计算机应用
Journal of Computer Applications
ISSN 1001-9081,CN 51-1307/TP

《计算机应用》网络首发论文

题目：联邦学习综述：概念、技术、应用与挑战
作者：梁天恺，曾碧，陈光
收稿日期：2021-10-26
网络首发日期：2022-01-04
引用格式：梁天恺，曾碧，陈光. 联邦学习综述：概念、技术、应用与挑战[J/OL]. 计算机应用. https://kns.cnki.net/kcms/detail/51.1307.TP.20211231.1727.014.html

Journal of Computer Applications 计算机应用 | ISSN 1001-9081 CODEN JYIIDU | http://www.joca.cn

文章编号:1001-9081(****)**-0000-00 | doi:10.11772/j.issn.1001-9081.2021101821

联邦学习综述：概念、技术、应用与挑战

梁天恺[1*]，曾碧[2]，陈光[1]

(1.广州广电运通金融电子股份有限公司，研究总院，广州 510006；2.广东工业大学，计算机学院，广州 510006)

(*通信作者电子邮箱 tiankai.liang@foxmail.com)

摘 要：在强调数据确权以及隐私保护的时代背景下，联邦学习作为一种新的机器学习范式，能够在不暴露各方数据的前提下达到解决数据孤岛以及隐私保护问题的目的。目前，基于联邦学习的建模方法已成为主流并获得很好的效果，因此对联邦学习的概念、技术、应用和挑战进行总结与分析具有重要的意义。本文首先阐述机器学习的发展历程和联邦学习出现的必然性，并给出联邦学习的定义与分类；接着，介绍并分析目前业界认可的三种联邦学习方法：横向联邦学习、纵向联邦学习和联邦迁移学习；然后，针对联邦学习的隐私保护问题，归纳并总结目前常见的隐私保护技术。此外，还对联邦学习的现有主流开源框架进行介绍与对比，同时给出了联邦学习的应用场景。最后，展望了联邦学习所面临的挑战和未来的研究方向。

关键词：联邦学习；隐私保护；横向联邦学习；纵向联邦学习；联邦迁移学习；开源框架

中图法分类号:TP181，TP309 **文献标识码:A**

Federated learning survey：concept, technology, application and challenge

LIANG Tiankai[1*], ZENG Bi[2], CHEN Guang[1]

(1.Research Institute, GRG Banking Equipment Limited Company, Guangzhou Guangdong 510006 China.;
2.School of Computer, Guangdong University of Technology, Guangzhou Guangdong 510006 China)

Abstract: Under the background of emphasizing data right confirmation and privacy protection, federated learning, as a new machine learning paradigm can solve the problem of data island and privacy protection without exposing the data of all participants. Since the modeling methods based on federated learning have become mainstream and achieved good effects, it is significant to summarize and analyze the concept, technology, application and challenge of federated learning. Firstly, the development process of machine learning and the inevitability of federated learning were elaborated, and the definition and classification of federated learning were given. Secondly, three federated learning methods (including horizontal federated learning, vertical federated learning and federated transfer learning) which were recognized by the industry currently were introduced and analyzed. Then, concerning the privacy protection issue of federated learning, the trending privacy protection technology was generalized and summarized. In addition, the typical open-source frameworks were introduced and compared, and the application scenarios of federated learning were given at the same time. Finally, the challenges and future research directions of federated learning were summed up.

Key words: federated learning; privacy protection; horizontal federated learning; vertical federated learning; a federated transfer learning; open-source framework

0 引言

在人工智能以及大数据技术蓬勃发展的时代，人们在享受着数据信息技术带来的便利外，也担忧着数据的安全性与隐私问题[1]。同时，随着数据确权的兴起，越来越多的实体开始强调数据的归属权和使用权，降低了不同实体之间的数据流通率，使各实体逐渐成为“数据孤岛”[2-5]。在此背景下，学者们开始研究如何在保证数据隐私安全的前提下打破“数据孤岛”现象，让数据的价值得到更大的发挥，提高人工智能算法的性能[6-7]。前人的研究成果主要从软件和硬件两个层面着手，实现数据的隐私保护，解决“数据孤岛”的问题[8-9]。

在硬件层面解决的主要思路是，在重要数据与可能的攻击者之间建立物理隔离，常见的技术有可信执行环境（Trusted Execution Environment，TEE）以及边缘计算（Edge Computing，EC）等。可信执行环境的解决方案是，将隐私数据和相应的数据处理过程置于一个可信的环境中，与外部服务请求者之间进行物理隔离，以此防止隐私数据的泄露

收稿日期: 2021-10-26; **修回日期**:2021-12-21; **录用日期**: 2021-12-23。

基金项目：国家自然科学基金资助项目（61672169），广东省自然科学基金资助项目（2021A1515012233）。

作者简介：梁天恺(1993—)，男(汉)，广东肇庆人，硕士研究生，主要研究方向：数据挖掘、人工智能、联邦学习；曾碧(1963—)，女(汉)，广东广州人，教授，博士，主要研究方向：智能信息处理、智能机器人；陈光(1981—)，男(汉)，广东广州人，工程师，博士，主要研究方向：人工智能、联邦学习。

[10-11]。总结而言，可信执行环境的建设难度相对较低，但需要对多方数据构建统一的可信环境，因此建设成本较高[12]。而边缘计算恰恰相反，其主要思路是，把各方设备的隐私数据和相应的数据操作限制在设备边缘，就近提供最近端的计算服务[13]。由于边缘计算的数据收集和数据运算等操作都是在设备的边缘环境进行的，无需将数据传输到主服务器，降低了敏感信息在传输过程和主服务器上泄露的可能性，有效解决了用户隐私泄露和数据安全问题，其次因为边缘计算能在边缘地带进行必要的计算分析与过滤，所以具备一定的应对数据爆炸的能力，有效降低边缘到中心的网络流量压力[14]。但是边缘计算对边缘设备的要求较高，其次在人工智能领域的应用上，边缘计算缺乏协调多方进行联合学习的能力，使其所习得的模型性能远低于集中式学习模型的性能[15-16]。

在软件层面解决的主要思路是，在数据以及通信层面，对数据进行加密，防止攻击者截获并破解隐私数据，主要的研究成果有网络安全通信协议以及密码学技术等[17]。比如通过密钥系统为客户机和服务器提供 C/S 认证服务的网络认证的 Kerberos 协议[18]；以及为数据提供安全加解密功能的密码学算法，如非对称加密算法：RSA（Rivest-Shamir-Adleman）算法、对称加密算法：美国提出的数据加密标准算法（Data Encryption Standard，DES）等[19-20]。然而量子计算的发展，使传统密码算法面临着巨大的挑战。因为量子具有高度的并行计算能力，所以量子计算机能在可接受的时间范围内破解传统的加密算法。例如，RSA 加密算法的解密计算——大整数分解问题，在传统计算机上需要指数级别的时间复杂度，而在量子计算机破解的时间复杂度为多项式级别的时间复杂度[21]。为解决传统的加密算法所存在的问题，后量子密码被提出。后量子密码算法的思路是：使用一些无法通过计算加速求解的数学问题，如多项式复杂程度的非确定性（Non-deterministic Polynomial，NP）完全问题、基于格、基于编码和基于多变元方程的数学问题等，来设计后量子算法，使得量子计算的算力优势无法在破解过程中发挥作用，以此防止密码被破解[22-23]。在软件层面的解决方案对硬件环境的要求低，且能提供较强大的数据隐私保护，但是如何利用加密后的数据协调多方进行高效的联合训练，成为机器学习领域的难点。

结合上述的研究现状，机器学习学者们提出了一种具备破解“数据孤岛”的能力，同时具备隐私保护能力的新范式——联邦学习（Federated Learning，FL）[24]。联邦学习能够在不暴露各方数据的前提下，协调各方进行联合学习，同时对硬件环境的改造较低[25]。

1 联邦学习的概念

本章将介绍机器学习的发展历程，阐述联邦学习出现的历史必然性，进而对联邦学习的定义与分类进行说明。

1.1 联邦学习的出现

随着智能化时代的到来，大规模数据被产生，如何从海量数据中提取有用的信息，让数据的潜在价值得到发挥并造福人类社会，催生了人工智能与机器学习技术[26-27]。回顾机器学习的发展历程，主要可以分为三大阶段：集中式学习阶段、分布式现场学习阶段，以及联邦学习阶段[28]。

集中式学习，是目前使用最广的学习模式，其基本思路是“模型不动，数据动”[29]。图 1 示出了集中式学习的框架图。此模式下，所有终端的数据需要被传输到主服务器上，由主服务器基于收集到的数据执行机器学习任务。即数据会被移动到主服务器，而模型以及模型的训练过程则被固定在主服务器上，称“模型不动，数据动”[30]。由于集中式学习把所有数据都集中到主服务器，使其所掌握的潜在的数据知识面更广，所以所习得的模型更能反映数据的潜在价值，性能相对更优[31]。另一方面，集中式学习虽然在传输数据的过程中使用了密码学进行加密，但是依旧面临着被破解的可能性，存在一定的数据安全隐患[32]。随着“数据确权”概念的深入，根据我国制定的《中华人民共和国个人信息保护法》[33]以及《中华人民共和国网络安全法》，越来越多的个人和企业开始强调数据的归属权和使用权[34]。因此，集中式学习模式已经不能够满足社会发展的要求，机器学习进入到分布式现场学习的阶段。

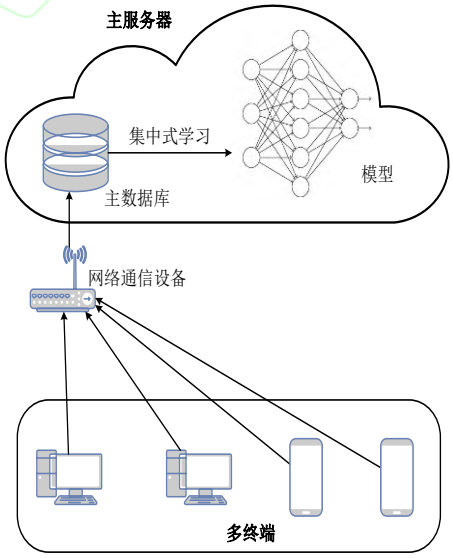

图 1　集中式学习框架

Fig. 1　Framework of centralized learning

分布式现场学习的提出，解决了数据安全和隐私保护的问题，其主要思路是一个系统的数据分别在来源端各自执行机器学习任务，最为典型的例子就是边缘计算[35]。边缘计算是分布式现场学习的一种实现方式，思路是把需要分析的数据限制在设备的边缘环境中进行现场学习，并将最终的学习结果汇聚到主服务器进行汇总和存储。这种把一个集中式学习任务分布到不同的设备边缘进行现场学习的方式，无需将敏感数据传输到主服务器进行学习，降低了敏感信息的流通

率，有效保护了各方的数据权益，但也导致了“数据孤岛”现象——由于各方缺乏数据上的沟通，导致一个系统内的数据无法交汇融合，无法得到最大的发挥，同时导致各方所学习到的知识过于片面，模型缺乏全局性和泛化能力[36]。

为了解决集中式学习存在的数据隐私问题，以及分布式现场学习的数据孤岛问题，联邦学习被提出，因此机器学习的发展历程也随之进入了第三阶段——联邦学习阶段[37]。

1.2 联邦学习的定义与分类

作为面向数据孤岛和隐私保护的机器学习解决方案，联邦学习最早由 H.Brendan McMahan 等人提出，应用于谷歌输入法 Gboard 系统，实现输入法的候选词预测[38-41]。与“模型不动，数据动”的集中式学习相反，联邦学习是一种“数据不动，模型动”的学习模式[42]。在联邦学习的过程中，各参与方不需要交换样本数据及其变体，仅需要交换与模型相关的中间数据及其变体，后由主服务器将中间数据进行安全聚合，并反馈给参与方，参与方则负责根据聚合后的模型信息进行己方模型的更新，有效保证了各参与方的敏感数据的安全性和隐私性，实现了在融合多个参与方的数据所蕴含的知识的同时保护隐私数据[43-45]。图 2 示出了联邦学习的架构图。

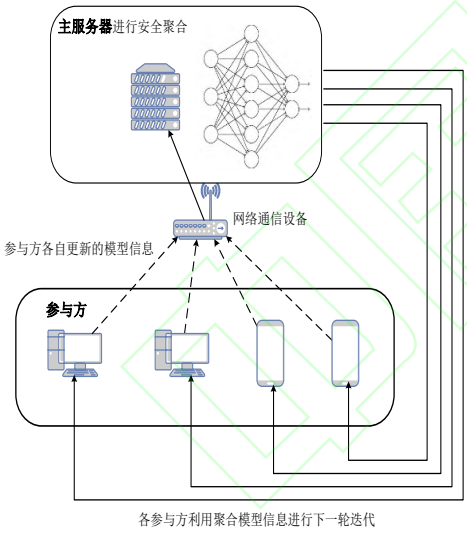

图 2 联邦学习的架构

Fig. 2 Architecture of federated learning

根据参与方数据集的特征空间和样本空间的分布，联邦学习可被分为：横向联邦学习、纵向联邦学习学习，以及联邦迁移学习[46-47]。假设 X 代表某个参与方的样本空间的某个样本数据，Y 代表某个参与方的特征空间。如图 3 所示，横向联邦学习（Horizontal Federated Learning，HFL）指的是两个参与方的数据集存在较大的特征空间重叠的情况[48]。此模式下，设定前提为各参与方的数据都是具备标签空间的。相反地，在具有较多样本数据重叠的参与方之间执行的联邦学习任务，称纵向联邦学习（Vertical Federated Learning，VFL），如图 4 所示[49]。此模式下，设定前提为只有一个参与方的数据具备标签空间，其余参与方的数据不具备标签空间。然而，在现实生活中，还可能存在两个在样本空间以及特征空间均存在较小重叠的数据集，此种情况下需要使用如图 5 所示的联邦迁移学习（Federated Transfer Learning，FTL）[50]。此模式下，设定前提和纵向联邦学习一样：只有一个参与方的数据是具备标签空间的。

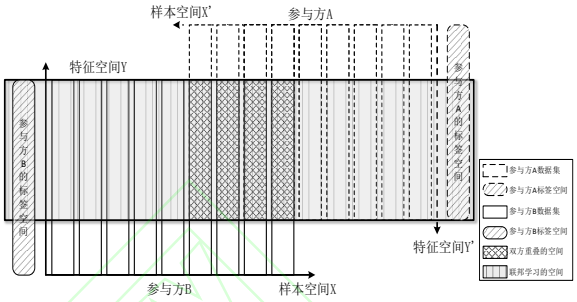

图 3 横向联邦学习

Fig. 3 Horizontal federated learning

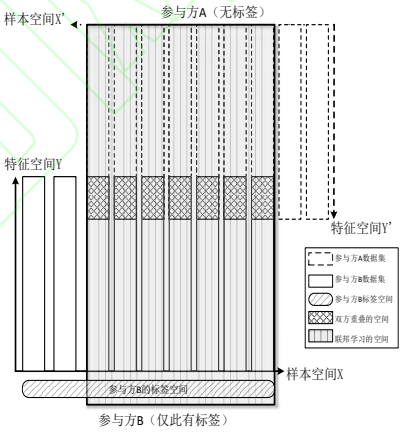

图 4 纵向联邦学习

Fig. 4 Vertical federated learning

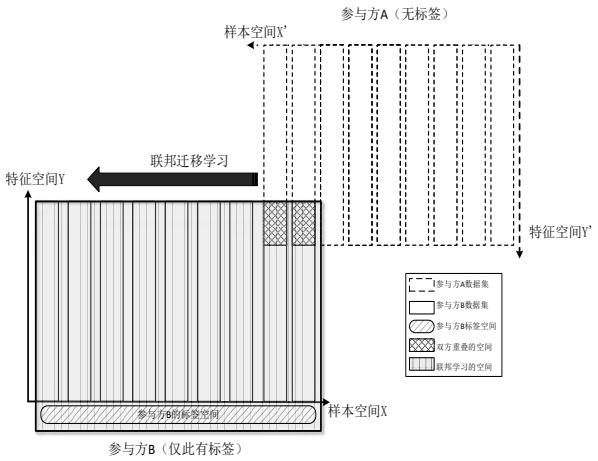

图 5 联邦迁移学习

Fig. 5 Federated transfer learning

2 横向联邦学习

横向联邦学习适用于参与方之间的特征空间的重叠面积较大的场景[51]。如图 3 所示，横向联邦学习的空间涵盖了多个参与方的样本数据，但所使用的特征空间仅限于各参与方之间的重叠部分，因此横向联邦学习也被称为按样本划分的联邦学习[52-54]。

作为最早被提出的联邦学习范式，横向联邦学习的应用比较广泛[55]。比如谷歌输入法的 Gboard 系统使用横向联邦学习，预测用户下一个词的输入[56]。传统做法是建议用户将数据传到主服务器上，然后再主服务器上基于所有用户数据，构建聚合预测模型。但是，随着隐私保护观念的深入，用户不希望隐私数据暴露，此时，联邦学习派上了用场。在横向联邦学习模式下，用户设备会把本地模型的模型信息传输到主服务器，主服务将所有的模型信息进行安全聚合，并将聚合信息加密后，广播给所有的用户设备，最后用户设备会根据主服务器的聚合信息来更新自身的本地模型[57-58]。在此学习模式下，用户设备会从主服务器的聚合信息中间接得到一些其他参与方的模型信息，即其他参与方的数据蕴含的新知识，从而提升所有用户设备的本地模型的泛化能力，提高预测模型的性能[59]。比如在该系统中存在用户 A、B，用户 A 是金融从业者，它的数据多集中在金融领域的用词上，而用户 B 是计算机行业从业者，它的数据多集中在计算机领域的用词，在横向联邦学习过程中，用户 A 的本地模型的构建过程中，借鉴了含有用户 B 的数据知识的聚合信息，因此用户 A 的本地模型对计算机行业用词的也具备预测能力[60]。

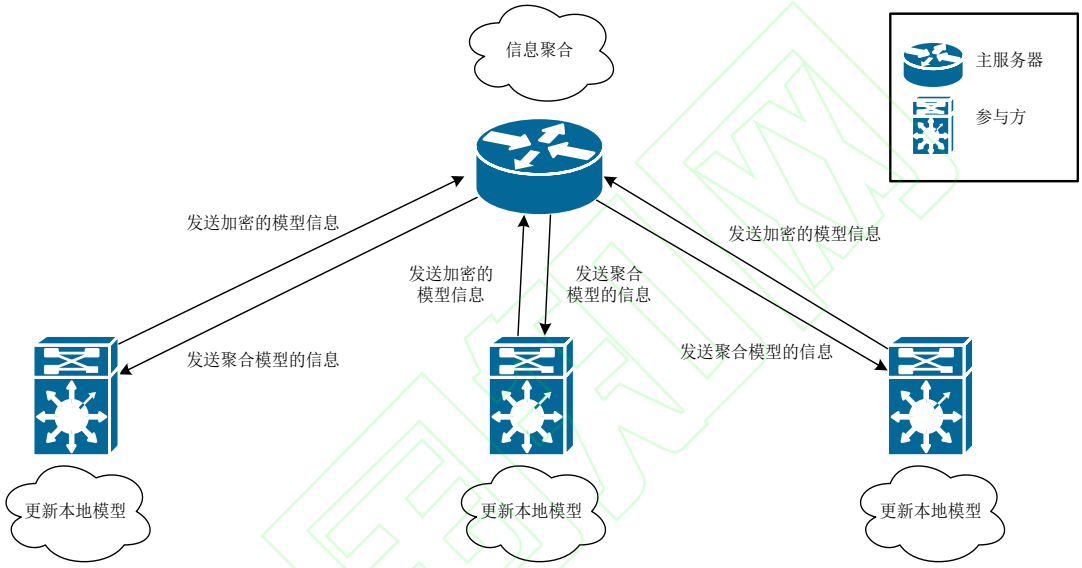

图 6　横向联邦学习架构

Fig. 6　Architecture of horizontal federated learning

图 6 示出了横向联邦学习的架构图，一般而言，横向联邦学习包括 5 个主要步骤[61]：

步骤 1：参与方根据自身数据集，构建本地模型；

步骤 2：参与方将本地模型的模型信息，如梯度，使用加密算法进行加密，如同态加密，然后把加密后的模型信息发送给主服务器[62]。

步骤 3：主服务器根据参与方的模型信息，进行安全聚合，常见的安全聚合算法有联邦平均算法（Federated Averaging Algorithm，FedAvg）以及异构联邦模型的聚合算法（FedProx 算法）[63-64]等。

步骤 4：主服务器将聚合后的信息，广播给所有参与方。

步骤 5：参与方对主服务器传来的聚合信息进行解密，据此更新本地模型。

重复以上步骤，直至达到预设的停止条件为止[65-66]。

总结而言，横向联邦学习的多方数据集的特征空间雷同，因此在联邦模型的训练过程中，不需要参与方之间进行中间计算结果的交换，而是由主服务器进行模型聚合，各方再根据最新的聚合模型信息进行本地模型的更新，能在不得知其他参与方源数据的情况下实现各方知识的交换。然而，横向联邦不适用于各参与方之间特征空间差异较大的跨领域联邦学习的情况，因此提出了纵向联邦学习[67-68]。

3 纵向联邦学习

与横向联邦学习相反，纵向联邦学习适用于参与方之间样本空间重叠面积较大的应用场景。从图 4 可以看出，因为纵向联邦学习是基于特征空间对样本数据进行划分，学习的数据空间仅包含了具备重叠特征的样本，所以纵向联邦学习又被称为按特征划分的联邦学习[69-70]。

因此在，纵向联邦学习更适合执行跨行业跨领域的机器学习任务，如微视与广告商合作提出的联邦广告投放系统。在此系统中，微视具备包括用户画像和用户点播记录等数据，广告平台则具备广告信息、产品信息以及用户购买记录等数据。可见双方的数据集的特征空间截然不同，但是可能存在相同用户。在此情况下，纵向联邦学习则可以在不泄露、不交换双方样本数据的同时聚合双方的数据特征和知识特征，

构建出一个联邦推荐模型，在提高微视用户的体验度和广告收益的同时提高广告方的营销收益，实现双赢局面[71]。

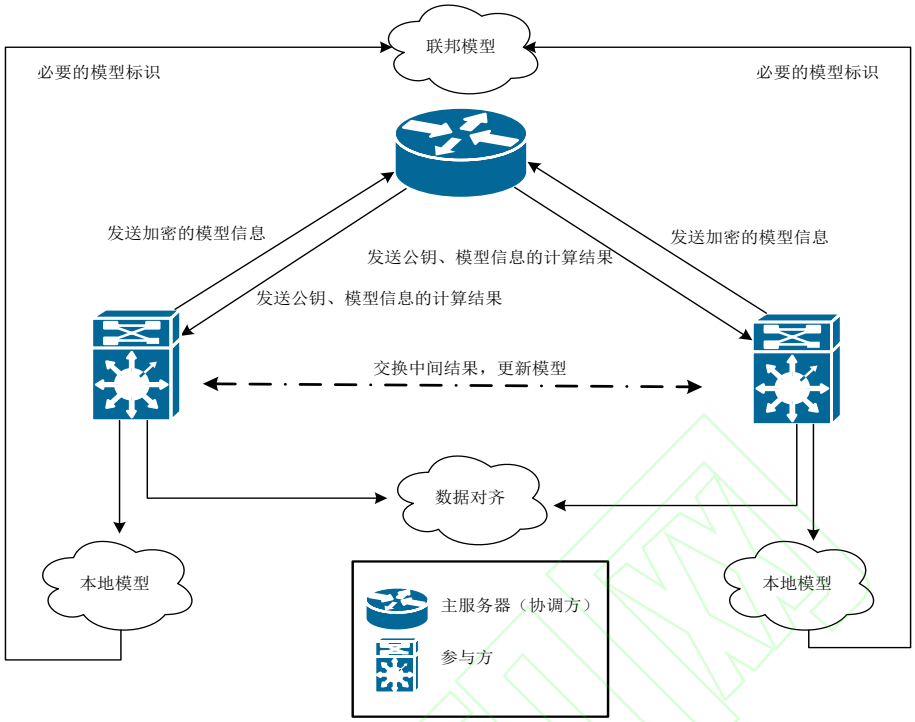

图 7　纵向联邦学习架构

Fig. 7　Architecture of vertical federated learning

图 7 给出了纵向联邦学习的架构图，特别说明，纵向联邦学习中，主服务器又叫协调方。纵向联邦学习的学习过程主要包括 5 个主要步骤[72]：

步骤1：数据对齐。数据对其的目的是在保护各参与方隐私和数据安全的前提下，找到共同样本，并给予共同样本执行联邦学习任务。常见的数据对齐方法有 SAHU A K 等人提出的算法[73]。此方法下，如要在参与方 A、B 之间进行数据对齐，则需要执行以下步骤：

（1）参与方 B 首先通过 RSA 加密算法，生成公钥 n、加密算法 e 以及解密算法 d，然后把(n, e)发送给参与方 A。

（2）参与方 A 接收到(n, e)后，将己方数据 A 进行哈希加密形成 H(A)，同时添加噪声 r，并对 r 使用加密算法 e 加密，得到密文：H(A)+e(r)，并传给参与方 B。

（3）参与方 B 拿到密文后，使用解密算法 d 进行解密得到 d(H(A)+e(r))=d(H(A))+d(e(r))=d(H(A))+r。同时，参与方 B 对己方数据 B 进行哈希加密，再通过解密算法 d 进行“解密”，得到 d(H(B))。然，后进行二次哈希加密，得到密文 B：H(d(H(B)))。最后将 d(H(A))+r 和密文 B 传送给参与 A。

（4）参与方 A 接收到参与方 B 的信息后，首先对 d(H(A))+r 去除噪声 r，得到 d(H(A))，再进行二次哈希得到 H(d(H(A)))，然后将其传送给参与方 B。

（5）可以看出，经过步骤（4）处理后，参与方 A 的加密数据为：H(d(H(A)))。同时，经过步骤（3）处理后，参与方 B 的加密数据为：H(d(H(B)))，两者处于一个数据纬度，因此参与方 B 方可以基于 H(d(H(A)))以及 H(d(H(B)))进行交集运算，最终得到双方的共同样本 ID。最后，将共同样本共享给其他方，完成数据对其的工作。

步骤 2：主服务器发送公钥给个参与方。同时，参与方基于共同样本构建初始本地模型，然后将加密后的模型信息，如梯度、损失值等，发送给主服务器[74]。

步骤 3：主服务器解密参与方的模型信息，同时计算参与方更新模型所必须的计算结果，并传送回参与方[75]。

步骤 4：参与方根据主服务器的计算结果，更新本地模型。同时，各方会把中间计算结果共享给其他参与方，用于协助对方计算梯度和损失值等模型信息[76]。

步骤 5-1：对于部分纵向联邦学习算法，参与方还会将本地模型的模型标识，发生给主服务器保存，以便在预测过程中，主服务器知道需要将新数据发送至哪些参与方进行联邦预测。如 secureBoost 算法中，参与方会把[记录 id, 特征, 阈值]以及分割后的样本空间，告知主服务器。同时，主服务器会当前的处理节点与参与方的划分信息进行关联。因此只有主服务器清楚整棵决策树的结构，当有新样本需要预测时，主服务器会将数据发至当前节点所关联的参与方，让参与方利用本地模型计算阈值，得知下一步的树搜索方向[77-78]。

步骤 5-2：特别地，部分需要全体参与方参与预测的纵向联邦学习算法，如安全联邦线性回归，则不需要参与方告知主服务器必要的模型标识[79]。

综上可得，纵向联邦学习中各方所掌握的特征不同，因此在训练联邦模型过程中，各方需要进行中间结果的交换，来帮助对方学习己方所掌握的特征知识[80]。

4 联邦迁移学习

区别于横向联邦学习以及纵向联邦学习，联邦迁移学习不需要主服务器（协调方）作为各参与方之间的协调者[81]。并且联邦迁移学习旨在让模型具备举一反三的能力，在各参与方的样本空间以及特征空间均存在较少交叉信息的情况下，使用迁移学习算法互助地构建模型[82]。学习模式可被总结为：使用某参与方在当前迭代中已训练好的模型参数，迁移到另外一个参与方上，协助它进行新一轮模型的训练。图 8 给出了典型的联邦迁移学习的架构图，主要包括以下步骤[83-84]：

步骤 1：参与方根据自身数据集，构建本地模型；

步骤 2：参与方分别运行各自的本地模型，获得数据表征，以及一组中间结果，加密后发送给对方。

步骤 3：对方利用接收到的中间结果，计算模型的加密梯度和损失值，加入掩码后发给原参与方。

步骤 4：各方对接收到的信息进行解密后发回给对方。然后各方利用发解密后的模型信息，更新各自的模型。

不断重复以上的步骤，直至损失收敛为止。在此过程中，相当于每个参与方都利用了对方的当前模型和数据潜在的表征，更新各自的本地模型，实现了迁移学习的联邦模式，即联邦迁移学习[85]。

一般而言，联邦迁移学习可被分为基于样本的联邦迁移学习、基于特征的联邦迁移学习、基于参数的联邦迁移学习以及基于相关性的联邦迁移学习[86]：

（1）基于样本的联邦迁移学习：又称基于实例的联邦迁移学习。基本思路是各参与方通过有选择地调整用于训练的样本的权重来减少不同参与方样本之间分布的差异性，并以此协同地训练得到一个联邦迁移模型。

（2）基于特征的联邦迁移学习：基本思路是通过最小化不同参与方之间的样本分布差异性或特征差异性来协同学习一个共同的特征空间，并以此特征空间来降低分类类别数或回归误差来实现联邦迁移模型的构建。

（3）基于参数的联邦迁移学习：又称基于模型的联邦迁移学习。基本思路是参与方利用其他方的模型信息或先验关系来初始化或更新本地模型，以此借鉴其他方的数据表征和知识。

（4）基于相关性的联邦迁移学习：对不同参与方的知识或特征空间进行相关性映射，并按照相关性顺序来利用其他参与方的知识映射更新本地模型，以此借鉴更多的知识。

总结而言，相对于传统的迁移学习，联邦迁移学习最大的特点是：其基于多方的数据表征来建模，但某参与方的数据不允许流向其他方，而传统的迁移学习则不做限制，因此联邦迁移学习有效保护了用户数据的隐私性和安全性[87]。

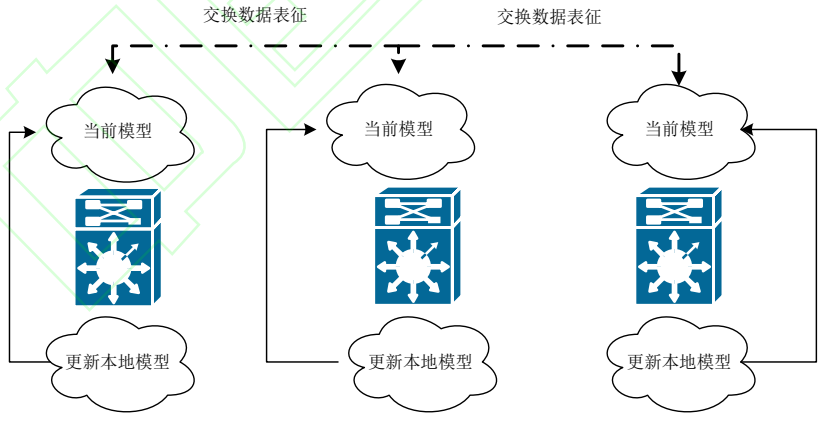

图 8　联邦迁移学习架构

Fig. 8　Architecture of federated transfer learning

5 联邦学习的隐私安全

联邦学习除了解决数据孤岛问题，使得各方数据可以进行联合学习外，还必须解决数据安全问题，实现各方的隐私保护[88]。

5.1 安全模型

安全模型是评价评价一个联邦学习系统是否满足隐私保护要求的标准之一。其要求一个安全的联邦学习系统应当满足以下几个安全属性[89]：

（1）隐私性：要求能有效保证系统内部各方的数据安全和隐私安全。

（2）正确性：每个参与方都能输出计算结果，且计算结果是正确的。

（3）公平性：系统能公平看待各方的计算贡献，公平地进行计算结果的聚合。

5.2 攻击模型

联邦学习想要满足安全模型的要求，通常会面临着四种常见的潜在敌手以及安全威胁。针对联邦学习系统的攻击模型主要包括：

（1）源自服务器的攻击[90]：

根据源自服务器的攻击行为，可以分为诚实但好奇的服务器敌手、恶意的服务器敌手，以及混合的服务器敌手：一个诚实但好奇的服务器，会试图从参与方的模型更新信息中反推出参与方的隐私数据特点等，但不会提供负反馈信息给参与者，使其错误地更改本地模型。相反地，恶意服务器不仅会试图从参与方的模型更新信息中反推出参与方的隐私数据特点等，还会恶意篡改聚合模型，或者提供错误的信息给参与方，破参与方的模型性能。

混合的服务器敌手则同时或者不间断地充当诚实但好奇的服务器敌手和恶意的服务器敌手。

（2）源自参与者的攻击[91]：

有的参与者是诚实但好奇的，它希望窃听其他参与方以及主服务器共享的数据信息，以期从中推理出某些有用的信息。这对联邦内部造成数据安全的威胁，同时它对模型更新会比较消极，不利于联邦模型性能的提升。其次，还有恶意的参与者存在，他们的主要目的是：反馈错误的模型信息到主服务器，使得联邦模型向着消极的方向更新迭代。同样地也存在混合类型的敌对参与方。

（3）源自外部的攻击[92]：

参与者和服务器之间通信更新时，通道上可能存在外部窃听者窃听信息，并由此反推出一些有关模型等的隐私数据，造成联邦内部的通信安全威胁。

（4）源自系统漏洞的攻击[93]：

联邦学习系统本身也可能存在潜在的安全薄弱点，比如系统架构设计不合理等。这些源自系统的漏洞使得攻击者可以发起数据攻击以及模型攻击：

数据攻击，主要是指参与者恶意修改数据标签或中间信息，破坏联邦学习的过程。

模型更新攻击：通过恶意地恶化本地模型，破坏全局模型的性能。

5.3 隐私保护

隐私保护技术经过多年的发展，演变出众多的隐私保护技术，这些隐私保护技术可以被用于联邦学习过程中，以此保证联邦内部各参与方的数据安全和隐私安全。常见的隐私保护技术，常见有不经意传输（Oblivious Transfer，OT）[94]、混淆电路（Garbled Circuit，GC）[95]、秘密共享（Secret Sharing，SS）[96]、隐私集合交集（Private Set Intersection，PSI）[97]、差分隐私（Differential Privacy，DP）[98]，以及同态加密（Homomorphic Encryption，HE）[99]等。

•不经意传输：发送方把多条数据基于不同的密钥加密，并将所有公钥发送给接收方，接收方按需使用特定的公钥生成随机数，双方再分别进行异或运算等，最后接收方只会得到特定数据的明文信息，其余数据的运算结果为乱码[100]。

•混淆电路：其属于不经意传输的一种应用，基本思路是：根据运算函数设计出一个电路，加密方首先对该电路进行加密，即加米饭负责电路的生成任务。解密方在不能得知原始电路的情况下，双方通过不介意传输使得解密方可以获得相应的数据，即解密方负责电路的解密任务[101]。

•秘密共享：基本思路是化整为散，方法是将需要计算的秘密分割成多份小秘密，分别分发给若干个参与方进行处理，最后将结果进行聚合。在此设计下，因为各方只得到了一小部分的秘密，无法重构出真是的秘密，保证了数据的安全性和隐私性[102]。

•隐私集合交集技术：其是一种基于多方的单独输入寻找多方数据的交集，并返回给特定方的技术。隐私集合交集技术常被用于联邦学习的数据对齐任务中[103]。

•差分隐私：基本思路是针对需要保密的数据，加入噪声的处理。该动作虽然有效保护了数据的安全性与隐私性，但噪声的加入会对计算结果产生一定的影响[104]。

•同态加密：相对于其他加密算法，同态加密的最大优势在于在计算过程中不需要频繁进行加解密的操作，可以直接对密文进行计算，且计算结果解密后得到的值，与直接使用明文计算得到的结果一致，有效提高了计算效率[105]。

6 联邦学习的应用

6.1 联邦学习的开源框架

随着联邦学习的发展与应用，出现了越来越多的开源框架，为联邦学习的理论落到真实的应用场景提供了开发条件。

目前主流的联邦学习开源框架主要包括：微众银行牵头提出的 FATE（Federated AI Technology Enabler）[106]框架、百度牵头提出的 PaddleFL（Paddle Federated Learning）[107] 框架、谷歌牵头提出的 TFF（TensorFlow Federated）[108] 框架，以及 OpenMind 牵头提出的 Pysyft 框架[109]。表 1 给出了以上几个联邦学习开源框架的对比。

FATE 框架作为国内目前比较优秀的联邦学习开源框架，支持横向联邦学习、纵向联邦学习以及联邦迁移学习的实现，同时还提供了其他框架所没有的联邦特征工程算法、Kubernetes 容器化应用和联邦在线推理[110]。

相对而言，PaddleFL 仅支持很想和纵向的联邦学习。而 Pysyft 和 TFF 框架仅实现了横向联邦学习的支持。目前三者均缺乏联邦树模型算法的实现，如梯度提升决策树（Gradient Boosting Decision Tree，GDBT）和 SecureBoost[111]。

6.2 联邦学习的应用场景

在对数据安全性以及隐私性要求较高的领域，比如智慧城市、智慧政务、智慧医疗、金融保险、物联网、跨域推荐以及多方推理等，联邦学习展现出了不可预估的前景[112]。

•智慧城市：随着企业与个人对隐私要求的提高，联邦学习可在保护各方数据的安全性与隐私性的前提下，将城市里各方的数据进行安全整合，为市民提供更便捷的城市服务。

•智慧政务：政务数据属于政府层面的隐私数据，导致政务数据库不能随意为第三方提供数据服务，限制了人工智能算法的性能提升，如贷款人风险评估等，无法融合公安部门的数据、征信部门的征信记录等数据特征，限制了评估算法的性能。联邦学习的出现，为数据孤岛问题提供了一种安全的解决方案。

•智慧医疗：医疗领域更注重个人数据的隐私性[113]。比如，多个医院需要协同合作，对患者进行 DNA 测序，以告知患者所患疾病。联邦学习就可以联合多个医院的不同数据集进行学习，训练出一个蕴含多个医院的不同知识的联邦模型，为患者 DNA 序列工作提供联邦预测的能力。如此，各医院的 DNA 库以及患者的 DNA 序列均互不可知，保证了多方的数据安全和隐私安全。

•金融保险：在金融保险行业，横向联邦学习可以为具有相同数据特征的金融机构，如多家银行，训练横向联邦模型。也可为具备不同数据特征的金融机构，如证券公司与信贷公司，训练纵向联邦模型。有效保护了金融数据的安全性，提高金融评估模型的性能。

•物联网：在当今万物互联的物联网时代的发展趋势下，联邦学习也为万物数据安全互联互通提供了可能性。比如谷歌输入法的 Gboard 系统，把多个装有 Gboard 的设备组成联邦，融合多方数据构建联邦学习，有效提高了输入法对不同行业以及输入习惯的用户的输入词预测任务的准确率。因此联邦学习随着物联网技术的发展以及隐私保护观念的深入，愈发具有巨大的潜力和潜在价值[114]。

•跨域推荐：其次，联邦学习在跨领域推荐也展现出了巨大的前景。比如视频网站和广告商的跨领域合作，提高双方的营收和用户活跃度。又比如网购平台与社交平台的合作，社交平台提供用户社交活动中出现的商品类别和社交圈特征等，网购平台提供商品信息和用户购买记录等，双方合作可以同时提高网购平台和社交平台针对用户的商品及服务的推荐准确度。

•多方推理：传统的机器学习算法的推理过程是基于一个集中式模型进行的，联邦学习的出现使得多方推理成为可能。多方推理是指各方不需要进行数据以及学习信息的交换，仅使用多方的本地模型进行联邦推理。此应用场景下，能更进一步地保护各方的数据和隐私安全，同时让推理过程融合更多的知识，提高推理结果的可靠性。

表 1　4 种主流的联邦学习开源框架对比

Table. 1　Comparison of 4 mainstream federated learning open source frameworks

框架	横向联邦学习	纵向联邦学习	联邦迁移学习	Kubernetes	树模型	联邦特征工程	联邦在线推理	支持的隐私保护算法
FATE	支持	支持	支持	支持	支持	支持	支持	同态加密 隐私共享 RSA、DiffieHellman
PaddleFL	支持	支持	不支持	不支持	不支持	不支持	不支持	差分隐私
TFF	支持	不支持	不支持	不支持	不支持	不支持	不支持	差分隐私
Pysyft	支持	不支持	不支持	不支持	不支持	不支持	不支持	同态加密 隐私共享

7 联邦学习面临的挑战

联邦学习虽然能有效解决数据孤岛和隐私保护的问题，同时也具有巨大的发展潜力和应用价值，但也面临着巨大的挑战：

（1）参与方难题：

作为联邦学习的成员，参与方是联邦学习的主要成员，也是联邦学习的基础，但联邦学习在参与方层面存在的难题也不少，目前最主要存在的是参与方激励以及参与方选择等难题。

参与方激励难题指的是如何吸引更多的参与方参与到联邦学习中，是限制联邦学习系统中的数据规模和数据多样性的提高，和联邦学习模型性能的提升的关键。因此联邦学习面临的挑战还包括如何建立一个完善的激励机制和分配机制，鼓励更多参与方的加入[115]。

其次，联邦学习还存在着如何识别诚实但好奇的半诚实参与方以及恶意的参与方，如何选择合适的参与方等参与方选择的难题。目前的联邦学习方法，所有参与方都是无差别地参与到联邦学习中。但是，对于一个参与方来说，可能并不是所有的其他参与方的模型信息对其都是有帮助的，因此研究一种可行且可信的诚实参与方识别算法，让参与方在学

习过程中可以自主地按需选择若干个安全的其他参与方的模型信息进行本地更新，也是联邦学习需要解决的问题之一。

（2）算力难题

联邦学习虽然可以在保护各方隐私的前提下，将多个设备联合在一起进行训练，有效提高了模型性能，然而在当今移动设备的算力下，仅有部分小运算量的算法如逻辑回归等可在设备端运行，但限制了主流的包含前后反馈过程的神经网络的实施。这也是联邦学习面临的巨大挑战之一[116]。

（3）通信难题

在联邦学习的过程中，各方之间需要频繁交换加解密以及模型相关的数据，而协调方往往需要等待所有参与方的中间数据都返回后才能进行安全聚合或其他数据处理，这对通信提出了较高的要求。如何提高通信信道的质量和容量，成为限制联邦学习发展的难题之一[117]。

（4）聚合难题

在联邦学习中，存在一个协调方对所有参与方的数据进行安全聚合和运算等。目前的联邦学习算法的常见聚合方式有 FedAvg 平均聚合以及 FedProx 异构聚合，但事实证明以上的聚合方法都会使得大部分联邦学习模型相对于集中式模型是有损的。其次，如何使得主服务器可异步地聚合各参与方的信息，提高参与方中途退出学习的应对能力，也是联邦学习亟需解决的难题之一[118]。随着技术的发展，目前也存在一些无损的联邦学习模型，如纵向联邦树模型 SecureBoost。可惜的是，目前的纵向联邦学习还存在一个巨大的问题——预测难题。

（5）预测难题

在纵向联邦学习中，只有协调方得知的是整个联邦的结构，而参与方得知的是与其数据特征相关的子模型的结构。因此在联邦预测过程中，需要协调方与参与方共同合作，才能预测出新样本的标签。一旦某个参与方推出联邦，该方所掌握的子树结构也会随之消失，严重影响联邦预测过程[119]。

（6）中心方等待聚合难题

在目前的联邦学习方法的学习中，中心方需要等待所有的参与方模型信息返回后，才会进行新一轮的信息聚合。如遇到参与方掉线或通信阻滞等问题，会导致中心方陷入无限的等待过程中，严重影响模型聚合以及联邦学习的效率。因此，如何提出一种能保证联邦学习效率和效果的中心方等待聚合的策略，也是联邦学习面临的挑战。

8 结语

数据确权和隐私保护降低了数据流通性，一定程度导致了数据孤岛的问题。联邦学习，作为一种能在保护隐私安全和数据安全前提下解决数据孤岛问题的解决方案，被提出并愈受关注。基于此，阐述了机器学习发展历程中的三大阶段，呈现出联邦学习出现的历史必然性。从联邦学习的定义到分类，再细化到横向联邦学习、纵向联邦学习和联邦迁移学习，总结了联邦学习的概念和技术。同时介绍了联邦学习的安全模型和目前主流的隐私保护技术。为了使联邦学习理论能落地到实际的开发与应用中，介绍了现有常见的开源框架，并对联邦学习的巨大潜力和可行的应用场景作出了总结与展望。但联邦学习同时还面临着巨大的挑战——参与方难题、算力难题、通信难题、聚合难题、预测难题以及中心方等待聚合难题等六大难题。

同时，随着新技术的发展，联邦学习未来也可融合更多新技术来解决更多的技术难题。比如，借鉴安全多方计算中电子选举的技术来实现联邦多方推理。其次，在智能体与环境交互的领域，强化学习占据着相当重要的地位，然而目前联邦学习的学习模式尚未覆盖强化学习，因此如何结合强化学习理论和隐私保护技术来实现联邦强化学习，也将成为重要的研究方向之一。另外，值得提出的是联邦学习理论中的隐私保护机制也有一定的研究空间，即如何使用更加安全的隐私保护技术（如区块链技术、后量子密码算法等）来保证联邦系统的安全性。

总而言之，在如今强调数据确权和隐私保护的时代背景下，联邦学习具有巨大的前景，但同时也存在许多技术攻关和技术融合的突破点，望综述能为联邦学习领域的研究提供一定的帮助和启发。

参考文献 (Reference)

[1] 王晋东,张明清,韩继红.信息系统安全技术策略研究[J].计算机应用研究,2001(5):61-63.(YE J D, ZHANG M Q, HAN J H.Research on security technic policy of information system[J].Application Research of Computers,2001(5):61-63.)

[2] 何柯,陈悦之,陈家泽. 数据确权的理论逻辑与路径设计[J]. 财经科学,2021, 3:43-55. (HE K, CHEN Y Z, CHEN J Z. Theoretical logic and path design of the confirmation of data property right[J]. Finance & Economics,2021, 3:43-55.)

[3] 闫境华, 石先梅.数据生产要素化与数据确权的政治经济学分析[J].内蒙古社会科学,2021,42(5):113-120. (YAN J H, SHI X M.A olitical economy analysis of data production factorization and data confirmation[J].Inner Mongolia Social Sciences,2021,42(5):113-120.)

[4] 何志峰. 主数据集成:打破信息共享的壁垒[J]. 上海信息化,2009(4):59-61. (HE Z F. Master data integration: breaking the barriers of information sharing[J]. Shanghai Informatization,2009(4):59-61.)

[5] Kasturi J, Brown A P, Brown P, et al. Interconnectivity of disparate nonclinical data silos for drug discovery and development[J]. Therapeutic innovation & regulatory science, 2014, 48(4): 498-506.

[6] 叶明,王岩.人工智能时代数据孤岛破解法律制度研究[J].大连理工大学学报(社会科学版),2019,40(5):69-77. (YE M,WANG Y. Research on the legal system of data island breaking in the age of artificial intelligence[J].Journal of Dalian University of Technology (social sciences),2019,40(5):69-77.)

[7] 杨强.AI 与数据隐私保护：联邦学习的破解之道[J].信息安全研究,2019,5(11):961-965.(YANG Q.AI and data privacy protection: the way to federated learning[J].Journal of Information Securyity Research,2019,5(11):961-965.)

[8] 周茂君,潘宁.赋权与重构区块链技术对数据孤岛的破解[J].新闻与传播评论,2018,71(5):58-67.(ZHOU M J, PAN N.Empowerment and reconstruction: blockchain technology's cracking of data islands[J].Journalism and Communication Review,2018,71(5):58-67.)

[9] JANG J, KANG B B. Securing a communication channel for the trusted execution environment[J]. Computers & Security, 2019, 83: 79-92.

[10] 郑显义,李文,孟丹.TrustZone 技术的分析与研究[J].计算机学报,2016,39(9):1912-1928.(ZHENG X W, LI W, MENG D.Analysis and research on trustzone technology[J].Chinese Journal of Computers,2016,39(9):1912-1928.)

[11] 王凤领.基于 IPSec 的 VPN 技术的应用研究[J].计算机技术与发展,2012,22(9):250-253.(WANG F L. Study on Application of VPN technology based on IPSec[J].Computer Technology and Development,2012,22(9):250-253.)

[12] VENTURA G. Performance of distributed system functions using a trusted execution environment: U.S. Patent 10,691,793[P]. 2020-6-23.

[13] WAZIR Z K,EJAZ A,SAQIB H,IBRAR Y,ARIF A. Edge computing: a survey[J]. Future Generation Computer Systems, 2019,97(AUG.):219-235.

[14] 施巍松,张星洲,王一帆. 边缘计算:现状与展望[J]. 计算机研究与发展,2019,56(1):69-89.(SHI W S, ZHANG X Z, WANG Y F. Edge computing: state-of-the-art and future directions[J]. Journal of Computer Research and Development,2019,56(1):69-89.)

[15] SHI W, CAO J, ZHANG Q, et al. Edge computing: Vision and challenges[J]. IEEE internet of things journal, 2016, 3(5): 637-646.

[16] OUYANG T, ZHOU Z, CHEN X. Follow me at the edge: mobility-aware dynamic service placement for mobile edge computing[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(10): 2333-2345.

[17] 王良民,倪晓铃,赵蕙.网络层匿名通信协议综述[J].网络与信息安全学报,2020,6(01):11-26. (WANG L M, NI X L, ZHAO H. Survey of network-layer anonymous communication protocols[J].Chinese Journal of Network and Information Security,2020,6(01):11-26.)

[18] SALTZER J H. On the Origin of Kerberos[J]. IEEE Annals of the History of Computing, 2021, 43(1): 89-91.

[19] YU H, KIM Y. New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices[J]. Electronics, 2020, 9(2): 246.

[20] VEERAMANIKANDAN K, MANJAMADEVI P, LATHA K. Secure image steganography combined with DES encryption[J]. Wireless Communication, 2015, 7(7): 228-231.

[21] 王亚辉,张焕国,王后珍. 基于 e 次根攻击 RSA 的量子算法[J]. 工程科学与技术,2018,50(2):163-169. (WANG Y H, ZHANG H G, WANG H Z. Quantum Algorithm for Attacking RSA Based on the ethRoot[J]. Advanced Engineering Sciences,2018,50(2):163-169.)

[22] BERNSTEIN D J, LANGE T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.

[23] 路献辉. 后量子密码算法[J]. 中国计算机学会通讯, 2018, 014(10):23-26. (LU X H. Post-quantum cryptographic algorithm[J]. Communications of CCF, 2018, 014(10):23-26.)

[24] ZHANG C, XIE Y, BAI H, et al. A survey on federated learning[J]. Knowledge-Based Systems, 2021, 216: 106775.

[25] 王壮壮,陈宏松,杨丽敏,等.联邦学习与数据安全研究综述[J].智能计算机与应用,2021,11(1):126-129,133. (WANG Z Z, CHEN H S, YANG L M, et al. Review of federal learning and data security[J]. Intelligent Computer and Applications,2021,11(1):126-129, 133.)

[26] LIANG T K, ZENG B, LIU J, et al. An unsupervised user behavior prediction algorithm based on machine learning and neural network for smart home[J]. IEEE Access, 2018(6): 49237-49247.

[27] 梁天恺,曾碧,刘建圻. 基于 FP-Growth 的智能家居用户时序关联操控习惯挖掘方法[J]. 计算机应用研究,2020,37(2):385-389. (LIANG T K, ZENG B, LIU J Q. FP-Growth-based user temporal association control habits mining method for smart home[J]. Application Research of Computers,2020,37(2):385-389.)

[28] HOWARD H. YANG, ZHAO ZHONGYUAN, TONY Q. S. QUEK. Enabling Intelligence at Network Edge: An Overview of Federated Learning[J]. ZTE Communications,2020,18(2):2-10.

[29] YANG Q,LIU Y,CHEN T, et al. Federated Machine Learning.[J].ACM Transactions on Intelligent Systems & Technology, 2019,10(1).1-19.

[30] 潘如晟,韩东明,潘嘉铖,等. 联邦学习可视化:挑战与框架[J]. 计算机辅助设计与图形学学报,2020,32(4):513-519. (PAN R C, HAN D M, PAN J C. Visualization for Federated Learning: Challenges and Framework[J]. Journal of Computer-Aided Design & Computer Graphics,2020,32(4):513-519.)

[31] MOTHUKURI V, PARIZI R M, POURIYEH S, et al. A survey on security and privacy of federated learning[J]. Future Generation Computer Systems, 2021, 115: 619-640.

[32] ZHU H, ZHANG H, JIN Y. From federated learning to federated neural architecture search: a survey[J]. Complex & Intelligent Systems, 2021, 7(2): 639-657.

[33] 十三届全国人大常委会第三十次会议 20 日表决通过《中华人民共和国个人信息保护法》[J]. 信息网络安全,2021(9):96. (The 30th meeting of the Standing Committee of the 13th National People's Congress passed the "Personal Information Protection Law of the People's Republic of China" on the 20th[J]. Netinfo Security,2021(9):96.)

[34] 陆康,刘慧,任贝贝,等. 智慧图书馆用户数据隐私保护研究 ——基于《中华人民共和国网络安全法》和《一般数据保护条例》的文本启示[J]. 图书馆理论与实践,2020(3):17-21.(LU K, LIU H, REN B B. Research on User Data Privacy Protection of Smart Libraries: Based on the Enlightenment of Cybersecurity Law of the People's Republic of China and General Data Protection Regulation[J]. Library Theory and Practice,2020(3):17-21.)

[35] MENDIBOURE L, CHALOUF M A, KRIEF F. Edge computing based applications in vehicular environments: Comparative study and main issues[J]. Journal of Computer Science and Technology, 2019, 34(4): 869-886.

[36] ABDULRAHMAN S, TOUT H, OULD-SLIMANE H, et al. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond[J]. IEEE Internet of Things Journal, 2021, 8(7): 5476-5497.

[37] 陈兵,成翔,张佳乐,等. 联邦学习安全与隐私保护综述[J]. 南京航空航天大学学报,2020,52(5):675-684. (CHEN B, CHENG X, ZHANG J L. Survey of Security and Privacy in Federated Learning[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2020,52(5):675-684.)

[38] McMahan H B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//AISTATS 2017: Proceedings of the 2017 International Conference on Artificial Intelligence and Statistics. Lauderdale: PMLR, 2017: 1273-1282.

[39] MCMAHAN H B, MOORE E, RAMAGE D, et al. Federated learning of deep networks using model averaging[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1602.05629v1

[40] Zhu H, Zhang H, Jin Y. From federated learning to federated neural architecture search: a survey[J]. Complex & Intelligent Systems, 2021, 7(2): 639-657.

[41] KONECNY J, MCMAHAN H B, RAMAGE D, et al. Federated optimization: distributed machine learning for on-device intelligence[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1610.02527.

[42] 周俊,方国英,吴楠. 联邦学习安全与隐私保护研究综述[J]. 西华大学学报(自然科学版),2020,39(4):9-17. (ZHOU J, FANG G Y, WU N. Survey on security and privacy-preserving in federated learning[J]. Journal of Xihua University,2020,39(4):9-17.)

[43] ENCHEVA S, TUMIN S. On improving quality of the decision making process in a federated learning system[C]//COCD 2008: Proceedings of the 5th International Conference on Cooperative Design, Visualization and Engineering. Chan: Springer, 2008: 192-195.

[44] BONAWITZ K, EICHNER H, GRIESKAMP W, et al. Towards federated learning at scale: system design[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1902.01046v1.

[45] XU J, DU W, XU Q, et al. Federated learning based atmospheric source term estimation in urban environments[J]. Computers & Chemical Engineering, 2021, 155: 107505.

[46] LI Q, WEN Z, HE B. Federated learning systems: vision, hype and reality for data privacy and protection[EB/OL]. [2021-10-19].https://arxiv.org/abs/1907.09693.

[47] XIA Q, YE W, TAO Z, et al. A survey of federated learning for edge computing: research problems and solutions[J]. High-Confidence Computing, 2021,1(1):100008-100051.

[48] CHAMIKARA M A P, BERTOK P, KHALIL I, et al. Privacy preserving distributed machine learning with federated learning[J]. Computer Communications, 2021, 171: 112-125.

[49] 王佳,苗璐.联邦学习浅析[J].现代计算机,2020(25):27-31, 36.(WANG J, MIAO L.Brief introduction of federated learning[J].Modern Computer,2020(25):27-31, 36.)

[50] AMIRI M M, GÜNDÜZ D. Federated learning over wireless fading channels[J]. IEEE Transactions on Wireless Communications, 2020, 19(5): 3546-3557.

[51] KAIROUZ P, MCMAHAN H B, AVENT B, et al. Advances and open problems in federated learning[EB/OL].[2021-10-19]. https://arxiv.org/pdf/1912.04977.

[52] LI T, SAHU A K, TALWALKAR A, et al. Federated learning: challenges, methods, and future directions[J]. IEEE Signal Processing Magazine, 2020, 37(3): 50-60.

[53] QIN Z, LI G Y, YE H. Federated learning and wireless communications[J]. IEEE Wireless Communications, 2021 ,28(5):134-140.

[54] LIU Y, YUAN X, XIONG Z, et al. Federated learning for 6G communications: challenges, methods, and future directions[J]. China Communications, 2020, 17(9): 105-118.

[55] KOURTELLIS N, KATEVAS K, PERINO D. Flaas: federated learning as a service[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/2011.09359.

[56] HARD A, RAO K, MATHEWS R, et al. Federated learning for mobile keyboard prediction[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1811.03604.

[57] YANG T, ANDREW G, Eichner H, et al. Applied federated learning: Improving google keyboard query suggestions[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1812.02903.

[58] CHEN M, MATHEWS R, OUYANG T, et al. Federated learning of out-of-vocabulary words[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1903.10635.

[59] ACAR D A E, ZHAO Y, MATAS R, et al. Federated learning based on dynamic regularization[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/2111.04263.

[60] LI Q, WEN Z, WU Z, et al. A survey on federated learning systems: vision, hype and reality for data privacy and protection[EB/OL]. [2021-10-19]. https://arxiv.org/pdf/1907.09693.

[61] LIU Y, JAMES J Q, KANG J, et al. Privacy-preserving traffic flow prediction: A federated learning approach[J]. IEEE Internet of Things Journal, 2020, 7(8): 7751-7763.

[62] 唐春明,胡业周. 基于多比特全同态加密的安全多方计算[J]. 计算机学报,2021,44(4):836-845.(TANG C M, HU Y Z. Secure Multi-Party Computation based on multi-bit fully homomorphic encryption[J]. Chinese Journal of Computers,2021,44(4):836-845.)

[63] 罗长银,陈学斌,马春地,等. 基于层析分析改进的联邦平均算法[J]. 计算机科学,2021,48(8):32-40.(LUO C Y, CHEN X B, MA C D,等. Improved federated average algorithm based on tomographic analysis[J]. Computer Science,2021,48(8):32-40.)

[64] 王健宗,孔令炜,黄章成,等. 联邦学习隐私保护研究进展[J]. 大数据,2021,7(3):130-149. (WANG J Z, KONG L W, HUANG Z C. Research advances on privacy protection of federated learning[J]. Big Data Research,2021,7(3):130-149.)

[65] LYU L, YU H, YANG Q. Threats to federated learning: a survey[EB/OL].[2021-10-20]. https://arxiv.org/pdf/2003.02133.

[66] WANG H, YUROCHKIN M, SUN Y, et al. Federated learning with matched averaging[EB/OL]. [2021-10-20]. https://arxiv.org/pdf/2002.06440.

[67] 夏家骏,鲁颖,张子扬,等. 基于秘密共享与同态加密的纵向联邦学习方案研究[J]. 信息通信技术与政策,2021(6):19-26.(XIA J Z, LU Y, ZHANG Z Y, et al. Research on vertical federated learning based on secret sharing and homomorphic encryption[J]. Telecommunications Network Technology,2021(6):19-26.)

[68] YANG K, JIANG T, SHI Y, et al. Federated learning via over-the-air computation[J]. IEEE Transactions on Wireless Communications, 2020, 19(3): 2022-2035.

[69] LIU Y, KANG Y, LI L, et al. A communication efficient vertical federated learning framework[EB/OL]. [2021-10-20]. https://arxiv.org/pdf/1912.11187.

[70] FENG S, YU H. Multi-participant multi-class vertical federated learning[EB/OL]. [2021-10-20]. https://arxiv.org/pdf/1912.11187.

[71] 宋凯,林宜蓁.联邦学习在腾讯微视广告投放中的实践[EB/OL]. [2021-10-20]. https://zhuanlan.zhihu.com/p/407387382.(SONG K, LIN Y Q.The Practice of Federated Learning in Tencent Microvision Advertising[EB/OL]. [2021-10-20]. https://zhuanlan.zhihu.com/p/407387382)

[72] ROMANINI D, HALL A J, Papadopoulos P, et al. Pyvertical: A vertical federated learning framework for multi-headed splitnn[EB/OL]. [2021-10-20]. https://arxiv.org/pdf/2104.00489.

[73] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems, 2020,(2): 429-450.

[74] SUN J, YANG X, YAO Y, et al. Vertical Federated Learning without Revealing Intersection Membership[EB/OL]. [2021-10-20]. https://arxiv.org/pdf/2106.05508.

[75] Hashemi N, Safari P, Shariati B, et al. Vertical Federated Learning for Privacy-Preserving ML Model Development in Partially Disaggregated Networks[C]//ECOC 2021: Proceedings of the 2021 European Conference on Optical Communication. Piscataway: IEEE, 2021: 1-4.

[76] Zhang Y, Wu Q, Shikh-Bahaei M. Vertical Federated Learning Based Privacy-Preserving Cooperative Sensing in Cognitive Radio Networks[C]//GC 2020: Proceedings of the 2020 IEEE Global Communications Conference. Piscataway:IEEE, 2020:1-6.

[77] CHENG K, FAN T, JIN Y, et al. Secureboost: A lossless federated learning framework[J]. IEEE Intelligent Systems, 2021.

[78] 张君如,赵晓焱,袁培燕. 面向用户隐私保护的联邦安全树算法[J]. 计算机应用,2020,40(10):2980-2985. .(ZHANG J R, ZHAO X Y,

YUAN P Y. Federated security tree algorithm for user privacy protection[J]. Journal of Computer Applications,2020,40(10):2980-2985.)

[79] 杨强,刘洋,程勇,等.联邦学习[M].北京:电子工业出版社,2020:77-80(YANG Q, LIU Y, CHENG Y.Federated learning[M].Publishing House of Electronics Industry ,2020:77-80)

[80] 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.(LIU J X, MENG X F. Survey on privacy-preserving machine learning[J]. Journal of Computer Research and Development, 2020, 57(2): 346.)

[81] 刘文炎, 沈楚云, 王祥丰, 等. 可信机器学习的公平性综述[J]. 软件学报, 2021, 32(5): 1404-1426.(LIU W Y, SHEN C Y, WANG X F. Survey on fairness in trustworthy machine learning[J]. Journal of Software, 2021, 32(5): 1404-1426.)

[82] 杨强,童咏昕,王晏晟. 鱼与熊掌可以兼得——“联邦迁移学习”直面小数据与隐私关切挑战[J]. 前沿科学,2019(2):61-66. (YANG Q, TONG Y X, WANG Y C. "Federal migration learning" faces the challenges of small data and privacy concerns[J]. Frontier Science,2019(2):61-66.)

[83] YANG H, HE H, ZHANG W, et al. Fedsteg: A federated transfer learning framework for secure image steganalysis[J]. IEEE Transactions on Network Science and Engineering, 2020(8):1084-1094.

[84] CHEN Y, QIN X, WANG J, et al. Fedhealth: A federated transfer learning framework for wearable healthcare[J]. IEEE Intelligent Systems, 2020, 35(4): 83-93.

[85] LIU Y, KANG Y, XING C, et al. A secure federated transfer learning framework[J]. IEEE Intelligent Systems, 2020, 35(4): 70-82.

[86] JU C, GAO D, MANE R, et al. Federated transfer learning for eeg signal classification[C]//EMBC 2020: Proceedings of the 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society. Piscataway: IEEE, 2020: 3040-3045.

[87] 肖林声,钱慎一. 基于使用 MapReduce 并行的同态加密和梯度选择的联邦迁移学习算法[J]. 网络空间安全,2021,12(1):32-40. (XIAO L S, QIAN S Y. Federated transfer learning algorithm based on parallel homomorphic encryption using mapreduce and gradient selection[J].Cyberspace security,2021,12(1):32-40.)

[88] DIMITRIADIS D, KUMATANI K, GMYR R, et al. Federated transfer learning with dynamic gradient aggregation[EB/OL]. [2021-10-20]. https://arxiv.org/pdf/2008.02452.

[89] SEIF M, TANDON R, LI M. Wireless federated learning with local differential privacy[C]//ISIT 2020: Proceedings of the 2020 IEEE International Symposium on Information Theory. Piscataway: IEEE, 2020: 2604-2609.

[90] HIESSL T, SCHALL D, KEMNITZ J, et al. Industrial federated learning–requirements and system design[C]// PAAMS 2020: Proceedings of the 2020 International Conference on Practical Applications of Agents and Multi-Agent Systems. Cham: Springer, 2020: 42-53.

[91] CHEN D, ZHAO H. Data security and privacy protection issues in cloud computing[C]//ICCSEE 2012: Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. Piscataway: IEEE, 2012, 1: 647-651.

[92] ZHANG D. Big data security and privacy protection[C]//ICMCS 2018: Proceedings of the 8th International Conference on Management and Computer Science. Atlantis: Atlantis Press, 2018(77): 275-278.

[93] WEI K, LI J, DING M, et al. Federated learning with differential privacy: Algorithms and performance analysis[J]. IEEE Transactions on Information Forensics and Security, 2020,(15): 3454-3469.

[94] NAOR M, PINKAS B. Efficient oblivious transfer protocols[C]//SODA 2001: Proceedings of the 2001 International Conference of Symposium on Discrete Algorithms. Plaza: SIAM, 2001: 448-457.

[95] KOLESNIKOV V, SCHNEIDER T. Improved garbled circuit: Free XOR gates and applications[C]//ICALP 2008: Proceedings of the 2008 International Colloquium on Automata, Languages, and Programming. Cham: Springer, 2008:486-498.

[96] KARNIN E, GREENE J, HELLMAN M. On secret sharing systems[J]. IEEE Transactions on Information Theory, 1983, 29(1): 35-41.

[97] DE C E, TSUDIK G. Practical private set intersection protocols with linear complexity[C]//FC 2010: Proceedings of the 2010 International Conference on Financial Cryptography and Data Security. Cham: Springer, 2010: 143-159.

[98] DWORK C. Differential privacy: A survey of results[C]//SAT 2008: Proceedings of the 2008 International Conference on Theory and Applications of Models of Computation. Cham: Springer, 2008: 1-19.

[99] NAEHRIG M, LAUTER K, VAIKUNTANATHAN V. Can homomorphic encryption be practical? [C]//CCSW 2011: Proceedings of the 3rd ACM workshop on Cloud computing security workshop. New York: ACM, 2011: 113-124.

[100] RABIN M O. How To Exchange Secrets with Oblivious Transfer[EB/OL]. [2021-10-21]. https://www.iacr.org/museum/rabin-obt/obtrans-eprint187.pdf.

[101] CARTER H, LEVER C, Traynor P. Whitewash: Outsourcing garbled circuit generation for mobile devices[C]//ACSAC 2014:Proceedings of the 30th Annual Computer Security Applications Conference. Louisiana: SWSIS, 2014: 266-275.

[102] BEIMEL A. Secret-sharing schemes: A survey[C]//ICCC 2011: Proceedings of the 2011 International Conference on Coding and Cryptology. Cham: Springer, 2011:11-46.

[103] HUANG Y, EVANS D, Katz J. Private set intersection: Are garbled circuits better than custom protocols?[C]//NDSSS 2012: Proceedings of the 2012 conference of Network and Distributed System Symposium. New York: ACM, 2012:11-14.

[104] DWORK C , ROTH A . The Algorithmic Foundations of Differential Privacy[J]. Foundations and trends in theoretical computer science, 2013, 9(3):211-407..

[105] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//STOC 2009: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009.

[106] LIU Y, FAN T, CHEN T, et al. FATE: An Industrial Grade Platform for Collaborative Learning With Data Protection[J]. Journal of Machine Learning Research, 2021, 22(226): 1-6.

[107] HU Y, ZHOU Y, XIAO J, et al. GFL: A Decentralized Federated Learning Framework Based On Blockchain[EB/OL].[2021-10-21]. https://arxiv.org/pdf/2010.10996v2.

[108] ZHU X, WANG J, HONG Z, et al. Federated learning of unsegmented chinese text recognition model[C]//ICTAI 2019: Proceedings of the 31st International Conference on Tools with Artificial Intelligence. Piscataway: IEEE, 2019: 1341-1345.

[109] ZILLER A, TRASK A, LOPARDO A, et al. PySyft: A Library for Easy Federated Learning[M]//Federated Learning Systems. Springer, Cham, 2021: 111-139.

[110] KOURTELLIS N, KATEVAS K, PERINO D. Flaas: Federated learning as a service[C]//Proceedings of the 1st Workshop on Distributed Machine Learning. New York: ACM, 2020: 7-13.

[111] KHOLOD I, YANAKI E, FOMICHEV D, et al. Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis[J]. Sensors, 2021, 21(1): 167.

[112] LI L, FAN Y, TSE M, et al. A review of applications in federated learning[J]. Computers & Industrial Engineering, 2020,149(5): 106854-106869.

[113] XU J, GLICKSBERG B S, SU C, et al. Federated learning for healthcare informatics[J]. Journal of Healthcare Informatics Research, 2021, 5(1): 1-19.
[114] KANG J, XIONG Z, NIYATO D, et al. Reliable federated learning for mobile networks[J]. IEEE Wireless Communications, 2020, 27(2): 72-80.
[115] NILSSON A, SMITH S, ULM G, et al. A performance evaluation of federated learning algorithms[C]//DIDL 2018: Proceedings of the 2nd Workshop on Distributed Infrastructures for Deep Learning. Rennes: github, 2018: 1-8.
[116] YAO J, ANSARI N. Enhancing federated learning in fog-aided IoT by CPU frequency and wireless power control[J]. IEEE Internet of Things Journal, 2020, 8(5): 3438-3445.
[117] KONEN J , MCMAHAN H B , YU F X , et al. Federated learning: strategies for improving communication efficiency[J]. Computing Research Repository, 2016, 16(10):5492-5502.
[118] KHAN L U, SAAD W, HAN Z, et al. Federated learning for internet of things: recent advances, taxonomy, and open challenges[J]. IEEE Communications Surveys & Tutorials, 2021, 23(3):1759-1799.
[119] CHAMANI J G, PAPADOPOULOS D. Mitigating Leakage in Federated Learning with Trusted Hardware[EB/OL].[2021-10-21]. https://arxiv.org/pdf/2011.04948.

This work is partially supported by the National Science Fund Subsidized Project of China(61672169); the Science Fund Subsidized Project of Guangdong Province(2021A1515012233).

LIANG Tiankai, born in 1993, master degree. His research interests include data mining, artificial intelligence and federated learning.

ZENG Bi, born in 1963, Ph. D., professor. Her research interests include intelligent information processing and intelligent robot.

CHEN Guang, born in 1981, Ph. D., engineer. His research interests include artificial intelligence and federated learning