter, Ben; …	2017	2015
8	*Federated Learning with Non-IID Data*	Yue Zhao; Meng Li; Liangzhen Lai; Naveen Suda;Damon Civin;Vikas Chandra	2018	1578
9	*Federated optimization: Distributed machine learning for on-device intelligence*	J Konečný, HB McMahan, D Ramage, P Richtárik	2016	1471
10	*Federated Multi-Task Learning*	Virginia Smith , Chao-Kai Chiang , Maziar Sanjabi , Ameet Talwalkar	2017	1396

注：引用量数据统计截止到 2023 年 3 月 31 日。

- 论文标题：***Communication-Efficient Learning of Deep Networks from Decentralized Data***

作者： H. Brendan McMahan, Eide Moore r, Daniel Ramage, Seth Hampson； Blaise

Agüera y Arcas

发表期刊：International Conference on Artificial Intelligence and Statistics (AISTATS), 2017

论文地址：https://www.aminer.cn/pub/599c7cc1601a182cd27d4688/

论文摘要：

现代移动设备可以访问大量适合学习模型的数据，这反过来又可以大大改善设备上的用户体验。例如，语言模型可以改进语音识别和文本输入，图像模型可以自动选择好的照片。然而，这些丰富的数据通常是隐私敏感的、数量庞大的，或者两者兼而有之，这可能会妨碍使用传统方法登录到数据中心并在那里进行训练。由此，学者们提出一种替代方案，将训练数据分布在移动设备上，并通过聚合本地计算的更新来学习共享模型，并将这种分布式方法称为联邦学习。本文提出了一种基于迭代模型平均的深度网络联邦学习的实用方法，并进行了广泛的实证评估，考虑五种不同的模型架构和四个数据集。实验表明，该方法对不平衡和非 IID 数据分布具有鲁棒性，这是该设置的一个定义特征。通信成本是主要限制因素，与同步随机梯度下降相比，该方法显示所需的通信轮次减少 10-100 倍。

- 论文标题：***Federated Machine Learning: Concept and Applications***

作者：Qiang Yang, Yang Liu, Tianjian Chen, Yongxin Tong

发表期刊：ACM Transactions on Intelligent Systems and Technology，Article No.: 12pp 1–19，2019

论文地址：https://www.aminer.cn/pub/5c9f688c6558b90bfa34dcb4

论文摘要：

今天的人工智能仍然面临两大挑战。一是在大多数行业中，数据以孤岛的形式存在；另一个是加强数据隐私和安全。本文为这些挑战提出了一个可能的解决方案：安全联邦学习。

除了谷歌在 2016 年首次提出的联邦学习框架之外，本文还引入了一个全面的安全联邦学习框架，其中包括横向联邦学习、纵向联邦学习和联邦迁移学习。本文提供了联邦学习框架的定义、体系结构和应用程序，并提供了关于这个主题的现有工作全面调查。此外，还提出了在组织间建立基于联邦机制的数据网络，作为在不损害用户隐私的前提下实现知识共享的有效解决方案。

- 论文标题：***Federated Learning: Strategies for Improving Communication Efficiency***

作者：Jakub Konecný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon

发表期刊：arXiv: Machine Learning (cs.LG)，2018

论文地址：https://www.aminer.cn/pub/58437725ac44360f1082f72b/

论文摘要：

联邦学习是一种机器学习设置，其目标是训练高质量的集中式模型，同时训练数据仍然分布在具有不可靠且相对较慢的网络连接的大量客户端上。本文考虑针对此设定的学习算法，在每一轮中，每个客户端根据其本地数据独立计算当前模型的更新，并将此更新传达给中央服务器，在那里客户端更新被聚合以计算新的全局模型。此设定中的典型客户端是手机，通信效率是最重要的。本文提出了两种降低上行链路通信成本的方法：一个是结构化更新，直接从使用较少数量变量参数化的受限空间中学习更新，例如低秩或随机掩码；另一个是草图更新，学习完整的模型更新，然后在将其发送到服务器之前使用量化、随机旋转和子采样的组合对其进行压缩。在卷积网络和循环网络上的实验表明，本文所提出的方法可以将通信成本降低两个数量级。

- 论文标题：*Advances and Open Problems in Federated Learning*

作者：Peter Kairouz, H. Brendan McMahan, Brendan Avent, Aurelien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Keith Bonawitz, Zachary Charles, et al. 58 authors

发表期刊：Foundations and Trends® in Machine Learning, no. 1 ， 2021

论文地址：https://www.aminer.cn/pub/5df20fc53a55acbe6bfcc74f/

论文摘要：

联邦学习是一种机器学习设定，许多客户端（例如移动设备或整个组织）在中央服务器（例如服务提供商）的编排下协同训练一个模型，同时保持训练数据的分散。联邦学习体现了集中数据收集和最小化的原则，可以减轻许多由传统的、集中的机器学习和数据科学方法造成的系统性隐私风险和成本。本文讨论了最近的联邦学习研究进展，并提出了广泛的开放式问题和挑战。

- 论文标题：***Federated Learning: Challenges, Methods, and Future Directions***

作者：Tian Li, Anit Kumar Sahu, Ameet Talwalkar, Virginia Smith

发表期刊：IEEE Signal Processing Magazine, no. 3 ， pp: 50-60，2020

论文地址：https://www.aminer.cn/pub/5d5e6b9a3a55acfce79a16af/

论文摘要：

联邦学习涉及在远程设备或孤岛数据中心（如移动电话或医院）上训练统计模型，同时保持数据本地化。在异构和潜在的大规模网络中进行训练会带来新的挑战，需要从根本上背离大规模机器学习、分布式优化和隐私保护数据分析的标准方法。本文讨论了联邦学习的独特特征和挑战，提出了横向联邦学习、纵向联邦学习、联邦迁移学习的范式。提供了当前方法的广泛概述，并概述了与广泛的研究社区相关的几个未来工作方向。

- 论文标题：***Towards Federated Learning at Scale: System Design***

作者：Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloé Kiddon, Jakub Konecný, Stefano Mazzocchi, H. Brendan McMahan, Timon Van Overveldt, David Petrou, Daniel Ramage, Jason Roselander

发表期刊：Proceedings of Machine Learning and Systems Volume: 1, pp： 374-388，2019

论文地址：https://www.aminer.cn/pub/5cede10bda562983788eae06/

论文摘要：

联邦学习是一种分布式机器学习方法，可以在大量分散数据的语料库上进行模型训练。本文基于 TensorFlow 为移动设备领域的联邦学习构建了一个可扩展的生产系统，描述了由此产生的高级设计，勾勒出一些挑战及其解决方案，并涉及未解决的问题和未来的方向。

- 论文标题：***Practical Secure Aggregation for Privacy-Preserving Machine Learning***

作者：Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, Karn Seth

发表期刊： Computer and Communications Security pp： 1175-1191，2017

论文地址：https://www.aminer.cn/pub/5a260c2817c44a4ba8a23355/

论文摘要：

本论文设计了一种新颖、通信高效、故障稳健的协议，用于高维数据的安全聚合。该协议允许服务器以安全的方式（即无需了解每个用户的个人贡献）计算来自移动设备的大型用户持有数据向量的总和，并且可以用于（例如，在联邦学习设定中）聚合用户提供的深度神经网络模型更新。本文在诚实但好奇且活跃的对手设置中证明了该协议的安全性，并表明即使任意选择的用户子集随时退出，也能保持安全性。本文评估了该协议的效率，并通过复杂

性分析和具体实现表明，即使在大型数据集和客户端池上，其运行时和通信开销仍然很低。对于 16 位输入值，本文的协议以明文形式发送数据，为 210 个用户和 220 维向量提供 1.73 倍的通信扩展，并为 214 个用户和 224 维向量提供 1.98 倍扩展。

- 论文标题：***Federated Learning with Non-IID Data***

作者：Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, Vikas Chandra

发表期刊：arXiv:1806.00582 [cs.LG], 2018

论文地址：https://www.aminer.cn/pub/ 5c8e41884895d9cbc6d5faf8/

论文摘要：

该项工作重点关注当本地数据非独立同分布（Non-IID）时联邦学习的统计挑战。首先展示，对于为高度偏斜的 Non-IID 数据训练的神经网络，联合学习的准确性显著降低，高达 55%，其中每个客户端设备仅在一类数据上训练。进一步表明，这种精度下降可以用权重偏差来解释，权重偏差可以用每个设备上类别分布和种群分布之间的地球移动器距离（EMD）来量化。作为一种解决方案，该文提出了一种策略，通过创建在所有边缘设备之间全局共享的一小部分数据来改进 Non-IID 数据的训练。实验表明，对于只有 5%的全球共享数据的 CIFAR-10 数据集，准确率可以提高 30%。

- 论文标题：***Federated Optimization: Distributed Machine Learning for On-Device Intelligence***

作者：Jakub Konecný, H. Brendan McMahan, Daniel Ramage, Peter Richtárik

发表期刊：arXiv preprint arXiv:1610.02527 (2016).

论文地址：https://www.aminer.cn/pub/58437725ac44360f1082ff8b/

论文摘要：

本文为机器学习中的分布式优化引入一个新的、相关性越来越强的设置，其定义优化的

数据不均匀地分布在大量节点上。其目标是培养一个高质量的称为联邦优化的集中模型。在这种情况下，通信效率是最重要的，而最小化通信轮数是主要目标。当将培训数据保存在usersu0027 移动设备本地，而不是将其记录到数据中心进行培训时，就出现了一个激励的示例。在联合优化中，这些设备被用作计算节点，对本地数据执行计算，以更新全局模型。假设在网络中有非常多的设备——与给定服务的用户数量一样多，每个用户只拥有一小部分可用数据的。特别是，本文预计本地可用的数据点数量要比设备数量少得多。此外，由于不同的用户使用不同的模式生成数据，可以合理地假设没有任何设备具有总体分布的代表性样本。本文证明了现有的算法不适合这种设定，并提出了一种新的算法，它显示了稀疏凸问题，出现了令人鼓舞的实验结果。这项工作还为联邦优化方面的未来研究奠定了基础。

- 论文标题：***Federated Multi-Task Learning***

作者：Virginia Smith, Chao-Kai Chiang, Maziar Sanjabi, Ameet Talwalkar

发表期刊：Advances in Neural Information Processing Systems 30 (NIPS), 2017

论文地址：https://www.aminer.cn/pub/599c797f601a182cd264476f/

论文摘要：

联邦学习在通过分布式设备网络训练机器学习模型方面带来了新的统计和系统挑战。在这项实验中，本文展示了自然适合处理这种设置统计挑战的多任务学习，并提出了一种新颖的系统感知优化方法 MOCHA，它对实际系统问题具有鲁棒性。本文的方法和理论首次考虑了分布式多任务学习的高通信成本、滞后性和容错性问题。与联合设置中的替代方法相比，所得到的方法实现了显著加速，正如作者通过模拟真实世界联合数据集所证明的那样。

6. 中美两国论文合作数量全球最多

AMiner 发现，四成以上的高被引论文存在着跨国科研合作，涉及到 37 个国家。如图 11 所示，中国和美国合作的论文数量最多，高达 23 篇；其次是美国和英国、中国和新加坡，两者之间各分别有 18 篇、11 篇的合作论文；之后，中国和英国、美国和韩国之间都各有 9 篇合作论文；中国和澳大利亚、中国和加拿大之间都各有 6 篇合作论文。其他各国家之间虽有合作但大部分为 5 篇及以下。

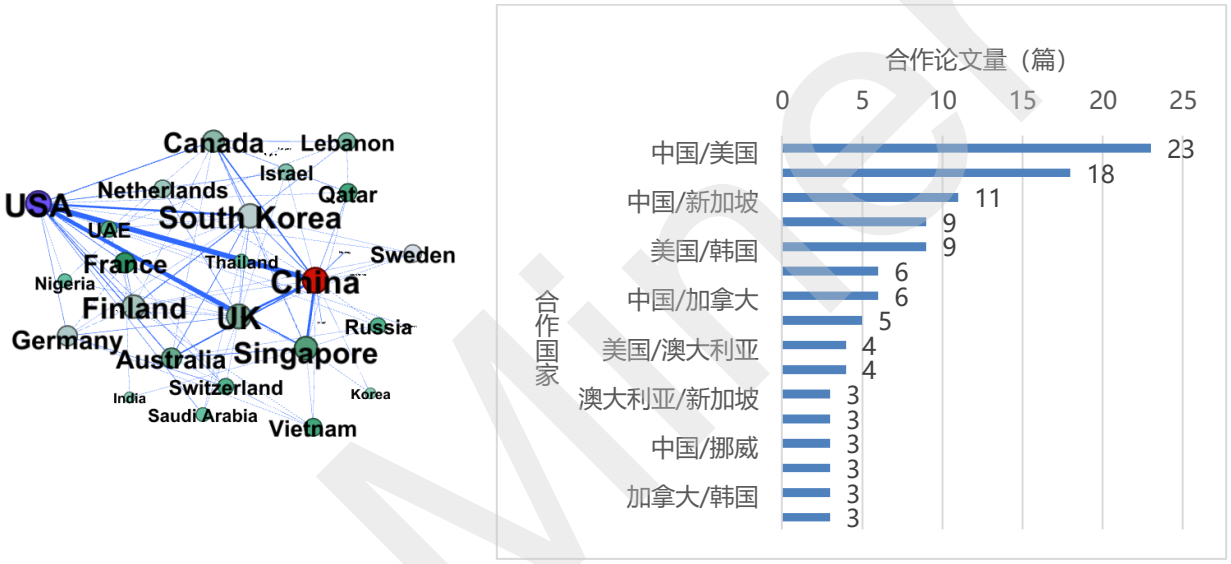


图 11 联邦学习高被引论文的国际合作 3 篇以上情况（2016–2022 年）

在中国的高被引论文之中，有 71.2%存在国际之间科研合作，涉及到 18 个国家。其中，有两篇中外合作论文涉及合作国家数量各多达 6 个。从中国在联邦学习领域所开展的国际合作情况看，美国是中国科研论文合作最多的国家，新加坡和英国也与中国开展了较多的合作，此外，中国还与澳大利亚、加拿大、挪威、韩国、日本等国进行过论文合作。中国与以上这些国家合作的高被引论文量较上期均有不同程度增加。

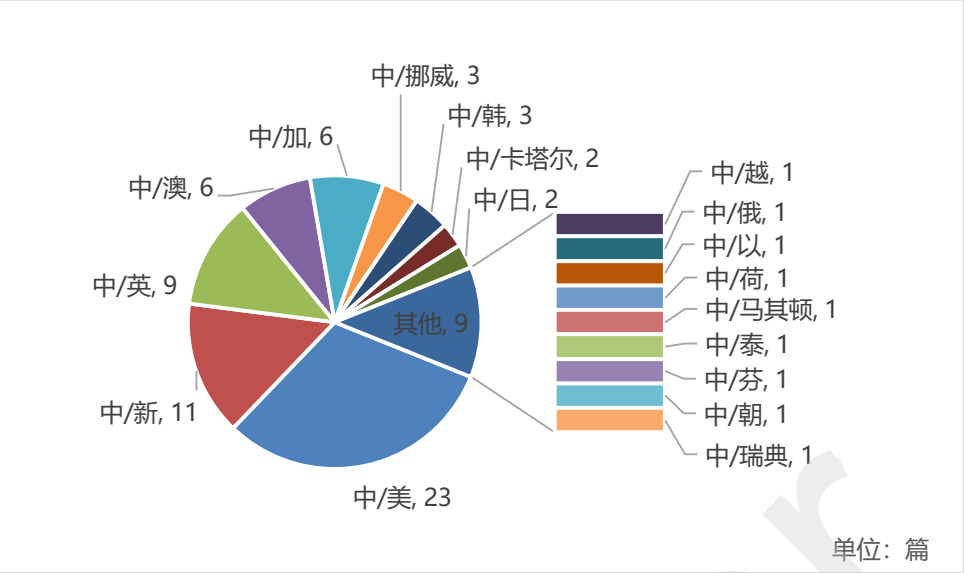


图 12 联邦学习高被引论文的中外合作情况（2016–2022 年）

7. 美英两国合作论文被引量全球领先

在各个国家之间合作发表的高被引论文之中，美国与英国合作论文引用量超越上期居于首位的美中合作论文被引情况，成为本期跨国合作论文被引量之首。美国与中国，以及新加坡与中国的合作论文被引用量依次居于第二、三位，详细情况如图 13 所示。由图可见，美国和英国、中国和美国的合作论文总引用量均超过万次，明显高于其他国家之间合作论文的学术影响力。从跨国合作的单篇论文被引用情况看，美国谷歌研究人员与沙特阿卜杜拉国王科技大学以及英国爱丁堡大学（苏格兰）学者等合作发表的论文 *Federated learning: Strategies for improving communication efficiency*[43]引用量最高，达 3577 次[44]。

43 Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). *Federated learning: Strategies for improving communication efficiency*. arXiv preprint arXiv:1610.05492.

44 论文的被引用量数据统计截至到 2023 年 3 月 31 日。

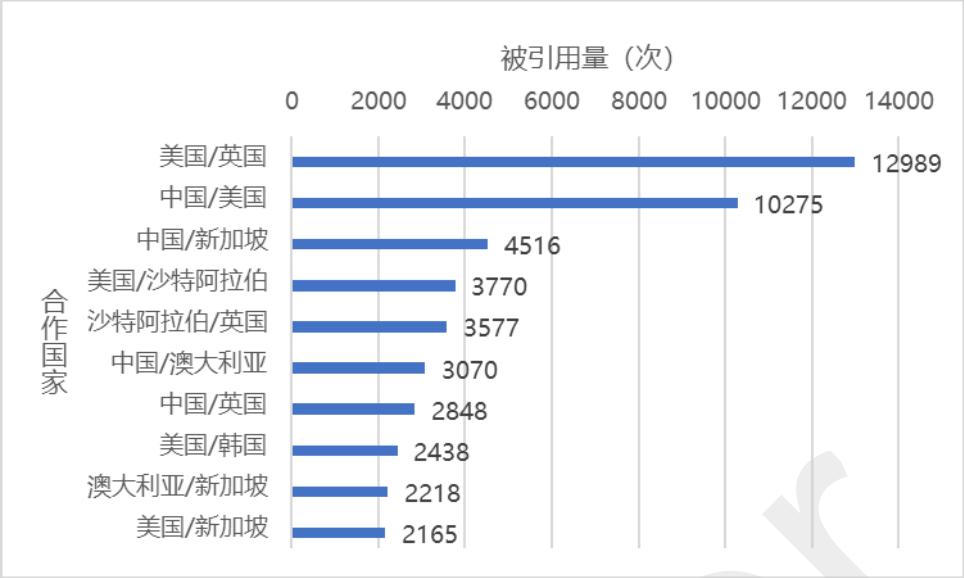


图 13 联邦学习国际合作论文的引用量 TOP10 国家组合（2016–2022 年）

8. 七成以上论文存在跨机构合作现象

国内外机构之间开展联邦学习论文合作较为常见。高被引论文中有 74.7%是通过机构之间合作发表的。在机构之间合作的论文之中，一篇论文合作机构数量少则两家、多则十几家，具体分布情况如图 14 所示。由图可见，由 2 家机构合作完成的论文占比最多，其次是由 3 家机构合作的论文占比。值得一提的是，合作机构数量最多的论文是 *The future of digital health with federated learning* [45]，该论文合作机构涵盖了来自德国的慕尼黑工业大学、德国癌症研究中心、海德堡大学医院，美国的宾夕法尼亚大学、范德比尔特大学、英特尔、国立卫生研究院，英国的伦敦帝国理工学院、伦敦国王学院、牛津大学、人工智能治理中心、OpenMined 和法国的奥金以及英伟达在各国的公司等共计 16 家机构。

45 Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H., Albarqouni, S., ... Maier-Hein, K. H. (2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1), 119–119.

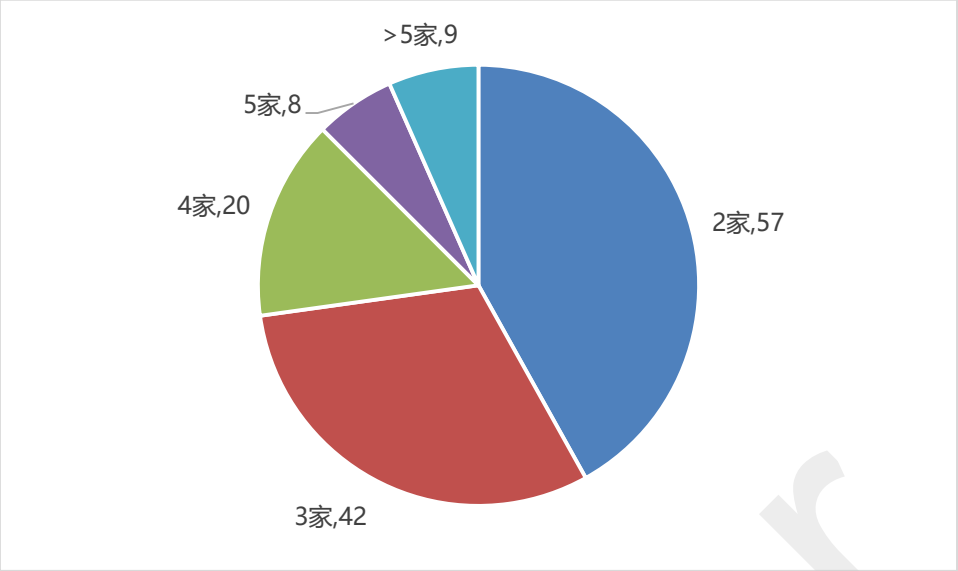


图 14 联邦学习合作论文的机构合作数量分布

9. 物联网期刊是发布高被引论文最多的渠道

从发布渠道看，2016-2022 年期间联邦学习的高被引论文发表在 80 多个期刊会议等渠道上。其中，有 13 个发行渠道（约占 15%）发布了 3 篇及以上高被引论文，如图 15 所示。由图 15 可知，高被引论文较多借助于发布在 ArXiv 渠道（由美国康奈尔大学运营维护的一个非盈利的数据库），有 22 篇；正式发布高被引论文最多的渠道是物联网领域顶级期刊 IEEE Internet of Things Journal，其次是人工智能领域国际学术会议——神经信息处理系统大会 NIPS （包括 workshop）以及 IEEE Transactions on Wireless Communications （IEEE TWC），分别各发布 11 篇、8 篇高被引论文。

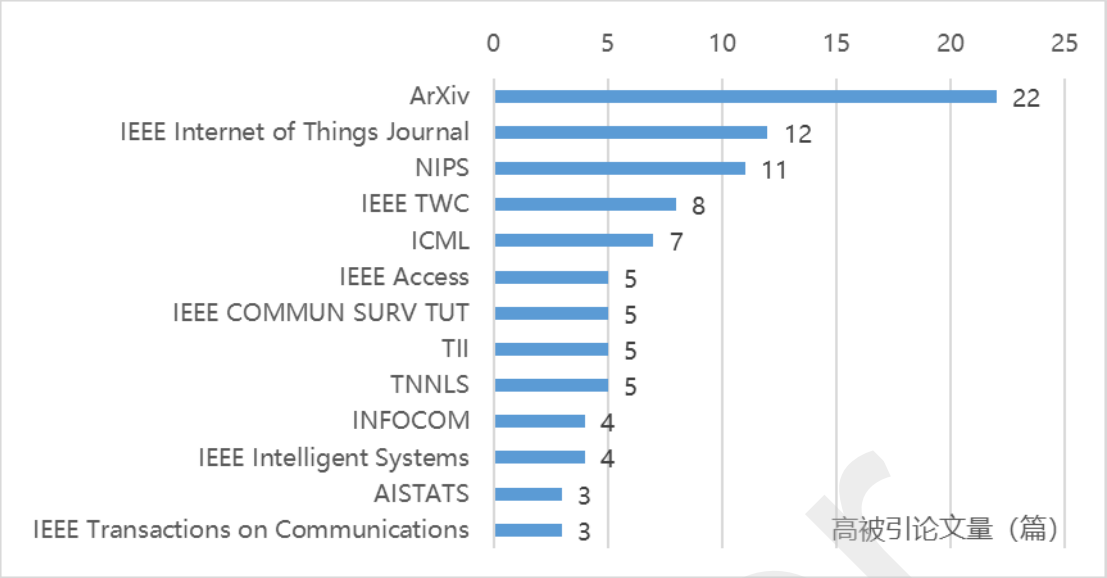


图 15 高被引论文的较多发布来源

ArXiv 上发表过的联邦学习最高引用论文是 2016 年的 *Federated Learning: Strategies for Improving Communication Efficiency*，该论文提出了结构化更新和草图更新这两种降低上行链路通信成本的方法，目标是利用联邦学习提高通信效率。发表在 IoT-J 上的最高被引论文是 2019 年的 *Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory*，该文提出了一种将声誉与契约理论相结合的有效激励机制，以激励具有高质量数据的高声誉移动设备参与模型学习。发表在 NeurIPS 上的最高被引论文是 *Federated Multi-Task Learning*，该论文发表于 2017 年，针对联邦学习在分布式设备网络上训练机器学习模型时统计和系统问题，提出了一种具有鲁棒性的系统感知优化方法 MOCHA。

10． 国际顶会相关论文收录量逐年增加

人工智能国际顶会（主会）所收录的联邦学习相关论文数量自 2019 年起呈现成倍增长趋势，如图 16 所示。2019 年仅 ICML、INFOCOM、IJCAI 三个会议收录了相关论文，共

计 6 篇。这些会议 2020 年收录联邦学习的论文量达 43 篇，2021 年收录相关论文量达 114 篇，2022 年收录联邦学习的论文量已达 185 篇。其中，联邦学习在 2019 年被收录论文最多的会议是 ICML，在 2020 年至 2022 年被收录论文最多的会议都是 NeurIPS，收录量分别是 17 篇、33 篇和 43 篇。

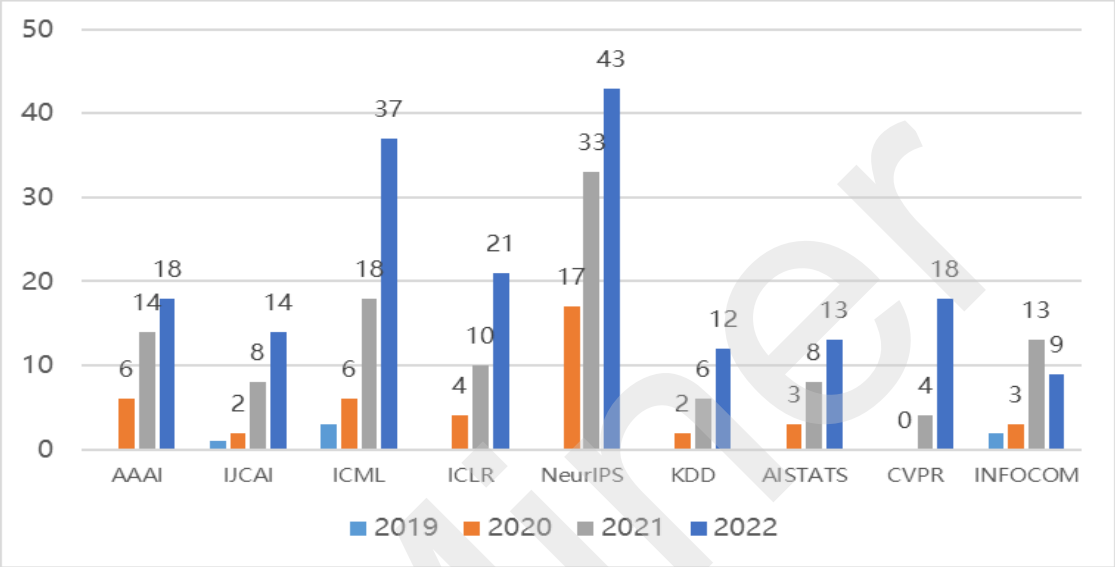


图 16 联邦学习国际顶会论文

3.1.3 联邦学习的特刊、书籍和综述

1. 特刊

据不完全统计，截至 2022 年底国内外关于联邦学习主题的特刊已出版的有十份，涉及到联邦学习技术及其在智能终端、网络安全、6G 等方面应用与挑战。这些特刊主题及出版方情况如表 3 所示。特刊的部分文章信息见附录三。

表 3 已出版的联邦学习主题的特刊

序号	特刊名称及链接	期刊（出版方）	影响因子/Citescore	已发表的论文量（篇）
1	*Special Issue on Federated Learning: Algorithms, Systems, and Applications*	ACM Transactions on Intelligent Systems and Technology, Volume 13, Issue 4-5	10.489/4.88	24
2	*Special Issue on Federated Learning for privacy preservation of Healthcare data in Internet of Medic*	IEEE Journal of Biomedical and Health Information, vol. 27, issue 2	7.021/10.2	23
3	*Special section on Enabling Blockchain and Federated Learning for Smart Services in Beyond 5G/6G Networks*	Computer Networks [46] (Elsevier)	4.474 / 8.1	7
4	*Special Issue on Federated Learning for Decentralized Cybersecurity Computers & Security*	Computers & Security [47] (Elsevier)	4.438 / 8.5	2
5	*Special Issue on Federated Machine Learning*	IEEE INTELLIGENT SYSTEMS [48] ((Volume: 35, Issue: 4, July-Aug. 1 2020)	3.405 / 9	10
6	*Special Issue "Federated and Transfer Learning Applications"*	Applied Sciences 2023, 13(9) (MDPI)	2.838/3.7	11
7	*Special Issue "Federated Learning: Challenges, Applications and Future"*	Electronics [49] (MDPI)	2.390 / 2.7	3
8	*Special Issue on AI-Based Federated Learning for 6G Mobile Networks*	Wireless Communications &	2.336 / 4.300	13

46 Aims and scope - Computer Networks | ScienceDirect.com by Elsevier

47 COSE | Computers & Security | Journal | ScienceDirect.com by Elsevier

48 https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9670

49 Electronics | An Open Access Journal from MDPI

序号	特刊名称及链接	期刊（出版方）	影响因子/Citescore	已发表的论文量（篇）
		Mobile Computing [50] (WILEY & Hindawi)		
9	*Special Issue Federated Learning-Enabled Lightweight Computing and Privacy-Preserving for AIoT*	Security and Communication Networks, Volume 2023 (Hindawi)	1.968/4.2	1
10	*Special Issue "Commemorative Special Issue: Adversarial and Federated Machine Learning: State of the Art and New Perspectives"*	Algorithms 2022, 15(8) (MDPI)	0.515/3.3	4

此外，还有六份特刊近期待截稿，如表 4 所示。

表 4 待发表的联邦学习特刊一览

序号	特刊名称及链接	期刊	截稿日期
1	***Special Issue*** *on Trustworthy Federated Learning*	IEEE Transactions on Neural Networks and Learning Systems (TNNLS)	6 月 1 日 2023
2	***Special Issue*** *"Advancements in Deep Learning and Deep Federated Learning Models"*	Big Data and Cognitive Computing	7 月 31 日 2023
3	***Special Issue*** *"Federated Learning: Applications and Future Directions"*	Journal of Sensor and Actuator Networks	8 月 15 日 2023
4	***Special Issue*** *on Federated Learning for Big Data Applications*	IEEE Transaction on Big Data	9 月 1 日 2023
5	***Special Issue****: Federated Learning Systems for Industrial Internet of Things and Blockchain: Trends and Challenges*	Human-Centric Intelligent Systems	9 月 30 日 2023
6	***Special Issue*** *on Federated Learning on*	Future Generation Computer	11 月 1 日

[50] AI-Based Federated Learning for 6G Mobile Networks | Hindawi

序号	特刊名称及链接	期刊	截稿日期
	the Edge: Challenges and Future Directions	Systems	2023

注：数据信息截至 2023 年 3 月 31 日。

2. 书籍

本报告重点推荐七本联邦学习领域的代表书籍，其中包括两本英文图书、五本中文图书。按照出版时间，相关书籍介绍如下。

书名-1	Federated Learning：Privacy and Incentive
作者	Qiang Yang, Lixin Fan, Han Yu
出版社	Springer International Publishing, Switzerland
出版时间	2020 年 第 1 版
正文语种	英文
ISBN	9783030630768
该书对联邦学习进行了全面而自成一体的介绍，从基础知识和理论到各种关键应用，隐私和激励因素是全书的重点。该书包含三个主要部分：首先，它引入了不同的隐私保护方法来保护联邦学习模型免受不同类型的攻击，例如数据泄漏和/或数据中毒；其次，介绍了旨在鼓励个人参与联邦学习生态系统的激励机制；三是描述了联邦学习如何在工业和商业中应用，以解决数据孤岛和隐私保护问题。	

书名-2	联邦学习 Federated Learning
作者	杨强，刘洋，程勇，康焱，陈天健，于涵
出版社	电子工业出版社
出版时间	2020-04-01 第 1 版
正文语种	中文
ISBN	9787121385223
该书是首部全面和系统论述联邦学习的中文著作。该书阐述了联邦学习的定义、分类和发展历程，并且介绍了与联邦学习紧密相关的基础知识，比如分布式机器学习和隐私保护技术。该书对联邦学习的每一分类，即横向联邦学习、纵向联邦学习和联邦迁移学习，所涉及的架构和算法进行了详尽的介绍。同时，该书也讨论了联邦强化	

学习，联邦学习的激励机制和应用实例。该书适合作为读者入门和探究联邦学习的第一本书。

书名-3	联邦学习技术及实战
作者	彭南博，王虎 等
出版社	电子工业出版社
出版时间	2021-03-01 第 1 版
正文语种	中文
ISBN	9787121405976
该书由京东科技集团有着多年联邦学习实战经验的工程人员合作编写，内容包括联邦学习基础、具体的联邦学习算法、联邦学习的产业应用和展望三个大部分，并给出较多案例。该书针对产业界在智能化过程中普遍面临的数据不足问题，详细地阐述了联邦学习如何帮助企业引入更多数据、提升机器学习模型效果。该书广泛介绍了联邦学习技术的实战经验，主要内容包括隐私保护、机器学习等基础知识，联邦求交、联邦特征工程算法，以及工程架构、产业案例、数据资产定价等。	

书名-4	联邦学习实战
作者	杨强，黄安埠，刘洋，陈天健
出版社	电子工业出版社
出版时间	2021-05-01 第 1 版
正文语种	中文
ISBN	9787121407925
该书是微众银行联邦学习团队在该领域的第二本专著。相较于第一本以理论和概述为主，该书以实战为主，兼顾对理论知识的系统总结。该书在联邦学习的理论知识基础上，主要介绍如何使用 Python 和 FATE 进行联邦学习建模，包括大量联邦学习的案例分析，筛选了经典案例进行讲解，部分案例用 Python 代码实现，部分案例采用 FATE 实现。此外，介绍了联邦学习相关的高级知识点，包括联邦学习的架构和训练的加速方法等。该书适合对联邦学习和隐私保护感兴趣的高校研究者和企业研发人	

员阅读。

书名-5	深入浅出联邦学习：原理与实践
作者	王健宗，李泽远，何安珣
出版社	机械工业出版社
出版时间	2021-05-01
正文语种	中文
ISBN	9787111679592
该书从理论与实践的双重维度对联邦学习进行了阐述，提供了可动手实践的源码案例，也分享了作者对联邦学习发展趋势的洞察和思考。全书分为四个部分。第一部分主要介绍了联邦学习的概念、由来、发展历史、架构思想、应用场景、优势、规范与标准、社区与生态等基础内容。第二部分详细讲解了联邦学习的工作原理、算法、加密机制、激励机制等核心技术。第三部分主要讲解了 PySyft、TFF、CrypTen 等主流联邦学习开源框架的部署实践，并给出了联邦学习在智慧金融、智慧医疗、智慧城市、物联网等领域的具体解决方案。第四部分概述了联邦学习的形态、联邦学习系统架构、当前面临的挑战等，并探讨了联邦学习的发展前景和趋势。	

书名-6	Federated and Transfer Learning
作者	Roozbeh Razavi-Far, Boyu Wang, Matthew E. Taylor, Qiang Yang
出版社	Springer Nature
出版时间	2022-09-30
正文语种	英文
ISBN	978-3-031-11747-3
该书汇集了从去中心化数据中学习、将信息从某领域转移到另一领域、解决了关于改善联邦学习的隐私和激励因素及其与转移学习和强化学习联系的理论问题等最新研究。该书适合于在应用联邦学习和迁移学习来解决不同类型现实世界问题的学生和学者，以及人工智能业、自动驾驶汽车和网络物理系统的科学家、研究人员和从业者。	

书名-7	联邦学习原理与算法

作者	耿佳辉　牟永利　李 青　容淳铭
出版社	机械工业出版社
出版时间	2023-06
正文语种	中文
ISBN	9787111728535
重点介绍了联邦学习计算机视觉及推荐系统等方面的应用，方便算法工程师拓展当前的算法框架，对金融、医疗、边缘计算、区块链等应用也做了详尽阐述。详细的代码以及对现有框架和开源项目的介绍是本书的一大特色。还提供了全部案例源代码下载和高清学习视频。该书受到三位院士推荐，属于国家出版基金项目。	

3. 综述

联邦学习自 2016 年提出以来，就吸引了学界和工业界的广泛兴趣。在联邦学习的各个领域如基础理论、系统设计方法、实施应用，面临的挑战和范式创新等都涌现了大量研究，相应地也产生了许多综述文章。这里我们基于综述的引用量和关注范围的多样性，选取了 9 篇综述进行介绍。详细信息如表 5 所示。

表 5 联邦学习综述性文章一览

序号	文章 Paper	范围 Scoping
1	*Federated Machine Learning: Concept and Application* [51]	General overview
	是联邦学习领域最早的综述，介绍了联邦学习的概念，分类，系统架构和涉及的主要技术方法。基于数据分布特点，该综述将联邦学习分为横向联邦学习，纵向联邦学习和联邦迁移学习，并列举了相关应用场景。此外，通过总结相关领域的论文，讨论了联邦学习与其它学习范式，如分布式学习，边缘计算和联邦数据库系统的关联和区别。	

[51] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," ArXiv190204885 Cs, Feb. 2019, Accessed: Jun. 16, 2021. [Online]. Available: http://arxiv.org/abs/1902.04885

序号	文章 Paper	范围 Scoping
2	*Advances and Open Problems in Federated Learning* [52]	General overview
	对联邦学习的理论和应用进行了系统和全面的介绍，涵盖了联邦学习的各个方面，包括定义，分类，效率和效能，数据隐私保护，攻击及故障的鲁棒性，参与方的公平性等，并重点探讨了联邦学习待解决的问题和面临的挑战，给研究员总结了联邦学习的研究方向。	
3	*Federated Learning: Challenges, Methods, and Future Directions* [53]	General overview
	主要讨论了联邦学习的特点及其相较于传统分布式计算面临的挑战，包括节点间的通信效率，系统的异构性，数据的不均匀性和隐私保护能力。通过深入分析这些问题提出了解决思路和未来研究方向。	
4	*A Survey on Federated Learning System: Vision, Hype and Reality for Data Privacy and Protection* [54]	System review
	作者主要从系统的角度对于联邦学习进行了归纳，分析和总结。首先，介绍了联邦学习系统的定义和系统组件。基于数据分布、机器学习模型、隐私保护技术、通信架构、系统规模和联邦的动机六个维度对现有联邦学习系统和方法进行了分类和研究总结，此外还探讨了联邦学习系统的设计方法、典型案例和未来的研究方向。	
5	*Federated Learning in Mobile Edge Networks: A Comprehensive Survey* [55]	mobile edge networks
	聚焦将联邦学习应用于移动端边缘计算。首先介绍了边缘计算的动机和如何与联	

52 P. Kairouz et al., "Advances and Open Problems in Federated Learning," ArXiv191204977 Cs Stat, Dec. 2019, Accessed: Aug. 10, 2020. [Online]. Available: http://arxiv.org/abs/1912.04977

53 T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/MSP.2020.2975749.

54 Q. Li et al., "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," ArXiv190709693 Cs Stat, Jan. 2021, Accessed: Jun. 16, 2021. [Online]. Available: http://arxiv.org/abs/1907.09693

55 W. Y. B. Lim et al., "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 2031–2063, thirdquarter 2020, doi: 10.1109/COMST.2020.2986024.

序号	文章 Paper	范围 Scoping
	邦学习结合进行联合模型训练。然后重点分析了基于联邦学习的边缘计算在通信成本、计算资源分配、数据隐私和数据安全方面所面临的挑战及未来研究方向。此外，介绍了联邦学习与边缘计算结合的一些应用和实现。	
6	*Threats to Federated Learning: A survey* [56]	Security and privacy
	从联邦学习系统的威胁模型及可能受到的攻击方式的角度进行了总结，主要聚焦会影响模型期望行为的“投毒”和“推断”攻击。	
7	*A Survey on Security and Privacy of Federated Learning* [57]	Security and privacy
	为研究员在联邦学习安全和隐私保护领域提供一个清晰的研究方向。该综述对联邦学习中所涉及的安全威胁和隐私隐患进行了全面的阐述，并且给出了可能降低这些安全威胁和隐私隐患的基本方法和可能带来的成本。	
8	*A Systematic Literature Review on Federated Machine Learning – From a Software Engineering Perspective* [58]	Software engineering perspective
	从软件工程的角度对联邦学习的研究进行了系统的分析和总结。该综述详细阐述了软件开发生命周期中的需求分析、背景理解、架构设计、系统实现和性能评估等各个环节所对应的联邦学习研究问题。	
9	*Federated Learning for Healthcare Informatics* [59]	Healthcare
	分析了联邦学习技术应用于医疗领域所面临的困难与挑战，并总结了现有的解决	

56 L. Lyu, H. Yu, and Q. Yang, “Threats to Federated Learning: A Survey,” ArXiv200302133 Cs Stat, Mar. 2020, Accessed: Jun. 16, 2021. [Online]. Available: http://arxiv.org/abs/2003.02133

57 V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, “A survey on security and privacy of federated learning,” Future Gener. Comput. Syst., vol. 115, pp. 619–640, Feb. 2021, doi: 10.1016/j.future.2020.10.007.

58 S. K. Lo, Q. Lu, C. Wang, H.-Y. Paik, and L. Zhu, “A Systematic Literature Review on Federated Machine Learning: From A Software Engineering Perspective,” ACM Comput. Surv., vol. 54, no. 5, pp. 1–39, Jun. 2021, doi: 10.1145/3450288.

59 Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, “Federated Learning for Healthcare Informatics,” ArXiv191106270 Cs, Aug. 2020, Accessed: Jun. 16, 2021. [Online]. Available: http://arxiv.org/abs/1911.06270

序号	文章 Paper	范围 Scoping
	方案。同时分享了联邦学习在医疗领域的应用场景。	

3.1.4 联邦学习研讨会最佳论文

一些人工智能国际学术顶会在年度会议举办期间，专门设立了联邦学习主题研讨会（workshop）并且评选出联邦学习领域最佳论文。2016 年至 2022 年期间人工智能顶会期间联邦学习专题研讨会的最佳论文共计发现 31 篇，它们来自包括 FL -NeurIPS、FL-IJCAI、FL-ICML 以及 FL -AAAI 四个顶会系列；此外，还有一篇来自阿里巴巴达摩院团队的论文因把图学习用在联邦学习上而获得 KDD 2022 应用科学方向“最佳论文奖”。

1． 七成以上最佳论文来自中美两国

基于论文一作的所属国家，发现联邦学习的最佳论文来自于美国、中国、瑞士、沙特阿拉伯、新加坡、韩国和法国七个国家，如图 17 所示。其中，美国的最佳论文有 13 篇，占 40.6%；中国的最佳论文有 12 篇，占 37.5%。中美两国合计占比达七成以上。

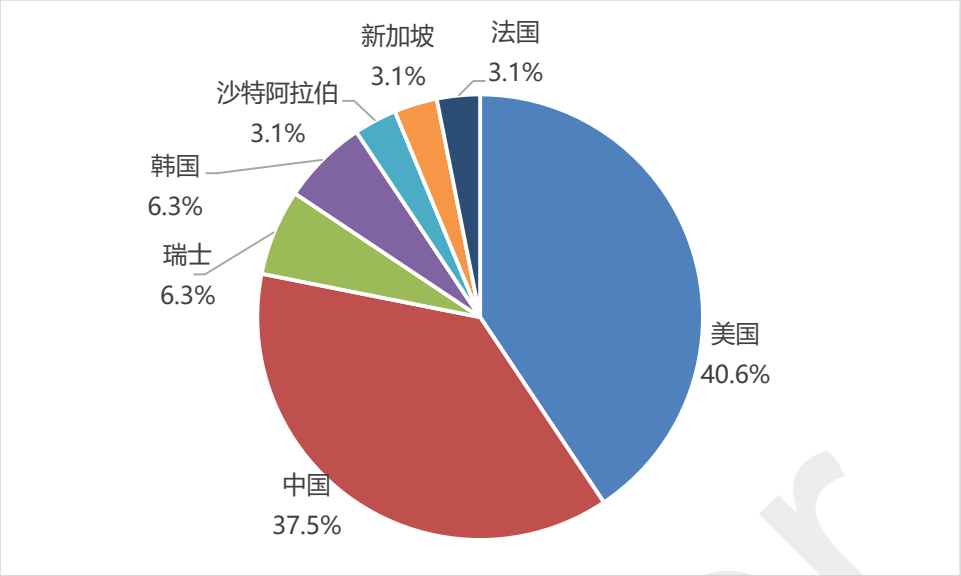


图 17 联邦学习 workshop 最佳论文国家分布

这些最佳论文的所有作者共计 130 位，来自美国、中国、瑞士、沙特阿拉伯、新加坡、韩国、俄罗斯、日本等 11 个国家的 50 多个不同机构，其中，有 6 位作者（Honglin Yuan，Junxue Zhang，Kai Chen，Tengyu Ma，Michael I. Jordan，Yiqiang Chen）参与了 2 篇最佳论文的研究。

2. 卡内基•梅隆和香港科大最佳论文量并列第一

从最佳论文一作的所在机构来看，美国的卡内基·梅隆大学（Carnegie Mellon University）与中国的香港科技大学（The Hong Kong University of Science and Technology)各分别获得 3 篇最佳论文,并列第一。美国的斯坦福大学(Stanford University)与伯克利大学（UC Berkeley）、瑞士的洛桑联邦理工（EPFL）以及中国的新奥集团 ENN 均分别获得 2 篇最佳论文，其余的 10 多家机构各自获得 1 篇最佳论文。

从最佳论文所有作者所在机构来看，中国的香港科技大学与 ENN 集团是出现最佳论文作者数量最多的机构，分别达 11 人次；其次为美国的卡内基·梅隆大学，出现最佳论文作者 10 人次；阿里巴巴与 IBM 依次出现 8 人次、7 人次的最佳论文作者；美国的伯克利大学

（University of California at Berkeley）和南加州大学，以及瑞士的 EPFL 这 3 家机构各出现 6 人次的最佳论文作者；美国的谷歌（Google）和斯坦福大学各出现 5 人次的最佳论文作者。具体信息如图 18 所示。

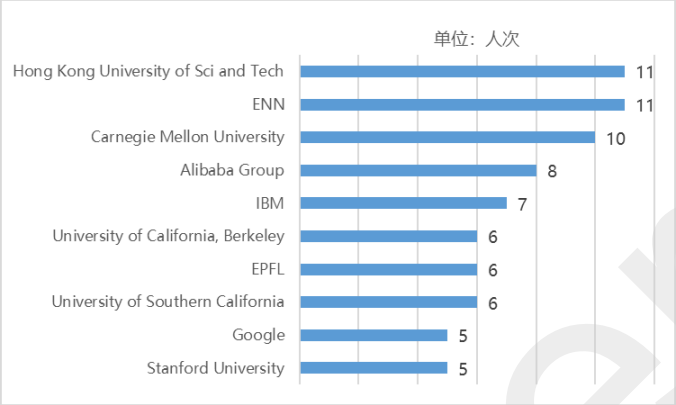


图 18 联邦学习 workshop 最佳论文作者数量 5 人次以上的机构分布

3. FL-IJCAI 获奖作者人次以中国居首，FL-NeurIPS 则以美国领先

FL-NeurIPS 与 FL-IJCAI 两个系列研讨会的获奖论文数量并列第一，分别评选出 12 篇最佳论文。所有这些最佳论文均是由多位作者合作完成的。FL-IJCAI 获奖论文相关作者共计 50 位，来自中国、新加坡、美国、瑞士、法国、韩国、澳大利亚、芬兰八个国家的 20 多个机构；FL-NeurIPS 获奖论文相关作者共计 45 位，来自美国、日本、中国、新加坡四个国家的 10 多个机构。

相比而言，中国作者在 FL-IJCAI 研讨会获奖论文中表现最突出，共计有 33 人次获奖，是美国作者在该研讨会获奖人次的 6 倍以上；美国作者则在 FL-NeurIPS 研讨会获奖论文中表现更突出，共计有 40 人次获奖。

其中，FL-NeurIPS 出现最佳论文作者次数最多的机构是美国的卡内基·梅隆大学（Carnegie Mellon University）（为 10 人次）。在 FL-IJCAI 系列 Workshop 中，出现

最佳论文作者次数最多的机构是中国的香港科技大学（The Hong Kong University of Science and Technology）（为 11 人次）。

FL-NeurIPS 与 FL-IJCAI 这两个研讨会评选的最佳论文具体信息如表 6 和表 7 所示。

表 6 FL-NeurIPS Workshop 最佳论文

Workshop 名称	序号	最佳论文标题	第一作者
FL-NeurIPS'22	1	*Conditional Moment Alignment for Improved Generalization in Federated Learning*	Jayanth Reddy Regatti (Ohio State University)
	2	*Mechanisms that Incentivize Data Sharing in Federated Learning*	Sai Praneeth Karimireddy (University of California, Berkeley)
FL-NeurIPS'21	1	*A Unified Framework to Understand Decentralized and Federated Optimization Algorithms: A Multi-Rate Feedback Control Perspective*	Xinwei Zhang (University of Minnesota)
	2	*Architecture Personalization in Resource-constrained Federated Learning*	Mi Luo (National University of Singapore)
	3	*Efficient and Private Federated Learning with Partially Trainable Networks*	Hakim Sidahmed (Google Research)
	4	*FLoRA: Single-shot Hyper-parameter Optimization for Federated Learning*	Yi Zhou (IBM Almaden Research Center)
	5	*Personalized Neural Architecture Search for Federated Learning*	Minh Hoang (Carnegie Mellon University)
	6	*Sharp Bounds for Federated Averaging (Local SGD) and Continuous Perspective*	Margalit R Glasgow (Stanford University)
FL-NeurIPS'19	1	*Private Federated Learning with Domain Adaptation*	Daniel Peterson（Oracle Labs）
	2	*FedMD: Heterogenous Federated Learning via Model Distillation*	Daliang Li（Harvard University）
	3	*Think Locally, Act Globally: Federated Learning with Local and Global Representations*	Paul Pu Liang（Carnegie Mellon University）

Workshop 名称	序号	最佳论文标题	第一作者
	4	*MATCHA: Speeding Up Decentralized SGD via Matching Decomposition Sampling*	Jianyu Wang (Carnegie Mellon University)

表 7 FTL-IJCAI Workshop 最佳论文

Workshop 名称	序号	最佳论文标题	第一作者
FL-IJCAI'22	1	*A General Theory for Client Sampling in Federated Learning*	Yann Fraboni (INRIA)
	2	*Visual Transformer Meets CutMix for Improved Accuracy, Communication Efficiency, and Data Privacy in Split Learning*	Sihun Baek (Yonsei University)
	3	*MetaFed: Federated Learning among Federations with Cyclic Knowledge Distillation for Personalized Healthcare*	Yiqiang Chen (Beijing Key Lab. of Mobile Computing and Pervasive Devices)
	4	*Cluster-driven Personalized Federated Learning for Natural Gas Load Forecasting*	Shubao Zhao (ENN)
FTL-IJCAI'21	1	*Robust Federated Learning with Attack-Adaptive Aggregation*	Ching Pui Wan (The Hong Kong University of Science and Technology)
	2	*A Contract Theory based Incentive Mechanism for Federated Learning*	Mengmeng Tian (Northeastern University, China)
	3	*Aegis: A Trusted, Automatic and Accurate Verification Framework for Vertical Federated Learning*	Cengguang Zhang (Hong Kong University of Science and Technology)
	4	*Learning Transferable Features With Deep Adaptation Networks*	Mingsheng Long (Tsinghua University & University of California)
FL-IJCAI'19	1	*Preserving User Privacy For Machine Learning: Local Differential Privacy or Federated Machine Learning?*	Huadi Zheng (Hong Kong Polytechnic University)

Workshop 名称	序号	最佳论文标题	第一作者
	2	*FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare*	Yiqiang Chen（Institute of Computing Technology, CAS）
	3	*Quantifying the Performance of Federated Transfer Learning*	Qinghe Jing(Hong Kong University of Science and Technology)
	4	*Federated Generative Privacy*	Aleksei Triastcyn and Boi Faltings (Ecole Polytechnique Fed´ erale de Lausanne´ Lausanne, Switzerland)

4. FL-ICML 系列最佳论文作者次数最多的机构是瑞士 EPFL 与韩国 KAIST

在 FL-ICML 系列 Workshop 中，联邦学习最佳论文有四篇，出现在 2020 和 2021 年(2022 年没有组织相关主题的 workshop)，均是由多位作者合作完成。相关论文作者共计 14 位，来自瑞士、沙特阿拉伯、美国、韩国、俄罗斯五个国家六个机构。没有来自中国的机构获得该系列 Workshop 最佳论文。其中，出现最佳论文作者次数最多的机构是瑞士的 EPFL（洛桑联邦理工学院）与韩国的 KAIST（韩国科学技术高等研究院），各自分别为 4 人次；具体信息如表 8 所示。

表 8 FL-ICML Workshop 最佳论文

Workshop 名称	序号	最佳论文标题	作者
FL-ICML'21	1	*Optimal Model Averaging: Towards Personalized Collaborative Learning*	Felix Grimberg（EPFL），Mary-Anne Hartley（EPFL），Sai Praneeth Karimireddy（EPFL），Martin Jaggi（EPFL）
	2	*Lower Bounds and Optimal Algorithms for Smooth and Strongly Convex Decentralized Optimization over Time-Varying Networks*	Dmitry Kovalev（KAUST），Elnur Gasanov（KAUST），Peter Richtarik（KAUST），Alexander Gasnikov (MIPT & ISP RAS)

Workshop 名称	序号	最佳论文标题	作者
FL-ICML'20	1	*Federated Accelerated Stochastic Gradient Descent*	Honglin Yuan（Stanford University），Tengyu Ma（Stanford University）
	2	*Federated Semi-Supervised Learning with Inter-Client Consistency*	Wonyong Jeong（KAIST），Jaehong Yoon（KAIST），Eunho Yang（KAIST & AITRICS），Sung Ju Hwang（KAIST & AITRICS）

5. FL-AAAI 系列最佳论文作者半数以上为华人

顶会 AAAI 于 2022 年首次开设了联邦学习研讨会，其主题是 Trustable, Verifiable and Auditable Federated Learning，并评选出 3 篇最佳论文，具体信息如表 9 所示。该系列 Workshop 获奖论文均是由多位作者合作完成，共计 14 位作者，来自美国、中国、日本三个国家四个机构。其中，华人作者有 9 位，占比六成以上。

表 9 FL-AAAI Workshop 最佳论文

Workshop 名称	序号	最佳论文标题	作者
FL-AAAI-22	1	*GEAR: A Margin-based Federated Adversarial Training Approach*	Chen Chen（Zhejiang University），Jie Zhang (Zhejiang University)，Lingjuan Lyu（Sony AI）
	2	*WT-Shapley: Efficient and Effective Incentive Mechanism in Federated Learning for Intelligent Safety Inspection*	Chengyi Yang（ENN），Jia Liu（ENN），Hao Sun（ENN），Tongzhi Li（ENN），Zengxiang Li（ENN）
	3	*SSFL: Tackling Label Deficiency in Federated Learning via Personalized Self-Supervision*	Chaoyang He（University of Southern California，USC），Zhengyu Yang（USC），Erum Mushtaq（USC），Sunwoo Lee（USC），Mahdi Soltanolkotabi（USC），Salman Avestimehr（USC）

3.1.5 高被引论文作者的人才地图与画像

1. 全球高被引论文作者主要聚集在美国和中国

基于 AMiner 系统，通过关键词组[60]在标题和摘要中检索 2016 年至 2022 年联邦学习相关论文数据，然后根据联邦学习领域论文被引用量进行排序，选取了排名前 3%的论文作为具有重大学术影响的高被引论文。对这些高被引论文进行数据挖掘而获取论文作者信息，通过命名消歧和信息抽取等大数据分析和挖掘技术，进行作者画像和人才相关分析。此外，还抽取论文作者发表该论文时的供职机构和国家信息，对不同国家和机构的研究者进行统计和特征分析。

在研究时段内，联邦学习领域高被引论文作者共计 898 位[61]，分布在亚洲、北美洲、欧洲以及大洋洲的 50 多个国家之中，所在国家分布如图 19 所示，从分布密度来看，这些学者主要聚集在东亚的中国（173 位）、新加坡（40 位），北美洲的美国（392 位）和欧洲的英国（44 位）、德国（29 位）等国家。

60 联邦学习关键词检索式：Federated Machine Learning OR Federated optimization OR federated learning OR federation learning OR (Privacy AND Distributed AND data mining) OR (Secure AND Distributed AND data mining) OR (Secure AND Multiparty) OR (Secure AND Multi-party) OR (privacy AND Multi-party) OR (privacy AND Multiparty) OR (Privacy AND Distributed AND machine learning) OR (Secure AND Distributed AND machine learning) OR (Privacy and joint learning) OR (Secure and joint learning) OR (Privacy AND Distributed AND deep learning) OR (Secure AND Distributed AND deep learning)

61 作者统计未去重，包含同一作者发表多篇高被引论文情况，下文同。

来源：AMiner 知因系统

图 19 联邦学习全球高被引论文作者位置分布（2016-2022 年）

2. 美国高被引论文学者量是中国的两倍以上

联邦学习高被引论文作者主要聚集在美国和中国，这两个国家拥有的学者数量分别为 392 位和 173 位，明显多于其他国家的学者数量，如图 20 所示。其他前十国家的学者数量的均不足百人。澳大利亚和英国的高被引论文作者数量并列第三。值得注意，美国的高被引论文作者数量全球最多，占全球四成以上，也是中国高被引论文作者数量的 2.3 倍。

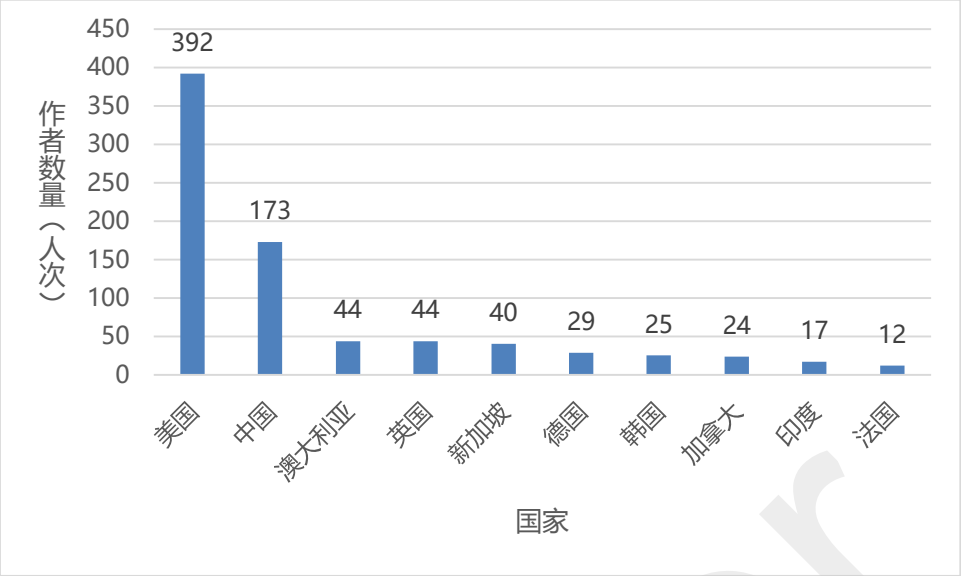


图 20 联邦学习高被引论文作者数量 TOP 10 国家（2016-2022 年）

3. 谷歌是高被引论文学者量最多的机构

基于对研究时段内相关高被引论文作者所供职机构信息的抽取分析，发现从全球范围来看，联邦学习领域高被引学者总量 TOP 10 机构之中，半数席位被美国机构占据，其余几家机构则来自中国、新加坡，其中，中国电子科技大学与英特尔公司并列第十，如图 21 所示。前十机构包括五家企业，分别是谷歌、IBM、英伟达、微众银行和英特尔；谷歌的高被引论文作者数量最多，其余各家机构的联邦学习领域研究学者数量在 10~20 位。

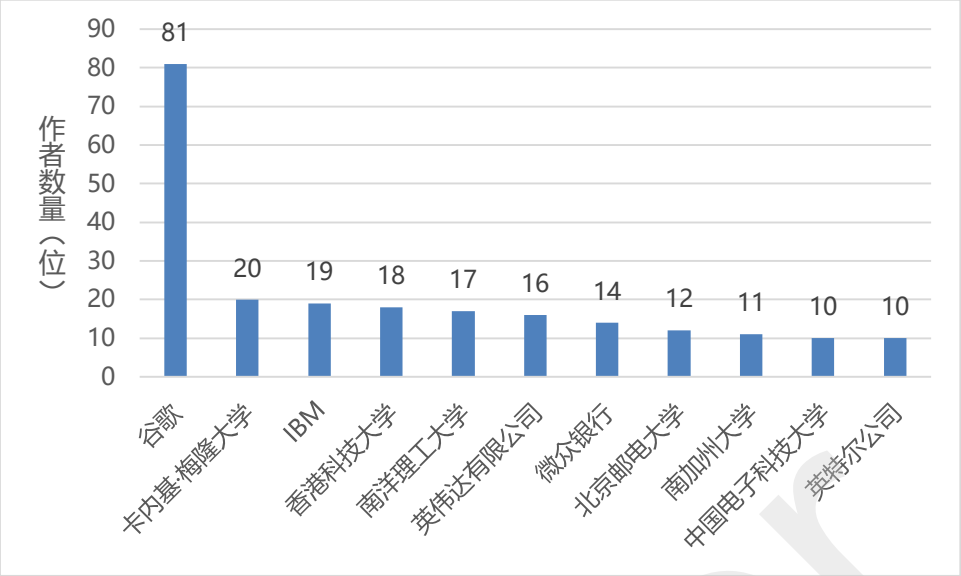


图 21 联邦学习领域高被引学者数量 TOP 10 机构（2016-2022 年）

4. 近三成高被引论文作者供职于企业

研究联邦学习的高被引论文作者之中，有 26.1%供职于企业，如图 22 所示。同时，如前文所述，高被引论文作者数量全球前十机构有约一半是企业，而且，谷歌的高被引论文作者数量最多。可见，在联邦学习领域，企业人才是一个不可忽视的研究群体。究其这种现象的原因，可能是由于联邦学习是一个起源于工业界且已落地于医疗、金融等应用场景的新技术，更是一个有活力、有前途的热门发展领域，工业界研究者有较多实践研究成果来发布。

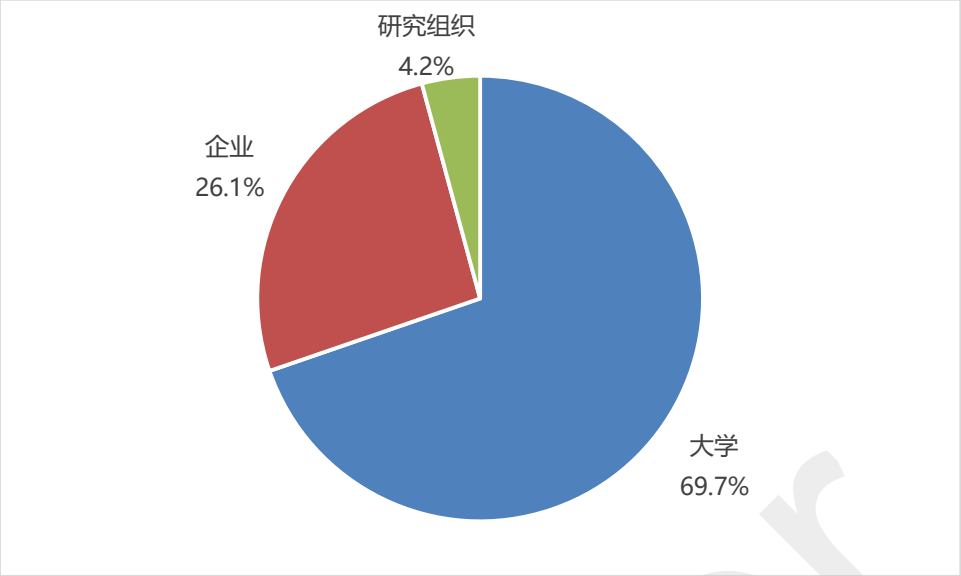


图 22 联邦学习高被引论文作者供职机构性质分布

5. 不同研究方向的代表学者画像

在 AMiner 学术搜索服务平台上，根据相关算法，通过对 AAAI、CCS、ICLR、ICML、IJCAI、NIPS、SP 等联邦学习领域顶尖学术会议近年来收录论文的挖掘，并结合热心网友的推荐和整理，筛选出了“联邦学习”主题领域 100 篇经典必读论文(简称 Topic 必读论文)。可以帮助用户快速了解该领域知识，从而提高学习效率。用户只需在检索框输入“Federated Learning”或中文“联邦学习”，就能看到联邦学习 TOPIC 页面（https://www.aminer.cn/topic/600e890992c7f9be21d74695），该页面中包括相关的简要概述和精选必读论文。每一篇必读论文由程序自动计算出了一句话内容概括作为“推荐理由”；必读论文列表支持按照发表年份、引用数、点赞数等进行排序，并在页面右侧，列出了相关作者的论文发表情况。

本部分简要介绍了联邦学习领域的代表性学者及其代表论文。其中，代表学者是指该学者的主要研究方向是联邦学习领域且其 H-index 值与至少 3 篇以上代表作论文的被引用量

均大于 30 [62]；学者的代表作论文则是指该学者在 2016-2022 年发表的引用量大于 30 [63] 的联邦学习相关的非综述论文，并且，该学者作为该篇论文的前两位作者或者通讯作者出现。限于报告篇幅，我们不能对所有学者逐一罗列，仅随机抽取了符合以上规则的部分学者作为展示，同时同一机构仅抽取一或两位以求尽量覆盖到更多不同机构的学者。最终所抽取的代表性学者按照其 H-index 值进行从高到低的顺序展示。如要获得更多学者信息，请查看网址 https://www.aminer.cn/ 获取更多联邦学习领域学者资料。

（1）联邦学习算法与理论方向

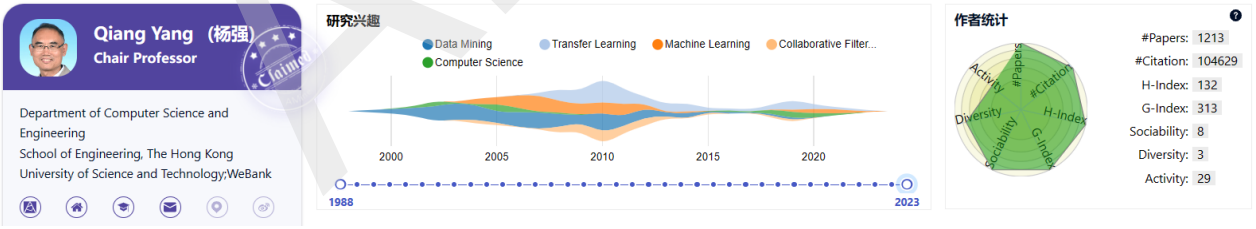
Qiang Yang（杨强）

香港科技大学 教授；微众银行 首席人工智能官

最高学位毕业院校：美国马里兰大学 博士

曾经任职：香港科技大学计算机与工程系主任、第四范式有限公司联合创始人、华为诺亚方舟研究实验室创始主任、加拿大 BC 省西蒙弗雷泽大学副教授/正教授、加拿大滑铁卢大学计算机科学助理/副教授等。

研究兴趣：人工智能、迁移学习、联邦学习、机器学习、数据挖掘



相关论文代表作：

62 H-index 值是基于 AMiner 数据库截至 2023 年 3 月 31 日的统计。

63 论文引用量数据统计截至到 2023 年 3 月 31 日。

序号	论文名称	论文地址	发表期刊/年份
1	*FedVision: An Online Visual Object Detection Platform Powered by Federated Learning*	https://www.aminer.cn/pub/5e257a973a55acdfeeb9ed85	AAAI, no. 08 (2020): 13172-13179
2	*A Fairness-aware Incentive Scheme for Federated Learning*	https://www.aminer.cn/pub/5e3e887a3a55ac6b075ba5a4	AIES, pp.393-399, (2020)
3	*FedBCD: A Communication-Efficient Collaborative Learning Framework for Distributed Features*	https://www.aminer.cn/pub/5f8d43449e795ea21af78f0a	arXiv preprint arXiv:1912.11187 (2019) / FL-NeurIPS 2019; IEEE Transactions on Signal Processing 2022
4	*A Secure Federated Transfer Learning Framework*	https://www.aminer.cn/pub/5ecbc8ab9fced0a24b522f2e/	IEEE Intelligent Systems, 35(4), 70-82.
5	*SecureBoost: A Lossless Federated Learning Framework*	https://www.aminer.cn/pub/5cede0ffda562983788df3f4/	IEEE Intelligent Systems (2021)
6	*Secure Federated Matrix Factorization*	https://www.aminer.cn/pub/5d06e46cda562926acc32de9/	IEEE Intelligent Systems (2020)
7	*Federated Machine Learning: Concept and Applications*	https://www.aminer.cn/pub/5c9f688c6558b90bfa34dcb4/	ACM Transactions on Intelligent Systems and Technology (TIST) 10.2 (2019): 1-19.
8	*Privacy-preserving Heterogeneous Federated Transfer Learning*	https://www.aminer.cn/pub/5dea0ee0930831239d97ec64/	2019 IEEE International Conference on Big Data (Big Data)

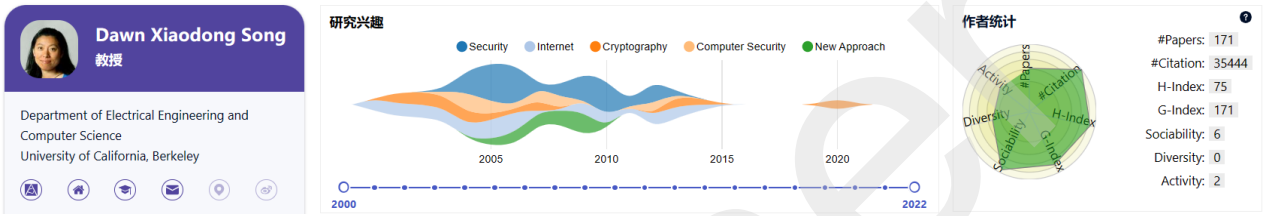
Dawn song（宋晓东）

加州大学伯克利分校电气工程与计算机科学系 教授

最高学位毕业院校：美国加州大学伯克利分校博士

曾经任职：卡内基·梅隆大学助理教授

研究兴趣：深度学习、区块链和去中心化系统，计算机安全、隐私和应用密码学，使用程序分析、算法设计和机器学习来确保安全和隐私。



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Epione: Lightweight Contact Tracing with Strong Privacy*	https://www.aminer.cn/pub/5ea9503e91e0118eb1e19f59/	IEEE Data Eng. Bull., no. 2 (2020): 95-107
2	*Keystone: An Open Framework for Architecting Trusted Execution Environments*	https://www.aminer.cn/pub/5e9c27d49fced0a24b1f07fe/	EuroSys '20: Fifteenth EuroSys Conference 2020 Heraklion Greece April, 2020, pp.1-16, (2020)
3	*The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Network*	https://www.aminer.cn/pub/5dd3bf513a55ac1bdd46d7e4/	CVPR, pp.250-258, (2019)
4	*The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Network*	https://www.aminer.cn/pub/5d70dfa83a55acf39f3e7f83/	USENIX Security Symposium, pp.267-284, (2019)
5	*Towards Pratical Differential Privacy for SQL Queries*	https://www.aminer.cn/pub/5a9cb64017c44a376ffb683a/	Proceedings of the Vldb Endowment, no. 5 (2018): 526-

			539
6	*Ekiden: A Platform for Confidentiality-preserving, Trustworthy, and Performant Smart Contracts*	https://www.aminer.cn/pub/5d67a2a73a55ac09fb007f8a/	EuroS&P, pp.185-200, (2019)
7	*Targeted Backdoor Attacks on Deep Learning System using Data Poisoning*	https://www.aminer.cn/pub/5a73cbc317c44a0b3035f0b8/	arXiv: Cryptography and Security, (2017)

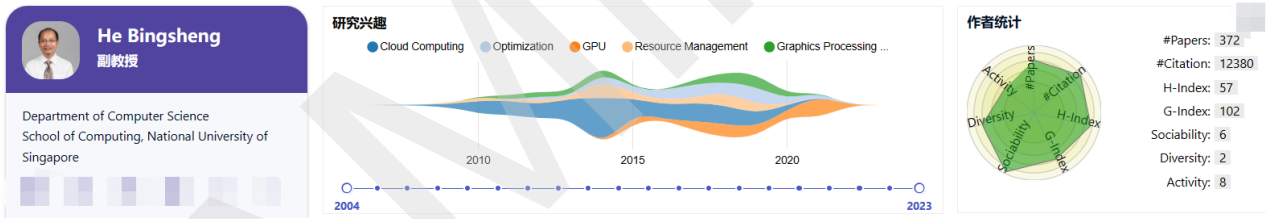
Bingsheng He

新加坡国立大学 副教授

最高学位毕业院校：香港科技大学 博士

曾经任职：南洋理工大学

研究兴趣：并行和分布式系统、云计算、高性能计算、数据库系统、大数据系统、GPGPU



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Federated Learning on Non-IID Data Silos: An Experimental Study*	https://www.aminer.cn/pub/601bc6bb91e011fcd67ef275/	ICDE 2022
2	*Model-Contrastive Federated Learning*	https://www.aminer.cn/pub/60645b1191e011538305d07d/	CVPR 2021
3	*Practical federated gradient boosting decision trees*	https://www.aminer.cn/pub/5e5e191893d709897ce4fa57/	*Proceedings of the AAAI Conference on Artificial Intelligence 34 (04), 4642-4649*

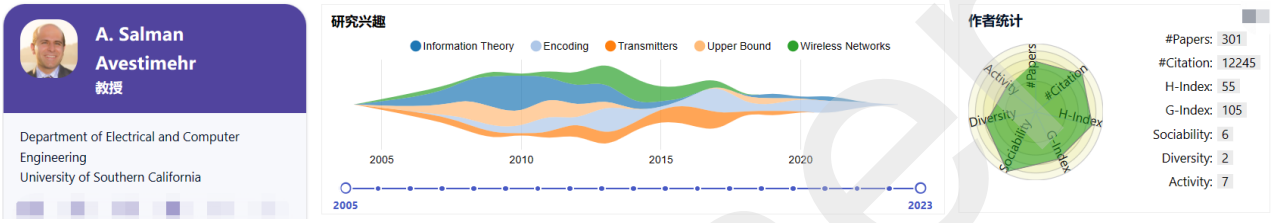
Salman Avestimehr

南加州大学 教授；FedML 首席执行官兼联合创始人

最高学位毕业院校：加州大学伯克利分校 博士

曾经任职：康奈尔大学助理教授、加州理工学院博士后

研究兴趣：信息论、机器学习、分布式计算、安全/隐私学习/计算、联邦学习



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*FedML: A Research Library and Benchmark for Federated Machine Learning*	https://www.aminer.cn/pub/5f2006a091e011d50a621c66/	*arXiv · Machine Learning (2020)*
2	*Group knowledge transfer: Federated learning of large cnns at the edge*	https://www.aminer.cn/pub/5f7fdd328de39f0828397e8d/	*Advances in Neural Information Processing Systems 33, 14068-14080*
3	*Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning*	https://www.aminer.cn/pub/5e43ccc23a55acdc32c30ff3/	*IEEE Journal on Selected Areas in Information Theory 2 (1), 479-489*

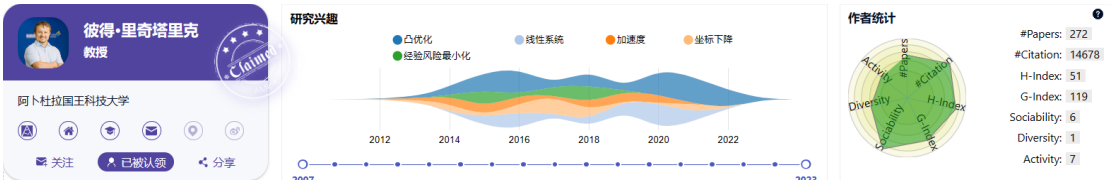
Peter Richtarik

阿卜杜拉国王科技大学 教授

最高学位毕业院校：康奈尔大学 博士

曾经任职：康奈尔大学 研究与教学助理，鲁汶天主教大学博士后，加州大学伯克利分校客座助理教授，爱丁堡大学 数学副教授，斯科国立大学物理与技术学院客座教授

研究兴趣：优化、机器学习、联邦学习、深度学习



相关论文代表作：

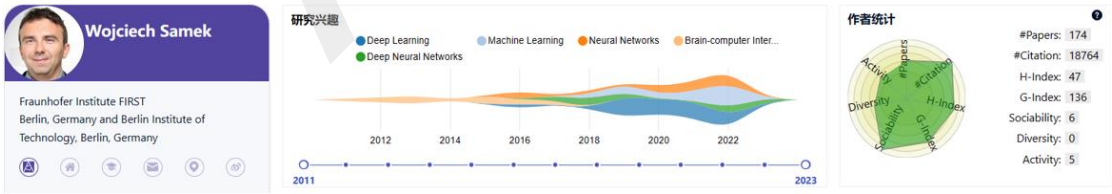
序号	论文名称	论文地址	发表期刊/年份
1	*Federated Optimization: Distributed Machine Learning for On-Device Intelligence*	https://www.aminer.cn/pub/58437725ac44360f1082ff8b/	arXiv preprint arXiv:1610.02527
2	*Federated Learning of a Mixture of Global and Local Models*	https://www.aminer.cn/pub/5e4672c93a55ac14f595d7f4/	arXiv preprint arXiv, 2020, 2002(05516)

Wojciech Samek

德国柏林理工学院电子工程与计算机系 教授

最高学位毕业院校：柏林工业大学 博士

研究兴趣：机器学习、可解释性深度学习、联邦学习



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Robust and Communication-Efficient Federated Learning from Non-i.i.d. Data*	https://www.aminer.cn/pub/5cede0f9da562983788d81e7/	IEEE transactions on neural networks (2020)

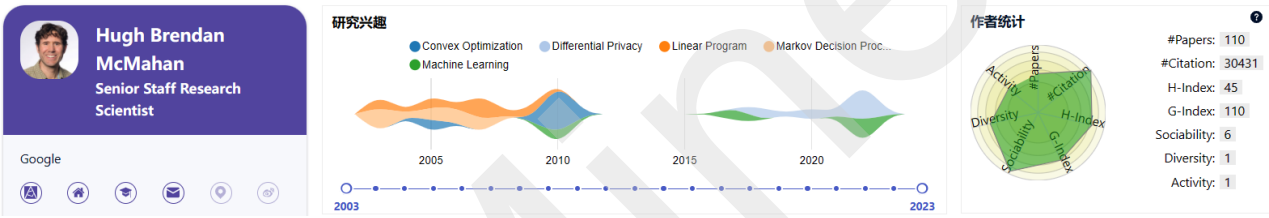
2	*Clustered Federated Learning: Model-Agnostic Distributed Multitask Optimization Under Privacy Constraints*	https://www.aminer.cn/pub/5d9b0cbe3a55acb0391990cf/	IEEE Transactions on Neural Networks and Learning Systems 32 (8), 3710-3722

H. Brendan Mcmahan

谷歌公司 研究科学家

最高学位毕业院校：美国卡耐基梅隆大学 计算机科学博士

研究兴趣：机器学习、联邦学习、分布式优化、差异隐私、深度学习



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Advances and Open Problems in Federated Learning*	https://www.aminer.cn/pub/5cede109da562983788e9865	Foundations and Trends® in Machine Learning, no. 1 (2019)
2	*Generative Models for Effective ML on Private, Decentralized Datasets*	https://www.aminer.cn/pub/5e5e18ca93d709897ce3198a/	ICLR (2020)
3	*Communication-efficient learning of deep networks from decentralized data*	https://www.aminer.cn/pub/599c7cc1601a182cd27d4688/	AISTATS, pp.1273-1282, (2017)
4	*Federated Optimization: Distributed Optimization for On-Device Intelligence*	https://www.aminer.cn/pub/58437725ac44360f1082ff8b/	arXiv preprint arXiv:1610.02527 (2016)
5	*Federated Learning: Stragegies for*	https://www.aminer.cn	arXiv preprint

	Improving Communication Efficiency	/pub/58437725ac44360f1082f72b/	arXiv:1610.05492 (2016)
6	*Can You Really Backdoor Federated Learning?*	https://www.aminer.cn/pub/5dd50ed43a55ac51376177ec/	arXiv preprint arXiv:1911.07963 (2019)

Ameet Talwalkar

美国卡耐基梅隆大学 助理教授

最高学位毕业院校：美国纽约大学 博士

曾经任职：Determined AI、加州大学洛杉矶分校

研究兴趣：机器学习，重点关注与自动化、公平性、可解释性和联邦学习相关的主题

相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Federated multi-task learning*	https://www.aminer.cn/pub/599c797f601a182cd264476f/	NeurIPS) 2017)
2	*Leaf: A benchmark for federated settings*	https://www.aminer.cn/pub/5c2c7a9217c44a4e7cf31290/	arXiv: Learning (2018)
3	*Expanding the reach of federated learning by reducing client resource requirements*	https://www.aminer.cn/pub/5c2c7a9217c44a4e7cf3168e/	arXiv: Learning (2018)

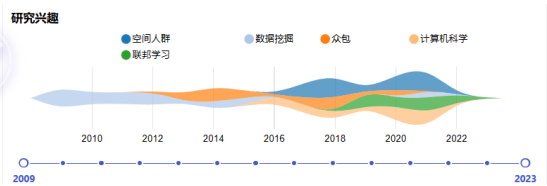
Yongxin Tong（童咏昕）

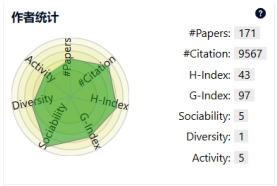
北京航空航天大学计算机科学与工程学院 教授

最高学位毕业院校： 香港科技大学 博士

曾经任职：北航计算机科学与工程学院软件开发环境国家重点实验室（SKLSDE）

研究兴趣：联邦学习、数据联邦、时空大数据分析、众包数据库、隐私保护数据分析





相关论文代表作：

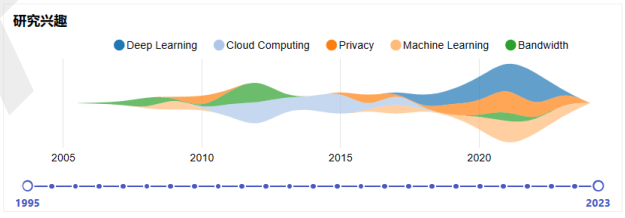
序号	论文名称	论文地址	发表期刊/年份
1	*Federated Machine Learning: Concept and Applications*	https://www.aminer.cn/pub/5c9f688c6558b90bfa34dcb4/	ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 12:1-12:19.
2	*Profit Allocation For Federated Learning*	https://www.aminer.cn/pub/5dea0ee0930831239d97ec63/	2019 IEEE International Conference on Big Data (Big Data), 2577-2586

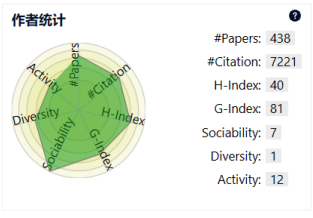
Bo Li（李博）

美国伊利诺伊大学厄巴纳-香槟分校 助理教授

最高学位毕业院校： 美国德克萨斯农工大学 博士

研究兴趣：对抗性机器学习、安全、隐私、大数据





相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*DBA: Distributed Backdoor Attacks against Federated Learning*	https://www.aminer.cn/pub/5e5e18ac93d709897ce25c7f/	International Conference on Learning Representations (ICLR),

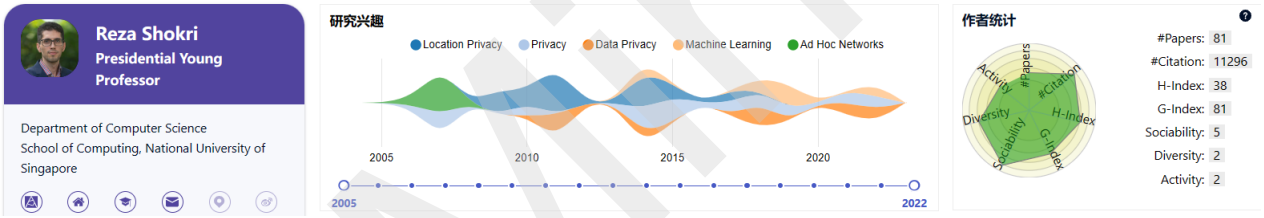
			2020
2	*CRFL: Certifiably Robust Federated Learning against Backdoor Attacks*	https://www.aminer.cn/pub/60bdde338585e32c38af5271/	International Conference on Machine Learning, 11372-11382，2021
3	*Attack-Resistant Federated Learning with Residual-based Reweighting*	https://www.aminer.cn/pub/5e0333623a55aca24ec3eee4/	arXiv preprint arXiv:1912.11464，2019

Reza Shokri

新加坡国立大学 教授

最高学位毕业院校：瑞士洛桑联邦理工学院 EPFL 博士

研究兴趣：计算机安全和隐私、机器学习



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning*	https://www.aminer.cn/pub/5ce3a8a0ced107d4c655642b	IEEE symposium on security and privacy, pp.739-753, (2019)
2	*Machine Learning with Membership Privacy using Adversarial Regularization*	https://www.aminer.cn/pub/5b67b4b417c44aac1c8672c6/	Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.
3	*Privacy Risks of Securing Machine*	https://www.aminer.cn	CCS, pp. 241-

	Learning Models against Adversarial Examples	/pub/5cf48a3dda56291d582a0290/	257, 2019.
4	*Synthesizing Plausible Privacy-preserving Localtion Traces*	https://www.aminer.cn/pub/57d063feac44367354297ed2/	IEEE Symposium on Security and Privacy, pp.546-563, (2016)
5	*Membership Inference Attacks against Machine Learning Models*	https://www.aminer.cn/pub/58437725ac44360f1083029c/	IEEE Symposium on Security and Privacy, (2017)

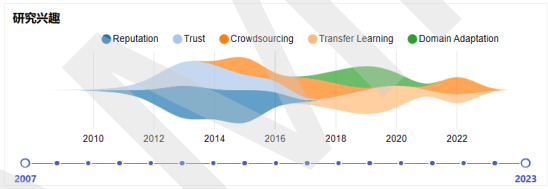
Han Yu

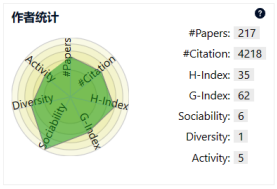
新加坡南洋理工大学 助理教授

最高学位毕业院校： 新加坡南洋理工大学 博士

曾经任职：惠普软件工程师、微众银行顾问

研究兴趣：可信联邦学习、人工智能伦理





相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*A Fairness-aware Incentive Scheme for Federated Learning*	https://www.aminer.cn/pub/5e3e887a3a55ac6b075ba5a4/	The 3rd AAAI/ACM Conference on AI, Ethics, and Society (AIES-20), 393–399 126 2020
2	*Privacy and robustness in federated learning: Attacks and defenses*	https://www.aminer.cn/pub/5fd7449591e011efa3cf5eff/	IEEE Transactions on Neural Networks and Learning Systems (TNNLS) 2022
3	*Collaborative fairness in federated learning*	https://www.aminer.cn/pub/5f48d8ba91e011096	Federated Learning: Privacy and Incentive,

		f95615d/	189-204 , (2020)

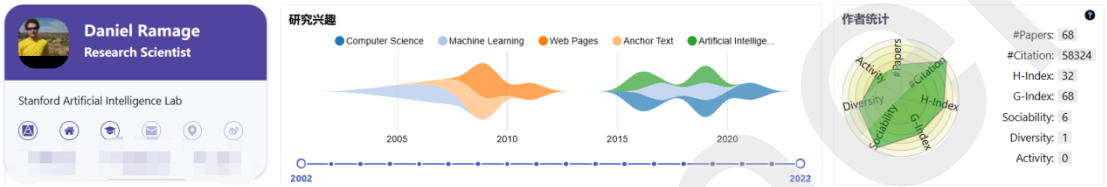
Daniel Ramage

斯坦福人工智能实验室 研究科学家

最高学位毕业院校：斯坦福大学 博士

曾经任职：谷歌研究、IBM 苏黎世研究实验室、微软研究院

研究兴趣：机器学习、联邦学习、安全隐私、自然语言处理、移动系统



相关论文代表作：

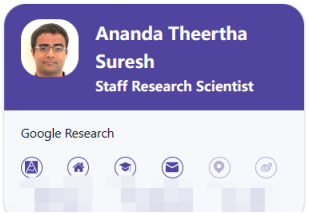
序号	论文名称	论文地址	发表期刊/年份
1	*Communication-Efficient Learning of Deep Networks from Decentralized Data*	https://www.aminer.cn/pub/599c7cc1601a182cd27d4688/	International Conference on Artificial Intelligence and Statistics (AISTATS) （2017）
2	*Federated learning for mobile keyboard prediction*	https://www.aminer.cn/pub/5c04966a17c44a2c747086ce/	Computing Research Repository (CoRR)（2018）

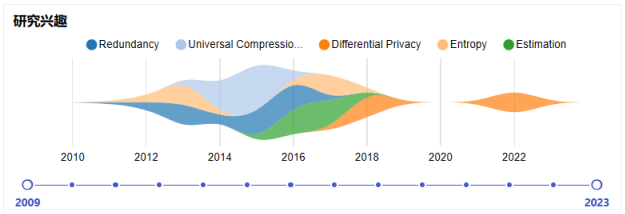
Ananda Theertha Suresh

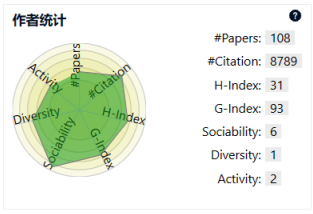
谷歌公司 高级研究科学家

最高学位毕业院校：美国加州大学圣地亚哥分校 博士

研究兴趣：联邦学习、统计分析、信息理论







相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Three Approaches for Personalization with Applications to Federated Learning*	https://www.aminer.cn/pub/5e5644103a55ac122e36c3f9/	arXiv:2002.10619 (2020)
2	*SCAFFOLD: Stochastic Controlled Averaging for Federated Learning*	https://www.aminer.cn/pub/5df20fc53a55acbe6bfcc74f	Foundations and Trends® in Machine Learning, 2019.
3	*Agnostic Federated Learning*	https://www.aminer.cn/pub/5cede0f7da562983788d5f5f/	CoRR, pp. 4615-4625, 2019./ International Conference on Machine Learning. PMLR, 2019.
4	*cpSGD: Communication-efficient and Differentially-private Distributed SGD*	https://www.aminer.cn/pub/5b3d98cc17c44a510f8021d3/	arXiv:1805.10559 (2018)
5	*Distributed Mean Estimation with limited Comunication*	https://www.aminer.cn/pub/58d82fcbd649053542fd6790/	International Conference on Machine Learning. PMLR, 2017

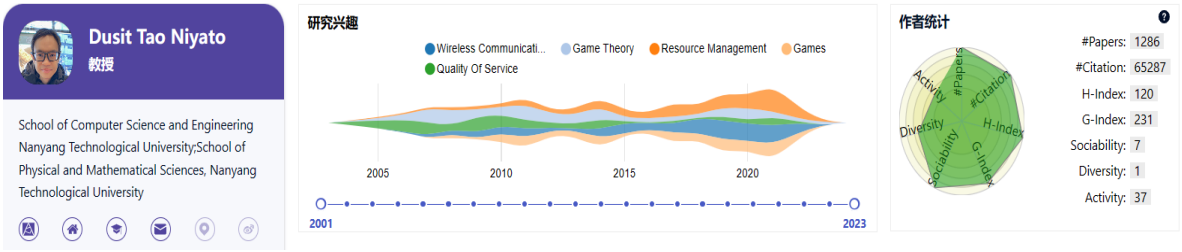
（2）联邦学习应用方面（边缘计算与区块链等）

Dusit Tao Niyato

新加坡南洋理工大学计算机科学与工程学院、物理与数学学院 教授

最高学位毕业院校：加拿大马尼托巴省温尼伯市曼尼托巴大学 博士

研究兴趣：可持续性、边缘智能、去中心化机器学习、激励机制设计



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Federated learning for 6G communications: Challenges, methods, and future directions*	https://www.aminer.cn/pub/5eda19d991e01187f5d6dc3b/	China Communications (2020) 17 (9), 105-118
2	*Completion Time and Energy Optimization in the UAV-Enabled Mobile-Edge Computing System*	https://www.aminer.cn/pub/5fae6475d4150a363cdb5cb9/	IEEE Internet of Things Journal 7 (8), 7808-7822 (2020)

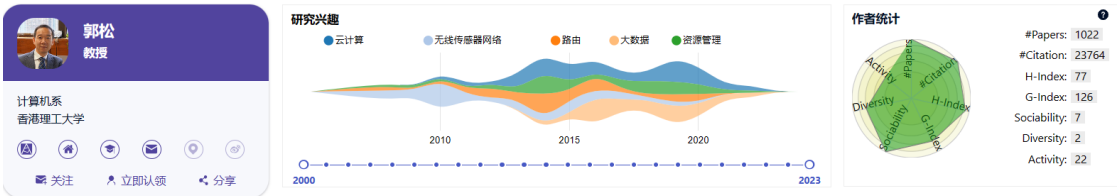
Song Guo

香港理工大学计算机系 教授

最高学位毕业院校：加拿大渥太华大学 博士

曾经任职：日本会津大学教授、北不列颠哥伦比亚大学助理教授、香港理工大学边缘智能实验室创始主任

研究兴趣：边缘智能、联邦学习、AI 赋能的物联网、边缘计算与区块链、分布式系统



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份

1	*A Learning-based Incentive Mechanism for Federated Learning*	https://www.aminer.cn/pub/5e5e19d993d709897ce8c5a1/	IEEE internet of things journal（2020）
2	*Experience-driven computational resource allocation of federated learning by deep reinforcement learning*	https://www.aminer.cn/pub/5f0eddbf9fced0a24b6837a2/	IEEE International Parallel and Distributed Processing Symposium (2020): 234-243
3	*Parameterized knowledge transfer for personalized federated learning*	https://www.aminer.cn/pub/6184a0d25244ab9dcb28c1d4/	Conference on Neural Information Processing Systems abs/2111.02862 (2021): 10092-10104.

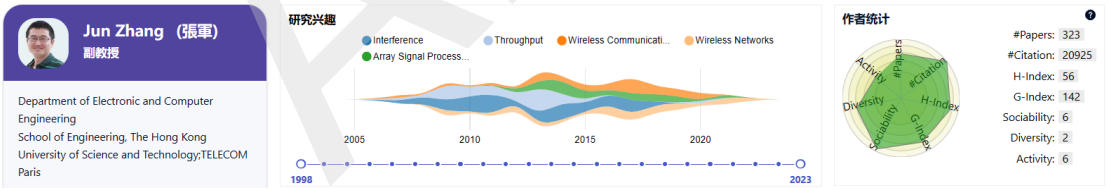
Jun Zhang

香港科技大学 副教授

最高学位毕业院校：德克萨斯大学奥斯汀分校 博士

曾经任职：香港理工大学电子及计算机工程学系副教授

研究兴趣：移动边缘计算、边缘人工智能、无线通信、联邦学习



相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Client-edge-cloud hierarchical federated learning*	https://www.aminer.cn/pub/5ee058479e795e01364d4290/	ICC 2020-2020 IEEE International Conference on Communications (ICC), 1-6

2	*Dynamic Computation Offloading for Mobile-Edge Computing with Energy Harvesting Devices*	https://www.aminer.cn/pub/57a4e91dac44365e35c98af6/	IEEE Journal on Selected Areas in Communications (2016) 34 (12), 3590-3605
3	*Hierarchical federated learning with quantization: Convergence analysis and system design*	https://www.aminer.cn/pub/6061a89091e0112c88b98337/	IEEE Transactions on Wireless Communications 22.1 (2023): 2-18.

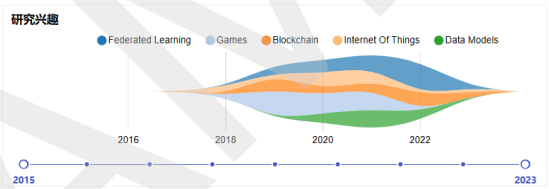
Zehui Xiong

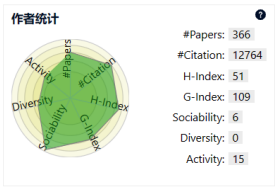
新加坡科技设计大学 助理教授

最高学位毕业院校：新加坡南洋理工大学 博士

曾经任职：新加坡阿里巴巴-南洋理工大学联合研究院

研究兴趣：网络系统的优化和智能、区块链与数据管理的安全和隐私保护、边缘人工智能系统的联邦机器学习、智能物联网的群体智能和边缘学习、无线通信的资源管理、元宇宙





相关论文代表作：

序号	论文名称	论文地址	发表期刊/年份
1	*Incentive Design for Efficient Federated Learning in Mobile Networks: A Contract Theory*	https://www.aminer.cn/pub/5cf48a42da56291d582a4fa7/	arXiv: Learning, 2019, abs/1905.07479(): 1-5.
2	*Incentive Mechanism For Reliable Federated Learning: A Joint Optimization Approach To Combining Reputation And Contract Theory*	https://www.aminer.cn/pub/5dfc9fecdf1a9c0c416551c0/	IEEE internet of things journal（2019）

3	*Reliable Federated Learning for Mobile Networks*	https://www.aminer.cn/pub/5e72344f93d709897cfc2710/	IEEE Wireless Communications（2020）

3.1.6 专利申请现状

基于 AMiner 和智慧芽专利数据库，通过联邦学习相关关键词检索式 [64]，在“标题/摘要/权利要求”中进行相关专利搜索，并按照受理局进行简单同族申请去重，统计截止日期为 2023 年 4 月 30 日。数据结果显示，2016 年至 2022 年七年期间，共计得到 5,968 件简单同族（共 9,277 条）联邦学习技术相关专利申请记录。

1. 全球专利申请总体呈现上升趋势

联邦学习的专利申请数自 2016 年以来呈现不断攀升的趋势，直至 2022 年达到峰值，其中，2019 年联邦学习专利申请的增长幅度最大，其次是 2020 年相关专利申请增幅，2019 和 2020 这两年的专利增长幅度均超过 100%；2021 年和 2022 年的联邦学习专利申请量基本持平，具体申请趋势情况如图 23 所示。预计接下来几年内，随着联邦学习技术的进一步发展，相关专利申请数量仍将热度不减。

[64]关键词检索式： TAC_ALL:("federated machine learning" OR "federated optimization" OR "federated learning" OR "federation learning" OR (privacy AND distributed AND "data mining") OR (secure AND distributed AND "data mining") OR (secure AND multiparty) OR (secure AND multi-party) OR (privacy AND multi-party) OR (privacy AND multiparty) OR (privacy AND distributed AND "machine learning") OR (secure AND distributed AND "machine learning") OR (privacy AND "joint learning") OR (secure AND "joint learning") OR (privacy AND distributed AND "deep learning") OR (secure AND distributed AND "deep learning")) AND APD:[20160101 TO 20221231]

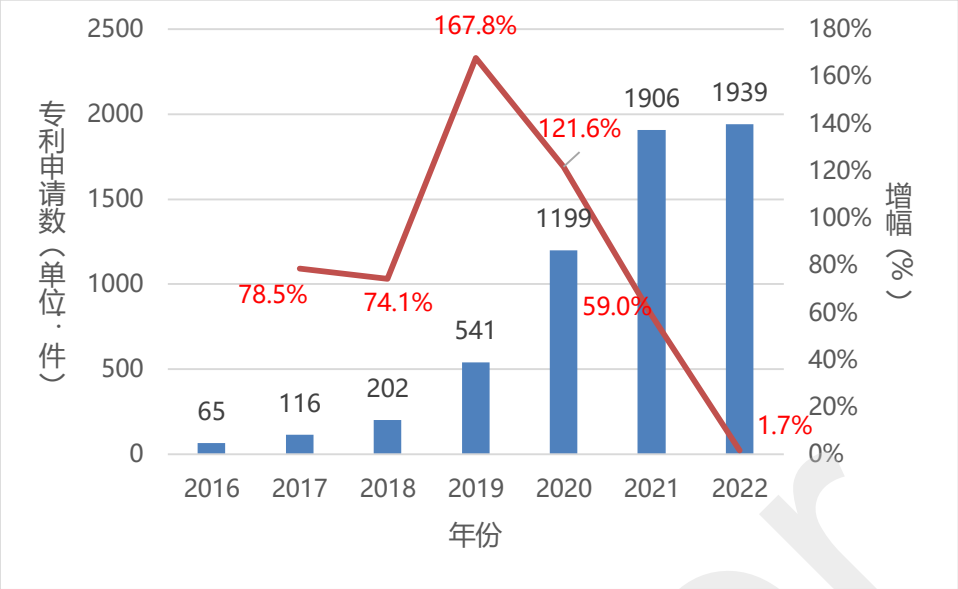


图 23 2016-2022 年联邦学习专利申请趋势

2. 全球专利受理情况以中国地区最多

全球范围内，近年来受理联邦学习专利申请数最多的地区是中国，有 4000 多件，约占全球受理总量的七成以上，数量优势非常突出，如图 24 所示。美国和世界知识产权组织等其他国家和地区的专利受理数量远远低于在中国的受理量。这反映出联邦学习技术创新和推广应用在中国地区相对比较热门。

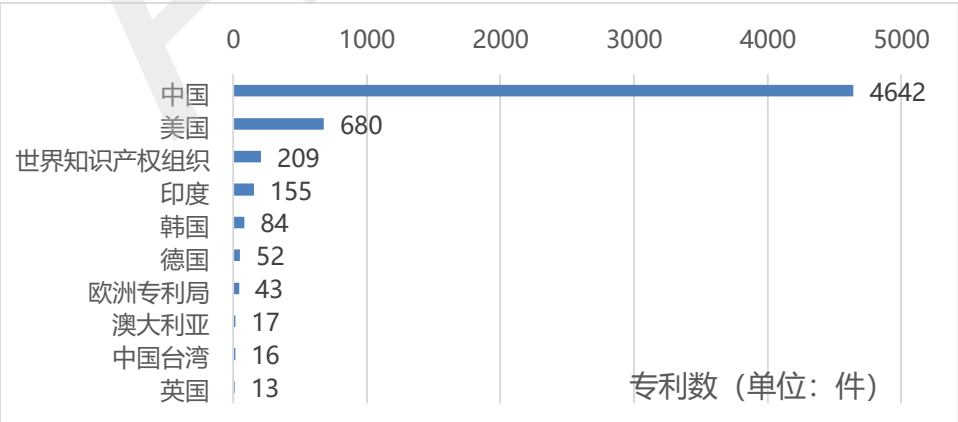


图 24 联邦学习专利申请全球受理局分布（2016-2022 年）

3. 中国是联邦学习技术第一大来源国

截至本报告时段，全球联邦学习第一大技术来源国为中国，中国联邦学习专利申请量占全球联邦学习专利总申请量的 75.8%；其次是美国，美国联邦学习专利申请量占全球联邦学习专利总申请量的 11.6%。韩国和印度虽然排名第三和第四，但是与排名第一的中国专利申请量差距较大。相关信息如图 25 所示。

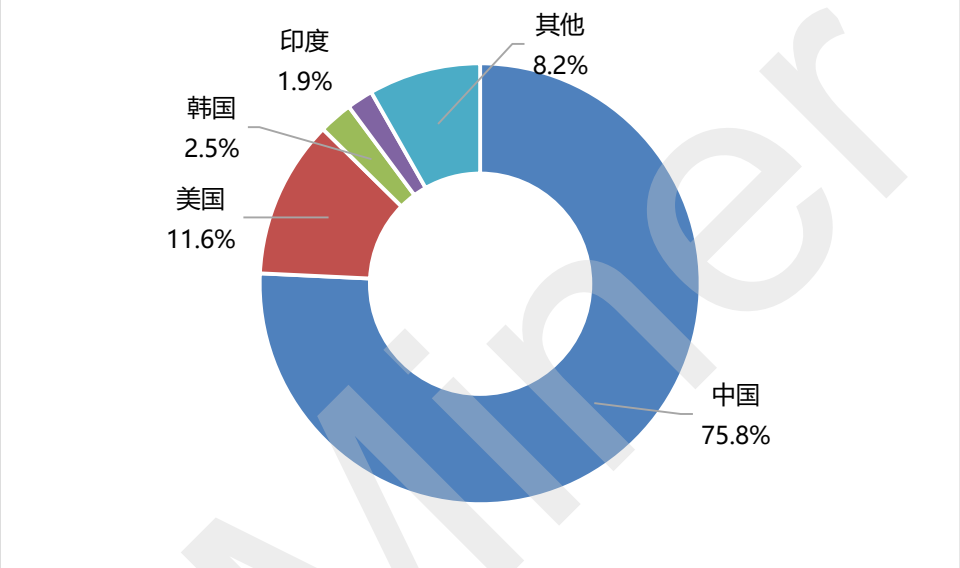


图 25 联邦学习专利申请技术来源国分布

4. 国内专利申请以北京、广东和浙江领先

国内近年来联邦学习专利申请量 TOP10 省市分别是北京、广东、浙江、上海、江苏、山东、陕西、四川、湖南和重庆，其中包括了较多的沿海地区省市，详细申请情况如图 26 所示。其中，北京、广东和浙江属于该领域第一梯队，专利申请量均高于 500 件，明显超过其他省市。北京在 2021 与 2022 年的专利申请量增长快速，超过广东成为国内领先城市。

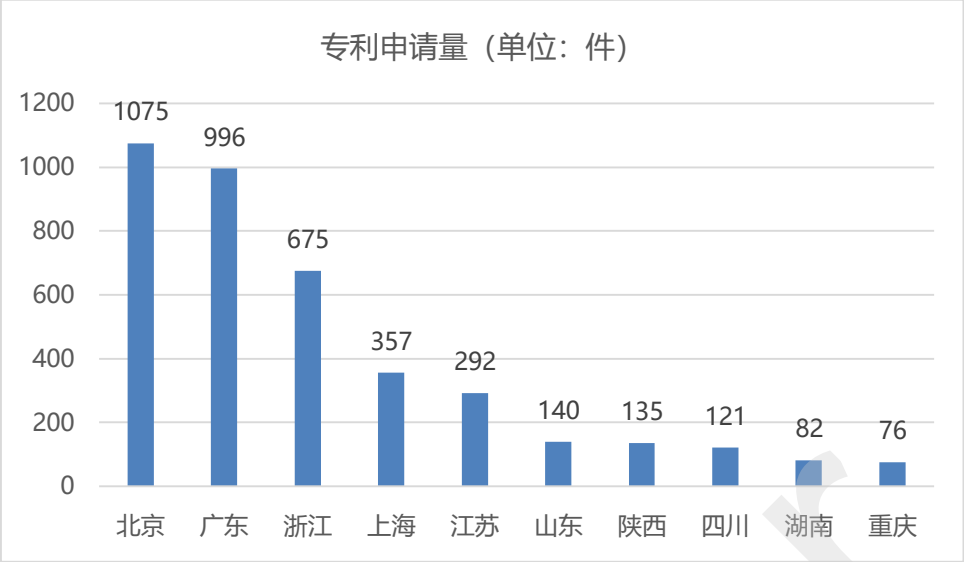


图 26 联邦学习专利量 TOP 10 国内省市分布（2016-2022 年）

5. 两家金融机构专利申请量较为突出

从专利申请人来看，联邦学习专利申请量 TOP10 的机构主要分布在中国和美国两个地区，依次占据八席和两席，同时，排名前 3 名机构都位于中国。具体情况如图 27 所示。TOP10 的机构中有两所高校即北京邮电大学、西安电子科技大学，其余都是全球顶尖的科技或者是互联网公司。相比上期报告，支付宝（杭州）信息科技有限公司与深圳前海微众银行股份有限公司这两家金融机构仍然保持在榜单的前两位，且它们的专利申请数均超过 200 件。本期包括三家新入榜机构，分别是华控清交信息科技(北京)有限公司、北京邮电大学、深圳致星科技有限公司。

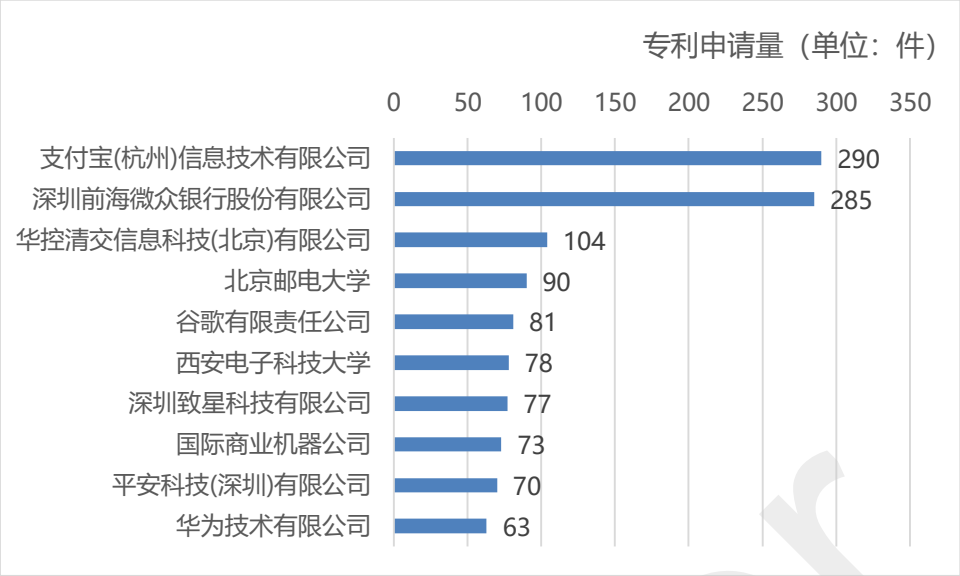


图 27 联邦学习专利申请量 TOP 10 机构（2016–2022 年）

6. 专利技术创新点最多聚焦于客户端与区块链

通过算法对联邦学习相关专利进行词频统计分析和文本聚类，提取该领域排名靠前的关键词并制作词云图，如图 28 所示。最热门的联邦学习技术主题词包括客户端、区块链、服务器、学习方法、电子设备、全局模型、机器学习、隐私保护、模型参数、模型训练、分布式等。与上期报告相比，除了安全与隐私保护，以及机器学习方法等方向，联邦学习本期的专利布局更多地聚焦于客户端、电子设备、全局模型、模型训练等方面。

图 28 联邦学习相关专利申请涉及的关键词云

7. 专利申请最多布局在机器学习与数据存取访问平台保护两个 IPC 分类

在联邦学习专利之中，申请数量最热门的专利 IPC 分类是 G06N20 机器学习〔2019.01〕，相应的专利申请约近三成；其次是 G06F21/62··（通过一个平台保护数据存取访问，例如使用密钥或访问控制规则〔2013.01〕[2013.01]），相关专利量居于第二位。详细信息如图 29 所示。

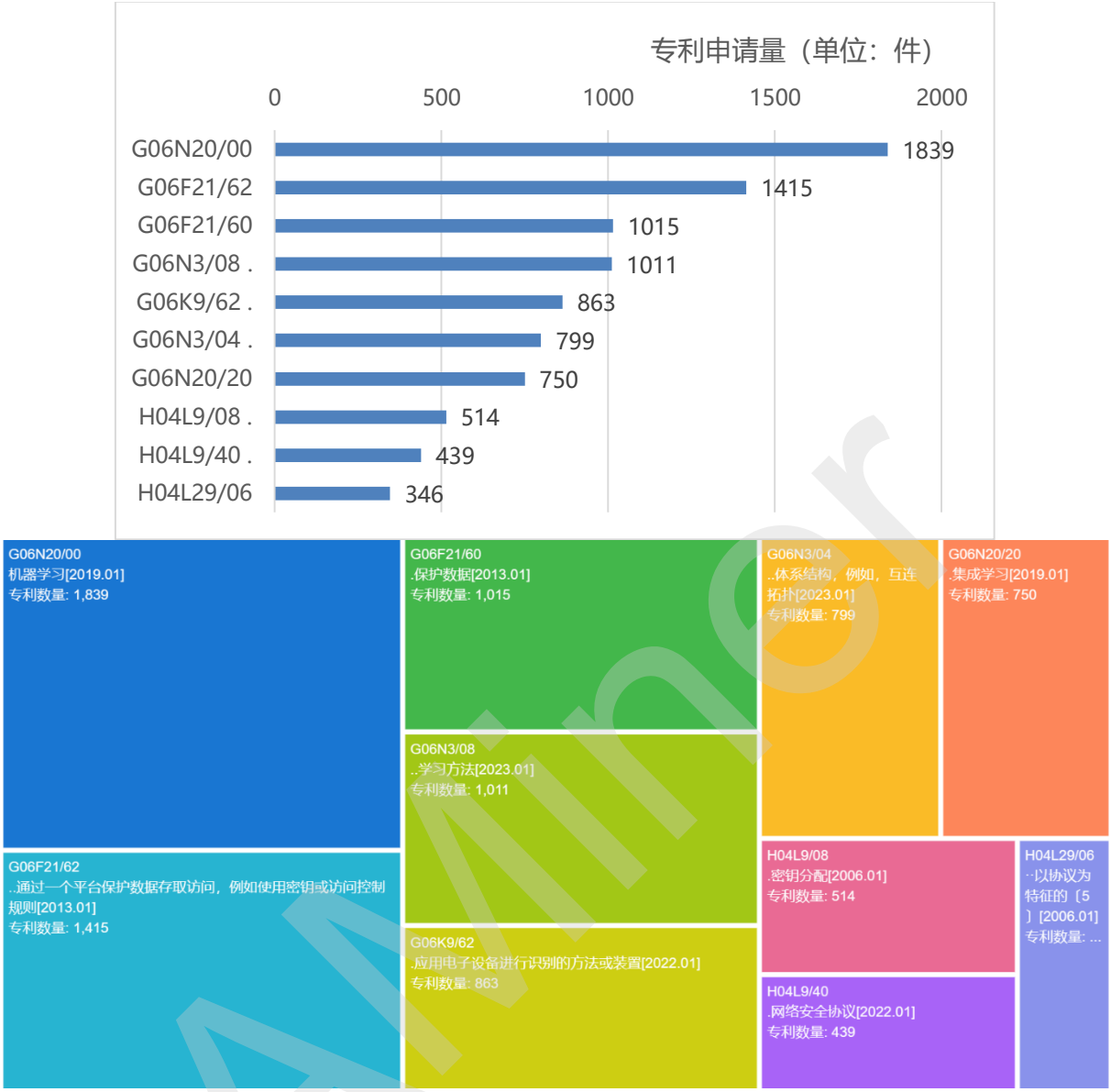


图 29 联邦学习专利申请量 TOP 10 的 IPC 分类

在联邦学习专利的数据存取访问平台保护、机器学习两个最热门申请的 IPC 分类下，领先专利申请机构主要来自中国和美国，详细情况如图 30 所示。其中，支付宝公司在 G06F21/62（数据存取访问平台保护）方面进行了最多数量的联邦学习专利布局，微众银行在 G06N20（机器学习）方面了进行最多数量的联邦学习专利布局，此外，北京邮电大学、谷歌公司都在机器学习、数据存取访问平台保护等不同分类的专利技术布局较均衡；华控清

交信息公司也较多布局在数据存取访问平台保护方面技术。

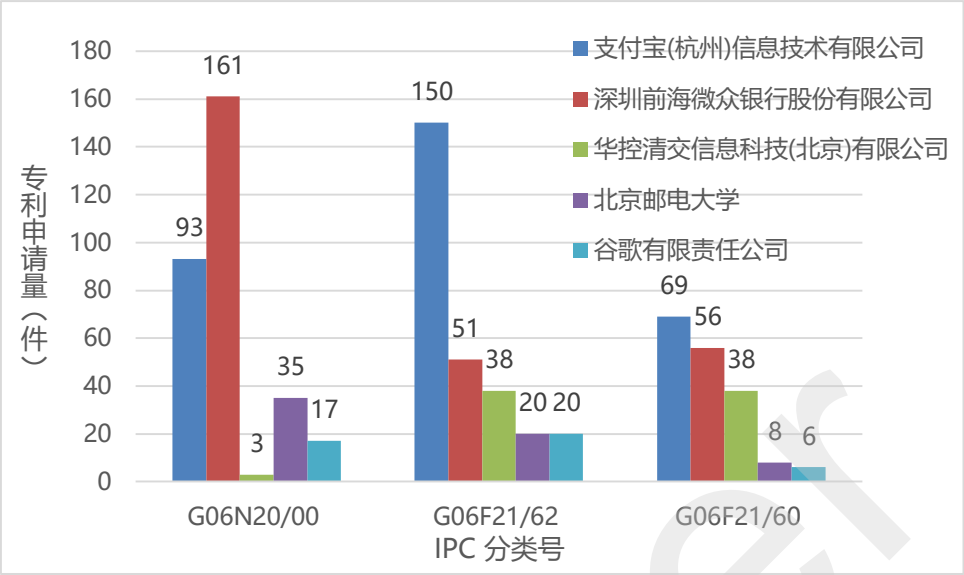


图 30 联邦学习专利 IPC 分类 TOP 3 专利领先申请人技术分布

8. 引入新兴技术创新点的联邦学习专利已开始萌芽

上期报告以来，联邦学习领域出现了一些技术主题创新，其中以可信联邦学习和大模型尤为火热。本报告期内，引入这些相关技术创新点的专利已经开始出现，虽然专利数量目前暂时还都很少，但是值得关注。

可信联邦学习相关专利 [65] 共计发现 58 件简单同族专利，分布在 2020 年（10 件）、2021 年（18 件）和 2022（37 件）。这些专利申请全部都来自中国，其中，可信联邦学习相关专利申请量最多的机构是深圳前海微众银行股份有限公司（4 件），紧随其后的是厦门大学（3 件）。最早的可信联邦学习专利是 2020 年 7 月由华南师范大学申请的“一种基于区块链的可信联邦学习方法、系统、装置及介质”（专利号 CN111966698A）。

65 来源：AMiner 和智慧芽专利数据库；关键词检索式=TAC:(可信联邦学习) OR TAC:(可信隐私计算) OR TAC:(联邦学习 AND (可解释性 OR 可溯源 OR 可审计 OR 可监管 OR 知识产权保护 OR 公平性 OR 技术普惠 OR 可证明 OR 效率可控))，在“标题/摘要/权利要求”中进行搜索，并按照受理局进行简单同族申请去重；统计截止日期为 2023 年 4 月 30 日。

引入大模型技术的联邦学习专利申请最早出现在 2021 年 4 月，是由深圳前海微众银行股份有限公司申请的“信息处理方法及系统”（专利号 CN113222175B）。本报告期内仅发现 4 件引入大模型技术的联邦学习相关专利[66]。详情如下所示。

申请时间	引入大模型技术的联邦学习专利情况	
2022-8	专利号	CN115408377A
	专利名称	一种基于联邦学习构建医学影像大模型的方法和装置
	申请人	北京智源人工智能研究院
	发明人	肖宏旺　黄文灏　叶启威　董思维　史业民　舒彧　曹岗　黄铁军
	摘要：本方法用于服务端，包括：利用医学影像公开数据进行预训练，得到全局初始化大模型；将所述全局初始化大模型分发至各个客户端；利用各个客户端上传的各自对应的本地大模型生成全局大模型，其中，本地大模型是各个客户端利用本地医学影像数据对所述全局初始化大模型进行优化训练得到的。本发明通过联邦学习的方式，充分发挥了集中化公开数据和各医院私有数据的协同价值，实现了高效、安全地共建医学影像大模型，提升模型稳定性和泛化能力，促进人工智能医学影像应用的发展，赋能医院端医疗影像 AI 系统。	
2022-5	专利号	CN114584406B
	专利名称	一种联邦学习的工业大数据隐私保护系统及方法
	申请人	湖南红普创新科技发展有限公司
	发明人	陈晓红　许冠英　徐雪松　胡东滨　梁伟　袁依格
	摘要：本发明的系统包括设备选择层、终端层、聚类层、边缘层以及云层。方法包括：根据筛选的终端设备采集工业数据；对工业数据进行聚类处理；将处理后的工业数据发送至边缘服务器，建立本地模型；云服务器根据接收的本地模型进行全局模型聚合和更新，并将全局模型下放至设备选择层筛选出的终端设备，实现数据共享。通过设备选择层对终端设备进行选择，并对工业数据聚类，满足了联邦学习数据样本同质性的要求，提高了联邦学习的聚合效率；通过边缘层与云层之间的建模、更新以及下放，提高了海量数据传输的速率，实现数据共享，并且保证数据的安全性。	
2021-7	专利号	CN113518007B 授权
	专利名称	一种基于联邦学习的多物联网设备异构模型高效互学习方法
	申请人	华东师范大学
	发明人	陈铭松　夏珺

66 来源：AMiner 和智慧芽专利数据库；关键词检索式= TAC_ALL:(联邦学习) AND TAC_ALL:(大模型 OR 大型语言模型 OR 基石模型 OR 大规模预训练模型 OR 提示工程 OR 涌现能力 OR 同质化 OR 生成预训练语言模型)，在“标题/摘要/权利要求”中进行搜索，并按照受理局进行简单同族申请去重；统计截止日期为 2023 年 4 月 30 日。

	摘要：本发明所述方法可以打破异构模型之间的知识壁垒，提高异构模型在各类物联网设备中的性能。在本方法框架中，不同的模型开始相互学习，两种模型都可以收敛到很好的结果。为了增加联邦学习的普适性，本发明提出一种基于深度相互学习的训练方法，考虑局部模型之间的知识共享过程。通过综合实验对本发明方法 PFL 进行了论证，可以在实际场景中在通信量和预测精度方面的有效性。	
2021-4	专利号	CN113222175A
	专利名称	信息处理方法及系统
	申请人	深圳前海微众银行股份有限公司
	发明人	何元钦　刘洋　陈天健
	摘要：本发明公开了一种信息处理方法及系统，包括：协作方根据协作方模型确定得到与各个数据提供方对应的中间模型并分别下发给对应的各个数据提供方；数据提供方根据数据提供方的私有数据，对接收到的用于作为其本地模型的中间模型和数据提供方的个性化模型进行知识蒸馏，得到训练后的个性化模型；数据提供方根据各个参与方共有的公共数据集，通过训练后的个性化模型进行预测得到输出数据并将输出数据发送至协作方；协作方根据输出数据和公共数据集，通过知识蒸馏对协作方模型进行训练，得到目标全局模型，用以执行数据提供方计算资源少于预设计算资源场景下的联邦学习的操作。本发明可以在有参与方计算资源少的场景下，有效地实现大模型训练。	

3.1.7 国家自然科学基金项目资助分析

根据基金组织官网上的公开数据，通过在项目标题中进行关键词[67]搜索，获取到了中国（含大陆、港澳）以及中外地区合作的联邦学习基金项目资助情况。从目前所获取数据的总体情况来看，虽然 2016 年至 2022 年间相关基金项目数量趋势略有上升，但是总量较少，共计发现 156 个联邦学习在各地区的获批基金项目，包括 102 个国家自然科学基金项目 NSFC，26 个香港地区的创新及科技基金项目，澳门科学技术发展基金项目 FDCT 以及国家自然科学基金委员会国际合作项目分别各有 14 个。这些获批项目的趋势分布如图 31 所示。

[67] 关键词检索式 = 联邦学习 OR 隐私保护 OR 分布式技术 OR 数据安全 OR 边缘计算 OR 可信执行环境

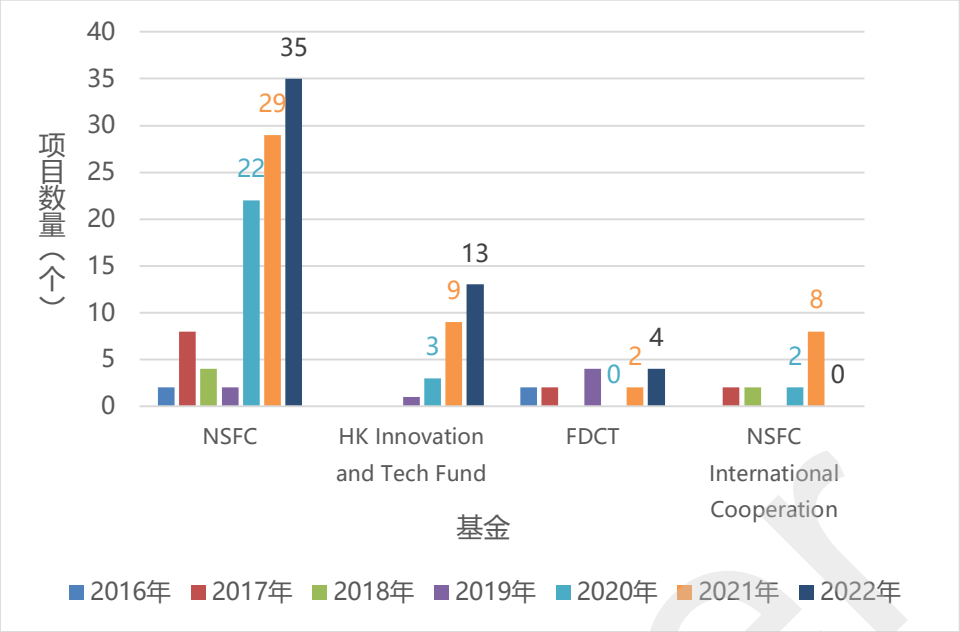


图 31 2016-2022 年几个国家地区联邦学习相关基金项目获批分布

注：NSFC 是指国家自然科学基金项目；HK Innovation and Tech Fund 是指香港创新及科技基金项目；FDCT 是指澳门科学技术发展基金；NSFC International Cooperation 是指国家自然科学基金委员会国际合作局合作项目。

1. NSFC 相关资助项目数量与金额近年来明显增加

2016 至 2022 年期间，联邦学习领域的国家自然科学基金项目共计获批 102 个，所获批项目分布在全国 22 个省份的 60 多家依托单位，涉及 20 多个学科，总资助金额达 5277 万元人民币。值得注意，2019 年之后，联邦学习相关基金项目获批势头增长明显：2020 至 2022 年的基金项目获批数量占总量的 84.3%，获资助金额占总额的 74.5%。如图 32 所示。

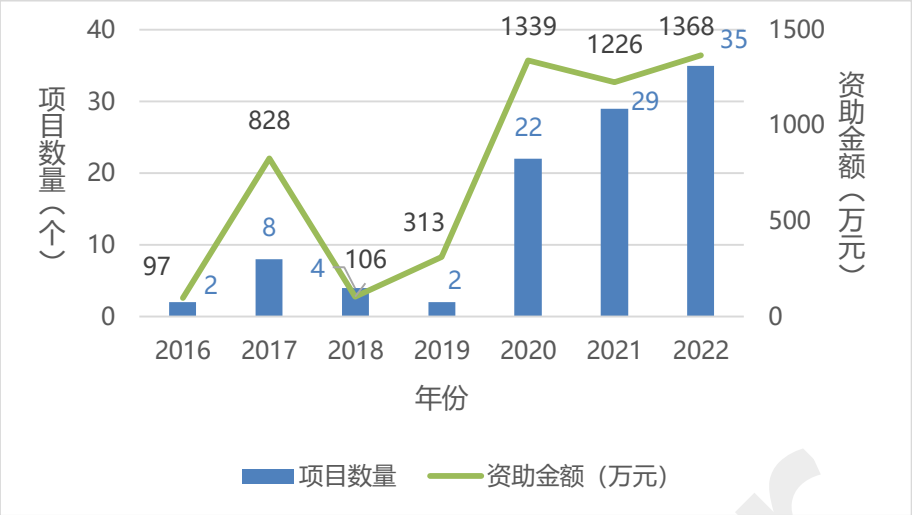


图 32 2016-2022 年联邦学习领域国家自然科学基金项目的获批趋势

（1）超九成资助集中在青年科学基金与面上项目

联邦学习领域的国家自然科学基金项目资助主要以青年科学基金项目和面上项目为主，这两类项目数量合计占 90%以上。其中，青年科学基金项目数量虽然最多，占比过半，但其获资助金额却低于面上项目类的资助金额。如图 33 所示。超百万级别的重大研究计划仅一项、联合基金项目仅四项。

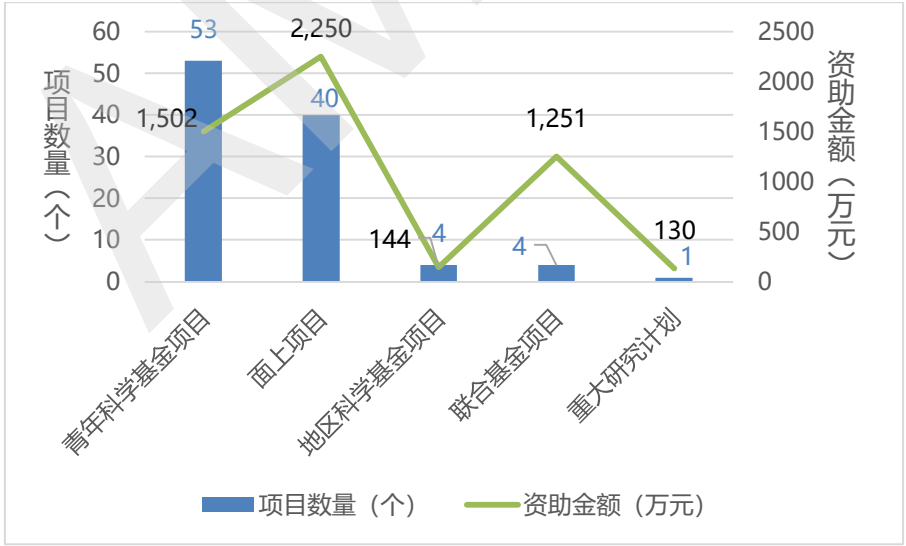


图 33 2016-2022 年联邦学习领域国家自然科学基金项目的资助类别

（2）集中在计算机科学、人工智能、电子学与信息系统三学科

联邦学习领域国家自然科学基金项目遍布医学科学部、管理科学部、数理科学部、工程与材料科学部、信息科学部的共计 20 多个学科。其中，信息科学部的基金项目最多，占比近九成。在信息科学部的基金项目之中，计算机科学、人工智能、以及电子学与信息系统三个学科所获批项目最多，位于前三。如图 34 所示。

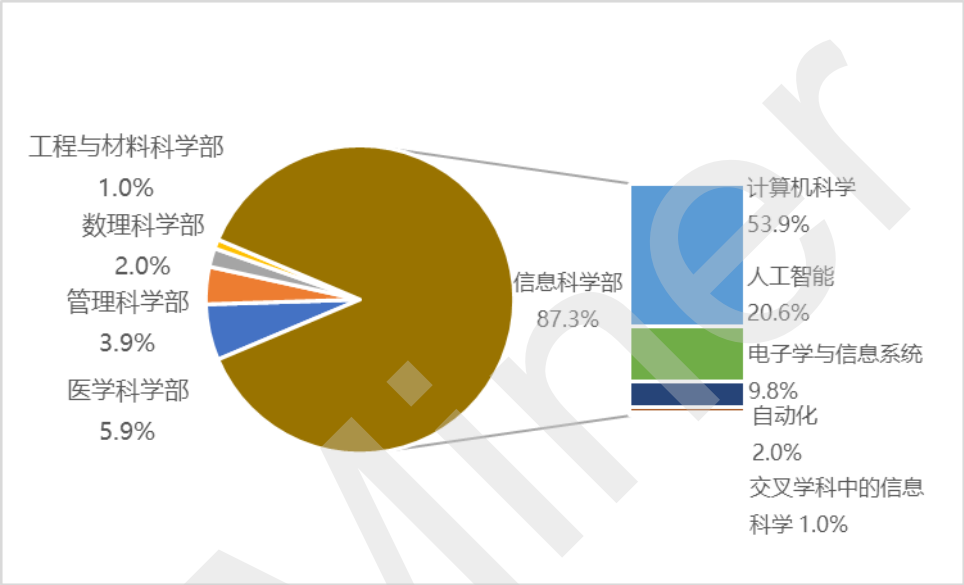


图 34 2016-2022 年联邦学习领域国家自然科学基金项目学科分布

（3）北京和广州两地所获批的基金项目量较多

联邦学习领域所获批的国家自然基金项目存在明显的地区差异。根据各个省份基金项目获批数量，大致可分为三个梯队：北京、广州位于第一梯队，所获批基金项目数量均大于 10 个；江苏、上海、浙江、湖北、辽宁、陕西、天津、四川这八个省份处于第二梯队，它们所获批基金项目数量在 5 个至 10 个之间；其余国内省份的所获批基金项目数量均不足 5 个，处于第三梯队。如图 35 所示。从获资助金额来看，浙江、北京、广东依次居于全国前三，其余省份所获项目的资助额则均不足 500 万元。

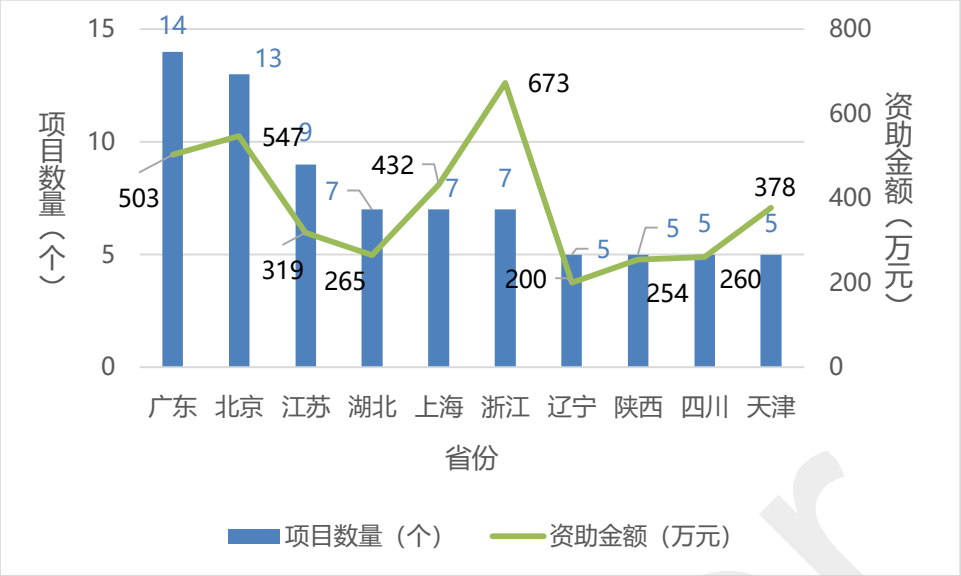


图 35 2016-2022 年联邦学习领域国家自然科学基金项目获批省份 TOP 10

（4）华中科技大学是基金项目获批最多的单位

联邦学习领域的国家自然科学基金项目的依托单位以高校为主，占比 90.2%。在获得基金项目的高校之中，985/211 学校获批的项目量约占总量的 61%。此外，近两年香港中文大学、香港浸会大学、香港中文大学 (深圳) 也获得了该领域的国家自然科学基金项目资助，成为不容忽视的一股力量。总体上，联邦学习领域基金项目获批最多的单位是华中科技大学，其次是浙江大学。如图 36 所示。

值得一提的是，哈尔滨工业大学获批的联合基金项目《城市重大基础设施灾害风险主动感知与精准管控》，所获资助金额最高，超 500 万元。该项目建立了城市重大基础设施灾害风险主动感知与精准管控的系统理论与方法，其中提出了系列城市重大基础设施主动监测方法与智能感知技术，包括移动群智感知技术与端边云协同联邦学习机制等。

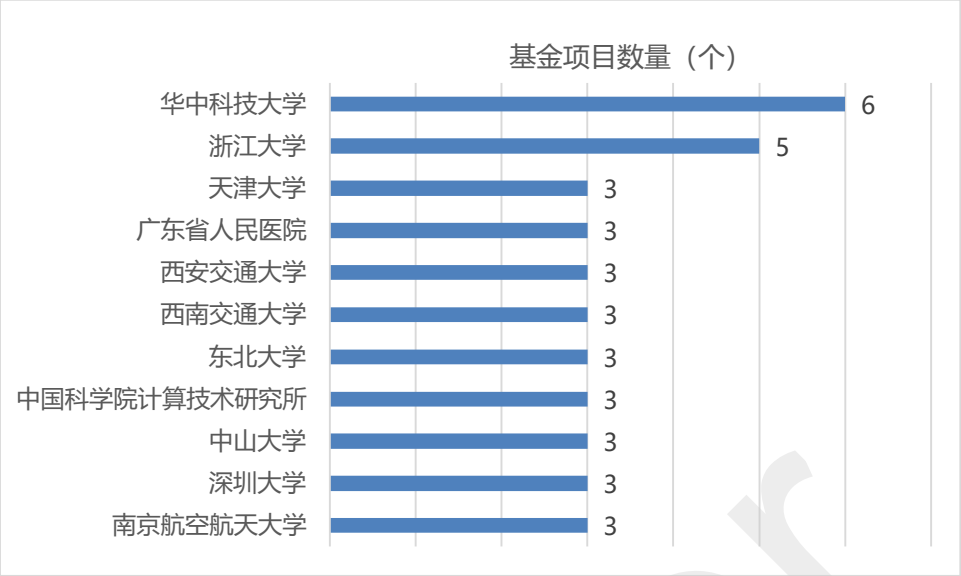


图 36 2016-2022 年联邦学习领域国家自然科学基金项目依托单位 TOP 10

2. 香港地区基金资助项目多于澳门基金资助量

本研究主要调研了香港创新及科技基金 (ITF) 与澳门科学技术发展基金 (FDCT) 项目。数据显示，针对联邦学习相关领域，香港创新及科技基金的资助项目数量略多于澳门科学技术发展基金资助的项目数量。

香港创新及科技基金由创新科技署管理，该基金旨在支持研究及发展、推动科技应用、培育科技人才、支援科技初创企业，以及培养创科文化。针对联邦学习领域，该基金在 2016-2022 期间资助过 26 个项目，趋势分布如图 37 所示。由图 37 可见，尽管项目数量较少，但是联邦学习相关的资助项目数量与资助金额均呈现逐年增加趋势。其中，最早的资助项目是 2019 年的一项创新及科技支援计划，即香港应用科技研究院的“物联网区块链：数据交换”项目，它基于有权限分布式分类账技术，解决实际案例应用中区块链累积物联网数据时量数可扩展性问题，以及智能交易合同、数据安全和隐私保护等问题。

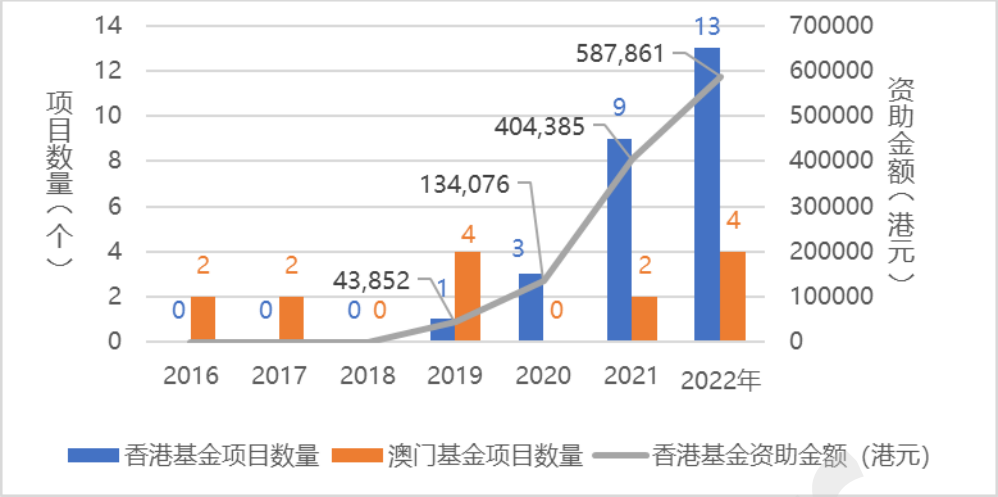


图 37 2016–2022 年香港创新及科技基金与澳门科学技术发展基金资助的联邦学习相关项目趋势

注：澳门科学技术发展基金未获取到项目资助金额数据。

在香港地区，联邦学习领域的创新及科技基金项目资助主要以研究人才库和创新及科技支援计划为主，这两类项目数量合计占 90%以上。其中，研究人才库项目资助量最多，有 13 个；创新及科技支援计划资助数量次之，有 11 个。如图 38 所示。所资助项目主要聚焦于资讯及通讯这个科技范畴，以及少量的电子与先进制造技术类。

从资助金额来看，超千万级别的资助计划有 3 个，它们均属于创新及科技支援计划，也均由香港应用科技研究院承担。其中，资助金额最多的项目是“硬件加速智能家居隐私及安全技术平台”，达到了 1313 万港元；“开放式银行智能个人助理”与“物联网的可信执行环境”两个项目的资助金额次之，分别均获得 1035 万港元资助。

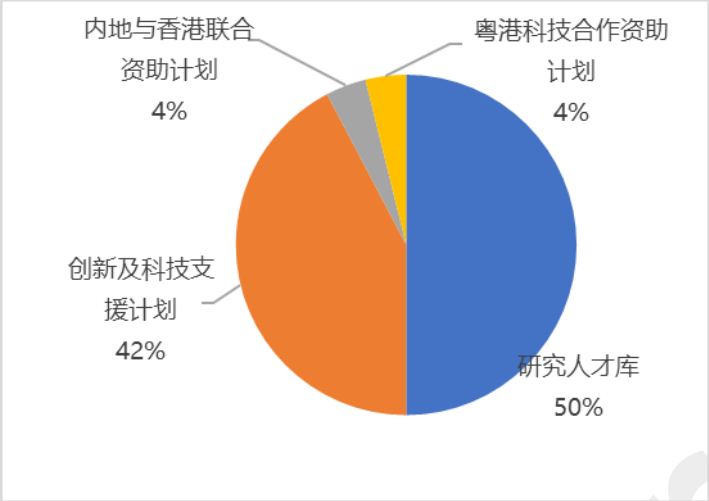


图 38 2016-2022 年联邦学习领域香港创新及科技基金资助项目分布

澳门科学技术发展基金是为了配合澳门特别行政区科技发展政策的目标，对有助于提升澳门特别行政区的科研实力、创新能力及竞争力的各类项目提供资助。数据显示，该基金在 2016 年至 2022 年期间共计资助了 14 个联邦学习相关项目。其中，2019 年与 2022 年资助的项目最多，分别有 4 个；2018 年与 2020 年则没有发现相关项目。在这 14 个项目之中，有 11 项是一般科研资助，还有一个是澳门科学技术发展基金与国家自然科学基金委员会联合科研资助项目。从项目申请者看，申请量最多的机构是澳门大学，有 5 个；其次是澳门科技大学基金会-澳门科技大学，申请了 4 个项目。

澳门地区这些被资助项目的研究主题涉及了分布式计算与隐私保护两个方面。其中，隐私保护的相关项目有 7 项，从 2017 年到 2022 年均都有项目涉及。此外，有 2 个项目研究了生物或医疗领域的相关联邦学习问题；2 个项目研究了分布式计算方法等。

3． 基金国际合作项目较多资助了安全与隐私研究方向

根据国家自然科学基金委员会官方网站的公开数据，通过在项目标题中进行关键词[68]搜

[68] 关键词检索式 = 联邦学习 OR 隐私保护 OR 分布式技术 OR 数据安全 OR 边缘计算 OR 可信执行环境

索，发现 2016 年至 2022 年间，国家自然科学基金委员会批准了 14 个联邦学习相关的国际合作基金项目。其中，2021 年获批的相关国际合作项目数量有 8 个，2017 年、2018 年与 2020 年均分别获批了 2 个，其余年份则未发现有联邦学习相关国际合作项目获批。

国家自然科学基金委员会所披露的这些联邦学习国际合作基金项目涉及到中国、英国、瑞典等 8 个地区之间的合作。相关基金合作分布如图 39 所示。所合作项目的研究主题大部分都与隐私保护或数据安全有关。其中，中国国家自然科学基金与英国皇家学会之间的自然科学基金合作交流项目较多，有 6 项，研究方向包括智慧医养物联网中隐私保护、机器学习的隐私保护以及基于联邦学习的脑疾病早期诊断等。

图 39 2016–2022 年联邦学习领域国家自然科学基金委员会 NSFC 国际合作项目

3.2 联邦学习框架与系统现状

近年来，联邦学习算法框架和系统的开发和部署正在蓬勃发展。目前，市面上既有许多开源的联邦学习框架平台，也有许多非开源的自研式框架平台。本部分通过 AMiner 数据

库中的新闻数据，分析梳理了国内外知名高校、科研机构、科技企业巨头、金融科技公司，以及初创公司等推出的主要联邦学习相关系统框架，具体信息如下。

3.2.1 开源框架

开源的联邦学习框架多数是由国内外企业推出发布的，高校科研机构发布的相对较少。Pysyft 是 2017 年也是最早推出开源框架，随后几年陆续有新的开源框架推出，2020 年开源的联邦学习框架数量最多，如图 40 所示。

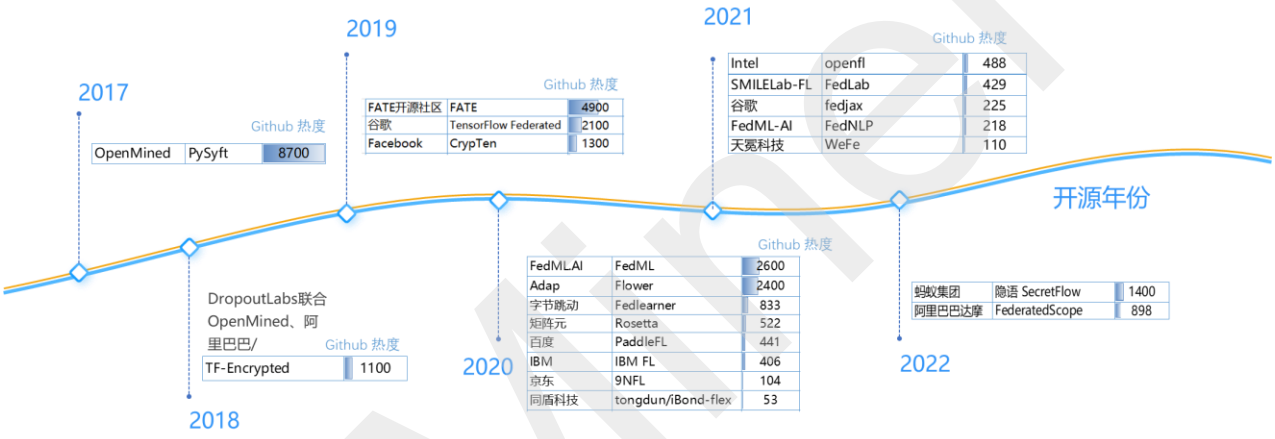


图 40 联邦学习框架开源趋势图

注：图中的数字代表该联邦学习框架在 GitHub 平台的热度值（截止到 2023 年 4 月 30 日）。其中，热度是指一个项目在 GitHub 上的 Star 数值；一个项目的 Star 数值越大，表示它的热度越高。

根据这些联邦学习框架在 GitHub（代码托管服务平台）上的热度排序（数据统计日期截至到 2023 年 3 月 31 日），发现 OpenMined 推出的 Pysyft 热度最高，FATE 开源社区的 FATE 热度居于第二，热度均超过 4000，FedML.AI 的 FedML、Adap 的 Flower、谷歌的 TFF 框架的热度也较高，均过 2000。联邦学习相关开源系统框架的详细信息如表 10 所示。

表 10 开源的联邦学习框架

GitHub 热度	发布方	系统名称	开源时间	系统特点
8700	OpenMined	PySyft	2017-7	● 一个用于安全和私有深度学习的 Python 库 ● 基于 PyTorch，使用 Unity Game Engine ● 安全多方计算 ● 联合学习、差异隐私
4900	FATE 开源社区	FATE	2019-2	● 工业级框架。分布式计算引擎支持 EGGROLL、Spark 等高性能计算引擎，AI 框架支持 Pytorch, TensorFlow, DeepSpeed ● 提供一站式的联邦模型企业级服务解决方案。提供多插件支持联邦学习企业和科研应用 ● 支持主流的分类、回归、聚类和迁移学习的联邦化算法 ● 提供多种安全计算协议支撑上层应用，支持同态加密协议、秘密共享协议、不经意传输协议和 DH 密钥交换算法等 ● 提供 40 多个联邦算法组件 ● FATE-LLM 模块支持 BERT，GPT-2，ChatGLM-6B, LLaMa 等多种大型自然语言处理模型
2600	FedML.AI	FedML	2020-7	● 支持分布式训练、移动设备/物联网训练、独立仿真 ● FedLLM 基于 MLOps 支持，具备 LLM 的训练、服务和可观察能力，在专有数据上构建企业自己的大模型
2400	Adap	Flower	2020-11	● 联邦学习框架，源自牛津大学的一个研究项目 ● 可定制、可扩展、可与任何机器学习框架一起使用
2100	谷歌	TensorFlow Federated	2019-3	● 可以选择 ML 模型架构 ● 模型设计理念以数据为主

GitHub 热度	发布方	系统名称	开源时间	系统特点
1400	蚂蚁集团	隐语 SecretFlow	2022-7	● 可信隐私计算框架，采用 Apache-2.0 协议 ● 统一支持 MPC、TEE、FL、HE、DP 等多种主流隐私计算技术 ● 密态计算设备 SPU ● " 明密文混合 "实现安全和性能的平衡 ● 多方安全计算
1300	Facebook	CrypTen	2019-10	● 安全多方计算
1100	DropoutLabs, OpenMined, 阿里巴巴	TF-Encrypted	2018-3	● 安全多方计算、同态加密 ● TensorFlow 中的加密机器学习框架
898	阿里巴巴达摩院	FederatedScope	2022-5	● 使用事件驱动的编程范式来构建联邦学习 ● 支持大规模、高效率的联邦学习异步训练，能兼容 PyTorch、TensorFlow 等不同设备运行环境，且提供丰富功能模块
833	字节跳动 bytedance	Fedlearner	2020-1	● 代码里有大量的 JS、HTML 模块 ● 强调联邦学习在推荐、广告等业务中的落地 ● 可输出性
522	矩阵元 LatticeX-Foundation	Rosetta	2020-8	● 安全多方计算 ● 基于 TensorFlow
488	Intel 英特尔实验室、英特尔物联网集团	openfl	2021-2	● Python* 3 项目 ● 开放式联合学习实用程序 ● 聚合器与框架无关
441	百度	PaddleFL	2020-2	● 可信计算 ● 基于飞桨（PaddlePaddle）和 Kubernetes ● 面向深度学习设计，提供在计算机视觉、自然语言处理、推荐算法等领域的联邦学习策略及应用场景 ● 简化大规模分布式集群部署

GitHub 热度	发布方	系统名称	开源时间	系统特点
				● 二次开发接口允许各方定义私有化的数据读取器 ● 提供了基础编程框架，并封装了一些公开的联邦学习数据集
429	SMILELab-FL	FedLab	2021-8	● 联邦机器学习的简单高性能计算框架
406	IBM	IBM FL	2020-11	● Python 框架，适用于企业环境 ● 用于私有云和公共云 ● 支持 Keras、PyTorch 和 TensorFlow 模型
225	谷歌	fedjax	2021-2	● 一种适用于研究、速度较快且简单易用的联邦学习模拟库
218	FedML-AI 南加州大学团队	FedNLP	2021-5	● 以研究为导向的联邦学习赋能 NLP 的 FedNLP 框架 ● 支持两种类型的模型：Transformer 和 LSTM
110	天冕科技 tianmiantech	WeFe	2021-9	● 同态加密算法 ● 内置多种常用机器学习算法和特征工程工具 ● 支持私有化、云端化以及安全一体机等多样化部署方式
104	京东	9NFL 九数联邦学习	2020 初	● 支持百亿级规模样本、百 T 级容量数据的超大规模的样本匹配、联合训练 ● 在电商推荐领域可实现线上业务落地 ● 实现分布式异步框架、Failover、拥塞控制等机制 ● 针对跨域与跨公网的复杂环境，设计了一系列的可用性与容灾的机制与策略
53	同盾科技	tongdun/iBond-flex	2020-2	● 一套标准化的联邦协议：约定了联邦过程中参与方之间的数据交换顺序，以及在交换前后采用的数据加解密方法

来源：根据公开资料整理

以上部分的联邦学习系统框架的详细介绍信息如下。

1. OpenMined——PySyft

PySyft 是开源社区 OpenMined 推出的一个用于安全和私有深度学习的 Python 库。它使用联邦学习、差分隐私和加密计算来解耦私人和敏感数据，可以在主要的深度学习框架中使用，例如 TensorFlow 和 PyTorch。PySyft 是在深度学习程序中启用可靠的隐私模型的首批尝试之一。

PySyft 的核心组件是称为 SyftTensor 的抽象。SyftTensors 旨在表示数据的状态或转换，并且可以链接在一起。链结构始终在其头部具有 PyTorch 张量，并且使用 child 属性向下访问由 SyftTensor 体现的变换或状态，而使用 parent 属性向上访问由 SyftTensor 体现的变换或状态。

开源地址：https://github.com/OpenMined/PySyft

PySyft 的系统框架如图 41 所示。

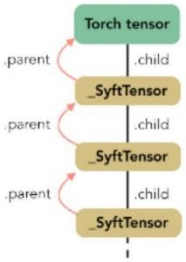


Figure 1: General structure of a tensor chain

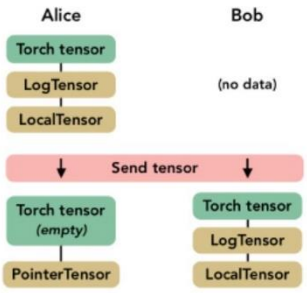


Figure 2: Impact of sending a tensor on the local and remote chains

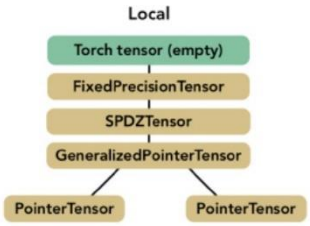


Figure 3: Chain structure of a SPDZ tensor

来源：https: //arxiv.org/pdf/1811.04017.pdf

图 41 OpenMined PySyft 系统框架

2． FATE 开源社区——FATE

FATE 开源社区是全球范围内规模较大的隐私计算联邦学习开源社区，拥有工业级联邦学习开源框架 FATE（Federated AI Technology Enabler），2019 年 2 月由微众银行开源发布，并于同年六月捐献给 Linux 基金会。当前，微众银行与工商银行、农业银行、中国银联、中国银行、建信金科、光大科技、中国电信、中国联通、中国移动等 25 家头部机构协力共建 FATE 开源社区为核心的联邦学习开源生态。FATE 开源框架累积发布 40 多个版本，覆盖 40 多种算法组件。中国信通院调查报告显示，FATE 开源框架有效降低了联邦学习的技术门槛，为很多 2020 年及之后出现的联邦学习产品的研发与应用提供了可靠的借鉴或参考。FATE 开源社区加速了联邦学习从“大厂”向小微 B 端企业的覆盖与普及的同时，让联邦学习产业生态及参与方从“单兵作战”走向生态化。

目前 FATE 开源社区的参与者多达 1200 余家企业和 500 余所高校和科研机构，牵头制定了国际标准 IEEE P3652.1《联邦学习架构和应用规范》，AIOSS 团标《信息技术服务 联邦学习 参考架构》等标准，撰写出版了《联邦学习》《联邦学习实战》等多本专著，为行

业提供理论和实践指导。

FATE 项目使用多方安全计算（MPC）以及同态加密（HE）技术构建底层安全计算协议，以此支持不同种类的机器学习的安全计算，包括逻辑回归、树算法、深度学习（人工神经网络）和迁移学习等。FATE 目前支持三种类型联邦学习算法：横向联邦学习、纵向联邦学习以及迁移学习。开源地址：https://github.com/FederatedAI/

FATE 整体架构如图 42 所示。FATE 主仓库包含 FederatedML 核心联邦算法库和多方联邦建模 Pipeline 调度模块 FATE-Flow，FATE 拥抱大数据生态圈，底层引擎支持使用微众银行自主研发的 EGGROLL 或者 Spark 进行高性能的计算。围绕 FATE 联邦学习生态，FATE 还提供了完整的联邦学习生态链，如联邦可视化模块 FATE-Board、联邦在线推理模块 FATE-Serving、联邦多云管理 FATE-Cloud，云原生联邦学习管理平台 KubeFATE， 联邦大模型 FATE-LLM 等。

来源：Architecture - FATE

图 42 FATE 系统架构

FederatedML 是 FATE 的联邦学习算法库模块，提供了 20+种联邦学习算法，支持纵

向联邦学习、横向联邦学习、联邦迁移学习三种联邦建模场景，覆盖了工业建模的数据处理、特征变换、训练、预测、评估的全建模流程。另外，封装了众多的多方安全计算协议以提供给上层算法的调度和支持联邦学习开发者的联邦算法开发。

FATE-Flow 为 FATE 提供了端到端联邦建模 Pipeline 调度和管理，主要包括 DAG 定义联邦建模 pipeline、联邦任务生命周期管理、联邦任务协同调度、联邦任务追踪、联邦模型管理等功能，实现了联邦建模到生产服务一体化。

FATE-Board 联邦学习建模的可视化工具，为终端用户提供可视化和度量模型训练的全过程。FATE-Board 由任务仪表盘、任务可视化、任务管理与日志管理等模块组成，支持模型训练过程全流程的跟踪、统计和监控等。

FATE-Serving 为 FATE 提供联邦在线推理服务，主要包含实时在线预测、集群管理与监控、在线模型管理与监控、服务治理等功能。

FATE-Cloud 是构建和管理联邦数据合作网络的基础设施，为跨机构间、机构内部不同组织间提供了安全可靠、合规的数据合作网络构建解决方案，实现多客户端的云端管理。

KubeFATE 为 FATE 提供云原生支持，提供云原生容器平台，灵活部署，自动化运维，支持 K8s，多云和跨云管理。

FATE-LLM 是基于 FATE 底座的构建的联邦大型框架，为大模型提供联邦学习支持，目前已经在横向联邦场景支持了 Bert、GPT-2、ChatGLM-6B、LLaMa 等大模型。

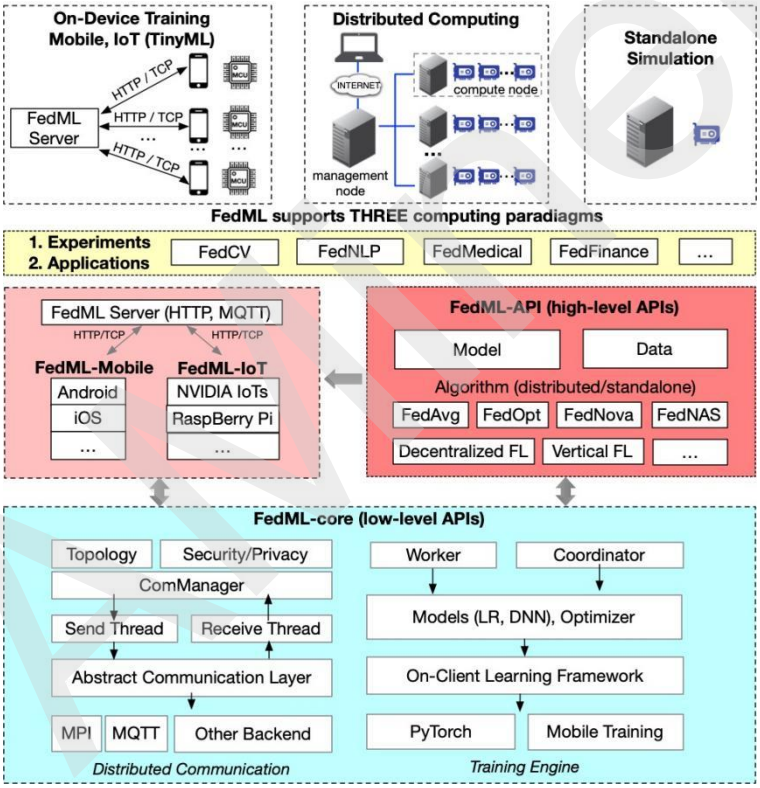
3． FedML.AI——FedML

FedML 是一个以研究为导向的联邦学习图书馆，支持分布式计算、移动/物联网设备上训练和独立模拟，可促进新的联合学习算法的开发和公平的性能比较。该成果曾获 NeurIPS

2020 联合学习研讨会最佳论文奖。发布方 FedML.AI 来自于美国南加州大学 USC 联合 MIT、Stanford、MSU、UW-Madison、UIUC 以及腾讯、微众银行等众多高校与公司联合发布的 FedML 联邦学习开源框架。其系统架构如图 43 所示。

FedML 还通过灵活且通用的 API 设计和参考基准实现和促进了各种算法研究。针对非 I.I.D 设置的精选且全面的基准数据集旨在进行公平比较。FedML 可以为联合学习研究社区提供开发和评估算法的有效且可重复的手段。

开源地址：https://github.com/FedML-AI/FedML

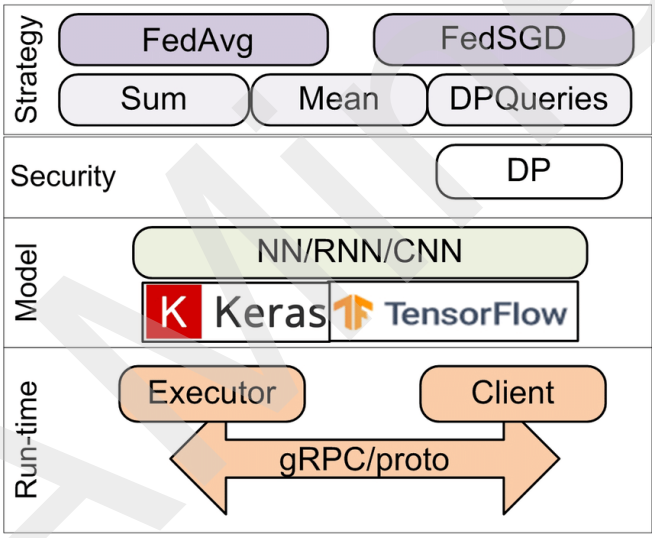


来源：FedML-AI/FedML，https://github.com/FedML-AI/FedML

图 43 FedML.AI/ FedML 系统架构

4. 谷歌——TensorFlow Federated，TFF

TensorFlow Federated project (TFF) 由谷歌公司开发和维护，是一个为联邦机器学习和其他计算方法在去中心化数据集上进行实验的开源框架。TFF 让开发者能在自己的模型和数据上模拟实验现有的联邦学习算法，以及其他新颖的算法。TFF 提供的建造块也能够应用于去中心化数据集上，来实现非学习化的计算，例如聚合分析。TFF 的接口有两层构成：联邦层（FL）应用程序接口（API）和联邦核心（FC）API。TFF 使得开发者能够声明和表达联邦计算，从而能够将其部署于各类运行环境。TFF 中包含的是一个单机的实验运行过程模拟器。该联邦学习的框架如图 44 所示。



来源：Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis [69]

图 44 谷歌 TFF 框架图

在实现方面，TensorFlow 专门为联邦学习推出了一个学习框架（TensorFlow

69 *Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis*, Dec 2020, https://www.researchgate.net/figure/Architecture-of-TensorFlow-Federated-TFF_fig4_348067413, uploaded by Evgeniy D. Shalugin

Federated，简称 TFF），现有的 TensorFlow（简称 TF）或 Keras 模型代码通过一些转换后就可以变为联邦学习模型，甚至可以加载单机版的预训练模型，以迁移学习的模式应用到分散式数据的机器学习中。

不同于分布式训练理念，**TFF 框架设计理念是以数据为主，**而不是代码分离上。在编写模型、训练代码的时候，将 clients 和 server 看作一个整体，同一个文件里不需要分割开 Server 端（S 端）和 Clients 端（C 端）的代码，C 端和 S 端的区分是在代码逻辑层面的。也就是说，用户在编写 TFF 代码时，不需要指明某段代码是应该运行在 C 端还是 S 端，仅需要指出每个数据是储存在 C 端/S 端、是全局唯一的还是有多份拷贝的即可。类似 TF 的 non-eager 模式，当用户编写完模型代码和训练代码后，TFF 会自动地将代码分别放置到 clients 和 server 设备上。用户只要关注模型架构、C&S 端交互的数据格式、聚合多 clients 模型的方式即可。

TFF 通过 Python 代码来编写运算逻辑，实际运行则是编译成另一种语言去执行，以便让模型能运行在真实分布式场景下。

开源地址：https://github.com/tensorflow/federated

5． 字节跳动——Fedlearner

字节跳动联邦学习平台 Fedlearner 基于字节跳动在推荐和广告领域积累的机器学习建模技术和个性化推荐算法，可以支持多类联邦学习模式，已经在电商、金融、教育等行业多个落地场景实际应用。该平台已经于 2020 年初开源并持续更新，开源地址：https://github.com/bytedance/fedlearner 。

Fedlearner 联邦学习平台整个系统包括控制台、训练器、数据处理、数据存储等模块，各模块对称部署在参与联邦的双方的集群上，透过代理互相通信，实现训练。

Fedlearner 双方在发起训练之前，必须要基于双方的数据进行求交，找出交集从而实现模型训练。训练数据求交的方式主要分为两种：流式数据求交、PSI 数据求交。

6. 百度——PaddleFL

PaddleFL 是一个基于百度飞桨（PaddlePaddle）的开源联邦学习框架。PaddleFL 提供很多联邦学习策略及其在计算机视觉、自然语言处理、推荐算法等领域的应用，例如，横向联邦学习（联邦平均、差分隐私、安全聚合）和纵向联邦学习（带 privc 的逻辑回归，带 ABY3 的神经网络）。研究人员可以用 PaddleFL 复制和比较不同的联邦学习算法。

此外，PaddleFL 还提供传统机器学习训练策略的应用，例如多任务学习、联邦学习环境下的迁移学习、主动学习。依靠 PaddlePaddle 的大规模分布式训练和 Kubernetes 对训练任务的弹性调度能力，PaddleFL 可以基于全栈开源软件轻松地部署。PaddlePaddle 背靠百度的信息库，提供的预训练模型的准确率较高。

开源地址：https://github.com/PaddlePaddle/PaddleFL 。

整体架构如图 45 所示。

来源：https://gitee.com/paddlepaddle/PaddleFL

图 45 百度 PaddleFL 整体架构

PaddleFL 中主要提供两种解决方案：Data Parallel 以及 Federated Learning with

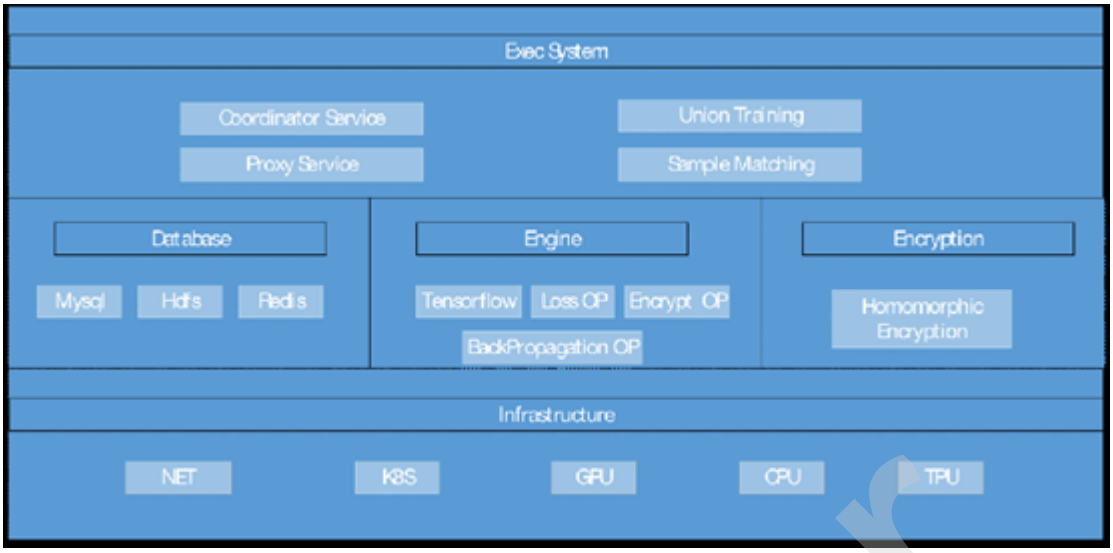
MPC (PFM)。通过 Data Parallel，各数据方可以基于经典的横向联邦学习策略（如 FedAvg，DPSGD 等）完成模型训练。此外，PFM 是基于多方安全计算（MPC）实现的联邦学习方案。作为 PaddleFL 的一个重要组成部分，PFM 可以很好地支持联邦学习，包括横向、纵向及联邦迁移学习等多个场景。

7. 京东——九数联邦学习 9NFL

京东自研的九数联邦学习平台（9NFL）于 2020 年初正式上线。9NFL 平台基于京东商业提升事业部 9N 机器学习平台进行开发，在 9N 平台离线训练、离线预估、线上推断（inference）、模型的发版等功能的基础上，增加了多任务跨域调度、跨域高性能网络、大规模样本匹配、大规模跨域联合训练、模型分层级加密等功能。整个平台可以支持百亿级/百 T 级超大规模的样本匹配、联合训练，并且针对跨域与跨公网的复杂环境，对可用性与容灾设计了一系列的机制与策略，保障整个系统的高吞吐、高可用、高性能。

开源地址：https://github.com/jd-9n/9nfl

9NFL 整体系统架构分为四大模块：整体调度与转发模块、资源管理与调度模块、数据求交模块、训练器模块。如图 46 所示。



来源：新浪 VR [70]

图 46 九数联邦学习平台（9NFL）

3.2.2 非开源框架与系统

非开源的联邦学习框架基本上都是由企业推出的。根据其正式发布时间进行排序，发现这些联邦学习框架最多集中发布于 2020 年，如图 47 所示。其中，发布时间较早的是翼方健数的联邦学习框架，以及星云 Clustar 的 AIOS，两者均于 2019 年发布。电信与银行两个领域已有行业级的联邦学习框架。其中，农业银行、光大、浦发等几家银行发布的联邦学习平台较多是基于 FATE 框架构建或延续的。

[70] 京东开源超大规模联邦学习平台，2020-09-15 来源：新浪 VR，http://vr.sina.com.cn/news/hz/2020-09-15/doc-iivhvpwy6836041.shtml

图 47 非开源的联邦学习框架发布趋势图

非开源联邦学习系统框架的详细信息如表 11 所示。

表 11 非开源的联邦学习系统一览

发布时间	发布方	系统名称	系统特点
2019 年 4 月 15 日	翼方健数	翼数坊 XDP	● 基于隐私计算的原理和应用 ● 通过多方安全计算 MPC/同态加密、联邦学习、安全沙箱计算/TEE 等技术实现 ● 通过自主研发的 DaaS 服务进行数据治理和清洗以达到数据可用
2019 年 9 月 5 日	星云 Clustar	AIOS	● 以联邦学习和区块链作为基础设施 ● 采用 FATE 联邦学习软件框架
2019 年 9 月 19 日	华为	NAIE	目前以横向联邦为基础，内置了众多联邦学习能力，包括联邦汇聚、梯度分叉、多方计算、压缩算法等。
2020 年底	星环科技	Sophon FL	● 底层为分布式架构，使用差分隐私、同态加密、不经意传输和可信计算等隐私保护机技术
2020 年 3 月 23 日	腾讯	Angel PowerFL	● 支持超大规模数据量的多方联合建模 ● 有高容错性 ● 不依赖于可信第三方
2020 年 4 月 23 日	上海富数科技	FMPC	● 密文训练联邦学习误差小于 1% ● 安全计算支持的算法包括：普通多方计算、统计分析、机器学习（LR、DT、RF、LightGBM 等） ● 机器学习训练收敛速度提高了 3 倍；匿踪查询 100 亿条+记录秒级响应

发布时间	发布方	系统名称	系统特点
			● 支持本地私有化、对等网络链接的部署
2020 年 5 月 27 日	光之树科技	天机可信计算框架、云间联邦学习平台	● 基于芯片 TEE 技术和其他加密技术的可信计算体系 ● 基于机器学习、深度学习算法和加密协议的安全计算框架
2020 年 8 月 28 日	平安科技	蜂巢平台	● 定位是服务于营销、获客、定价、风控、智慧城市和智慧医疗 ● 支持传统的统计学习以及深度学习的模型，比如逻辑回归、线性回归、树模型等 ● 提供加密方式，支持同态加密等多方安全计算机制。在模型训练中，对梯度进行非对称加密，整合梯度和参数优化、更新模型；最后加密原始传输数据，实现推理结果 ● 支持单机和多机训练 ● 可使用 CPU 和 GPU 训练 ● 支持多种深度学习框架，如 TensorFlow，Keras，Pytorch，Mxnet
2020 年 10 月 12 日	京东数科	Fedlearn	● 提出了并行加密算法、异步计算框架、创新联邦学习等技术架构，达到融合亿级规模数据的能力 ● 在通讯方面，引入中心化数据交换的概念，使得数据交换独立于参与方 ● 采用异步计算框架，提高了模型训练速度，并推动异步联邦学习的发展 ● 应用于信贷风控、智能营销等方向
2020 年 12 月	中国电信	天翼云诸葛 AI-联邦学习平台	● 加密的分布式机器学习技术 ● 使用多方安全计算、数据加密等核心技术 ● 高性能加密算法库
2021 年 2 月	华为云	FedAMP	● 首创自分组个性化联邦学习框架，引入了一种注意消息传递机制 ● 让拥有相似数据分布的客户进行更多合作，并对每个客户的模型进行个性化定制 ● 已被集成至华为云一站式 AI 开发管理平台 ModelArts 联邦学习服务中
2021 年 4 月	华为云	可信智能计算服务	● 基于安全多方计算 MPC、区块链等技术 ● 实现了联盟管理、计算节点管理、联邦数据分析作业、

发布时间	发布方	系统名称	系统特点
		TICS	联邦机器学习作业、联邦预测作业等功能
2021 年 6 月	联易融	蜂隐联邦学习平台	● 支持本地化与 SAAS 部署，可应用于供应链金融业务中，合同、票据 OCR、关键要素提取、文本分类等图像和 NLP 场景下的深度学习联合建模
2021 年 6 月	洞见科技	洞见数智联邦平台（INSIGHTTONE）	● 基于隐私计算和区块链技术的金融级隐私保护计算平台产品
2021 年 7 月	百度	百度点石联邦学习平台	● 兼容 PaddleFL ● 采用集群分布式、并发计算、算法优化等策略 ● 提供数据核实、匿踪查询、联合分析、联合建模、在线预测等 ● 支持私有化+公有云的部署方式，并且能够与区块链、边缘计算等业务进行融合
2021 年 9 月	中国人工智能产业发展联盟 AIIA	电信领域联邦学习技术架构	● 支持多参与方或多计算结点之间在不共享原始数据的基础上联合进行高效的模型训练 ● 与物联网、边缘计算、5G/6G 等技术相结合，支撑智能化应用
2021 年 9 月	中国移动	基于联邦学习的分布式智能架构	● 四项关键技术：多主体协同训练、网络能力登记、动态成员管理、训练策略调优 ● 正式写入 3GPP R18 技术标准 TS 23.288
2021 年 11 月	新心数科	新心数述联邦学习平台	● 多方安全计算金融应用技术
2021 年 12 月	字节跳动安全研究团队	火山引擎 Jeddak 联邦学习平台	● 融合了多方安全计算 MPC、全同态加密 FHE、差分隐私 DP、可信计算 TEE 等多种技术
2022 年 2 月	中国银联	中国银联联邦学习平台	● 多方安全计算 ● 采用开放云原生架构
2022 年 11 月	中国工商银行	联邦学习平台	● 企业级框架 ● 算法层、技术框架层均基于开源 FATE 框架；AI 工作站为自主开发 ● 具备数据安全引入、数据安全对齐、数据安全计算三大优势
2022 年 11 月	光大银行	光大联邦学习平台	● 基于 FATE 框架构建，引入了区块链平台、联合激励模型等 ● 采用 Exchange 星型模式进行部署

来源：根据公开资料整理

以上部分非开源的联邦学习系统平台的介绍信息如下。

1. 腾讯——Angel PowerFL

Angel Power FL（原名 AngelFL）安全联合计算是基于腾讯自研的多数据源联合计算技术，提供安全、易用、稳定、高性能的联邦机器学习、联合数据分析解决方案，助力数据融合应用。它构建在 Angel 机器学习平台[71]上，利用 Angel--PS 支持万亿级模型训练的能力，将很多在 Worker 上的计算提升到 PS（参数服务器）端；Angel PowerFL 为联邦学习算法提供了计算、加密、存储、状态同步等基本操作接口，通过流程调度模块协调参与方任务执行状态，而通信模块完成了任务训练过程中所有数据的传输。采用去中心的架构设计，全自动化流程，算法支持 LR、XGBoost、PCA、用户自定义神经网络模型（如 MLP、CNN、RNN、Wide&Deep，DeepFM, DSSM 等）[72]。Angel PowerFL 联邦学习已经在腾讯金融云、腾讯广告联合建模等业务中开始落地。目前主要应用产品是腾讯云安全隐私计算。Angel Power FL 目前没有开源，平台架构如图 48 所示。腾讯于 2021 年 1 月 22 日申请公开“联邦学习方法、装置、计算机设备及介质”专利信息，公开号为 CN112257876A。

71 github.com/Angel-ML

72 Angel PowerFL 安全联合计算_联邦学习_联合数据分析 - 腾讯云 (tencent.com)

来源：腾讯 Angel PowerFL 联邦学习平台[73]

图 48 腾讯 AngelFL 联邦学习系统架构图

2. 京东科技——Fedlearn

京东数字科技集团（简称：京东数科，现名：京东科技）于 2020 年 10 月推出自主研发的联邦学习平台 Fedlearn。Fedlearn 平台具有“六位一体”核心能力：多自研联邦学习算法、多方同态加密、轻量级分布式架构、区块链与联邦学习融合、数据安全容器、一站式操作平台。

京东科技 Fedlearn 平台具有三大特点：

第一，在数据和模型隐私方面，不同参与方之间没有直接交换本地数据和模型参数，而

73 Angel PowerFL 安全联合计算_联邦学习_联合数据分析 - 腾讯云 (tencent.com)

是交换更新参数所需的中间数值。为了避免从这些中间数值中恢复数据信息，采用增加扰动的方法对这些数值进行保护，确保了数据和模型的隐私安全；

第二，在通讯方面，引入中心化数据交换的概念，使得数据的交换独立于参与方；

第三，采用异步计算框架，提高了模型训练的速度。

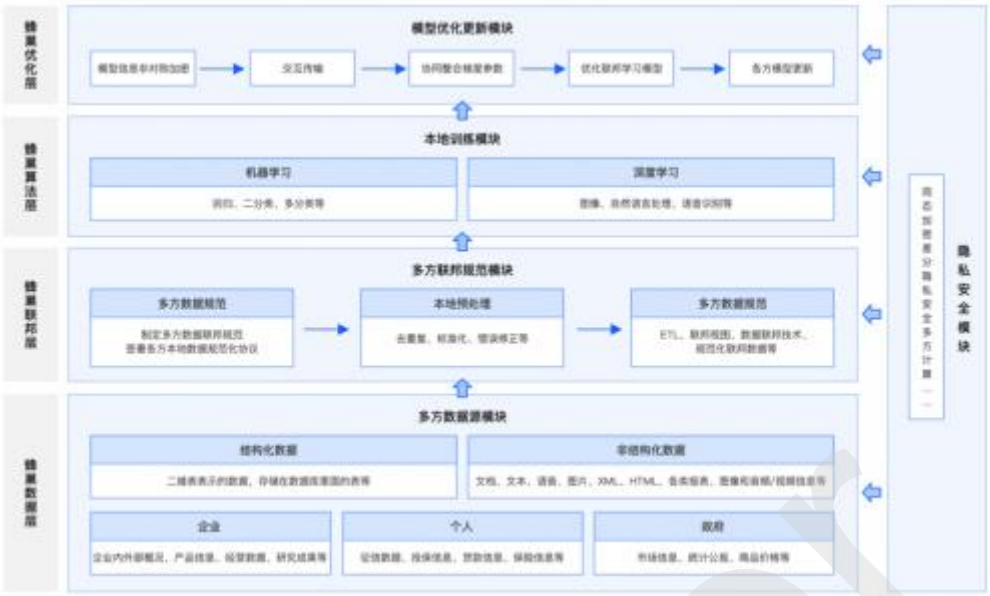
Fedlearn 平台融合了密码学、机器学习、区块链等联邦学习算法，搭建出一套安全、智能、高效的链接平台，在各机构数据不用向外传输的前提下，通过联合多方机构数据，实现共同构建模型等多方数据联合使用场景，获得加成效应。相较于传统的数据共享交换方法，Fedlearn 平台创新性地提出了并行加密算法、异步计算框架、创新联邦学习等技术架构，在保证数据安全的前提下提升学习效率，并逐步达到融合亿级规模数据的能力。

京东科技 Fedlearn 平台实现了“基于核的非线性联邦学习算法”。这一方法不传输原始样本及梯度信息，充分保护数据隐私；并使用首创的双随机梯度下降，大大提高计算速度，充分利用计算资源，通过增加扰动提高数据的安全保护。

产品地址：https://www.jddglobal.com/products/digitalgateway

3． 平安科技——蜂巢

平安科技研发的蜂巢联邦智能平台，是数据安全保护、企业数据孤岛、数据垄断、数据壁垒等问题的商用级解决方案。它能够让参与方在不共享原始数据的基础上联合建模，从技术上打破数据孤岛，从而综合化标签数据，丰富用户画像维度，从整体上提升模型的效果，实现 AI 协作。蜂巢平台的功能框架如图 49 所示。



来源：平安官网链接 https://tech.pingan.com/

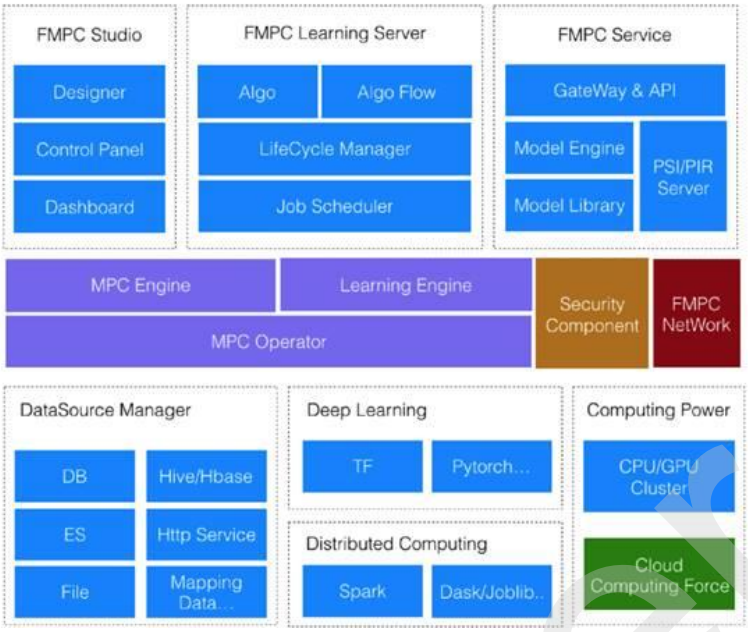
图 49 蜂巢平台功能结构

平安科技联邦智能平台蜂巢的建模是在保护用户隐私的前提下进行。原始数据不离开用户，建模所交换的是模型的中间参数和梯度。此外，采用 GPU 等异构计算芯片来加速联邦学习的加密和通信过程，从而达到效率升级的效果。

4. 富数科技——FMPC

富数多方安全计算平台（FMPC）是上海富数科技旗下产品，目前未开源，主要通过体验或者服务购买方式使用。产品官网地址：https://www.fudata.cn/

FMPC 目前公开的技术架构如图 50 所示。



来源：两大主流联邦学习产品体验_hellompc 的博客-CSDN 博客

图 50 富数科技 FMPC 系统架构

FMPC 架构具有以下**特点**：

① 联邦学习：原始数据不出门，参与各方本地建模；没有敏感数据流通，只交互中间计算结果；整个模型被保护，参与各方只有自己模型参数；私有化部署；开放 API 快速开发；支持主流机器学习算法，如 LR, DT, RF, Xgboost 等；建模速度快 3 倍；密文训练精度误差<1%。

② 多方安全计算：落地应用计算量 1.1 万+次/天；支持多方数据安全求交；支持一次多项式；支持多方归因统计分析；支持多方多维数据钻取分析；私有化部署。

③ 匿踪查询：支持 100 亿+条记录；秒级响应时间；查询授权存证；甲方查询信息不泄露；加密隧道避免中间留存；私有化部署。

④ 联盟区块链：联盟节点 30+；高性能扩展 1 万 TPS；合约调用 20 万次/天；电子存证和智能合约；隐私保护协议；快捷部署场景应用；开源开发社区。

5. 星云 Clustar ——AIOS

星云 AIOS（AI Operating System）是一款具备高性能、高可靠、高灵活及高扩展特性的人工智能操作系统，由高性能 AI 加速中间件、深度学习训练平台及数据推理平台三个子系统构成，为用户提供数据处理、模型训练、推理服务及 AI 应用等完整的 AI 解决方案。总体框架如图 51 所示。

来源：星云 Clustar 官网

图 51 星云 AIOS 系统框架

AIOS 产品矩阵 [74]

① 星云联邦数据网络（数据）：通过 API 提供服务，隐私保护的大数据安全连接平台，以联邦学习和区块链作为基础设施，拼接多方数据源，建立企业间数据合作的安全桥梁，实现企业效能和数据价值的最大化。

② 星云联邦计算平台（框架）

FATE 联邦学习软件框架，由多个主要功能模块构成：联邦算法仓库、联邦训练服务、联

74 来源：星云 Clustar 官网 https://www.clustarai.com/productService/guardianDock/privacyDataSystem

邦推理服务、可视化面板。企业可以轻松的通过可视化面板直接对各类联邦算法模型进行调用与实验，可大幅降低联邦学习的使用门槛。

星云 FATE 企业版，为基于数据隐私保护的安全建模过程提供丰富的可视化呈现，为终端用户提供可视化和度量模型训练的全过程，支持模型训练过程全流程的跟踪、统计和监控等，帮助模型开发人员快速搭建联邦学习任务，可根据客户需求深度定制开发。

来源：星云 Clustar 官网

图 52 星云 FATE 企业版联邦架构层

③ 星云隐私计算一体机（算力）

针对数据使用方和数据提供方提供不同产品方案：一体机完美融合 CPU/GPU/FPGA 服务器、FATE 和 FDN，开箱即用，大大降低了企业使用联邦学习的门槛；密态计算效率提升 400%、降低延迟 300%、降低功耗 70%，强大算力推动各方数据协作，实现数据资产变现。

6. 光之树科技——天机、云间

光之树科技旗下有**天机可信计算框架**和**云间联邦学习平台**两个隐私计算产品，提供从共享模型训练即“云间”联邦学习到基于芯片 TEE 技术的“天机”机密计算在内的全流程、多场景安全多方计算框架，保护数据资产权益，安全发挥数据价值。

① 天机可信计算框架

天机可信计算框架于 2019 年 8 月发布。它是一个基于芯片中的可信执行环境（TEE：Trusted Execution Environment）和其他加密技术的可信计算体系，主要通过将数据从共享到联合计算在硬件创建的可信执行环境中进行的方式，从而做到数据可用不可见，确保了数据隐私、安全和合规。它具有的安全机制可同时保护模型和计算过程中的数据，可直接运行机器学习级别的高复杂度计算 / 模型，兼容当前主流的大数据和机器学习框架包括 xgboost、scikit-learn（支持逻辑回归等算法）、TensorFlow 等。用户无需二次开发，可快速部署于公有云、私有云或线下环境，并兼容主流数据库以及数据服务。它搭配区块链用于数据存证和权限控制，做到数据使用全程可追溯可审计。

来源：光之树官网[75]

图 53 天机可信计算框架总体框架图

② 云间联邦学习平台

云间联邦学习平台是基于机器学习、深度学习算法和加密协议的安全计算框架。数据无需离开本地，主要通过将模型下发到数据联盟本地服务器训练的模式，以最小的数据交互对模型进行更新和迭代的计算方法，从而达到保证数据安全性的前提下多方联合计算的目的。

75 来源：光之树官网 https://www.guangzhishu.com/

应用于普惠金融、贸易金融、保险反欺诈、供应链金融等场景。具有以下优势：

a. 安全性：通过联邦学习特有的算法保证数据不出本地，并通过加密协议确保数据交互的安全性。

b. 一键式训练和模型部署：拥有自动建模功能，支持多种机器学习和深度学习的联邦学习训练和模型部署。

c. 可视化：对训练状态和训练效果进行全方位监控。

d. 快速部署：支持多种数据库的接入，快速进行私有化部署。

e. 场景多样性：支持多种场景，包括横向和纵向学习。

7. 翼方健数——翼数坊 XDP

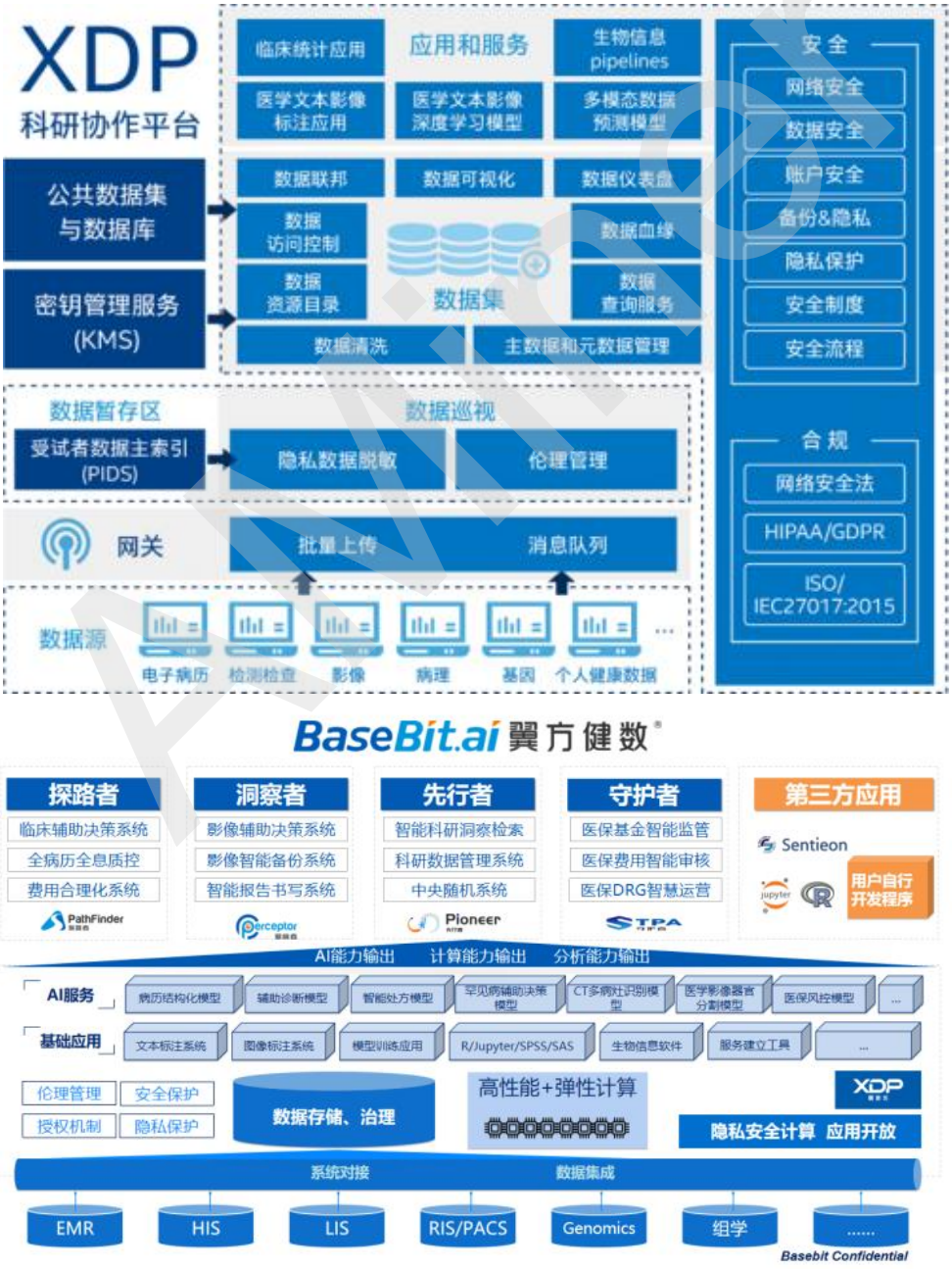
翼方健数通过多方安全计算 MPC/同态加密、联邦学习、安全沙箱计算/TEE 等前沿技术，实现数据“可用而不可见”，提出“数据和计算互联网”（IoDC）的概念并付诸实践。在技术运用层面，翼方健数自主研发的 DaaS 服务，可以对多组学数据、表型数据、临床数据进行数据治理和清洗，达到数据可用的状态，从而实现不分享原始数据、数据在平台内授权使用、通过计算来分享数据的价值这一目的。

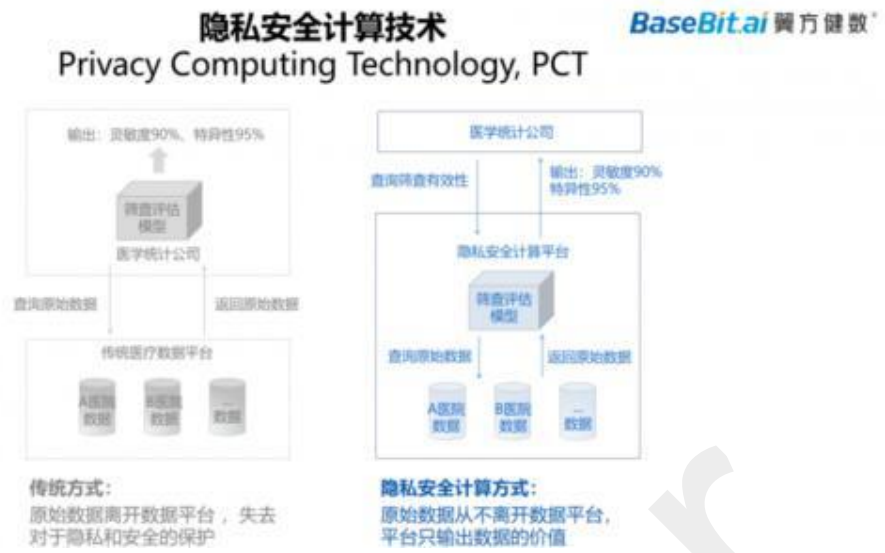
2019 年 4 月 13 日，医疗数据隐私计算平台 XDP 翼数坊 v1.0 发布。翼数坊 XDP 利用隐私安全计算技术，实现合理的、授权下的数据价值共享，创造数据流通性，降低数据科学的门槛。翼数坊 XDP 平台的整体设计从最底层开始，完全基于隐私计算的原理和应用。采用了一系列新型技术，包括多方安全计算、同态加密、联邦学习、可信执行环境、零知识验证等，具有开放、安全、整合、高效、智能五大性能。

XDP 平台可基于智能合约技术追溯源数据集，建立“数据血缘”。此外，XDP 构筑出的封闭的数据存储和计算环境，将从各医疗机构采集到的数据进行清洗、脱敏、归一，形成 DaaS

数据集后进行加密，杜绝数据的泄露。形成的数据权限管理系统，可以确保平台用户所有者授权后才能使用数据，数据所有者的权益也可以得到保障。

平台数据仅限于在平台内使用，即使被授权的数据也不能离开平台，从而进一步保护数据所有者的权益。XDP 平台上可以关联、集成并融合各个医疗机构、检验检查以及健康数据；数据应用方面，XDP 平台拥有分层可扩展的技术架构，能够实现高密度存储、快速访问和迅速分析计算，并且支持多种人工智能模型的建立，从而多角度直观分析和展示数据。





来源：翼方健数官网 [76]

图 54 翼数坊 XDP 平台总体架构

8. AIIA——电信领域联邦学习技术架构

2021 年 9 月 27 日，中国人工智能产业发展联盟（AIIA）正式发布《电信领域联邦学习技术应用白皮书》[77]。该白皮书由中国信息通信研究院、中国移动通信有限公司研究院、联通数字科技有限公司、华为技术有限公司等共同编写。该白皮书对联邦学习应用于电信行业的技术潜力与应用前景进行了分析，并介绍了电信联邦学习技术架构（如图 55 所示）、技术分类、部署框架与关键优化技术等内容。白皮书指出，电信领域联邦学习的发展与落地应用尚处于发展初期，通过需求牵引提升关键技术，强化电信联邦学习标准与测评工作，可加快电信联邦学习落地应用与产业发展。

[76] 来源：翼方健数官网 https://www.basebit.me/

[77] 来源：AIIA 正式发布《电信领域联邦学习技术应用白皮书》

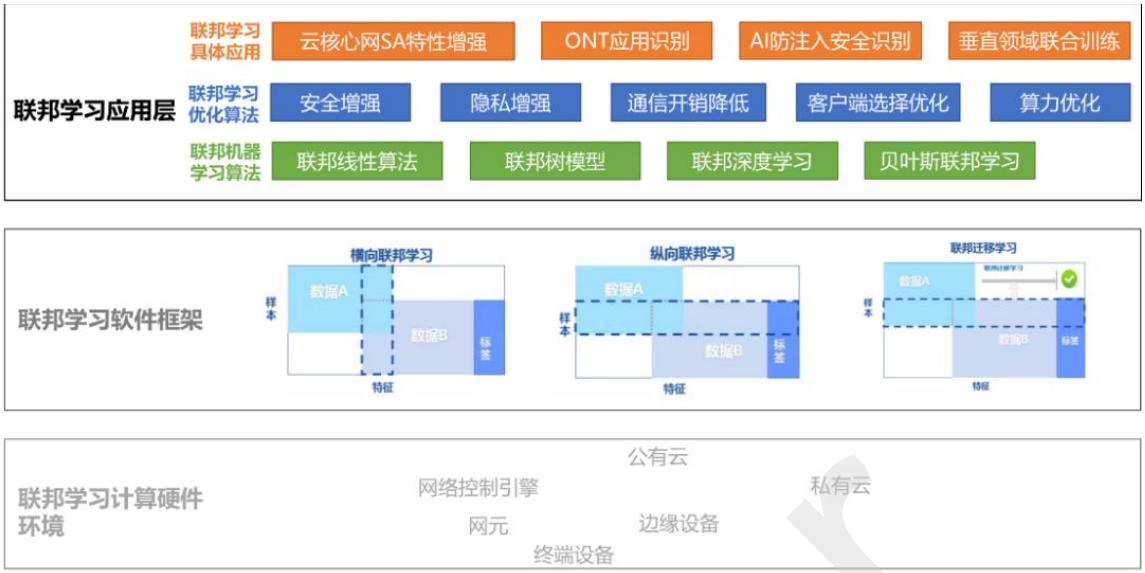


图 55 电信领域联邦学习技术架构

9. 中国工商银行——工行联邦学习平台框架

工商银行依托自主建设的数据安全技术平台及联邦学习等隐私计算技术平台，强化数据安全和个人信息保护，挖掘数据价值，促进数据智能化应用。其中，数据安全技术平台框架分为安全服务、核心功能、基础能力三层；工商银行自研推出的企业级联邦学习平台，目前上线平台已具备数据安全引入、数据安全对齐、数据安全计算三大优势，为金融数据安全合规地流通和使用提供可靠的技术产品。联邦学习平台框架分为技术框架层、算法层、AI 工作站三层，如图 56 所示。其中 AI 工作站主要为工行自主开发，目前已经完成可视化建模流水线、模型管理、隐私求交三个部分的工程开发，能够初步满足用户的联邦需求。算法层基于开源 FATE 框架集成了横向联邦、纵向联邦的算法。技术框架层延续 FATE 框架的算法，主要集成同态加密的安全协议，后续需要通过外部引入完善安全协议。

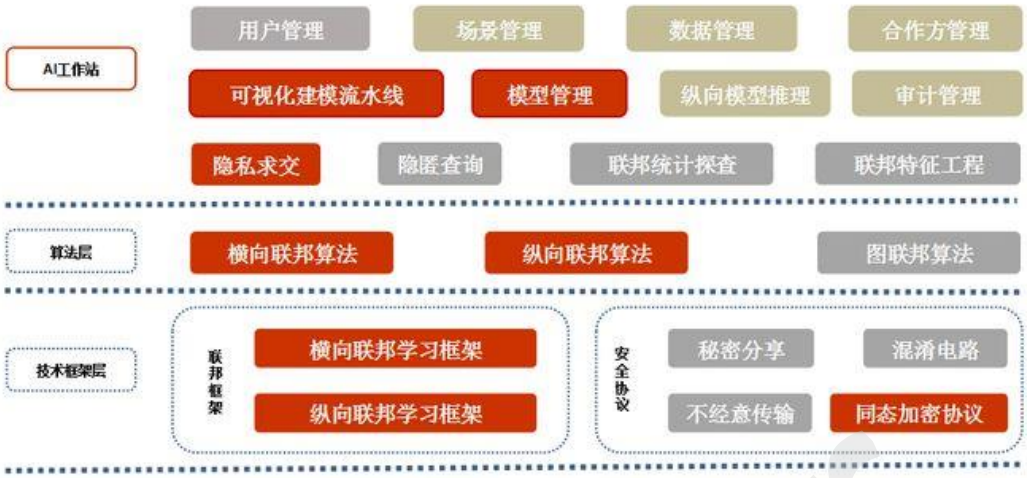


图 56 工行联邦学习平台框架

3.3 联邦学习行业应用现状

通过新闻事件分析挖掘和搜索系统 NewsMiner 数据库，从已公开的新闻数据发现，联邦学习技术的行业应用最早出现在 2018 年，当时被应用在金融、IT 和通信领域，后来几年其应用探索逐渐扩展到智慧城市、教育、汽车等其他多个行业领域。

1. 在金融业应用

联邦学习在金融业应用目前处于框架设计、模型构建、合作探索、在几个业务场景中初步试点的阶段，应用主要体现在软硬件解决方案、数据安全、隐私保护、信贷营销、金融风险管理等方面。推进联邦学习在金融业应用落地的参与主体主要是科技公司（百度、腾讯、京东等）、互联网金融机构（微众银行、蚂蚁金服等）、少数传统商业银行（江苏银行、浦发银行、建设银行等）等。相关信息如表 12 所示。

表 12 2016–2022 年度联邦学习技术在金融业应用动态

金融业应用场景	标题	年-月	来源
金融风险管理	建设银行创新合作伙伴揭晓 京东数科、科大讯飞、同盾科技等企业入选	2018-06	CSDN

金融业应用场景	标题	年-月	来源
数据安全、隐私保护	蚂蚁金服推出“摩斯 MORSE”多方安全计算平台	2018-08	CSDN
小微信贷	微众银行开源 FATE	2019-02	新华网
解决数据孤岛问题	微众银行与瑞士再保险合作探讨联邦学习技术如何解决数据孤岛的挑战，助力保险行业共同发展。	2019-5	同花顺
深度联合建信用模型、客服、侦测欺诈	同盾科技与招联金融共建 AI 创新实验室 联邦学习为主攻方向之一	2019-06	新华网
高性能分布式异构计算技术、软硬件解决方案	星云和微众达成合作，推动 AI 新技术联邦学习的发展	2019-08	科学中国
提升金融服务质量、安全深入地挖掘数据价值	微众银行和腾讯云合作升级 联邦学习携手神盾沙箱共建行业标杆	2019-09	搜狐
数据价值共享、加速金融行业转型进化	英特尔助力平安科技联邦学习落地	2019-09	新浪
多方联合建模	蚂蚁金服基于 MPC 的共享学习	2019-09	ITPUB
支持多方纵向联邦建模、支持 spark 引擎、支持 FATEServing 服务治理、支持 secureboost 在线预测、支持公有云和私有云部署和使用	微众银行发布 FATE v1.1，联合 VMware 中国研发开放创新中心云原生实验室的团队发布 KubeFATE 项目。FATEBoard：简单高效，联邦学习建模过程可视化	2019-11	贤集网
打造大规模 AI 协作通用方案	微众银行与蒙特利尔学习算法研究所合作打造安全金融 AI 实践	2019-12	腾讯
智能化信用卡	江苏银行与腾讯安全举行联邦学习线上发布会，将联合共建“智能化信用卡管理联合实验室”，围绕联邦学习开展合作	2020-04	CSDN
金融数据保密、信贷业务综合评估、控制企业技术升级成本	编织联邦学习的产业路径，腾讯向金融智能化的更远处进发	2020-04	搜狐
信用卡管理	江苏银行与腾讯安全共建“智能化信用卡管理联合实验室”，围绕联邦学习开展合作。	2020-5	腾讯
金融产品管理、营销、安全风控、客户服务、运营管理	百度金融安全计算平台（度信）建设与实际应用	2020-06	腾讯安全
普惠金融试点应用	腾讯安全灵鲲与浦发银行、北京金控合作的“多方数据学习‘政融通’在线融资项目”入选北京金融	2020-8	第一财经

金融业应用场景	标题	年-月	来源
	科技创新监管第二批 11 个试点名单，成为基于联邦学习的普惠金融试点应用。		
信贷风控	腾讯安全天御凭借其在信贷风控场景的落地实践，荣获首个 CCF-GAIR “联邦学习应用奖”	2020-08	搜狐
反诈骗技术、普惠金融	反诈骗、管控金融风险，腾讯安全发力联邦学习技术	2020-09	新浪
金融服务、风险识别能力、数字营销	京东数科自研联邦学习平台 Fedlearn，助力数据安全保护并大幅提升学习效率	2020-10	机器之心
电商营销、广告投放、个性化内容推荐、广告推荐	字节跳动破局联邦学习：开源 Fedlearner 框架，广告投放增效 209%	2020-10	CSDN
金融风控、营销	光大科技加入 FATE 联邦学习社区技术指导委员会（TSC）并贡献关键算法源码——基于 “可验证秘密分享技术” 研发的 “联邦学习平台多方安全求和算法”	2021-1	搜狐
数字信贷	新网银行联合多家金融机构、互联网公司、公共单位，探索联邦学习在数字信贷领域的应用，将商业银行的金融大数据挖掘和建模经验与互联网公司、数据生态和公共单位丰富的客户画像数据及完善的大数据支持环境相结合，打破数据孤岛、保护客户隐私、实现数据价值。	2021-3	中国金融电脑
健康险的保险获客	数鸣科技获过亿元 A 轮融资，用 AI 算法赋能医疗健康险	2021-3	新浪
银行风险管理	京东金融云携手平安蜂巢联合开发出行业领先的跨平台联邦建模数据合作安全保护方案，应用于不同联邦学习平台之间的实时通信，实现了联邦学习跨平台的重大创新突破。双方基于联邦学习技术进行联合开发和方案部署，为平安银行提升风险管理自动化水平赋能，在两方数据特征无需出库的前提下，较单方模型效果提升 30%以上。	2021-3	金融界
数据融合应用	央行启动金融数据综合应用试点	2021-5	新华网
信贷风险控制、金融营销与广告投放	微众银行的普惠金融 AI 全布局	2021-6	雷锋网
数据安全与保障数据合规流通	星云 Clustar 与 VMware 联合发布联邦学习企业级解决方案	2021-9	新华网

金融业应用场景	标题	年-月	来源
数据共享应用	北京法定数字货币试验区揭牌，中国人民银行副行长范一飞表示，要深度挖掘数据价值，重点要集中在数据治理、数据应用、数据保护方面。探索应用多方安全计算、联邦学习等技术，实现数据可用不可见、数据不动价值动。	2021-9	新浪
金融数据安全与合规流通	星云 Clustar 与 VMware 联合发布联邦学习企业级解决方案	2021-9	中国网
中小微企信贷评估	应科院伙渣打及 PAOB 以联盟式学习为中小微企进行信贷评估	2021-10	hk01.com
辅助医疗保险金给付理赔核算	14 家产险强制险理赔 跨入 2.0 版	2021-10	工商时报
金融风控	工商银行的联邦学习系统已应用于风控等多个场景，比如，引入北京金控的不动产数据，与行内贷款企业的时点贷款余额、注册资本、账户余额等数据联合建立企业贷中预警监测模型，该模型提升准召率约 4%，进一步提升了工商银行的风险监测业务能力。	2021-11	新浪
数据安全、隐私保护	凌华科技与致星科技携手打造边缘联邦学习的一体机，以应对集中式机器学习训练中的数据时延与隐私保护问题，充分保障数据隐私安全，可应用于着重隐私的金融、医疗、零售、互联网等领域。	2022-07	搜狐
数据安全、隐私保护	度小满貔貅隐私计算平台通过国家金融科技测评中心(银行卡检测中心)联邦学习金融应用测评。	2022-11	数据猿
外汇业务监管及风险评估	中国工商银行联合青海省外管局融合工行客户画像、人民币交易、客户信用和外管局外汇交易等业务数据，利用联邦学习技术，将双方数据加密后进行隐私求交，在不获得对方特征数据的情况下进行联邦学习建模，在双方本地部署计算节点、搭建联邦学习平台，全链路保障合作双方业务数据隐私安全；建立关注指数模型、共享模型，实现个人客户风险评分，提前预判客户合规风险程度。	2022-11	安全内参
银行风控策略优化	中国民生银行罗勇：联邦学习技术助力银行风控策略组合优化，在保护用户信息不泄露的前提下将多元、多维度的数据纳入联合风控模型中，实现更精细的洞察，构建更精准的风控模型。另一方	2022-12	和讯网

金融业应用场景	标题	年-月	来源
	面，金融机构与外部机构之间也可基于联邦学习技术，利用多维度数据建立联合金融风险模型、择优导流、共享黑名单等，在数据没有离开本地的情况下，扩充多方特征或样本，提高模型效果。		
信息合规共享	兴业银行利用隐私计算技术，实现了反洗钱信息合规共享与优质企业联合发卡试点	2022-12	央广网

来源：根据公开资料整理

2. 在医疗业应用

联邦学习在医疗业应用目前处于研究探索、项目试点的阶段，参与主体不仅有科技公司，而且有较多的国内外权威科研机构、大学院所、医疗机构。国际性科技期刊 Nature《自然》曾发表关于联邦学习在医疗领域应用的文章，展示出联邦学习技术医疗应用的强大潜力，如表 13 所示。新冠疫情期间，通过使用联邦学习和来自各地区各医疗机构的数据来开发模型的研究意愿和实践较强烈。

表 13 《自然》关于联邦学习技术在医疗业应用相关文章

应用场景	论文	简介	来源
精准医疗、医疗数据隐私保护	*Swarm Learning for Decentralized and Confidential Clinical Machine Learning*	引入分散式机器学习方法 Swarm Learning 来整合各地医疗数据，它结合了边缘计算、基于区块链的点对点网络和协调，无需中央协调器即可保持机密性。	Nature, no. 7862 (2021): 265-270
医疗成像及潜在攻击向量和未来	*Secure, Privacy-Preserving and Federated Machine Learning in Medical Imaging*	为了促进旨在改善患者护理的大型数据集科研并保护患者隐私，必须实施技术解决方案以同时满足数据保护和利用的需求。该文概述了当前和下一代联合、安全和隐私保护人工智能的方法，重点是医学成像应用，以及医学成像及其他领域的潜在攻击向量和未来前景。	Nature Machine Intelligence, no. 6 (2020): 305-311

医疗数据集分析；医疗用药诊断；精准 / 个性化医疗	*Federated Learning in Medicine: Facilitating Multi-Institutional Collaborations Without Sharing Patient Data*	表明通过多个数据私有机构合作而增加的数据访问可以更多地有益于训练模型质量。联邦学习的临床采用有望对精准/个性化医学产生催化影响。	Scientific reports, no. 1 (2020): 12598
数字健康	*The Future of Digital Health with Federated Learning*	如果无法获得足够的数据，机器学习将无法充分发挥其潜力，并最终无法从研究过渡到临床实践。本文探讨了联邦学习如何为数字健康的未来提供解决方案，并强调需要解决的挑战和注意事项。	NPJ DIGITAL MEDICINE, no. 1.0 (2020): 119

联邦学习在医疗行业已开展的项目，不仅包括系统平台，而且具体落地到脑卒预测、识别脑肿瘤、预测新冠患者的氧气需求等实践。其应用主要体现在医疗影像、医疗诊断、医疗数据安全与数据孤岛问题、隐私保护、疾病预测、疾病库建设等方面。已公开的应用信息如表 14 所示。

表 14 2016–2022 年度联邦学习技术在医疗业应用动态

医疗业应用场景	标题	年-月	来源
解决信息孤岛，提供数据安全和授权使用机制	医疗数据隐私计算平台 XDP 翼数坊 v1.0 全球首发	2019-04	搜狐
医疗成像	英伟达在 MICCAI 2019 上发布首个面向医学影像的隐私保护型联邦学习系统	2019-10	摩尔芯闻
医疗服务患者数据保护	英伟达推出了 NVIDIA Clara 联邦学习	2019-12	极客公园
生物医药、健康管理、养老旅游、医疗设备、健康保险、保健食品等	Hitacea (医图亚) 打造成为基于区块链+联邦学习等新兴技术的亚洲首家全链条大健康科技产业平台	2020-04	科学中国
疾病预测	腾讯天衍实验室联合微众银行研发医疗联邦学习 AI 利器让脑卒中预测准确率达 80%	2020-04	CSDN
医疗诊断	英特尔和宾夕法尼亚大学佩雷尔曼医学院组建医疗联盟研发用以识别脑肿瘤的人工智能模型	2020-05	中电网

医疗业应用场景	标题	年-月	来源
AI 影像辅助诊断、高精度疾病检测、多维分析以及 3D 术前规划与模拟	商汤科技 SenseCare®□智慧诊疗平台推出包含胸部 CT、胸部 X 线、心脏冠脉、病理、骨肿瘤等多款产品解决方案	2020-07	趣味科技
保护用户隐私建模、医保基金控费、个人与机构拒付识别、医学影像辅助诊断、医院运营、临床医疗、健康管理、科研教学	腾讯医疗健康携手微众银行成立联合实验室	2020-08	TechWeb
医学统计分析、临床试验模、药物研发	中科院上海药物所联合华为云发布基于 ModelArts 平台的药物联邦学习服务	2020-09	飞象网
药物隐私数据保护 药物研发	同济大学与微众银行 AI 团队协同提出了一种基于联邦学习的协同药物定量构效原型系统 FL-QSAR	2020-12	科学中国
临床验证评估、医学影像辅助诊断	德国癌症研究中心、伦敦国王学院、麻省总医院、NVIDIA、斯坦福大学和范德堡大学推出 MONAI （Medical Open Network for AI）	2020-12	电子发烧友
电子病例相似性搜索、病人表征学习、SplitNN、社区特异性模型、预测健康风险	康奈尔大学研发团队发现联邦学习将可应用于众多生物医学领域的场景 论文：*Federated Learning for Healthcare Informatics*	2021-5	澎湃新闻
辅助医生诊疗	推出拟人化、全技能的“主动式 AI 医生”，「左手医生」获得 1 亿元 B 轮融资	2021-8	36 氪
新冠患者对呼吸器的需求预测	来自美国、英国、加拿大、日本、韩国、泰国、巴西以及台湾等国家地区 20 间医院及研究机构，共同开发能够精准预测新冠患者对呼吸器的需求程度，透过先进 AI 技术辅助医事人员预测患者的氧气需求，以便最有效率地安置患者，使医疗资源达到更适切的运用。	2021-10	中时新闻网
医学成像、基因分析、肿瘤学和新冠肺炎 （COVID-19） 研究	NVIDIA 利用 FLARE 进行联邦学习，将协作式 AI 带入医疗健康及其他领域	2021-11	英伟达中国
AI 诊疗、新冠 CT 数据采集	华中科技大学、剑桥大学、斯坦福大学、约翰霍普金斯大学等国内外权威科研机构提出基于联邦学习开源医学人工智能计算框架（UCADI）	2021-12	机器之心

医疗业应用场景	标题	年-月	来源
	论文：*Advancing COVID-19 Diagnosis with Privacy-Preserving Collaboration in Artificial Intelligence*		
精准医疗	英特尔与高雄荣总、纬创打造 OWL 数字病理平台，同步实现数字化病理学	2021-12	ETtoday 财经云
疾病预测	零氪科技提出的基于联邦学习的多中心数据处理框架 FedCIE 正在逐步应用，该模型基于零氪的医疗数据治理能力，特别是在病历深度结构化、患者画像、科研主题库建设等方面的深厚积累，能够解决单中心数据孤岛的问题，使各中心间数据能力彼此共享。目前，FedCIE 已被用来训练信息抽取模型、疾病预测模型等，并应用在多个项目上，取得了安全与高效的双重收益。	2022-02	金融界
医疗辅助诊断、健康险风险等级评估、对某种疾病患者的社会行为做出风险评估、实现个性化智能诊疗	同盾科技李晓林：可信 AI 生态系统，将成为下一代 AI 医疗的基础设施	2022-04	雷锋网
医疗影像	医疗集团 Aster DM Healthcare 旗下的 Aster 创新研究中心与英特尔公司、人工智能企业 CARPL.ai 合作，在印度开发并推出一款基于 AI 的健康数据平台。该健康数据平台应用了英特尔的开源框架 OpenFL，已经使用喀拉拉邦、班加罗尔和维杰亚瓦达等地 Aster 医院的医院数据进行了测试，共提取了超过 125000 张胸部 x 射线图像，使用双位点方法训练 CheXNet AI 模型，并通过模型检测 x 射线报告中的异常。	2022-07	雷锋网
医疗数据安全、隐私保护	采用英特尔 SGX，医渡云打造了一个多方安全计算解决方案，又通过多中心医学研究全场景解决方案，部署了临床研究开展、药械试验与研究等。锘崴科技打造的锘崴信 隐私保护计算平台，支持华西医院等在内的多家三甲医院和大学，完成了强直性脊柱炎的全基因组关联研究分析，有效解决了基因数据共享中存在的隐私安全问题。锘崴科技还开发了一个 PICOTEES 隐私保护查询在线系统，实现带有隐私保护的罕见病查询，	2022-08	数据猿

医疗业应用场景	标题	年-月	来源
	已在复旦大学附属儿科医院取得了令人满意的应用表现。		
疾病预测预警、辅助诊断、专病库建设	华西二院选择翼方健数来搭建数据开放服务平台及先心病专病库。数据开放服务平台内置同态加密、联邦学习、安全沙箱等多种隐私计算技术，实现数据的隐私保护和安全流通。	2022-12	BaseBit 翼方健数

来源：根据公开资料整理

3. 在电信业应用

联邦学习的最初提出就是为了解决移动设备数据训练问题，可以看作是其在电信业的最早应用。从公开的新闻数据看，联邦学习在电信业应用探索从 2018 年开始至今，应用场景从早期的通信资源分配已扩展到近期的客户体验和精准营销、6G 和卫星网络等。其中的参与主体主要是大型通信运营商、软硬件制造商等。相关信息如表 15 所示。

表 15 2016-2022 年度联邦学习技术在电信行业应用动态

电信业应用场景	标题	年-月	来源
车联网通信	华为数字算法实验室利用联邦学习原理解决车联网中可靠低延迟通信的联合功率和资源分配问题	2018-07	arXiv.org
智能手机	谷歌发布全球首个移动端分布式机器学习系统，数千万手机同步训练	2019-02	亿欧
联邦节点管理、边缘节点管理、联邦实例运行	华为 NAIE 联邦学习服务助力华为 CloudMSE 基于业务感知（Service Awareness, SA）技术的业务管理	2019-09	知乎
数据采集、模型训练、推理判断及智能预测	中国移动在 3GPP 标准引入基于联邦学习的分布式智能架构	2020-07	通信世界
识别业务流量后的带宽控制、阻塞控制、业务保障，用户信用评估、用户满意度提升	华为 CloudMSE 的业务感知（Service Awareness，SA）技术	2020-10	知乎
精确营销并推荐最佳产品权益	天津移动打造基于“联邦学习+区块链”的多方安全计算引擎系统-“珍珑”，在运营商、本地生	2020-12	C114 技术

电信业应用场景	标题	年-月	来源
	活、视频内容、交通出行等多行业数据的支撑下，实现精确的营销识别，并推荐最佳产品权益，让区块链+联邦学习成为智慧零售的引擎、智脑。		
语音识别、打字预测、更新系统	苹果和谷歌运用联邦学习技术，在不获取原始数据的情况下更新基于云的机器学习系统。此前，谷歌使用该技术来使其移动打字预测与语言趋势保持同步;苹果已使用它来更新语音识别模型的研究。	2021-6	Wired
6G 网络、卫星互联网	北邮深研院与天仪研究院共建“天算星座”，首发星计划明年择机发射	2021-11	中国科技网
手机用户体验提升	手机 AI 怎么突然就智商井喷了？高通提出了一种手机端的联邦学习方法，既能使用手机用户语音训练模型，同时保证语音数据隐私不被泄露。	2021-12	搜狐
客户体验管理	联邦学习在移动通信网络智能化的应用，进行客户体验感知模型训练	2022-2	移动通信[J]

来源：根据公开资料整理

4. 在 IT 行业应用

联邦学习在 IT 业应用动向主要聚焦于数据安全和基于数据的增值服务方面，主要参与者是互联网科技公司以及一些有地方政府背景的数据交易所，如表 16 所示。

表 16 2016-2022 年度联邦学习技术在 IT 行业应用动态

IT 行业应用场景	标题	年-月	来源
用户数据保护	腾讯云发布数据安全解决方案数盾	2018-05	腾讯
隐私数据安全流转	ARPA 测试网 1.0 版本 ASTRAEA 正式发布	2019-03	金色财经
可扩展分布式数据协作	趣链科技自主研发 BitXMesh 正式发布	2019-05	太平洋电脑
联合学习、联合计算、数据共享、模型训练	光之树发布天机可信计算框架和云间联邦学习平台	2019-08	搜狐
跨行业数据融合、隐私保护	富数科技结合联邦学习和安全多方计算技术推出了富数安全计算平台	2019-08	凤凰网

IT 行业应用场景	标题	年-月	来源
面向产业应用的工具组件	百度发布 3 项深度学习前沿技术工具组件：联邦学习 PaddleFL、图神经网络 PGL 和多任务学习 PALM 等	2019-11	钱江晚报
提出知识联邦框架	同盾科技人工智能研究院深度学习实验室发布成果：“面向联邦学习的加密神经网路”	2019-09	极客网
扩大光大联邦学习生态圈	光大科技加入 FATE 联邦学习社区技术指导委员会（TSC）并贡献关键算法源码	2020-01	新华网
数据脱敏及去标识化、加密算法支持、DMZ 区建设	同盾科技联邦学习技术加持 让数据“可用不可见”	2020-03	网易
大数据安全	平安科技联邦智能平台“蜂巢”落地	2020-09	搜狐
解决数据交易过程中确权困难、定价困难、隐私保护困难等问题	北部湾大数据交易中心建设运营取得初步成效	2021-1	人民网
支撑数据使用权交易	北京国际大数据交易所成立 探索全国数据交易新样板	2021-3	财经网
根据用户浏览习惯进行广告投放	新技术刚测试就被禁 谷歌“杀死”Cookies 真能重写规则?	2021-4	新浪
用户数据保护	抹掉你的网络痕迹，从未如此简单。谷歌宣称，从今年起，所有用户的所有使用数据都会默认在 18 个月后自动删除	2021-7	搜狐
公共数据交易	深圳已经在筹备数据交易所等多项基础设施建设 预计今年底可开始公共数据交易	2021-8	新浪
广告平台客户隐私数据保护	SaaS+云计算，能打开汇量科技的增长空间吗?	2021-10	OFweek 物联网
解决企业信息安全及隐私外泄	科技园推金融科技虚拟实验室 采用「联邦学习」技术保数据安全	2021-11	香港经济日报

来源：根据公开资料整理

5. 在其他行业应用

2019 年以来，智慧城市、教育、汽车/自动驾驶等领域也尝试引入联邦学习技术，进行了相关的应用探索，如表 17 所示。

表 17 2016-2022 年度联邦学习技术在其他行业应用动态

行业	应用场景	标题	年-月	来源
智慧城市	智慧城市政务、安全、交通、医疗、物流，跨部门、跨领域、跨区域的即时数据处理和数据融合	京东城市基于城市计算和联邦学习技术打造的产品“数字网关”	2019-10	技术前线
	公共安全、智能交通、智能能源	京东城市发布了城市操作系统升级版本“智能城市操作系统 2.0”	2019-12	链财经
	重大灾难中的人群疏散；零售、物流业的仓库选址	微众银行 AI 团队可视化再获新里程碑，两篇论文获 EuroVis 2020 收录	2020-03	CSDN
	城市交通监测	星云 Clustar 打造智慧城市领域的数据集 CityNet	2020-09	腾讯
	城市管理、公安、社区安防	微众银行与特斯联在北京宣布成立“AIoT 联合实验室”	2019-12	贤集网
	信用城市、市域治理现代化、智能商业等	京东数科联邦数字网关、区块链技术获工信部网络安全应用试点示范项目殊荣	2020-12	央广网
	市域治理现代化	京东科技搭建雄安新区数字孪生城市的数字底座	2021-3	时代在线
	电力数据共享	以安全合规为基础推进电力数据开放共享	2021-9	北极星输配电网
	城市用电预测	特斯联基于九章算法赋能平台打造了联邦学习算法引擎，向学术科研生态提供基于联邦学习数据使用的 API 接口。实现城市及产业数据安全研究	2022-04	IT 之家
教育	教育客户广告跑量、课程客户获课续费	字节跳动与教育行业结合，基于 Fedlearner，提升客户的续课率	2020-10	CSDN
	未成年人防沉迷处理	支付宝公开未成年人防沉迷专利	2021-7	新浪
智慧零售	居民消费	苏宁控股与科大讯飞联合推进数字经济发展，提高 AI 普惠能力	2020-11	新浪
	促成企业的交叉销售	创略科技尝利用联邦学习更多促成企业的交叉销售，可以降低获客成本、提高客户留存率、培养客户忠诚度	2021-11	钛媒体
汽车/自动驾驶	共享数据、云计算	英伟达发布了用于自动驾驶和机器人的软件定义平台 NVIDIA DRIVE AGX Orin	2019-12	镁客网
	汽车产品质量检测	将 AI 视觉应用于质量管理，「菲特智能检测」完成数千万元 A+轮融资	2021-3	36 氪

行业	应用场景	标题	年-月	来源
	用户行为数据建模	自动驾驶除了能省人工费，还能节省 10%油耗	2021-7	第一财经

来源：根据公开资料整理

4. 联邦学习发展趋势

4.1 研究趋势

4.1.1 总体趋势

根据关键词，从 AMiner 数据库中查找出联邦学习相关论文，其中包含论文所在领域的分支术语和年份，统计含有这些术语的论文数量，给出论文量排名前十的术语，再统计这些术语的起止年份，划分时间窗格，生成大数据智能的发展趋势河流图，如图 57 所示。

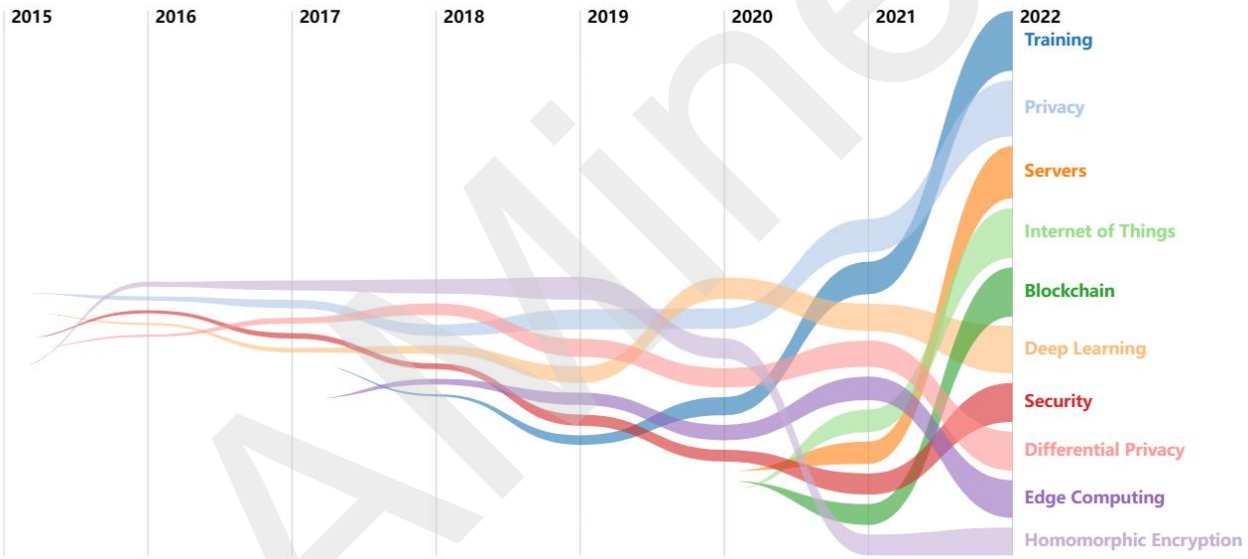


图 57 联邦学习技术发展趋势

来源：AMiner 知因系统。（注：图中的每个色带表示一个技术术语，其宽度表示该技术在当年的热度，与当年的论文数量呈正相关；各项技术在每一年份中按照其热度进行排序，热度越高的技术，其位置越排在靠上方。）

由图 57 可见，本期的联邦学习热度前十的研究主题依次分别是：Training（训练）、Privacy（隐私）、Servers （服务器端）、Internet of Things（物联网）、Blockchain（区块链）、Deep Learning（深度学习）、Security（安全）、Differential Privacy（差分隐私）、Edge Computing（边缘计算）、Homomorphic Encryption（同态加密）。整体

来看，这些研究主题均呈现平稳上升的发展趋势，其中，近一年来研究热度增幅最大的主题是数据训练以及安全，物联网次之。

对比上期热点，本期的联邦学习技术研究热度前十主题仍然聚焦于安全与隐私技术方面，数据训练相关研究增幅较大，在应用方面更加突出了物联网与移动设备方面研究的同时，区块链再度入榜。本期没能上榜的研究热点主题还有关于 Cloud Computing（云计算）、Mobile Device（移动设备）、Optimization Problem（优化问题）、Communication Effiency（沟通效率）等方面的问题研究，以及联邦学习在 Healthcare（医疗保健）方面的应用研究。

4.1.2 联邦学习与大模型技术的融合趋势

1． 联邦大模型是 AI 大模型时代的产物

从近两年的发展动向看，联邦学习研究的重点，集中在如何同时兼顾数据隐私保护和模型性能、学习效率等目标，即可信联邦学习的核心问题上。可信联邦学习是一种增强型的联邦学习。它结合了隐私计算各种技术，不仅保证了原始数据的隐私安全和模型的可证安全，还保证学习过程的高效率和模型的可用性、模型决策机制的可解释性、普惠性及模型的可溯源和审计监管。

联邦大模型则是人工智能发展进入大模型时代的产物。2022 年底以来，对联邦大模型的研究，是可信联邦学习在预训练大模型方面的应用与延申。大模型是具有数十亿甚至上百亿参数的深度神经网络模型，是大数据、大算力、强算法的结合，被认为是人工智能走向通用化的关键技术。但是，大模型在训练和应用的过程中，仍然面临着诸多风险隐患，其中三个主要挑战是：1）目前大多数高质量数据来源于有限的公域数据，来自阿伯丁大学、麻省理工大学、图宾根大学的 Pablo Villalobos 等 6 位计算机科学家在论文《我们会用完数据

吗？机器学习中数据集尺度的局限性分析》中预测，ChatGPT 等大模型训练所需的高质量语言数据将在 2026 年之前耗尽。也就是说当公域数据消耗殆尽时，如何在保护数据隐私的前提下，合规合法地利用手机等终端设备上的私域数据，成为解决大模型训练数据不足问题的关键；2）企业想要将大模型应用于各自的特定领域（比如，法律，金融，和医疗），需要使用私有的领域数据对预训练的大模型进行微调。然而，优质的领域数据往往分散于不同的相关企业。将这些领域数据收集在一起微调大模型，又会带来数据隐私泄露的风险；3）训练大模型需要消耗大量计算资源，这使得大模型很难被计算资源有限的中小型公司采用。作为一种分布式机器学习范式，联邦学习以“数据不动模型动，数据可用不可见”为关键特性，为大模型的未来发展提供了新思路。

（1）联邦学习与大模型结合有助于构建安全合规的数据生态

联邦学习与大模型的结合，能够解决大模型运行过程中存在的数据隐私与安全问题。联邦学习提供了一种保护数据隐私与打破垄断的技术解决方案，这个技术特性使得它与大模型的结合能够进一步解决数据安全、隐私保护等问题。

基于联邦学习的大模型是值得关注的研究新方向。目前的研究包括多种场景下的联邦大模型解决方案，例如：1）横向的同构大模型场景，大模型微调阶段，通过引入分层，利用 Adapter，Prompt tuning Aggregation 机制，解决全量模型聚合的通讯代价过高问题；2) 纵向的多方模型异构场景，各方数据等资源不同，模型不同，通过知识蒸馏（Knowledge Distillation）进行联邦学习；3）大模型指导“小模型”进行联邦学习场景，在客户端算力有限，而服务端算力充足，拥有大模型的情况下，引入知识蒸馏等方法，各个客户端通过“小模型”进行联邦学习，实现大模型到小模型的知识迁移 [78]。

[78] Wang B, Zhang Y J, Cao Y, et al. Can Public Large Language Models Help Private Cross-device Federated

联邦大模型可以在合法合规的前提下，一方面利用分散在各参与方的算力和数据，融合联邦学习和 AIGC 相关技术，实现异构数据分布式安全训练，让各参与方在保护各自数据安全与用户隐私的前提下，使用技术手段进行 AI 协作，既能保证安全可靠和公信力，又能打破数据孤岛、防止数据滥用和算法歧视等；另一方面，让散落于各行业、各机构的不同规模的大模型得以交流与融合，共同构建覆盖各行业各领域的数据与模型生态，打破垄断，进一步提升大模型的规模、质量和通用性。

（2）联邦学习技术在提升大模型数据安全与隐私防护中的局限

联邦学习和大模型的结合也存在着诸多严峻挑战，主要体现在计算代价、通信开销、隐私泄露、模型安全等方面。

首先，联邦大模型由于参数量巨大，需要海量的数据和强大的计算基础设施进行预训练，训练和推理过程所需要的计算资源与时间通常很多，导致其计算代价十分高昂。其次，联邦大模型应用也面临较高的通信开销。巨大的参数量意味着，联邦大模型的不同学习节点之间同步或交换数据所需的网络带宽与时间也随之增加，从而导致通信开销大、成本较高。此外，联邦大模型技术应用存在较大的隐私泄露风险。大模型所收集和聚合分布在不同节点的数据中可能包含用户的敏感信息与个人隐私数据，或者模型与数据容易遭受云服务提供商的监控与访问，都容易导致隐私泄露。最后，攻击者可能通过大模型的输出或中间表达反向推导模型的参数或训练数据，获取隐私或敏感信息；或者可能通过构造恶意输入误导大模型的学习方向，从而造成安全隐患。

（3）联邦学习大模型开源框架已实现落地

联邦学习大模型技术框架已有发布。截至目前，发现市场上有三家机构推出了联邦大模

Learning?[J]. arXiv preprint arXiv:2305.12132, 2023

型框架：FATE、FedLLM、和 PrimiHub，它们均是横向联邦。

FATE 联邦大模型 FATE-LLM

2023 年 4 月，联邦学习隐私计算开源平台 FATE 正式发布联邦大模型 FATE-LLM 功能模块[79]，支持 GPT-2 等大模型。FATE-LLM 功能模块是基于“小模型协作”的思路，通过将联邦学习和大模型结合，FATE-LLM 在各参与方的敏感数据不出本地域的前提下，根据各方实际数据量进行算力投入，联合进行大模型训练。基于此技术方案，至少 30 家参与方可以通过 FATE 内置的预训练模型同时进行横向联邦，利用各自隐私数据进行联邦大模型微调。过程中使用了安全聚合（Secure Aggregation）机制对各家模型数据进行保护。5 月份，FATE-LLM 发布了对清华 GLM 大模型的支持，集成 GLM 的 FATE-LLM 将会为国内用户提供更好的中文大模型应用落地选择。

项目地址：https://github.com/FederatedAI/FATE/releases/tag/v1.11.0

FedLLM

2023 年 4 月，FedML AI 平台发布了 FedLLM [80]，这是一个支持 MLOps 的训练管道，除了具备 LLM 的训练、服务和可观察能力外，还允许在专有数据上构建特定领域的 LLM。该平台支持数据协同、计算协同和模型协同，支持集中式和异地分布式 GPU 集群训练，以及数据孤岛的联邦学习。 FedLLM 兼容流行的 LLM 库，如 HuggingFace 和 DeepSpeed，旨在提高效率和安全/隐私。 FedML 用户和开发人员只需添加 100 行源代

79 FATE 开源社区发布联邦大模型 FATE-LLM，突破数据与算力壁垒，信阳日报，2023 年 4 月 17 日，https://new.qq.com/rain/a/20230417A03Z0X00

80 Releasing FedLLM: Build Your Own Large Language Models on Proprietary Data using the FedML Platform ，2023 年 4 月 27 日，https://blog.fedml.ai/releasing-fedllm-build-your-own-large-language-models-on-proprietary-data-using-the-fedml-platform/

码即可开始使用。在企业环境中部署和编排培训的复杂步骤都由 FedML MLOps 平台处理。

项目地址: https://github.com/FedML-AI/FedML/tree/master/python/app/fedllm

PrimiHub 联邦学习大模型

2023 年 4 月，原语科技在企业级开源隐私计算平台 PrimiHub 上开源了联邦学习大模型[81]，实现了基于联邦学习的大模型训练和预测，它允许多个参与者在保护各自数据隐私的同时，共同训练一个大型的深度神经网络模型。PrimiHub 联邦学习大模型是一个多模态、多任务、多领域的联邦预训练模型，它可以理解和生成文本，并支持多种语言和场景，可以应用于搜索、推荐、对话、翻译、摘要、创作等多个领域。PrimiHub 联邦学习大模型是基于预训练模型 ChatGLM6B（多模态、多任务、多领域，可以理解和生成文本、图像、音频、视频等各种类型的数据，并支持多种语言和场景）。PrimiHub 可以让用户在自己的设备上参与联邦学习，保护数据隐私和安全，同时享受大模型带来的智能服务。通过 Ptuning 技术，实现通过调整一部分权重获得和调整全部参数一样效果的模型调参，降低了联邦学习的计算和资源开销。基于新的 PrimiHub SDK，仅需一行命令，即可实现基于联邦学习的大模型的训练。PrimiHub 联邦学习大模型的模型参数量为 60 亿（6b，6000M），面向横向联邦场景。

项目地址：https://github.com/primihub/primihub

使用指引：https://docs.primihub.com/docs/advance-usage/create-tasks/fedreated-learning/chatglm/

（4）联邦大模型行业应用将更广泛

从已发布的联邦大模型来看，其行业应用现覆盖到金融、零售、工业、内容生产等多个

81 PrimiHub 联邦学习大模型开源，打破数据限制，保护数据隐私安全，https://juejin.cn/post/7226548855692181559

场景，未来将延伸到更多行业领域。FATE-LLM 大模型相关应用场景包括在金融领域的智能客服、内容风控、金融资讯情感分析、文本意图识别、营销场景智能创意生成和优化等。PrimiHub 联邦学习大模型可以应用于搜索、推荐、对话、翻译、摘要、创作等多个领域，为用户提供更丰富、更精准、更个性化的内容和服务。

2. 联邦学习大模型相关论文

基于 AMiner 数据库在论文标题与摘要进行关键词[82]搜索，结果发现，截至 2023 年 5 月联邦学习研究涉及大模型技术与应用研究的论文数量较少。这些论文研究涉及了大模型使用联邦学习作为学习框架、联邦学习环境下的自然语言处理任务、模型参数微调、性能优化算法等。联邦学习与大模型融合的相关论文如表 18 所示。其中，被引量最高的是一篇综述，该文讨论了联邦自然语言处理中的主要挑战，包括算法挑战、系统挑战以及隐私问题，以及对现有的联邦 NLP 评估方法和工具。

根据论文一作所属国家机构划分，发现这些论文来自中国、美国、瑞典、澳大利亚、新加坡、加拿大 6 个国家 16 家机构。论文较多的国家是中国和美国，依次有 6 篇、5 篇文章。此外，这些论文第一作者之中有半数以上为华人。

表 18 引入大模型技术的联邦学习相关论文

论文标题及链接	一作及其所属国家/机构	发表年份	被引量
Federated learning meets natural language processing: a survey	Ming Liu，【澳】Deakin University	2021	25

82 关键词检索式=（“federated learning” OR “federation learning”）AND（“Large Language Model” OR LLM OR “Foundation Model” OR prompt OR Prompt-tuning OR GPT OR “Generative Pre-Training transformer” OR AIGC OR "AI Generated Content"）

论文标题及链接	一作及其所属国家/机构	发表年份	被引量
FedBERT: When Federated Learning Meets Pre-training	Yuanyishu Tian，【中】Huazhong University of Science and Technology	2022	18
Scaling Federated Learning for Fine-C17tuning of Large Language Models	Agrin Hilmkil，【瑞典】Peltarion	2021	12
Federated learning with dynamic transformer for text to speech	Zhenhou Hong，【中】Ping An Technology (Shenzhen) Co., Ltd	2021	11
Where to begin? exploring the impact of pre-training and initialization in federated learning	John Nguyen，【美】Meta AI	2022	11
Scaling Language Model Size in Cross-Device Federated Learning	Jae Hun Ro，【美】Google	2022	10
Federated Learning for Personalized Humor Recognition	Xu Guo，【新】Nanyang Technological University	2022	5
FedQAS: Privacy-Aware Machine Reading Comprehension with Federated Learning	Addi Ait-Mlouk，【瑞典】Uppsala University	2022	3
Training Vision Transformers in Federated Learning with Limited Edge-Device Resources	Jiang Tao，【中】Tianjin University	2022	1
CyclicFL: A Cyclic Model Pre-Training Approach to Efficient Federated Learning	Pengyu Zhang，【中】East China Normal University	2023	0
Exploring Parameter-Efficient Fine-tuning for Improving Communication Efficiency in Federated Learning	Guangyu Sun，【美】University of Central Florida	2022	0
Foundation Models for Transportation Intelligence: ITS Convergence in TransVerse	Chen Zhao,【中】University of Chinese Academy ofSciences	2022	0
On the importance and applicability of pre-training for federated learning	Hong-You Chen，【美】Ohio State University	2023	0
Practical Takes on Federated Learning with Pretrained Language Models	Ankur Agarwal,【加】Huawei Noah’s Ark Lab, Montréa	2023	0

论文标题及链接	一作及其所属国家/机构	发表年份	被引量
Towards Building the Federated GPT: Federated Instruction Tuning	Jianyi Zhang，【美】Duke University	2023	0
When Federated Learning Meets Pre-trained Language Models' Parameter-Efficient Tuning Methods	Zhuo Zhang，【中】Harbin Institute of Technology, Shenzhen	2022	0

注：论文被引量统计截至 2023 年 6 月 12 日。

来源：AMiners 数据库

4.2 技术成熟度

技术成熟度指单项技术或技术系统在研发过程中所达到的一般性可用程度[83]。研究机构 Gartner 发布的技术成熟度曲线（Hype Cycle）因模型较成熟，已被广泛用来评估新科技的可见度，目前已成为科技产业界技术预测的风向标。

基于 Gartner 近年发布的相关技术成熟度曲线，本报告发现，联邦学习于 2019 年首次出现在 Gartner 数据科学与机器学习技术成熟度曲线（Hype Cycle for Data Science and Machine Learning）之中，并且被视为“在分布环境下的训练机器学习算法的重要创新”[84]。这表明联邦学习技术应用趋势发展较快，自诞生后仅用了三年时间就吸引了投资者、企业家和消费者的关注，也吸引到 Gartner 对该技术应用影响的研究。

此后两年，联邦学习相继出现在其他四个 Gartner 的技术成熟度曲线里面，分别是 2020 与 2021 年发布的数据科学与机器学习技术成熟度曲线、以及 2021 年的隐私技术成熟度曲

83 朱毅麟.技术成熟度对航天器研制进度的影响[J]. 航天器工程，2009，18(2)：9.

84 Hype Cycle for Data Science and Machine Learning, 2019，ARCHIVEDPublished 6 August 2019 - ID G00369766 -By Shubhangi Vashisth, Alexander Linden, et al, https://www.gartner.com/document/3955984?ref=solrAll&refval=295245018

线（Hype Cycle for Privacy）与公用事业行业 IT 技术成熟度曲线（Hype Cycle for Utility Industry IT），详细情况如表 19 所示。

由表 19 可见，在这些技术成熟度曲线之中，联邦学习都是处于“创新触发期”（Innovation Trigger），效益评级均为“高”，都属于“新兴”技术，到达生产高峰期（the Plateau of Productivity）的时间都预计为 5~10 年，且市场渗透率（Market Penetration）都低于 1%。

表 19 联邦学习相关 Gartner 技术成熟度曲线

Hype Cycle	Time	Benefit Rating	Maturity	Time to Plateau	Market Penetration
Hype Cycle for Data Science and Machine Learning, 2019 [85]	Innovation Trigger	High	Emerging	5~10 年	Less than 1% of target audience
Hype Cycle for Data Science and Machine Learning, 2020 [86]	Innovation Trigger	High	Emerging	5~10 年	Less than 1% of target audience
Hype Cycle for Data Science and Machine Learning, 2021 [87]	Innovation Trigger	High	Emerging	5~10 年	Less than 1% of target audience
Hype Cycle for Data Science and Machine Learning, 2022 [88]	Innovation Trigger	-	-	5~10 年	-
Hype Cycle for Privacy,	Innovation	High	Emerging	5~10 年	Less than 1% of

85 Hype Cycle for Data Science and Machine Learning, 2019, ARCHIVEDPublished 6 August 2019 - ID G00369766 -By Shubhangi Vashisth, Alexander Linden, et al, https://www.gartner.com/document/3955984?ref=solrAll&refval=295245018

86 Hype Cycle for Data Science and Machine Learning, 2020, 28 July 2020 G00450404,Analyst(s): Shubhangi Vashisth, Alexander Linden, Jim Hare, Pieter den Hamer,https://www.gartner.com/document/3988118

87 Hype Cycle for Data Science and Machine Learning, 2021， August 2021- ID G00747536- By Farhan Choudhary, Alexander Linden, Jim Hare, Pieter den Hamer, Shubhangi Vashisth，https://www.gartner.com/interactive/hc/4004274?ref=explorehc

88 https://pages.dataiku.com/gartner-hype-cycle-dsml

2021 [89]	Trigger-				target audience
Hype Cycle for Privacy, 2022	Innovation Trigger-	-	-	5~10 年	-
Hype Cycle for Utility Industry IT, 2021 [90]	Innovation Trigger	High	Emerging	5~10 年	Less than 1% of target audience

来源：Gartner 公司

值得关注的是，在 2019 年“数据科学与机器学习”技术成熟度曲线之中，由于首轮风投刚开始以及边缘数据收集问题等因素影响，当年 Gartner 预计联邦学习技术按照当时进行中的研究进展“不太可能在 5 到 10 年内”达到“生产高峰期”（the Plateau of Productivity）。随着隐私法规的激增、对数据隐私保护的需求增加，以及集中收集和存储大数据难度的增加等多个驱动因素影响，联邦学习被采用的范围和程度逐年增加。在 2020 年之后的技术成熟度曲线之中，虽然联邦学习技术仍然都处于“创新触发期”（Innovation Trigger），但相比 2019 年，联邦学习在 2020 年距离“期望膨胀期”（Peak of Inflated Expectations）又更近一步，已经度过了公司初创和第一轮风投的发展阶段，正处于“第一代产品期、价格高、大量客户化定制”（First-generation products,high price, lots of customization needed）的阶段；在 2021-2022 年距离“期望膨胀期”（Peak of Inflated Expectations）再近一步，进入了早期采用者调查（Early adopters investigate）阶段 [91]。

而在隐私技术成熟度曲线（Hype Cycle for Privacy）与公用事业行业 IT 技术成熟度

89 Hype Cycle for Privacy, 2021, Published 13 July 2021 • ID G00743765, By Bart Willemsen, https://www.gartner.com/interactive/hc/4003504?ref=explorehc

90 Hype Cycle for Utility Industry IT, 2021, Published 21 July 2021 • ID G00747517, By Nicole Foust, https://www.gartner.com/interactive/hc/4003853?ref=explorehc

91 Gartner Hype-Cycle: Everything You Need To Know，https://www.wowso.me/blog/gartner-hype-cycle

曲线（Hype Cycle for Utility Industry IT）中，联邦学习则是于 2021 年开始[92]才占有一席之地的。这主要是由于联邦学习的采用在过去一年加速发展，特别是因为它在新冠流行期间已成功用于医疗保健，以及该技术特别适用于例如物联网、网络安全、隐私、数据货币化和数据共享等受监管行业。

4.3 市场化与商业化趋势

联邦学习技术在国内外发展快速。有公开资料可查的联邦学习研究或应用单位已超过百家[93]。联邦学习可以被看成是一种连接联邦成员的大数据资产“连接”工具，具有非常广泛的市场应用价值，适用于医学研究、金融风控、医疗、智慧城市、移动互联网等多个实际场景。一些大型企业也开展了联邦学习技术的战略布局和应用，推出了相关的行业解决方案和项目，这反映出联邦学习的市场需求较热。

随着国内外相关标准和法规的完善和实施，以及解决方案和开源项目的不断迭代，联邦学习技术的未来应用场景将持续增加。未来能否出现大规模联邦学习商业化应用，将主要与网络带宽问题密切相关。这是因为联邦学习需要非常大量的中间结果交互，在某些场景下需要超过 100Mb/s 的网络带宽才能在有效的时间内完成建模，而某些银行仅支持 2Mb/s 的网络带宽，在样本量较大的情况下，这可能导致建模时间长达数月，无法满足业务的需求。5G 技术的发展和信息高速公路的建设，将会促进联邦学习大规模商业化应用的实现。

此外，联邦学习未来市场与商业化的实际落地将出现更多的异构场景下的应用。应用场景可分为同构场景和异构场景。同构场景指的是两个企业属于相同或相近的领域，所拥

92 联邦学习首次被纳入 Gartner 隐私计算技术成熟度曲线，东方财富网，2021-08-09

93 一文读懂联邦学习的前世今生，东科技技术说，2020-11-17，
https://blog.csdn.net/JDDTechTalk/article/details/109738346

有的数据性质相似、特征相近，但是样本不同。如在银行和金融机构间的合作，双方拥有的不同的用户样本，但是样本属性同质，这种场景下使用横向联邦学习，可达到将双方样本放到一起的建模效果。异构场景指的是两个企业分属不同的领域，所拥有的数据性质不同、特征不同，但是有重叠的样本 ID。比如银行与互联网公司之间的合作，双方有重叠的用户 ID，但是企业间各自拥有用户不同的特征，如银行有用户的收入和交易行为，互联网公司有用户的社交或出行行为，这种场景下使用纵向联邦学习建模，可达到特征增加的建模效果。在当前的联邦学习市场化应用中，同构场景下的探索更为成熟。未来将出现更多的联邦学习在行业垂直领域的应用尤其是异构场景下的应用。

4.4 国内外相关标准

技术标准化建立与实施是联邦学习技术落地应用的重要依据。通过研制和建立联邦学习的国内标准（如团体标准和国家标准）与国际标准（如 IEEE 企业标准），制定联邦学习的算法框架规范、使用模式和使用规范，可帮助更多行业和海内外不同类别的实体在保证用户隐私和数据安全的情况下，合作共赢、建立更准确的数据模型，同时，也给人工智能在不同产业中的实际落地提供可行性依据。

截至目前，联邦学习领域已经由企业或行业联盟协会发起并建立了初步的企业级国际标准和国家级团体规范。部分标准信息如表 20 所示。

表 20 联邦学习相关国内外标准

领域	类别	标准名称	发布方	发布时间
人工智能	团体规范标准	《信息技术服务联邦学习参考架构》 [94]	中国人工智能开源软件发展联盟	2019 年 6 月

94 国内首个联邦学习标准正式出台,微众银行 AI 团队领衔，2019-07-01，

领域	类别	标准名称	发布方	发布时间
			（AIOSS）	
	国际标准	IEEE P3652.1《联邦学习架构和应用规范》（Guide for Architectural Framework and Application of Federated Machine Learning）	电气与电子工程师协会 (IEEE) 标准委员会（SASB）	2021 年 3 月
5G 通信	国际标准	NWDAF（Network Data Analytics Function-5G 网络 AI）的联邦学习技术标准[95]	3GPP 通过，由亚信科技与中国移动共同提交	2020 年 7 月
	国际标准	《面向物联网和智慧城市/社区的联邦机器学习需求及参考架构》（Requirements and Reference Architecture of IoT and Smart City & Community Service based on Federated Machine Learning）[96]	华中科技大学、中国信科、中兴通讯、中国联通和中国移动共同提交，在国际电信联盟（ITU）获批正式立项	2020 年 7 月
	团体标准	《基于联邦学习的数据流通产品技术要求与测试方法》[97]	中国通信标准化协会	2020 年 7 月
金融	行业标准	《多方安全计算金融应用技术规范》（JR/T 0196-2020）[98]	中国人民银行	2020 年 11 月

随着国际与国内联邦学习标准的相继出台，在未来发展中，相关标准的实施与执行将是联邦学习领域的发展重点，影响着该技术作为下一代人工智能协作网络基础的能力。能够有效推行标准化的联邦学习技术规范，不仅有利于来自不同行业、不同业务类别的企业在开展

https://www.sohu.com/a/323923758_99974896

95 国内首个联邦学习标准正式出台,微众银行 AI 团队领衔，2019-07-01，https://m.sohu.com/a/323923758_99974896

96 华中科技大学牵头制定的全球首个面向物联网与智慧城市的联邦学习参考架构国际标准正式获批立项，中国教育在线，2020-07-29

97 中国信通院解读“隐私计算系列标准与测试方法” 2021-01-25, https://www.sohu.com/a/446614289_735021

98 央行发布《多方安全计算金融应用技术规范》 确保数据安全，2020-12-24，https://www.cebnet.com.cn/20201224/102711761.html

业务或进行合作的过程中合法合规地共同使用数据、保护用户隐私和数据安全，而且有助于建立更为准确的数据模型，进而促进该技术走向成熟化和开启大规模工业化应用。

4.5 生态建立与发展

国际与国内联邦学习标准的相继出台有力促进了联邦学习生态的建立与发展。随着更多行业的更多企业机构加入和布局该技术的应用，联邦学习生态逐渐从当前的跨地域、跨平台互联互通向开放通用的方向进发[99]。

截至目前，联邦学习生态建设较成规模的有 FATE 开源社区与开放群岛（Open Islands）开源社区。其中，FATE 开源社区成立于 2019 年，是面向全球隐私计算联邦学习开源生态中的开发者、贡献者、用户及生态伙伴建立的学习与交流平台，拥有全球首个工业级安全联邦学习框架；现有 3000 多位来自近千家企业及科研机构的开发者参与社区生态共建。开放群岛开源社区成立于 2022 年 5 月，是由深圳数据交易有限公司联合包括中国信通院、鹏城实验室、中经社、国家超级计算深圳中心等国家智库及研究机构，以及中国工商银行、平安银行、建信金科、华为云、腾讯云等大型企业及科技公司共计近 50 家发起单位牵头成立的国内首个国际化自主可控隐私计算开源社区，促进全国性科技资源开放共享，推动数据要素流通关键基础技术发展，打通数据、平台、机构之间的孤岛，实现跨地区、跨地域、跨平台互联互通。

未来在联邦联盟中，所有成员的数据在合法合规下可以带来真正的价值流动，为自身带来收益，同时各个行业还可以建立各自的联邦数据网络，不同行业的网络间还将有所交甚至

[99] 联邦学习开源社区 FATE 技术委员会 2021 年第二次会议召开，2021 年 7 月 5 日，baidu.com

连接紧密[100]，从而促进各自行业良性发展。在良好的联邦学习生态联盟中，联邦学习参与方，不仅可以获得相关的技术支持等服务与产品，快速便捷地完成相关应用的开发部署工作，而且可以在良好的开源环境下，更加高效、准确地自建模型、联合建模、共享模型、共建联邦学习生态。联邦学习生态的建立，需要学术界和产业界的共同推动[101]，使之成为参与各方机构之间数据合作的桥梁，从而挖掘数据背后的真正的知识和价值。

100 微众银行人工智能部、鹏城实验室、腾讯研究院、中国信通院云大所、平安科技、招商局金融科技、电子商务与电子支付国家工程实验室(中国银联)：《联邦学习白皮书 V2.0》，深圳，2020 年，第 28-30 页。

101 微众银行首席 AI 官杨强：建立联邦学习生态需学术和产业界共同推动 [N] TechWeb，2020 年 11 月 16. 日 http://www.myzaker.com/article/5fb1f78a8e9f0945d855fd1d/

5. 结语

通过回顾联邦学习技术从 2016 年被提出至 2022 年的发展，可以发现该技术研究热度逐年上升，研究论文数量和专利申请量都在逐年增多。总体而言，相比其他国家，我国学术界和产业界对联邦学习科研和推广应用更为热衷。

全球联邦学习论文发布量以中美两国为引领。从论文影响力来看，六成以上高被引论文来自中国和美国，同时中美两国合作的论文数量也最多。全球高被引论文数量最多的机构是谷歌，最多的大学是卡内基·梅隆大学。中国的高被引论文量较多（3 篇及以上）的机构是北京邮电大学（4 篇）、香港科技大学（4 篇）、中山大学（3 篇）以及深圳市大数据研究院（3 篇）。

人工智能国际顶会研讨会评选出的联邦学习最佳论文来自于美国、中国、瑞士、沙特阿拉伯、新加坡和韩国六个国家，其中，美国的最佳论文数量占 40.6%，中国的占 37.5%，中美两国合计占比达七成以上。就单个机构的最佳论文数量而言，美国的卡内基·梅隆大学与中国的香港科技大学并列第一。

全球高被引论文作者主要聚集在美国和中国。美国的高被引论文作者数量最多，占全球四成以上，同时也是中国高被引论文作者数量的 2.3 倍。就机构而言，高被引学者数量较多的机构主要位于美国、中国、新加坡，其中，中国拥有该领域高被引学者数量较多的机构是香港科技大学、微众银行、北京邮电大学、中国电子科技大学。值得注意，企业人才（例如供职于谷歌等）是联邦学习领域中的一个不可忽视的研究群体，因为全球研究联邦学习的高被引论文作者之中，有 26.1%供职于企业。

在专利申请方面，中国是受理联邦学习专利申请数最多的地区，约占全球受理总量的七

成，约是在美国受理专利量的 7 倍，数量优势非常突出。联邦学习专利申请量 TOP10 的机构主要分布在中国和美国两个地区，同时，专利申请量排名前三的机构都位于中国。从国内地域布局来看，近年来联邦学习专利申请量领先的地区主要是北京、广东、浙江、上海、江苏等省市。

从技术研究热点看，联邦学习研究较多聚焦于机器学习方法模型、模型训练、隐私保护等主题。自 2021 年开始明显加大了物联网相关的联邦学习研究力度。联邦学习目前的专利布局也主要聚焦安全与隐私保护方向，以及机器学习方法、模型训练等方面。这反映出联邦学习应用已越来越接近于“生产高峰期”。

本报告还展示了联邦学习不同细分研究方向上的代表学者学术画像，梳理了市面上主要的联邦学习系统框架，以及在 IT 科技、金融、医疗健康、通信、智慧城市、智慧零售、教育、汽车等多个行业落地应用场景，并探讨了该技术的市场化与商业化趋势，以及推行的国内外标准与建立联邦学习生态等问题。

联邦学习从技术维度上解决了人工智能发展过程中的安全问题，从产业维度上解决了合法合规训练数据的问题，被学术界和产业界寄予厚望。中国已经成为联邦学习技术的深度参与方，国内企业和科研机构积极参与联邦学习的技术研发和应用，以及标准制定。未来，随着人工智能技术和应用的不断升级，联邦学习的技术研发仍将较多聚焦于数据安全与隐私保护，其应用场景还将进一步扩大和深入。

附录一 联邦学习领域顶级国际期刊会议列表

以《CCF 推荐国际学术期刊和会议目录》为数据来源，并征求领域顾问专家意见而确定。

序号	期刊/会议名称	简称
1	ACM Conference on Computer and Communications Security	CCS
2	The Network and Distributed System Security Symposium	NDSS
3	USENIX Security Symposium	USENIX Security
4	IEEE Symposium on Security and Privacy	SP
5	International Conference on Learning Representations	ICLR
6	Neural Information Processing Systems	NIPS
7	Machine Learning and Systems	MLSys
8	Distributed AI	DAI
9	IEEE International Conference on Distributed Computing Systems	ICDCS
10	International Conference on Machine Learning	ICML
11	AAAI Conference on Artificial Intelligence	AAAI
12	International Joint Conference on Artificial Intelligence	IJCAI
13	ACM Transactions on Intelligent Systems and Technology	——
14	IEEE International Conference on Big Data	——
15	Nature	NATURE
16	IEEE Internet of Things Journal	——
17	IEEE Transactions on Industrial Informatics	IINF
18	IEEE Transactions on Parallel and Distributed Systems	TPDS
19	IEEE Transactions on Big Data	——
20	Future Generation Computer Systems	——
21	Procedia Computer Science	——
22	Journal of Network and Computer Applications	——
23	Computer Networks	——
24	Computers & Security	——
25	Network and System Security	NSS
26	IEEE International Conference on Communications	ICC
27	International Conference on Machine Learning and Intelligent Communications	MLICOM

附录二 《联邦学习架构和应用规范》简介

IEEE P3652.1《联邦学习架构和应用规范》（Guide for Architectural Framework and Application of Federated Machine Learning）相关信息如下。

1. 目标 （Purpose）

本规范的目的是为 AI 工业应用提供可行的解决方案，即集体使用数据而无需直接交换数据。在隐私和数据保护问题变得越来越重要的情况下，本规范有望促进协作，将促进并允许使用分布式数据源来开发 AI，而不会违反法规或道德考量。（The purpose of this guide is to provide a feasible solution for industrial application of AI -- using data collectively without exchanging data directly. This guide is expected to promote and facilitate collaborations where privacy and data protection issues have become increasingly important. This guide will promote and enable to use of distributed data sources for the purpose of developing AI without violating regulations or ethical considerations. ）

2. 范围 （Scope）

联合学习定义了一种机器学习框架，该框架允许从分布在数据所有者之间的数据构建一个集体模型。本规范提供了跨组织的数据使用和模型构建的蓝图，同时满足了所适用的隐私，安全和法规要求。它定义了联合机器学习的体系结构框架和应用程序准则，包括：1）联合学习的描述和定义，2）联合学习的类型和每种类型适用的应用场景，3）联合学习的性能评估，以及 4）相关法规要求。（Federated learning defines a machine learning framework that allows a collective model to be constructed from data that is distributed across

data owners. This guide provides a blueprint for data usage and model building across organizations while meeting applicable privacy, security and regulatory requirements. It defines the architectural framework and application guidelines for federated machine learning, including: 1) description and definition of federated learning, 2) the types of federated learning and the application scenarios to which each type applies, 3) performance evaluation of federated learning, and 4) associated regulatory requirements.)

附录三 联邦学习特刊的部分已发表文章

研究时段内，联邦学习相关特刊的已发表文章按照期刊影响因子及刊文顺序如下。

Computer Networks 联邦学习特刊已发表文章

期刊 Computer Networks 的联邦学习特刊主题是“Special section on Enabling Blockchain and Federated Learning for Smart Services in Beyond 5G/6G Networks”[102]，相关文章于 2021 年相继发表在该期刊的 Volume 203-205 上。相关的联邦学习文章共 7 篇，相关介绍如下。

卷号	序号	论文标题及链接	作者	被引量（次）	亮点
203	1	*A blockchain-based Fog-oriented lightweight*	Thar Baker, Muhammad	23	提出了一种响应式和轻量级的框架，该框架采

102 Computer Networks | Enabling Blockchain and Federated Learning for Smart Services in Beyond 5G/6G Networks | ScienceDirect.com by Elsevier

卷号	序号	论文标题及链接	作者	被引量（次）	亮点
		framework for smart public vehicular transportation systems	Asim, Hezekiah Samwini, Nauman Shamim, ... Rajkumar Buyya		用区块链进行身份验证，利用雾计算对分布式应用程序云计算的改进，提供高效、安全的交通系统。
	2	*Optimal pricing-based computation offloading and resource allocation for blockchain-enabled beyond 5G networks*	Kaiyuan Zhang, Xiaolin Gui, Dewang Ren, Tianjiao Du, Xin He	11	提出了两种基于定价的方案来解决这两个计算卸载问题，其中分析了贝叶斯-纳什均衡和斯塔克尔伯格均衡。
	3	*Deep data plane programming and AI for zero-trust self-driven networking in beyond 5G*	Othmane Hireche, Chafika Benzaïd, Tarik Taleb	18	提出了一个以支持跨多个域的完全分布式的可信赖 SelfDN 框架。
204	1	*Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing*	Yichen Wan, Youyang Qu, Longxiang Gao, Yong Xiang	27	建议将启用区块链的 FL 与启用差异隐私 (DP) 的 Wasserstein 生成对抗网络 (WGAN) 集成，以保护 B5G 网络中边缘设备的模型参数。
	2	*Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks*	Zain Abubaker, Nadeem Javaid, Ahmad Almogren, Mariam Akbar, ... Jalel Ben-Othman	15	为传感器物联网 (IoST) 提出了一种支持超越第五代 (B5G) 的区块链恶意节点检测模型，还为 IoST 提出了一种使用级联加密和特征评估过程的安全服务提供方案。
	3	*Federated learning for malware detection in IoT devices*	Valerian Rey, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet	130	调查了联邦学习在物联网恶意软件检测方面的可能性，并提出了一个使用联合学习来检测影响物联网设备的恶意软件的框架。

卷号	序号	论文标题及链接	作者	被引量（次）	亮点
205	1	*A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept*	Nidal Nasser, Zubair Md Fadlullah, Mostafa M. Fouda, Asmaa Ali, Muhammad Imran	13	设想了一个保护隐私的流行病响应网络，该网络使用概念验证的空中-地面网络系统为移动用户实体/设备（UE）提供服务。通过利用无人驾驶飞行器（UAV），提出了一种轻量级的联合学习模型，可以使用单个 UE 使用环境传感器和可穿戴设备收集的数据，以协作方式私下学习高精度的医学（例如 COVID-19）症状。

注：表中文章的被引用量统计截至 2023 年 3 月 31 日。

Computers & Security 联邦学习特刊已发表文章

期刊 Computers & Security 的联邦学习特刊主题是“Special section on Federated Learning for Decentralized Cybersecurity” [103]，相关文章于 2021 年 10 月相继发表。相关的联邦学习文章截止目前共 2 篇，相关介绍如下。

序号	论文标题及链接	作者	被引量（次）	亮点
1	*Digestive neural networks: A novel defense strategy against inference attacks in federated learning*	Hongkyu Lee, Jeehyeong Kim, Seyoung Ahn, Rasheed	27	提出了一种消化神经网络（DNN），一种附加在 FL 上的独立神经网络。DNN 会最大限度地提高 FL 的

103 COSE | Computers & Security | Federated Learning for Decentralized Cybersecurity | ScienceDirect.com by Elsevier

序号	论文标题及链接	作者	被引量（次）	亮点
		Hussain, ... Junggab Son		分类准确度，同时最大限度地降低推理攻击的准确度。所提出的 DNN 在基于梯度共享和权重共享的 FL 机制上都表现出显著的性能。
2	*Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things*	Devrim Unal, Mohammad Hammoudeh, Muhammad Asif Khan, Abdelrahman Abuarqoub, ... Ridha Hamila	52	提出了一种将区块链与 FL 集成以提供隐私保护和安全大数据分析服务的实用方法。为了保护用户数据和训练模型的安全性，建议利用模糊散列来检测 FL 训练模型中的变化和异常，以防止中毒攻击。

注：表中文章的被引用量统计截至 2023 年 3 月 31 日。

IEEE INTELLIGENT SYSTEMS 联邦学习特刊已发表文章

IEEE INTELLIGENT SYSTEMS 联邦学习特刊的主题是“Special Issue on Federated Machine Learning”[104]，相关文章发表在该期刊的 2020 年第 35 卷，第 4 期。相关的联邦学习文章共 10 篇，相关介绍如下。

序号	论文标题及链接	作者	被引量（次）	亮点
1	*Introduction to the Special Issue on Federated Machine Learning*	Yang Liu, Han Yu, and Qiang Yang	1	展示所刊文章的主要内容亮点

104 Federated Learning, IEEE INTELLIGENT SYSTEMS，JULY/AUGUST 2020，VOLUME 35, NUMBER 4

序号	论文标题及链接	作者	被引量(次)	亮点
2	*Preserving User Privacy for Machine Learning: Local Differential Privacy or Federated Machine Learning?*	Huadi Zheng, Haibo Hu, and Ziyang Han	51	比较了在物联网应用中 LDP 和 FL 的可实现效率和隐私保护属性
3	*Joint Intelligence Ranking by Federated Multiplicative Update*	Chi Zhang, Yu Liu, Le Wang, Yuehu Liu, Li Li, and Nanning Zheng	6	提出了一种隐私保护矩阵分解方法，该方法在自动驾驶等许多智能系统中具有潜在的适用性
4	*Distributed Privacy Preserving Iterative Summation Protocols*	Yang Liu, Qingchen Liu, Xiong Zhang, Shuqi Qin, and Xiaoping Lei	0	开发了一种用于隐私保护的分布式迭代协议，该协议对节点的动态加入和离开具有弹性，可以成为增强动态 FL 系统中隐私保护的有用技术
5	*SMSS: Secure Member Selection Strategy in Federated Learning*	Kun Zhao, Wei Xi, Zhi Wang, Jizhong Zhao, Ruimeng Wang, and Zhiping Jiang	6	寻求通过选择那些具有更多共同实体的数据所有者加入 FL 模型训练来解决来自不同数据所有者的不同数据质量问题
6	*Federated Generative Privacy*	Aleksei Triastcyn and Boi Faltings	43	关注隐私保护数据共享问题，提出基于 GAN 的方法来生成人工数据样本以支持联合平均操作，而无需公开敏感的本地信息
7	*A Sustainable Incentive Scheme for Federated Learning*	Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang	75	着眼于 FL 设置中的激励机制设计重要问题，开发了一个公平意识的利润分享计划，以激励数据所有者参与联邦学习
8	*A Secure Federated Transfer Learning Framework*	Yang Liu, Yan Kang, Chaoping Xing, Tianjian Chen, and Qiang Yang	438	提出了第一个联邦迁移学习方法，帮助 FL 应用程序处理那些样本空间和特征空间重叠的都很罕见的具有挑战性的情况

序号	论文标题及链接	作者	被引量(次)	亮点
9	*FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare*	Yiqiang Chen, Xin Qin, Jindong Wang, Chaohui Yu, and Wen Gao	573	报告了在医疗保健应用领域应用 FTL 的经验
10	*Proxy Experience Replay: Federated Distillation for Distributed Reinforcement Learning*	Han Cha, Jihong Park, Hyesung Kim, Mehdi Bennis, and Seong-Lyun Kim	21	提出了一种在分布式深度强化学习中提高通信效率和保护私人信息的方法

注：表中文章的被引用量统计截至 2023 年 3 月 31 日。

Electronics 联邦学习特刊已发表文章

期刊 Electronics 的联邦学习特刊主题是 Special Issue "Federated Learning: Challenges, Applications and Future"[105]，相关文章于 2021 年 8 月发表，截止目前共发表 1 篇，相关介绍如下。

序号	论文标题及链接	作者	被引量(次)	亮点
1	*Multi-Party Privacy-Preserving Logistic Regression with Poor Quality Data Filtering for IoT Contributors*	Kennedy Edemacu; Jong Wook Kim	1	提出了一个多方隐私保护逻辑回归框架。具体来说，在分布式设置中提出了一种新的度量梯度相似性，使用该度量梯度相似性来过滤掉来自质量较差数据的数据贡献者的参数；采用同态加密解决隐私挑战。

105 Electronics | Special Issue : Federated Learning: Challenges, Applications and Future (mdpi.com)

Wireless Communications and Mobile Computing 联邦学习特刊已发表文章

期刊 Wireless Communications and Mobile Computing 的联邦学习特刊主题是“Special Issue on AI-Based Federated Learning for 6G Mobile Networks” [106]，相关文章在 2021 年 5 月至 12 月相继发表。相关的联邦学习文章共 13 篇，相关介绍如下。

序号	论文标题及链接	作者	被引量（次）	亮点
1	*Multimedia Concepts on Object Detection and Recognition with F1 Car Simulation Using Convolutional Layers*	Amutha Balakrishnan, Kadiyala Ramana , Gaurav Dhiman , Gokul Ashok, Vidhyacharan Bhaskar, Ashutosh Sharma , Gurjot Singh Gaba ,Mehedi Masud , and Jehad F. Al-Amri	12	提出了一种基于全局特征和轮廓检测图像中对象的框架。
2	*Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges*	Muhammad Muzamil Aslam, Liping Du , Xiaoyan Zhang , Yueyun Chen , Zahoor Ahmed , and Bushra Qureshi	24	研究了 6G CR 网络通信的预测应用、可能的技术和安全问题。

106 AI-Based Federated Learning for 6G Mobile Networks | Hindawi

序号	论文标题及链接	作者	被引量(次)	亮点
3	*Image Recognition Method for Pitching Fingers of Basketball Players Based on Symmetry Algorithm*	Wanquan Chen	2	提出一种基于对称算法的篮球运动员投球手指动作识别方法，构建采集模型，对篮球运动员投球手指动作图像进行边缘轮廓检测和自适应特征分割，并采用固定阈值对手指进行分割。
4	*An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication*	Sumaya Sanober, Izhar Alam, Sagar Pande, Farrukh Arslan, Kantilal Pitambar Rane, Bhupesh Kumar Singh, Aditya Khamparia, and Mohammad Shabaz	72	在互联网商务和银行领域，提出了一种将 Spark 与深度学习方法相结合的新框架，还实现了不同的机器学习技术来检测欺诈。
5	*Hierarchical Coordinated Control Method for Multiload DC Microgrid Units*	Zhigang Zhang, Jinping Mo	1	设计了微电网的分层控制结构，根据微电网的控制目标和控制时间尺度进行分层，采用多智能体技术实现分层控制结构。针对微电网能量协调和优化的需求，提出了微电网并网和/或离网模式的运行策略。
6	*Prediction of Traffic Generated by IoT Devices Using Statistical Learning Time Series Algorithms*	Shilpa P. Khedkar, R. Aroul Canessane, and Moslem Lari Najafi	19	对使用经典时间序列和人工神经网络的物联网流量预测模型进行了完整概述。
7	*Design and Simulation of Capacitive MEMS Switch for Ka Band Application*	Vinay Bhatia, Sukhdeep Kaur, Kuldeep Sharma, Punam Rattan,	25	针对 Ka 波段应用设计并分析了具有电容接触的射频 MEMS 开关。

序号	论文标题及链接	作者	被引量(次)	亮点
		Vishal Jagota, Mohammed Abdella Kemal		
8	*Location and Layout of Common Storage and Multichannel Common Distribution considering Time Windows*	Biqin Hu, Bin Yang, Wei Jiang, Zhe Yang, Mohammed Abdella Kemal	0	以多渠道共存共发为研究对象，结合实际配送情况，考虑时间窗条件下共存共发模式的选址和配送路径优化，采取链接时间窗的形式。与分配时间完成效率，并以时间完成效率对目标函数形成反向约束，从而实现“最小化总成本和满足时间窗口”的双目标优化。
9	*Scalable and Storage Efficient Dynamic Key Management Scheme for Wireless Sensor Network*	Vipin Kumar, Navneet Malik, Gaurav Dhiman, Tarun Kumar Lohani	13	提出了一种可扩展且存储高效的无线传感器网络密钥管理方案（SSEKMS），该方案为网络建立三种类型的密钥：网络中所有节点共享的网络密钥，共享的集群密钥对于集群，以及每对节点的成对密钥。
10	*Nonholonomic Wheeled Mobile Robot Trajectory Tracking Control Based on Improved Sliding Mode Variable Structure*	Hua Cen, Bhupesh Kumar Singh	15	探索非完整轮式移动机器人跟踪系统；分析了运动学模型和滑模控制模型，采用基于滑模的增强变结构对机器人进行轨迹跟踪控制。
11	*Hybrid Resource Environmental Value Chain Model Based on a Discrete Time Algorithm*	Wenting Cao, Melkamu Teshome Ayana, Rongwei Gao	0	提出了一种基于离散时间算法的混合资源环境价值链模型。
12	*A New Hybrid Deep Learning Algorithm for Prediction of Wide Traffic Congestion in*	G. Kothai, E. Poovammal, Gaurav Dhiman,	36	提出了一种新的混合增强型长短期记忆集成(BLSTME)和卷积神经网

序号	论文标题及链接	作者	被引量（次）	亮点
	Smart Cities	Kadiyala Ramana, Ashutosh Sharma, Mohammed A. AlZain, Gurjot Singh Gaba, Mehedi Masud		络（CNN）模型，该模型将 CNN 的强大功能与 BLSTME 相结合，以协商车辆的动态行为并预测有效地在道路上的交通拥堵。
13	*CPIDM: A Clustering-Based Profound Iterating Deep Learning Model for HSI Segmentation*	Kriti Mahajan, Urvashi Garg, Mohammad Shabaz	50	提出了一种在一定程度上减少了 HSI 空间领域中深度学习方法问题的方法，并基于聚类的深度方法评估了所提出的分割技术，用于 HSI 分割的迭代深度学习模型 CPIDM。

注：表中文章的被引用量统计截至 2023 年 3 月 31 日。

参考文献

[1] Ammad-Ud-Din, M., Ivannikova, E., Khan, S. A., Oyomno, W., Fu, Q., Tan, K. E., & Flanagan, A. (2019). Federated collaborative filtering for privacy-preserving personalized recommendation system. *arXiv preprint arXiv*:1901.09888.

[2] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017, October). Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1175-1191).

[3] Chen, M., Mathews, R., Ouyang, T., & Beaufays, F. (2019). Federated learning of out-of-vocabulary words. *arXiv preprint arXiv*:1903.10635.

[4] Girgis, A. M., Data, D., Diggavi, S., Kairouz, P., & Suresh, A. T. (2021). Shuffled model of federated learning: Privacy, accuracy and communication trade-offs. *IEEE journal on selected areas in information theory*, 2(1), 464-478.

[5] Gu, B., Dang, Z., Li, X., & Huang, H. (2020, August). Federated doubly stochastic kernel learning for vertically partitioned data. *In Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining* (pp. 2483-2493).

[6] Gulshan, V., Peng, L., Coram, M., Stumpe, M. C., Wu, D., Narayanaswamy, A., ... & Webster, D. R. (2016). Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. *jama*, 316(22), 2402-2410.

[7] IEEE Guide for Architectural Framework and Application of Federated Machine Learning (IEEE 3652.1-2020), https://www.techstreet.com/ieee/standards/ieee-p3652-1?gateway_code=ieee&vendor_id=7453&product_id=2183131

[8] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2019). Advances and open problems in federated learning. *arXiv preprint arXiv*:1912.04977.

[9] Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv*:1610.05492

[10] Li, A., Liu, R., Hu, M., Tuan, L. A., & Yu, H. (2023). Towards Interpretable Federated Learning. *arXiv preprint arXiv*:2302.13473.

[11] Li, B., Fan, L., Gu, H., Li, J., & Yang, Q. (2022). FedIPR: Ownership verification for federated deep neural network models. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(4), 4521-4536.

[12] Li, J., & Huang, H. (2020, August). Faster secure data mining via distributed homomorphic encryption. *In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (pp. 2706-2714).

[13] Li, T., Hu, S., Beirami, A., & Smith, V. (2021, July). Ditto: Fair and robust federated learning through personalization. In *International Conference on Machine Learning* (pp. 6357-6368). PMLR.

[14] Li, T., Sahu Anit, K., Talwalkar, A., & Smith, V. (2020) Federated Learning: Challenges, Methods, and Future Directions, *IEEE Signal Processing Magazine*, 37.3: 50-60. DOI: 10.1109/MSP.2020.2975749.

[15] Liu, D., Miller, T., Sayeed, R., & Mandl, K. D. (2018). Fadl: Federated-autonomous deep learning for distributed electronic health record. a*rXiv preprint arXiv*:1811.11400.

[16] Liu, Y., Kang, Y., Xing, C., Chen, T., & Yang, Q. (2020). A secure federated transfer learning framework. *IEEE Intelligent Systems*, 35(4), 70-82.

[17] Liu, Y., Zhang, X., Kang, Y., Li, L., Chen, T., Hong, M., & Yang, Q. (2022). FedBCD: A communication-efficient collaborative learning framework for distributed features. *IEEE Transactions on Signal Processing*, 70, 4277-4290.

[18] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data[J]. In *Artificial Intelligence and Statistics* (pp. 1273-1282). PMLR.

[19] McMahan, H. B., Moore, E., Ramage, D., & y Arcas, B. A. (2016). Federated learning of deep networks using model averaging. *arXiv preprint arXiv*:1602.05629.

[20] Pandey, S. R., Tran, N. H., Bennis, M., Tun, Y. K., Manzoor, A., & Hong, C. S. (2020). A crowdsourcing framework for on-device federated learning. *IEEE Transactions on Wireless Communications*, 19(5), 3241-3256.

[21] So, J., Güler, B., & Avestimehr, A. S. (2020). Byzantine-resilient secure federated learning. *IEEE Journal on Selected Areas in Communications*, 39(7), 2168-2181.

[22] Trustworthy federated learning, Springer Cham, 2023

[23] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. *Advances in neural information processing systems*, 30.

[24] Waymo. Waymo. [OL]. [2020-02-17]. https://waymo.com

[25] Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., ... & Poor, H. V. (2020). Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security*, 15, 3454-3469.

[26] Xie, C., Chen, M., Chen, P. Y., & Li, B. (2021, July). Crfl: Certifiably robust federated learning against backdoor attacks. In *International Conference on Machine Learning* (pp. 11372-11382). PMLR.

[27] Xu, G., Li, H., Liu, S., Yang, K., & Lin, X. (2019). Verifynet: Secure and verifiable federated learning. *IEEE Transactions on Information Forensics and Security*, 15, 911-926.

[28] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2), 1-19. DOI:https://doi.org/10.1145/3298981

[29] Zhang, C., Li, S., Xia, J., Wang, W., Yan, F., & Liu, Y. (2020). {BatchCrypt}: Efficient homomorphic encryption for {Cross-Silo} federated learning. In *2020*

USENIX annual technical conference (*USENIX ATC 20*) (pp. 493-506).

[30] Zhang, X., Kang, Y., Chen, K., Fan, L., & Yang, Q. (2022). Trading off privacy, utility and efficiency in federated learning. *ACM Transactions on Intelligent Systems and Technology*.

[31] Zhang, Z., Yang, Y., Dai, Y., Wang, Q., Yu, Y., Qu, L., & Xu, Z. (2023, July). FedPETuning: When Federated Learning Meets the Parameter-Efficient Tuning Methods of Pre-trained Language Models. In *Findings of the Association for Computational Linguistics*: ACL 2023 (pp. 9963-9977).

[32] 百度.Apollo 自动驾驶解决方案[OL]. 2020-02-17. http://apollo.auto/

[33] 国内首个联邦学习标准正式出台，微众银行 AI 团队领衔 [N]，2019-07-01，https://www.sohu.com/a/323923758_99974896

[34] 获 IEEE 全票通过，首个联邦学习国际标准将正式推行[N]，2020-09-29，https://blog.csdn.net/m0_46317295/article/details/108870325

[35] 京东数科首度公开联邦学习战略全布局[N]，2020-06-03，*京东数科*，https://www.asmag.com.cn/news/202006/103870.html

[36] 联邦学习致力解构大模型下的数据生态与安全之困．*新华网*．2023-06-02. http://www.xinhuanet.com/fortune/2023-06/02/c_1212194942.htm

[37] 联邦学习最新医疗场景发布，同济大学刘琦教授团队与微众银行杨强教授 AI 团队合作打破药物数据共享壁垒[N]，*机器之心*，2020-12-17，https://www.jiqizhixin.com/articles/2020-12-17-7

[38] 商汤科技 SenseCare 创“心”升级,探索“联邦学习”入选欧洲计算机视觉国际会议(ECCV) [N]，2020-07-20，*慧聪网*，https://med.hc360.com/26/268213.html

[39] 特斯拉.Autopilot 系统介绍[OL].[2020-02-17]. https://www.tesla.cn/autopilot

[40] 腾讯天衍实验室联合微众银行研发医疗联邦学习 AI 利器让脑卒中预测准确率达 80% [N]，*搜狐*，2020-04-13，https://www.sohu.com/a/387647468_120230267

[41] 腾讯医疗健康携手微众银行成立联合实验室，联邦学习破解隐私难题 [N]，2020-08-22，*维科网*，https://www.ofweek.com/medical/2020-08/ART-11106-8450-30454114.html

[42] 微众银行人工智能部，鹏城实验室，腾讯研究院，中国信通院云大所，平安科技，招商局金融科技，电子商务与电子支付国家工程实验室(中国银联)：《联邦学习白皮书 V2.0》，深圳，2020 年.

[43] 微众银行首席 AI 官杨强：建立联邦学习生态需学术和产业界共同推动 [N] *TechWeb*，2020-11-16, http://www.myzaker.com/article/5fb1f78a8e9f0945d855fd1d/

[44] 央行发布《多方安全计算金融应用技术规范》 确保数据安全 [N]，2020-12-24，https://www.cebnet.com.cn/20201224/102711761.html

[45] 杨强，刘洋，程勇，康焱，陈天健：《联邦学习》，*电子工业出版社*：北京，2020 年:8-10.

[46] 杨强、刘洋、陈天健等：《联邦学习》，*中国计算机学会通讯*，2018 年版第 11 期，第 49-55 页.

[47] 一文读懂联邦学习的前世今生[N]，东科技技术说，2020-11-17，https://blog.csdn.net/JDDTechTalk/article/details/109738346

[48] 英特尔联手宾夕法尼亚大学 采用“联邦学习”技术的 AI 识别脑肿瘤 [N]，TechWeb，2020.05.26，http://www.techweb.com.cn/ucweb/news/id/2791494

[49] 拥抱“新基建”京东数科成立产业 AI 中心 [N]，*三言财经*，2020-03-19 https://www.sohu.com/a/381337566_100117963

[50] 这家银行运用“联邦学习”，为金融与科技融合“上保险”[N]. *财经头条*.2020-03-24，https://t.cj.sina.com.cn/articles/view/5675440730/152485a5a02000sg9m?from=tech

[51] 中科院上海药物所蒋华良院士团队联合华为云，发布 AI 药物联邦学习服务 [N]，*极客公园*，2020-09-30, http://www.geekpark.net/news/267104

[52] 字节跳动在联邦学习领域的探索及实践[N]. 字节跳动.2021-01-14，https://segmentfault.com/a/1190000038984381

[53] 《中华人民共和国民法总则》，中华人民共和国中央人民政府，http://www.gov.cn/xinwen/2017-03/18/content_5178585.htm#1

[54] 《中华人民共和国网络安全法》，中共中央网络安全和信息化委员会办公室、中华人民共和国国家互联网信息办公室，http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[55] 2019 年我国数字经济规模达 35.8 万亿元[N]，2020-11-16，人民网-强国论坛，http://www.people.com.cn/big5/n1/2020/1116/c32306-31932847.html

致谢

本报告撰写过程中，得到了杨强、范力欣、康焱、李博、刘洋、周柚池、蔡杭、范涛、邬克、何芸等多位业内人士的大力帮助和支持。他们在报告架构的创新设计、联邦学习知识树构建、重要定义和概念核验、技术完整性与专业性审核、经典算法评估筛选、以及核心文献数据核查与创新性分析等多个关键环节提供了宝贵的意见和建议，并做出了重要贡献，在此谨向以上人员致以诚挚的感谢。

版权说明

AI TR

www.aminer.cn

vip.aminer.cn/analysis/

智谱·AI

Open Islands