中国人民大学
RENMIN UNIVERSITY OF CHINA

联邦学习文献综述

作　　者：于佳鑫

学　　院：信息学院

专　　业：计算机科学与技术

年　　级：大二

学　　号：2022201895

完成日期：2024 年 2 月 26 日

摘要

随着大数据和机器学习的迅猛发展，联邦学习作为一种分布式学习方法逐渐引起了广泛关注。本文通过深入探讨联邦学习的基本概念，包括横向联邦学习、纵向联邦学习和联邦迁移学习等分类，以及详细介绍了其架构。进一步分析了联邦学习在通讯效率和安全性方面面临的挑战，着重讨论了通讯效率短板和安全性缺陷，涉及到典型隐私保护技术、全局隐私和本地隐私。此外，本文对联邦学习领域的研究热点和应用前景进行了综合评述，突出了其在实际应用中的潜在价值。

关键词：联邦学习、通讯效率、隐私保护技术、研究热点、应用前景

Abstract

With the rapid development of big data and machine learning, Federated Learning has gained widespread attention as a distributed learning method. This paper thoroughly explores the fundamental concepts of Federated Learning, including classifications such as Horizontal Federated Learning, Vertical Federated Learning, and Federated Transfer Learning, along with a detailed examination of its architecture. Furthermore, challenges in terms of communication efficiency and security are analyzed, with a focus on communication bottlenecks and security deficiencies, encompassing typical privacy protection techniques, global privacy, and local privacy. Additionally, the paper provides a comprehensive review of the research hotspots and application prospects in the field of Federated Learning, highlighting its potential value in practical applications.

Key Words: Federated Learning, Communication Efficiency, Privacy Protection Techniques, Research Hotspots, Application Prospects.

内容目录

1 引言

许多机器学习算法需要大量的数据，然而，在大多数行业中，数据分散在不同的组织中。这使得机器学习技术的实现比我们想象的更加困难。

是否有可能通过跨组织传输数据，将数据融合在一个共同的网站上？事实上，由于隐私安全、行业竞争和复杂的管理程序等原因，在很多情况下，要打破数据源之间的壁垒是非常困难的，甚至是不可能的。数据以孤岛的形式存在[1]，这种现象在金融、政府、供应链等多个领域都很常见。

在这种情况下，联邦学习作为一种无需交换用户原始数据的协作学习方式，受到了越来越多的关注，成为一个新的研究热点。

2 联邦学习基本概念

2.1 联邦学习

联邦学习的工作原理是这样的：客户端从本地的数据中学习来改进当前的共享模型，然后将更改汇总为一个小的重点更新。只有对模型的更新才使用加密通信发送到中心服务器，在那里它会立即与其他用户更新进行平均，以改进共享模型。所有训练数据都保留在客户端，没有单独的更新存储在中心服务器中。

总的来说，联邦学习提供更智能的模型，更低的延迟和更少的功耗，同时保护用户隐私。

2.2 联邦学习的分类

在不同的场景中，客户端之间持有的数据集特征各不相同。假设 Dm 代表客户端 m 持有的数据，I 表示样本空间 ID,Y 表示数据集的标签信息，X 表示数据集的特征信息，因此，一个完整的训练数据集 D 应由(I,Y,X)构成。

根据参与训练客户端的数据集特征信息 X 的不同，联邦学习被分为横向联邦学习、纵向联邦学习和联邦迁移学习[2]。

2.2.1 横向联邦学习

横向联邦学习的特点是数据集特征 X 和标签信息 Y 相同，但样本 ID 不同（图 1）。例如，两家地区性银行可能在各自地区拥有截然不同的用户群，其用户的交集非常小。但是，它们的业

务非常相似，因此特征空间是相同的。

横向联邦学习的公式表达如下：

$$X_m = X_n, Y_m = Y_n, I_m \neq I_n, \forall D_m, \forall D_n, m \neq n \quad (5)$$

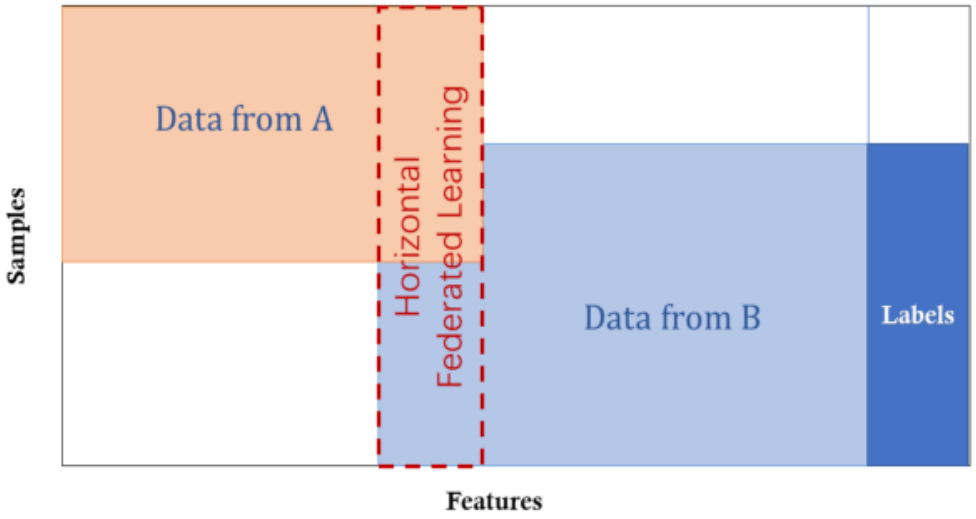

图 1 横向联邦学习

2.2.2 纵向联邦学习

纵向联邦学习或基于特征的联邦学习（图 2），适用于两个数据集共享相同的样本 ID 空间但特征空间不同的情况。例如，考虑同一城市的两家不同公司，一家是银行，另一家是电子商务公司。它们的用户集可能包含该地区的大部分居民，因此它们的用户空间的交集很大。但是，由于银行记录的是用户的收支行为和信用等级，而电子商务保留的是用户的浏览和购买记录，因此它们的特征空间截然不同。假设我们希望双方都有一个基于用户和产品信息的产品购买预测模型。纵向联邦学习就是将这些不同的特征聚合起来，以保护隐私的方式计算训练损失和梯度，利用双方的数据协同建立模型。

纵向联邦学习的公式表达如下：

$$X_m \neq X_n, Y_m \neq Y_n, I_m = I_n, \forall D_m, \forall D_n, m \neq n \quad (6)$$

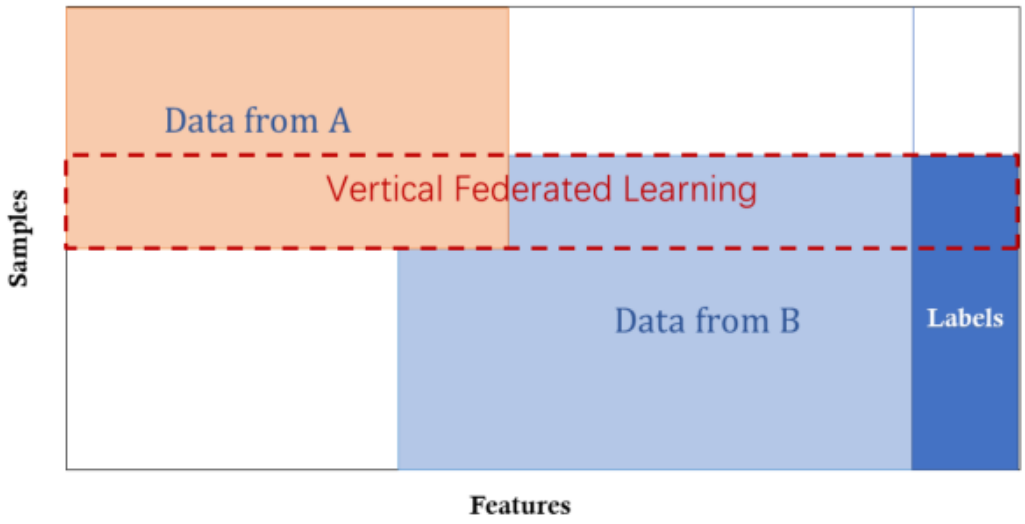

图 2 纵向联邦学习

2.2.3 联邦迁移学习

联邦迁移学习适用于两个数据集不仅在样本上不同，而且在特征空间上也不同的情况。假设有两家机构，一家是位于中国的银行，另一家是位于美国的电子商务公司。一方面，由于地理位置的限制，两家机构的用户群体有很小的交集。另一方面，由于业务不同，双方的特征空间只有一小部分重叠。在这种情况下，可以应用迁移学习[3]技术，为联盟下的整个样本和特征空间提供解决方案（图 3）。具体来说，利用有限的共同样本集学习两个特征空间之间的共同表示，然后应用于只具有单方特征的样本预测

联邦迁移学习是对现有联邦学习系统的重要扩展，因为它能处理的问题超出了现有联合学习算法的范围。

联邦迁移学习的公式表达如下：

$$X_m \neq X_n, Y_m \neq Y_n, I_m \neq I_n, \forall D_m, \forall D_n, m \neq n \quad (7)$$

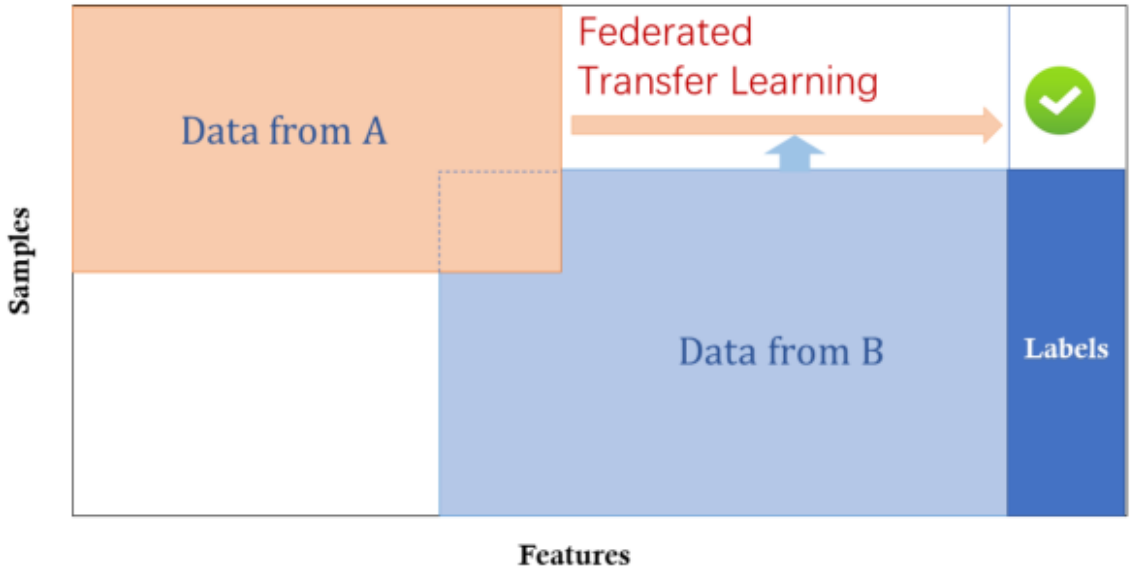

图 3 联邦迁移学习

2.3 联邦学习的架构

本节主要介绍联邦学习的一般架构。值得注意的是，横向和纵向联邦学习系统的架构在设计上有很大不同，所以进行分别介绍。

2.3.1 横向联邦学习

横向联合学习系统的典型架构如图 4 所示。在该系统中，具有相同数据结构的 k 个参与者在参数或云服务器的帮助下协作学习一个机器学习模型。这种系统的训练过程通常包括以下四个步骤：

- 步骤 1：参与者在本地计算训练梯度，利用加密[4]、差分隐私[5]或秘密共享[6]技术掩盖部分梯度，并发送掩盖后的梯度。将结果发送到服务器；
- 步骤 2：服务器执行安全聚合，而不了解任何参与者的信息；
- 步骤 3：服务器将汇总结果发回给参与者；
- 步骤 4：参与者利用解密梯度更新各自的模型；

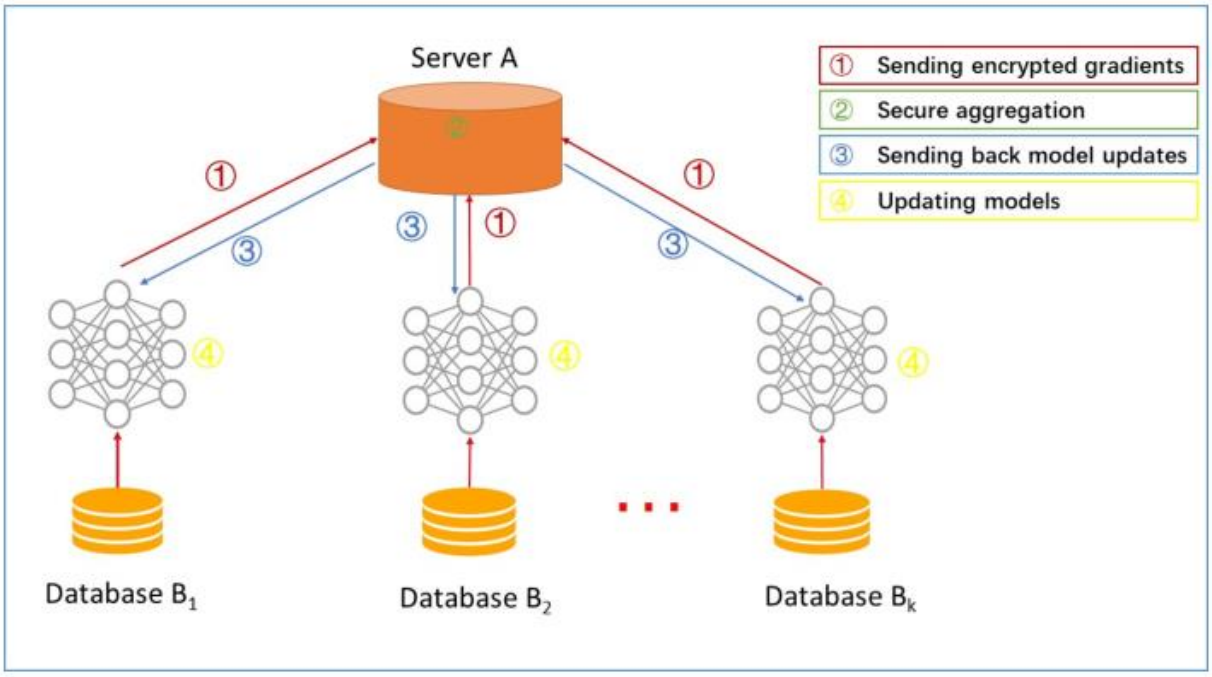

图 4 横向联邦学习的架构

通过上述步骤不断迭代，直到损失函数收敛，从而完成整个训练过程。这种结构与特定的机器学习算法（逻辑回归、DNN 等）无关，所有参与者将共享最终的模型参数。

2.3.2 纵向联邦学习

假设 A 公司和 B 公司希望联合训练一个机器学习模型，它们的业务系统各自拥有自己的数据。此外，B 公司也有模型需要预测的标签数据。出于数据隐私和安全考虑，A 和 B 不能直接交换数据。为了确保训练过程中数据的保密性，需要第三方合作者 C 的参与。

联合学习系统由两部分组成，如图 5 所示。

第 1 部分：加密实体对齐。由于两家公司的用户组成并不相同，系统使用基于加密的用户 ID 对齐技术（ [7, 8] ），在不暴露甲乙双方各自数据的情况下确认双方的共同用户。在实体对齐过程中，系统不会暴露互不重叠的用户。

第 2 部分：加密模型训练加密模型训练。确定共同实体后，我们就可以利用这些共同实体的数据来训练机器学习模型。训练过程可分为以下四个步骤（如图 4 所示）：

- 步骤 1：合作者 C 创建加密对，将公钥发送给 A 和 B；
- 步骤 2：A 和 B 加密并交换梯度和损耗计算的中间结果。
- 步骤 3：A 和 B 分别计算加密梯度并添加额外的掩码，B 还计算加密损失；A 和 B 将加密值发送给 C；
- 步骤 4：C 解密并将解密后的梯度和损耗发回给 A 和 B；A 和 B 消除梯度掩码后，相应地更新模型参数。

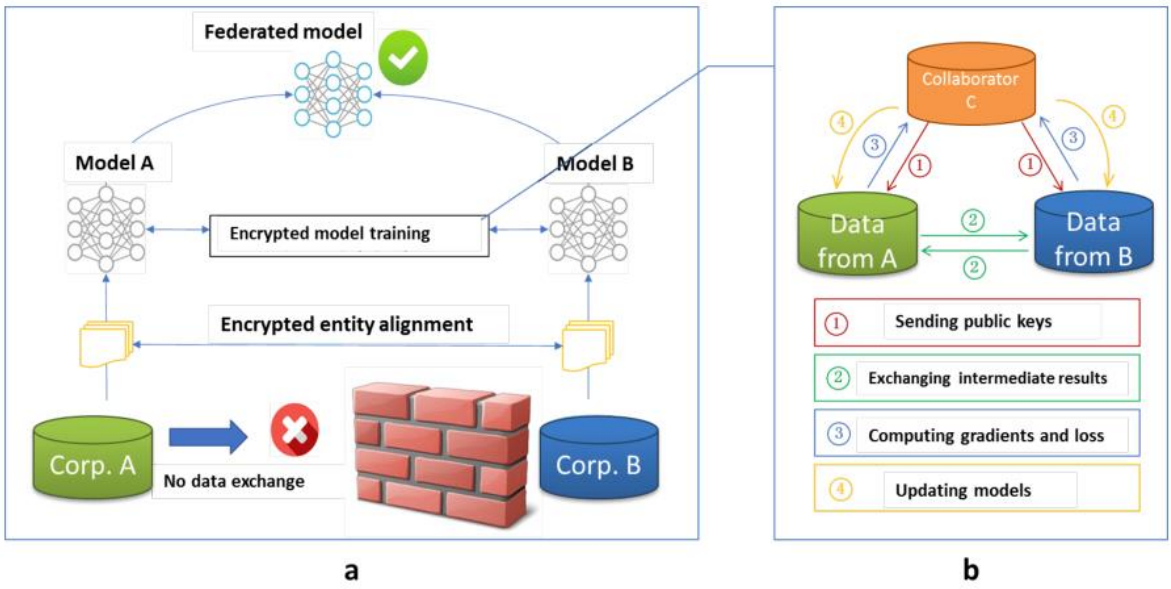

图 5 纵向联邦学习的架构

3 联邦学习存在的挑战和进展

自从提出联邦学习概念以来，该领域迅速引起了广泛的学术关注和研究。然而，目前仍存在许多亟待解决的威胁与挑战。最为核心的问题包括通信效率明显不足和隐私安全仍有缺陷，这些问题严重制约了联邦学习的进一步发展与应用。针对这些挑战，许多研究者提出了各种解决方法，取得了一些进展。

3.1 通讯效率短板明显

在传统的机器学习中，通信成本相对较小，计算成本占主导地位。相比之下，在联邦学习中，通信成本占主导地位：由于单个设备上的数据集与总数据集相比都很小，而且现代智能手机拥有相对较快的处理器。因此与许多模型类型的通信成本相比，计算基本上是免费的。

除此之外，由于客户端的训练数据通常基于特定用户的使用情况，所以任何一个本地数据集都不能代表总体的分布情况，也就是说，数据是非独立同分布的。在这种情况下，会造成训练过程难以收敛、通讯轮数过多的情况。

目前的研究中针对通信效率的改进主要有以下几种方法：

1. 算法优化：

算法优化是对分布式机器学习框架的改进，使得该框架更加适用于大量客户端、高频率、低容量、数据 Non-IID 的联邦学习环境。

在分布式学习框架中，客户端每进行一次 SGD，机器学习模型就会向中心服务器上传本

轮产生的优化更新。Mc Mahan 等[9]针对这个问题提出 Fed Avg 算法，要求客户端在本地多次执行 SGD 算法，然后与中心服务器交互模型更新，实现用更少的通信轮数训练出相同精度的模型。相比于基准算法 Fed SGD[10]，其在训练不同神经网络的通信轮数上减少了 1%～10%。

自 Fed Avg 算法提出后，许多研究对其进行了拓展和改进。Fed Avg 算法存在一些缺陷，包括在服务器端聚合时根据客户端数据量分配权重容易受到拥有大量重复数据客户端的影响，以及客户端只执行 SGD 算法和执行固定次数的 SGD 算法限制了模型训练速度。为解决这些问题，Li[12]等提出了 Fed Prox 算法，根据客户端设备的系统资源执行可变次数的 SGD 算法，加快了模型收敛速度并减少了模型更新数据的量。另一方面，Liu[13]等提出了 MFL 方案，利用动量梯度下降在本地模型更新阶段，显著提升了模型训练的收敛速度。Huang[14]等提出了 Lo Ada Boost 算法，通过分析客户端更新的交叉熵损失，迭代自适应调整本地客户端的迭代次数，相对于传统的 Fed Avg 算法，取得了显著的准确度和收敛速度提升。

2. 压缩：

压缩方案通常分为两种：梯度压缩和全局模型压缩。通常情况下，梯度压缩相比于全局模型压缩对通信效率的影响更大，因为互联网环境中上行链路速度比下载链路速度慢得多，交互通信的时间主要集中在梯度数据上传阶段。

在横向联邦学习中，面临着大量本地客户端的挑战，其中每个客户端的网络连接难以保证稳定可靠，低质量的通信会显著降低通信速度。为应对这一问题，Konečný[15]等提出了结构化更新和草图更新算法，要求客户端在一个低秩或随机掩码后的有限空间中进行模型学习，通过草图更新算法对模型更新进行压缩，虽然在 SGD 迭代方面减慢了收敛速度，但在通信效率上有所提升。Caldas[16]等将这种方法应用于全局模型更新的压缩中，同时引入了 Federated Dropout 思想，通过服务器随机选择全局模型的较小子集并采用压缩操作，减少了对客户端设备资源的影响，允许培训更高容量的模型，同时接触到更多样化的用户。另一方面，Reisizadeh[17]等结合算法优化与压缩的思路，提出 Fed PAQ 算法，要求服务器只选择少数客户端参与训练，客户端减少上传本地模型次数并在上传前进行量化更新操作以减小通信量。

3. 分散训练：

在联邦学习中，通常采用星形拓扑结构作为通信模型，但这种方式常常导致中心服务器的通信成本过高。为了解决这个问题，人们提出了分散拓扑结构作为一种替代方案，其中客户端只与它们的邻居进行通信，而不是直接与中心服务器通信。这种分散拓扑在低带宽或高时延网络环境中被证明比星形拓扑更快地进行模型训练[18]。在分散拓扑中，边缘服务器扮演关键角色，首先聚合来自客户端设备的本地更新，然后充当客户端与中心服务器进行交互[19]。这种架构的优势在于降低了通信成本，并提高了联邦学习的效率。

3.2 安全方面仍有缺陷

联邦学习通过仅交换模型更新数据，而不共享源数据的方式来保护用户隐私，然而，在真实的网络环境中，各种攻击手段层出不穷。如图 5 所示，联邦学习主要面临 3 种威胁：恶意客户端修改模型更新，破坏全局模型；恶意分析者通过模型更新的信息推测源数据的隐私信息；恶意服务器企图获得客户端的原始数据。

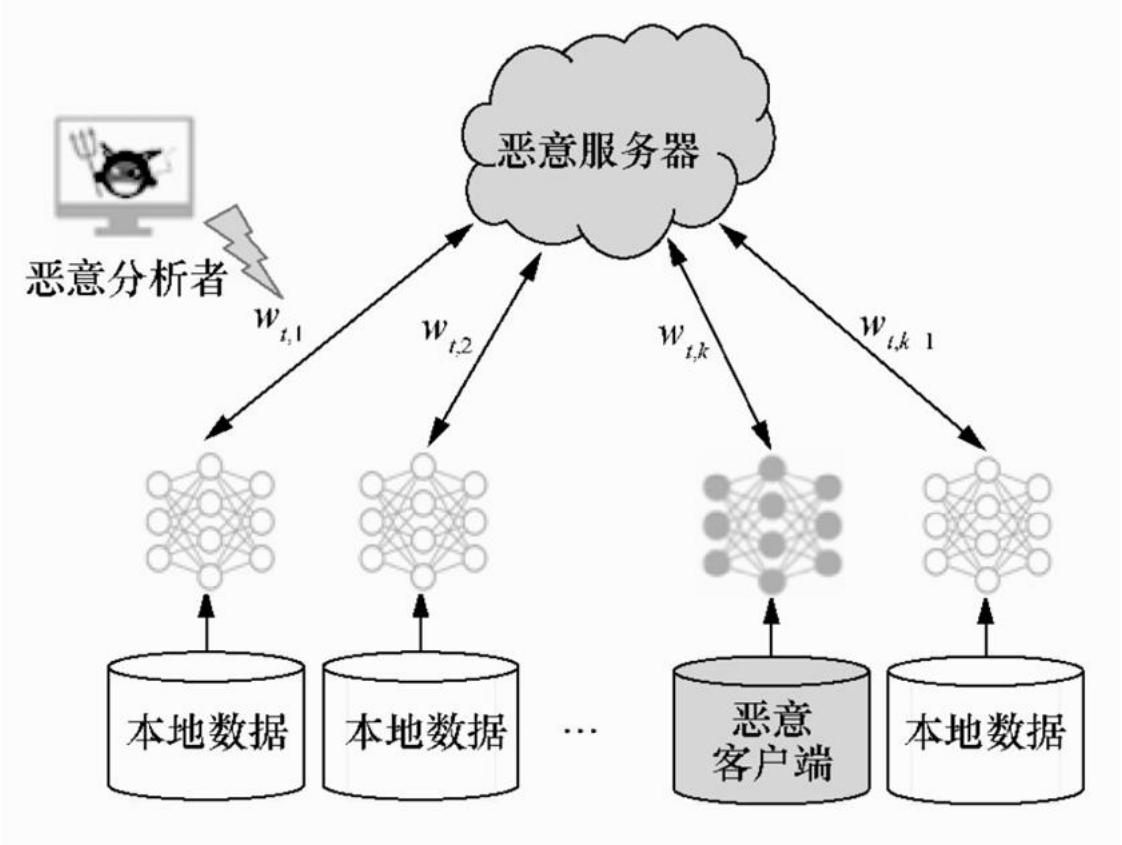

图 5 联邦学习中的安全威胁

3.2.1 典型隐私保护技术

现有的方案主要通过结合典型隐私保护技术来提供进一步的隐私增强，如差分隐私、安全多方计算、同态加密等技术，这些技术在之前的研究中已经被广泛应用于传统机器学习的隐私保护[20]。

1. 安全多方计算（SMC）：安全多方计算的研究焦点是在没有可信第三方的条件下，参与训练各方安全计算的一个共同的约束函数。通过混淆电路、不经意传输、秘密分享等技术实现多方共同运算，并确保各方数据的安全性。
2. 差分隐私：差分隐私涉及在数据中添加噪声，或使用泛化方法模糊某些敏感属性，直到第三方无法分辨出个人，从而使数据无法还原，以保护用户隐私。然而，这些方法的根本原因仍然是需要将数据传输到其他地方，而且这些工作通常需要在准确性和隐私之间做出权衡。

3. 同态加密：同态加密能够直接对密文数据进行密码学运算，最终运算结果经解密后与在明文上直接运算结果一致。同态加密分为全同态加密和部分同态加密，其中部分同态加密分为乘法同态和加法同态，若一个算法既满足乘法同态又满足加法同态，则称为全同态加密算法。

3.2.2 全局隐私

在全局隐私中，假设存在一个受信任的服务器，外部敌手可能是恶意客户端、分析师等。恶意客户端可以从中心服务器接收到它们参与轮的所有模型迭代信息，分析师可以在不同的训练轮中使用不同的超参数来研究模型迭代信息。因此，对中间迭代过程和最终模型进行严格的加密保护十分重要。

在联邦学习中，为应对恶意客户端可能获取模型贡献和数据信息的风险，研究者提出了差分隐私保护的算法。这些算法能够在模型训练中隐藏客户端的贡献，通过加密模型更新信息，同时在足够多客户端参与时，保持较小的性能损失。

3.2.3 本地隐私

为应对不可信服务器和恶意敌手的反演攻击，研究者采用安全多方计算、同态加密等技术实现模型信息的无损加解密。Secure Aggregation 模型通过秘密分享使服务器无法解密客户端的梯度信息，降低了恶意服务器的风险[21]。其他改进包括 Mandal[22]引入非交互式密钥交互计算技术，Dong[23]在通信效率算法中应用秘密分享与同态加密，Hao[24]通过改进同态加密算法提供后量子安全性。在纵向联邦学习中，Cheng 等提出 Secure Boost[25]算法，通过改进 XG Boost 模型和加法同态加密，在保护隐私的同时实现了与非隐私保护联邦学习相同的模型精度。

4 联邦学习的研究热点和应用前景

4.1 研究热点

不同于传统的分布式机器学习技术，海量客户端与 Non-IID 数据集对联邦学习提出了新的挑战。联邦学习的研究不仅需要掌握机器学习技术，还需要掌握分布式算法优化、密码学、压缩量化、统计等技术。除了上文中已经提到的方向，还有一些其他研究方向值得探索。

1. 系统异构：在联邦学习中，系统异构是一个显著的挑战，因为参与训练的客户端在硬件配置、网络带宽、电池容量等方面存在差异。联邦学习架构通常限制了参与训练的设备数量，且客户端可靠性不一，可能因网络故障或算力限制而中途退出。这种系统级别的异构对整体模型性能构成巨大挑战。为应对这种异构，适用于联邦学习的算法需要满足三个要求：适应客户

端的低参与率，兼容不同硬件结构，并能容忍训练设备的中途退出。

2. 无线通信：随着 5G 技术的普及，联邦学习逐渐应用于无线网络领域。在无线通信中，由于带宽有限，需要对模型更新进行量化压缩，而存在量化误差时的模型更新鲁棒性是一个重要的考虑因素。此外，无线通信中的噪声和干扰也是研究的焦点，因此开发适用于无线通信的联邦学习算法具有研究价值。这些方向的研究将有助于推动联邦学习在复杂场景中的应用和发展。

4.2 应用前景

作为一种创新的建模机制，联合学习可以在不损害数据隐私和安全的情况下，对来自多方的数据进行联合模型训练，因此在销售、金融和其他许多行业中有着广阔的应用前景，在这些行业中，由于知识产权、隐私保护和数据安全等因素，无法直接汇总数据来训练机器学习模型。

1. 智慧零售：智慧零售旨在通过机器学习技术提供个性化服务，包括产品推荐和销售服务。在实际应用中，相关数据如用户购买力、个人偏好和产品特征可能分散在不同企业或部门。通过联邦学习，这些数据可以在不暴露企业信息的情况下建立模型，实现数据隐私和安全的同时为客户提供个性化服务，实现互惠互利。

2. 智慧医疗：在医疗领域，敏感的医疗数据分布在不同医疗中心和医院中，导致数据难以获取，影响机器学习模型的性能。联邦学习通过将各医疗机构联合起来形成一个大型医疗数据集，提高了机器学习模型的效果。这有望推动智慧医疗发展，提升医疗保健水平。

3. 智慧城市：随着人工智能、物联网和 5G 技术的发展，智慧城市成为可能。然而，城市的不同信息部门产生大量数据形成数据孤岛，难以整合。联邦学习的异构数据处理能够解决这一问题，帮助构建迅速响应市民需求的智慧城市。同时，基于智慧城市构建的机器学习模型为企业提供个性化服务带来了更多机遇。

5 结束语

在本文中，我们努力深入探讨了联邦学习的基本概念、分类、架构以及面临的挑战与进展。通过对通讯效率和安全性的分析，我们揭示了在联邦学习中仍存在的一些问题，如通讯效率短板和安全性缺陷。尽管面临这些挑战，联邦学习作为一种分布式学习方法在解决隐私问题和数据集中式存储的需求上表现出了巨大的潜力。

对联邦学习研究热点和应用前景的综合评述显示，这一领域正迅速发展，并在各个领域展现出广泛的应用前景。未来，我们期待看到更多关于通讯效率改进和安全性增强的研究，以推动联邦学习在实际应用中更广泛地发挥作用。

最后，我需要诚实的指出，我对这一复杂领域的理解还有待加深。但我相信，通过不懈的努力，联邦学习将在不久的将来成为解决分布式学习和隐私保护挑战的有效工具。

参考文献

[1] 微众银行 AI 项目组.联邦学习白皮书 V1.0[R].2018.We Bank AI Project Team. Federated learning white paper V1.0[R].2018.

[2] YANG Q,LIU Y,CHEN T, et al. Federated machine learning: Concept and applications[J].ACM Transactions on Intelligent Systems and Technology (TIST),2019,10(2):1-19.

[3] Sinno Jialin Pan and Qiang Yang. 2010. A Survey on Transfer Learning. IEEE Trans. on Knowl. and Data Eng. 22, 10(Oct. 2010), 1345–1359. https://doi.org/10.1109/TKDE.2009.191

[4] Le Trieu Phong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai. 2018. Privacy-Preserving DeepLearning via Additively Homomorphic Encryption. IEEE Trans. Information Forensics and Security 13, 5 (2018),1333–1345.

[5] Reza Shokri and Vitaly Shmatikov. 2015. Privacy-Preserving Deep Learning. In Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). ACM, New York, NY, USA, 1310–1321. https://doi.org/10.1145/2810103.2813687

[6] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, DanielRamage, Aaron Segal, and Karn Seth. 2017. Practical Secure Aggregation for Privacy-Preserving Machine Learning. InProceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). ACM, New York,NY, USA, 1175–1191. https://doi.org/10.1145/3133956.3133982

[7] Gang Liang and Sudarshan S Chawathe. 2004. Privacy-preserving inter-database operations. In International Conference on Intelligence and Security Informatics. Springer, 66–82.

[8] Monica Scannapieco, Ilya Figotin, Elisa Bertino, and Ahmed K. Elmagarmid. 2007. Privacy Preserving Schema and Data Matching. In Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data (SIGMOD'07). ACM, New York, NY, USA, 653–664. https://doi.org/10.1145/1247480.1247553

[9] MCMAHAN H B,MOORE E,RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[J].Artificial Intelligence and Statistics,2017:1273-1282.

[10] CHEN J,PAN X,MONGA R, et al. Revisiting distributed synchronous

SGD[J].arXiv preprint arXiv:1604.00981,2016.

[11] XIAO P,CHENG S,STANKOVIC V, et al. Averaging is probably not the optimum way of aggregating parameters in federated learning[J].Entropy,2020,22(3):314.

[12] LI T,SAHU A K,ZAHEER M, et al. Federated optimization in heterogeneous networks[J].arXiv preprint arXiv:1812.06127,2018.

[13] LIU W,CHEN L,CHEN Y, et al. Accelerating federated learning via momentum gradient descent[J].IEEE Transactions on Parallel and Distributed Systems,2020,31(8):1754-1766.

[14] HUANG L,YIN Y,FU Z, et al. LoAdaBoost: loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data[J].PLoS ONE,2020 15(4):1-6.

[15] KONEČNÝJ,MCMAHAN H B,YU F X, et al. Federated learning:strategies for improving communication efficiency[J].arXiv preprint arXiv:1610.05492,2016.

[16] CALDAS S,KONEČNY J,MC-MAHAN H B, et al. Expanding the reach of federated learning by reducing client resource requirements[J]. arXiv preprint arXiv:1812.07210,2018.

[17] REISIZADEH A,MOKHTARI A,HASSANI H, et al. Fedpaq:a communication-efficient federated learning method with periodic averaging and quantization[C]//International Conference on Artificial Intelligence and Statistics.2020:2021-2031.

[18] LU X,LIAO Y,LIO P,et al.Privacy-preserving asynchronous federated learning mechanism for edge network computing[J].IEEE Access,2020,8:48970-48981.

[19] LIU L,ZHANG J,SONG S H,et al.Edge-assisted hierarchical federated learning with non-iid data[J].arXiv preprint arXiv:1905.06641,2019.

[20] 刘俊旭,孟小峰.机器学习的隐私保护研究综述[J].计算机研究与发展,2020,57(2):346.

[21] BONAWITZ K,IVANOV V,KREUTER B,et al.Practical secure aggregation for privacy-preserving machine learning[C]//Proceedings of the 2017 ACM Sigsac Conference on Computer and Communications Security.2017:1175-1191.

[22] MANDAL K,GONG G,LIU C.NIKE-based fast privacy-preserving high-dimensional data aggregation for mobile devices[R].CACR Technical Report,2018.

[23] CHENG K,FAN T,JIN Y,et al.Secureboost:a lossless federated learning framework[J].arXiv preprint arXiv:1901.08755,2019.

[24] DONG Y,CHEN X,SHEN L,et al.EaSTFLy:efficient and secure ternary federated learning[J].Computers&Security,2020,94:1-15.

[25] HAO M,LI H,LUO X,et al.Efficient and privacy-enhanced federated learning

for industrial artificial intelligence[J].IEEE Transactions on Industrial Informatics,2019,16(10):6532-6542.