联合机器学习：概念与应用

QIANG YANG，香港科技大学，香港
杨柳，中国 Webank
陈天健，中国万维网畔
童永新，中国北京航空航天大学

当今的人工智能仍然面临两大挑战。一个是在大多数行业中，数据以孤立岛屿的形式存在。另一个是加强数据隐私和安全。针对这些挑战，我们提出了一种可能的解决方案：安全的联合学习。除了谷歌在2016年首次提出的联合学习框架外，我们还介绍了一个全面的安全联合学习框架，其中包括水平联合学习、垂直联合学习和联合转移学习。我们提供了联合学习框架的定义、架构和应用，并对该主题的现有作品进行了全面调查。此外，我们还提出了基于联合机制在组织间构建数据网络的建议，作为在不损害用户隐私的情况下共享知识的有效解决方案。

CCS 概念：- **安全与隐私**； - **计算方法** → **人工智能**；**机器学习**；*监督学习*；

其他关键词和短语：联合学习、GDPR、迁移学习

ACM 参考格式：

Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong.2019.联合机器学习：概念与应用。*ACM Trans.Intell.Syst.Technol.*10, 2, Article 12 (February 2019), 19 pages. https://doi.org/0000001.0000001

1 引言

2016年是人工智能（AI）时代到来的一年。随着AlphaGo[59] 击败人类顶尖围棋选手，我们真正见证了人工智能（AI）的巨大潜力，并开始期待更复杂、更前沿的人工智能技术在无人驾驶汽车、医疗、金融等诸多领域的应用。如今，人工智能技术几乎在各行各业都大显身手。然而，当我们回顾人工智能的发展历程时，也不可避免地会发现，人工智能的发展经历了几起几落。人工智能会出现下一个低谷吗？什么时候会出现，又是因为什么因素？目前公众对人工智能的兴趣部分是由大数据的可用性推动的：2016年的AlphaGo共使用了30万盘棋作为训练数据，取得了优异的成绩。

随着AlphaGo的成功，人们自然希望像AlphaGo这样以大数据为驱动的人工智能能尽快在我们生活的方方面面实现。然而，现实情况却让人有些失望：除了少数几个行业外，大多数领域都只有有限的数据，或者数据贫乏。

作者地址杨强，香港科技大学，中国香港；电子邮箱：qyang@cse.ust.hk；刘洋，万维网，中国深圳；电子邮箱：yangliu@webank.com；陈天健，万维网，中国深 圳 ； 电 子 邮 箱 ： tobychen@webank.com；童永新（通讯作者），北京航空航天大学大数据与脑计算高级创新中心，中国北京；电子邮箱：yxtong@buaa.edu.cn。

2157-6904/2019/2-art12 $15.00
https://doi.org/0000001.0000001

这些数据的质量参差不齐，使得人工智能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，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。一般来说，任何人工智能项目所需的数据都涉及多种类型。例如，在人工智能驱动的产品推荐服务中，产品销售商拥有产品信息、用户购买数据，但却没有描述用户购买能力和支付习惯的数据。在大多数行业中，数据都是以孤岛的形式存在。由于行业竞争、隐私安全和复杂的管理程序等原因，即使是同一公司不同部门之间的数据整合也面临重重阻力。要整合分散在全国各地和各机构的数据几乎是不可能的，或者成本过高。

与此同时，随着人们对大公司损害数据安全和用户隐私的认识不断提高，对数据隐私和安全的重视已成为世界性的重大问题。有关公共数据泄露的新闻引起了公众媒体和政府的极大关注。例如，Facebook 最近的数据泄露事件就引起了广泛的抗议[70]。为此，世界各国都在加强保护数据安全和隐私的法律。欧盟于 2018 年 5 月 25 日实施的《通用数据保护条例》（GDPR）[19] 就是一个例子。GDPR （图 1）旨在保护用户的个人隐私和数据安全。它要求企业在用户协议中使用清晰、通俗的语言，并赋予用户 "被遗忘权"，即用户可以删除或撤回其个人数据。违反该法案的企业将面临严厉的罚款。美国和中国也在制定类似的隐私和安全法案。例如，中国 2017 年颁布的《网络安全法》和《民法总则》要求，互联网企业不得泄露或篡改其收集的个人信息，在与第三方进行数据交易时，需确保拟签订的合同遵守法定的数据保护义务。这些法规的制定显然将有助于建立一个更加文明的社会，但也将对目前人工智能领域普遍采用的数据交易程序提出新的挑战。

更具体地说，人工智能领域的传统数据处理模式通常涉及简单的数据传输模式，即一方收集数据并传输给另一方，另一方负责清理和融合数据。最后，第三方将利用整合后的数据建立模型，供其他各方使用。模型通常是作为服务出售的最终产品。这种传统程序面临着上述新数据法规和法律的挑战。此外，由于用户可能不清楚模型的未来用途，因此交易违反了 GDPR 等法律。因此，我们面临的困境是，我们的数据以孤岛的形式存在，但在很多情况下，我们却被禁止将数据收集、融合和使用到不同的地方进行人工智能处理。如何从法律上解决数据碎片化和孤立化的问题，是当今人工智能研究人员和从业人员面临的一大挑战。

在本文中，我们将概述一种称为*联合学习的*新方法，它是应对这些挑战的一种可能的解

决方案。我们调查了有关联合学习的现有工作，并提出了一个全面安全的联合学习框架的定义、分类和应用。我们讨论了如何将联合学习框架成功应用于各种业务。在推广联合学习的过程中，我们希望将人工智能开发的重点从提高模型性能（目前人工智能领域的大多数人都在这样做）转移到研究符合数据隐私和安全法律的数据整合方法上。

2 联合学习概述

联合学习的概念是由谷歌最近提出的[36, 37, 41]。他们的主要想法是基于分布在多个设备上的数据集建立机器学习模型，同时防止数据泄露。最近的改进主要集中在克服以下问题上

图 1.GDPR：欧盟数据保护条例

统计挑战[60, 77]和提高联合学习的安全性[9, 23]。还有一些研究致力于使联合学习更加个性化[13, 60]。上述工作都集中在设备上的联合学习，其中涉及分布式移动用户交互，海量分发中的通信成本、不均衡的数据分发和设备可靠性是一些需要优化的主要因素。此外，数据是按用户 Ids 或设备 Ids 分割的，因此在数据空间中是*横向*的。这项工作与保护隐私的机器学习（如文献 [58]）非常相关，因为它也考虑了分散协作学习环境中的数据隐私问题。为了将联合学习的概念扩展到组织间的协作学习场景，我们将最初的 "联合学习 "扩展为所有隐私保护分散协作机器学习技术的一般概念。在 [71] 中，我们初步概述了联合学习和联合转移学习技术。在本文中，我们将进一步研究相关的安全基础，并探讨与其他几个相关领域（如多代理理论和隐私保护数据挖掘）的关系。在本节中，我们对联合学习进行了更全面的定义，其中考虑到了数据分区、安全性和应用。我们还描述了联合学习系统的工作流程和系统架构。

2.1 联合学习的定义

定义 N 个数据所有者 $\{/_1, .../_N\}$，他们都希望通过整合各自的数据 $\{D_1, ...D_N\}$ 来训练一个机器学习模型。传统的方法是将所有数据放在一起，使用 $D = D_1 \cup ... \cup D_N$ 来训练一个模型 k_{SUM}。联合学习系统是一个学习过程，在这个过程中，数据所有者合作训练一个模型 k_{FED}，在这个过程中，任何数据所有者 $/_i$ 不会将其数据 D_i 暴露给他人[1]。此外，k_{FED}，表示为 2_{FED} 的准确性应该非常接近 k_{SUM}，2_{SUM} 的性能。形式上，设 δ 为非负实数。

$$|2_{FED} - 2_{SUM}| < \delta \quad (1)$$

我们就说联合学习算法有 δ - 精度损失。

2.2 联合学习的隐私保护

隐私是联合学习的基本特性之一。这需要安全模型和分析来提供有意义的隐私保证。在本节中，我们将简要回顾和比较联合学习的不同隐私技术，并确定防止间接泄漏的方

法和潜在挑战。

[1] 数据安全的定义在不同情况下可能有所不同，但需要提供有意义的隐私保证。我们将在第 2.3 节中举例说明安全定义

安全多方计算（SMC）。SMC 安全模型自然涉及多方，并在定义明确的模拟框架中提供安全证明，以保证完全零知识，即每一方除了输入和输出外一无所知。零知识是非常理想的，但这种理想特性通常需要复杂的计算协议，而且可能无法高效实现。在某些情况下，如果能提供安全保证，披露部分知识也是可以接受的。以较低的安全要求换取较高的效率，利用 SMC 建立安全模型是可能的[16]。最近，有研究[46]使用 SMC 框架训练具有两个服务器和半诚实假设的机器学习模型。参考文献[33]使用 MPC 协议进行模型训练和验证，而用户不会泄露敏感数据。最先进的 SMC 框架之一是 Sharemind [8]。参考文献 [44] 提出了一个 3PC 模型 [5, 21, 45]，其中有一个诚实的多数，并考虑了半诚实和恶意假设的安全性。这些工作要求参与者的数据在非共谋服务器之间秘密共享。

*差异隐私。*另一种研究使用的技术是差分隐私[18]或 k 匿名性[63] 来保护数据隐私[1, 12, 42, 61]。差分隐私、k-匿名和多样化[3]等方法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。在文献[23]中，作者为联合学习引入了一种差异隐私方法，通过在训练过程中隐藏客户端的贡献来增加对客户端数据的保护。

*同态加密。*同态加密[53]也被采用，通过机器学习过程中加密机制下的参数交换来保护用户数据隐私[24, 26, 48]。与差分隐私保护不同的是，数据和模型本身不会被传输，也不会被对方的数据猜到。因此，原始数据层面泄露的可能性很小。最近的研究采用同态加密技术在云上集中和训练数据[75, 76]。在实践中，加性同态加密[2]被广泛使用，需要对机器学习算法中的非线性函数进行多项式近似评估，从而在准确性和隐私性之间进行权衡[4, 35]。

*2.2.1 间接信息泄露。*联盟学习的先驱作品暴露了中间结果，如随机梯度下降（SGD）等优化算法的参数更新[41, 58]，但没有提供安全保证，当这些梯度与数据结构（如图像像素）一起暴露时，实际上可能会泄露重要的数据信息[51]。研究人员曾考虑过这样一种情况，即联合学习系统中的某个成员恶意攻击其他成员，允许插入后门以学习其他成员的数据。在文献[6]中，作者证明了在联合全局模型中插入隐藏后门的可能性，并提出了一种新的"约束-扩展 "模型中毒方法，以减少数据中毒。在[43]中，研究人员发现了协作式机器学习

系统中的潜在漏洞，即协作学习中各方使用的训练数据容易受到推理攻击。他们表明，敌对参与者可以推断出成员资格以及与训练数据子集相关的属性。在[62]中，作者揭露了与不同方之间梯度交换相关的潜在安全问题，提出了梯度下降方法的安全变体，并证明它可以容忍一定数量的拜占庭工人。

研究人员也开始考虑将区块链作为促进联合学习的平台。在文献[34]中，研究人员考虑了一种区块链联合学习（BlockFL）架构，通过利用区块链交换和验证移动设备的本地学习模型更新。他们考虑了最优区块生成、网络可扩展性和鲁棒性等问题。

2.3 联盟学习的分类

在本节中，我们将讨论如何根据数据的分布特征对联合学习进行分类。

让矩阵 D_i 表示每个数据所有者 i 持有的数据。矩阵的每一行代表一个数据所有者 i *的*数据。样本，每列代表一个特征。同时，有些数据集可能还包含标签数据。我们用 X 表示特征空间，用 Y 表示标签空间，用 I 表示样本 ID 空间。例如，在金融领域，标签可能是用户的信用；在营销领域
标签可能是用户的购买欲望；在教育领域，Y 可能是学生的学位。特征 X、标签 Y 和样本 Ids I 构成了完整的训练数据集（I, X, Y）。数据方的特征空间和样本空间可能不尽相同，我们将联合学习分为以下几类
根据数据在特征和样本 ID 空间中如何在各方之间分配，可分为横向联合学习、纵向联合学习和联合转移学习。图 2 显示了双方场景下的各种联合学习框架。

*2.3.1 水平联合学习。*水平联合学习或基于样本的联合学习是在数据集共享相同特征空间但样本不同的情况下引入的（图 2a）。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。参考文献[58]提出了一种协作式深度学习方案，参与者独立训练，只共享参数更新子集。2017 年，谷歌提出了一种针对安卓手机模型更新的水平联合学习方案[41]。在该框架中，使用安卓手机的单个用户在本地更新模型参数，并将参数上传到安卓云，从而与其他数据所有者共同训练集中模型。文献[9]还介绍了一种安全聚合方案，以保护联合学习框架下聚合用户更新的隐私。参考文献[51]在模型参数聚合中使用了加法同态加密，以提供针对中央服务器的安全性。

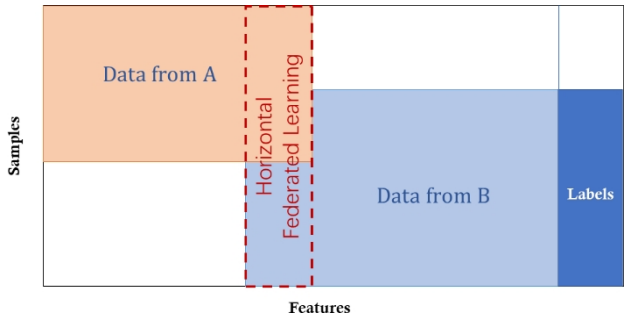
文献[60]提出了一种多任务式联合学习系统，允许多个站点分别完成不同的任务，同时共享知识并保证安全。此外，他们提出的多任务学习模型还能解决高通信成本、散兵游勇和容错问题。在文献[41]中，作者建议建立一种安全的客户端-服务器结构，在这种结构中，联合学习系统按用户划分数据，并允许在客户端设备上建立的模型在服务器站点上协作建立一个全局联合模型。建立模型的过程确保了数据不会泄漏。同样，在 [36] 中，作者提出了改善通信成本的方法，以促进基于分布在移动客户端上的数据的集中模型的训练。最近，一种名为深度梯度压缩的压缩方法[39]被提出来，以大大降低大规模分布式训练中的通

信带宽。

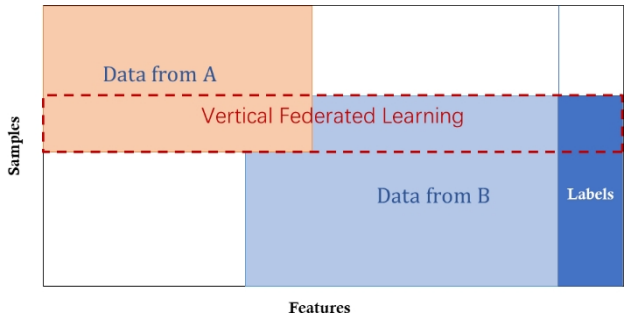
我们将横向联合学习概括为

$$X_i = X_j, Y_i = Y_j, I_i \neq I_j, \forall D_i \ , \ D_j, i \neq j \tag{2}$$

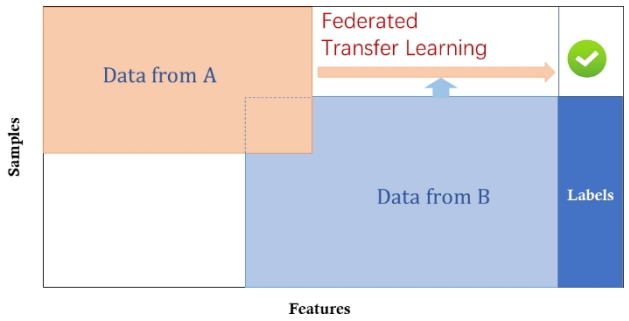
安全性定义。横向联合学习系统通常假定参与者是诚实的，并保证服务器的安全[9, 51]。也就是说，只有服务器可以破坏



(a) 横向联合学习



(b) 垂直联合学习



(c) 联合转移学习

图 2.联合学习的分类

数据参与者的隐私。这些著作都提供了安全证明。最近还提出了另一种考虑到恶意用户的安全模型[29]，提出了额外的隐私挑战。在训练结束时，通用模型和整个模型参数会暴露给所有参与者。

*2.3.2 垂直联合学习。*有人提出了针对垂直分区数据的隐私保护机器学习算法，包括合作统计分析 [15]、关联规则挖掘 [65]、安全线性回归 [22、32、55]、分类 [16] 和梯度下降 [68]。最近，参考文献[27, 49]提出了一种垂直联合学习方案，用于训练保护隐私的逻辑回归模型。作者研究了实体分辨率对学习效果的影响，并对损失函数和梯度函数应用了泰勒近似方法，从而可以采用同态加密进行隐私保护计算。

垂直联合学习或基于特征的联合学习（图 2b）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。在这样的联邦机制下，每个参与方的身份和地位都是一样的，联邦制度帮助大家建立起 "共同富裕 "的策略，这也是这个系统被称为 "联邦学习 " 的原因。因此，在这样的系统中，我们有：

$$\mathrm{X}_i \neq \mathrm{X}_j, \mathrm{Y}_i \neq \mathrm{Y}_j, I_i = I_j \; \forall \mathrm{D}_i, \mathrm{D}_j, i \neq j \tag{3}$$

*安全定义。*垂直联合学习系统通常假定参与者诚实但有好奇心。例如，在双方合作的情况下，双方互不串通，最多有一方被对手破坏。安全定义是，对手只能从被其破坏的客户端获取数据，而不能从另一个客户端获取输入和输出所显示之外的数据。为了促进双方之间的安全计算，有时会引入一个半诚实第三方（STP），在这种情况下，假定 STP 不会与任何一方串通。SMC 为这些协议提供了正式的隐私证明 [25]。在学习结束时，每一方只持有与自己的特征相关联的模型参数，因此在推理时，双方还需要合作生成输出。

*2.3.3 联合迁移学习（FTL）。*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。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[50] 技术，为联盟下的整个样本和特征空间提供解决方案（图 2c）。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。FTL 是对现有联合学习系统的重要扩展，因为它能处理的问题超出了

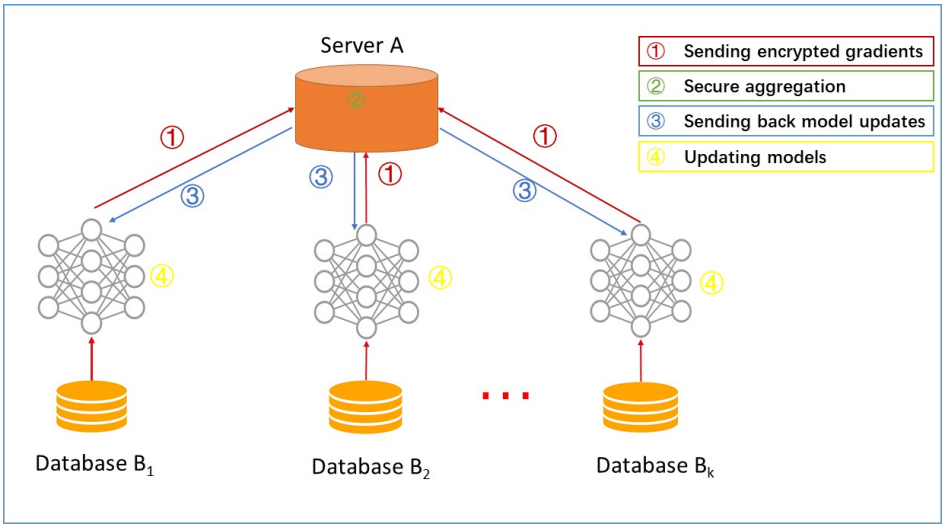


图 3.横向联合学习系统的架构

现有联合学习算法的范围：

$$X_i \neq X_j, Y_i \neq Y_j, I_i \neq I_j \ \forall D_i, D_j, i \neq j \tag{4}$$

*安全定义。*联合转移学习系统通常涉及两方。正如下一节所述，其协议与垂直联合学习中的协议类似，在这种情况下，垂直联合学习的安全定义可以在此扩展。

2.4 联合学习系统的架构

在本节中，我们将举例说明联合学习系统的一般架构。请注意，横向和纵向联合学习系统的架构在设计上有很大不同，我们将分别介绍。

*2.4.1 水平联合学习。*横向联合学习系统的典型架构如图 3 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。一个典型的假设是，参与者是诚实的，而服务器是诚实但好奇的，因此不允许任何参与者向服务器泄漏信息[51]。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[51]、差分隐私[58]或秘密共享[9]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。

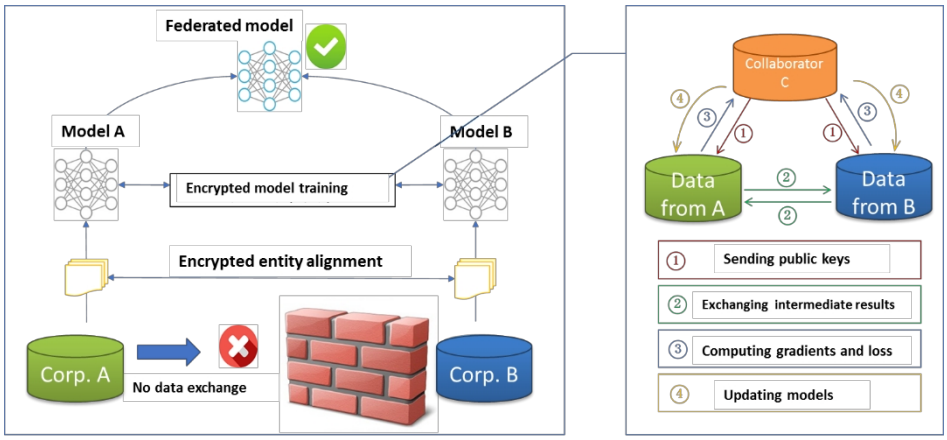


图 4.垂直联合学习系统的架构

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。

*安全分析。*如果使用 SMC [9] 或同态加密 [51]进行梯度聚合，上述架构可以防止半诚实服务器泄漏数据。但在另一种安全模型中，它可能会受到在协作学习过程中训练生成对抗网络（GAN）的恶意参与者的攻击 [29]。

*2.4.2 垂直联合学习。*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。在此，我们假设合作者 C 是诚实的，不会与 A 或 B 串通，但 A 和 B 之间是诚实但相互猜疑的。可信第三方 C 是一个合理的假设，因为 C 可以由政府等权威机构扮演，也可以由英特尔软件防护扩展（SGX）[7] 等安全计算节点替代。联合学习系统由两部分组成，如图 4 所示。

*第 1 部分*加密实体对齐。由于两家公司的用户组并不相同，系统使用基于加密的用户 ID 对齐技术（如 [38, 56] ），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。
  际关系；

- **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。

下面我们以线性回归和同态加密为例说明训练过程。要使用梯度下降法训练线性回归模型，我们需要安全地计算其损失和梯度。假设学习率 η、正则化参数 λ、数据*设置* $\{x_i^A\}_{i\in D_A}, \{x_i^B, y_i\}_{i\in D_B}$，*以及对应于特征空间* x, Θ *的模型参数。*以及与 x^A 的特征空间相对应的模型参数 Θ_A、Θ_B、x_i^B 训练目标分别为

$$\min_{\Theta_A, \Theta_B} \sum_i \left\| \Theta_A x_i^A + \Theta_B x_i^B - y_i \right\|^2 + \frac{\lambda}{2}\left(\|\theta_A\|_A^2 + \|\theta_B\|^2 \right) \quad (5)$$

让 $u_i^A = \Theta_A x_i^A$，$u_i^B = \Theta_B x_i^B$，加密损失为：

$$[[L]] = [[\sum_i ((u_i^A + u_i^B - y_i)^2) + \frac{\lambda}{2}(\|\theta_A\|_A^2 + \|\theta_B\|^2)]] \quad (6)$$

其中加法同态加密表示为[[-]]。设 $[[L_A]] = [[\sum_i ((u_i^A)^2) + \frac{\lambda}{2}\Theta_A^2]]$、$[[L_B]] = [[\sum_i ((u_i^B - y_i)^2) + \frac{\lambda}{2}\Theta_B^2]]$，且 $[[L_{AB}]] = 2\sum_i ([[u_i^A]](u_i^B - y_i))$，那么

$$[[l]] = [[l_A]] + [[L_B]] + [[L_{AB}]] \quad (7)$$

同样，设 $[[d_i]] = [[u_i^A]] + [[u_i^B - y_i]]$，则梯度为：

$$[\frac{\partial L}{\partial \Theta_A}] = \sum_i [[d_i]] x_i^A + [[\lambda \Theta_A]] \quad (8)$$

$$[\frac{\partial L}{\partial \Theta_B}] = \sum_i [[d_i]] x_i^B + [[\lambda \Theta_B]] \quad (9)$$

表 1.垂直联合学习的训练步骤：线性回归

	甲方	乙方	缔约方 C
步骤 1	初始化 Θ_A	初始化 Θ_B	创建一对加密密钥，向 A 和 B 发送公开密钥；
步骤 2	计算 $[[u_i^A]]$、$[[L_A]]$ 并发送给 B；	算 $[[u_i^B]]$、$[[d_i^B]]$、$[[L]]$、向 A 发送 $[[d_i^B]]$，发送 $[[L]]$ 至 C；	
步骤 3	初始化 R_A，计算 $[[\frac{\partial L}{\partial \Theta_A}]] + [[R_A]]$ 并发送至 C；	初始化 R_B，计算 $[[\frac{\partial L}{\partial \Theta_B}]] + [[R_B]]$ 并发送至 C； 更新 Θ_B	C 解密 L，发送 $\frac{\partial L}{\partial \Theta_A} + R_A$ 到 A，$\frac{\partial L}{\partial \Theta_B} + R_B$ 到 B；
步骤 4	更新 Θ_A		

什么是 是什么 获得	Θ_A	Θ_B	

表 2.垂直联合学习的评估步骤：线性回归

	甲方	乙方	审问者 C
步骤 0			向 A 和 B 发送用户 ID i；
步骤 1	计算 u_i^A 并发送给 C	计算 u_i^B 并发送给 C;	得到结果 $u_i^A + u_i^B$；

具体步骤见表 1 和表 2。在实体对齐和模型训练过程中，A 和 B 的数据在本地保存，训练中的数据交互不会导致数据隐私泄露。需要注意的是，潜在的信息泄露给 C 可能会被视为侵犯隐私，也可能不会。在这种情况下，为了进一步防止 C 从 A 或 B 处获取信息，A 和 B 可以通过添加加密的随机掩码来进一步向 C 隐藏自己的梯度。因此，在联合学习的帮助下，双方实现了合作训练一个共同的模型。因为在训练过程中，每一方得到的损失和梯度与他们在没有隐私限制的情况下利用在一个地方收集到的数据共同建立一个模型时得到的损失和梯度完全相同，**也就是说**，这个模型是无损失的。模型的效率取决于加密数据的通信成本和计算成本。在每次迭代中，A 和 B 之间发送的信息随着重叠样本数的增加而增加。因此，采用分布式并行计算技术可以进一步提高该算法的效率。

*安全分析。*表 1 所示的训练协议不会向 C 透露任何信息，因为 C 所学习到的只是掩码梯度，而且掩码矩阵的随机性和保密性是有保证的 [16]。在上述协议中，A 方在每一步都能学习到自己的梯度，但这并不足以让 A 根据等式 8 从 B 处学习到任何信息，因为标量乘法协议的安全性是建立在无法求解 n 个以上未知数的 n 个等式的基础上的 [16, 65]。在此，我们假设样本数 N_A 远大于 n_A，其中 n_A 是特征数。同样，乙方无法从 A.因此，协议的安全性已得到证明。请注意，我们假设双方都是
半诚实。如果一方是恶意的，通过伪造输入来欺骗系统，例如，甲方只提交了一个非零输入，只有一个非零特征，它就可以知道该输入的 u^B 值。
该样本的特征。它仍然无法判断 x^B 或 Θ_i。 $_B$不过，这种偏差会使 i
下一次迭代时，另一方会发出警报，从而终止学习过程。在训练过程结束时，每一方（甲方或乙方）仍然不知道另一方的数据结构，只获得与自己特征相关的模型参数。在推理时，双方需要协同计算预测结果，步骤如表 2 所示，这仍然不会导致信息泄露。

*2.4.3 联合迁移学习。*假设在上述垂直联合学习示例中，甲方和乙方只有很小的重叠样本集，而我们感兴趣的是学习甲方所有数据集的标签。为了将其覆盖范围扩展到整个样本

空间，我们引入了迁移学习。具体来说，迁移学习通常涉及学习甲方和乙方特征之间的共同表示，并通过利用源域方（本例中为乙方）的标签来最小化目标域方预测标签的误差。因此

甲方和乙方的预测结果与垂直联合学习场景中的预测结果不同。在推理时，仍然需要双方计算预测结果。

*2.4.4 激励机制。*为了使不同组织之间的联合学习完全商业化，需要开发一个公平的平台和激励机制[20]。模型建立后，模型的性能将在实际应用中体现出来，这种性能可以记录在永久数据记录机制（如区块链）中。提供更多数据的组织将获得更好的收益，而模型的有效性取决于数据提供者对系统的贡献。这些模式的有效性基于联盟机制分配给各方，并不断激励更多组织加入数据联盟。

上述架构的实现不仅要考虑隐私保护和多个组织间协同建模的有效性，还要考虑如何奖励贡献更多数据的组织，以及如何利用共识机制实施激励。因此，联合学习是一种 "闭环 " 学习机制。

3 相关作品

联盟学习能让多方协作构建机器学习模型，同时保持各自训练数据的私密性。作为一项新技术，联合学习有多条原创性线索，其中一些根植于现有领域。下面，我们将从多个角度解释联合学习与其他相关概念之间的关系。

3.1 保护隐私的机器学习

联盟学习可视为保护隐私的分散协作式机器学习，因此它与多方保护隐私的机器学习密切相关。过去有很多人致力于这一领域的研究。例如，参考文献[17, 67]提出了针对垂直分区数据的安全多方决策树算法。Vaidya 和 Clifton 针对垂直分割数据提出了安全关联挖掘规则[65]、安全 k-means [66]、Naive Bayes 分类器 [64]。参考文献[31]提出了一种水平分割数据关联规则算法。针对垂直分割数据 [73] 和水平分割数据 [74] 开发了安全支持向量机算法。参考文献[16]提出了多方线性回归和分类的安全协议。参考文献 [68] 提出了安全的多方梯度下降方法。上述工作都使用了安全多方计算（SMC）[25, 72]来保证隐私。

Nikolaenko 等人[48] 利用同态加密和 Yao 的乱码电路，在横向分割数据上实现了线性回归的隐私保护协议，参考文献[22, 24]则提出了纵向分割数据的线性回归方法。这些系统直接解决了线性回归问题。参考文献[47]用随机梯度下降法（SGD）解决了这一问题，他们还提出了逻辑回归和神经网络的隐私保护协议。最近，又有人提出了三服务器模型的后续

工作[44]。Aono 等人 [4] 提出了一种使用同态加密的安全逻辑回归协议。Shokri 和 Shmatikov[58]提出了通过交换更新参数来训练横向分割数据的神经网络。参考文献[51]使用加法同态加密来预先保护梯度的隐私并增强系统的安全性。随着深度学习的不断发展，保护隐私的神经网络推理也受到了广泛关注[10, 11, 14, 28, 40, 52, 54]。

3.2 联合学习与分布式机器学习

横向联合学习乍一看与分布式机器学习（Distributed Machine Learning）有些相似。分布式机器学习涉及很多方面，包括训练数据的分布式存储、计算任务的分布式操作、模型结果的分布式分发等。参数服务器 [30] 是分布式机器学习的一个典型元素。作为加速训练过程的工具，参数服务器将数据存储在分布式工作节点上，通过中心调度节点分配数据和计算资源，从而更高效地训练模型。在横向联合学习中，工作节点代表数据所有者。它对本地数据拥有完全的自主权，可以决定何时以及如何加入联合学习。而在参数服务器中，中心节点始终掌握着控制权，因此联合学习面临的学习环境更为复杂。其次，联合学习强调模型训练过程中数据拥有者的数据隐私保护。有效的数据隐私保护措施可以更好地应对未来日益严格的数据隐私和数据安全监管环境。

与分布式机器学习一样，联合学习也需要处理非 IID 数据。文献[77]指出，如果本地数据不具有同源性，联合学习的性能就会大大降低。对此，作者提供了一种类似于迁移学习的新方法来解决这一问题。

3.3 联合学习与边缘计算

联盟学习可视为边缘计算的操作系统，因为它提供了协调和安全的学习协议。在 [69] 中，作者考虑了使用基于梯度下降的方法训练的通用机器学习模型。他们从理论角度分析了分布式梯度下降的收敛边界，并在此基础上提出了一种控制算法，该算法可确定局部更新与全局参数聚合之间的最佳权衡，从而在给定的资源预算下最小化损失函数。

3.4 联合学习与联合数据库系统

联合数据库系统 [57] 是一种集成多个数据库单元并将集成系统作为一个整体进行管理的系统。联盟数据库概念的提出是为了实现多个独立数据库的互操作性。联合数据库系统通常使用分布式存储来存储数据库单元，实际上每个数据库单元中的数据都是异构的。因此，在数据类型和存储方面，它与联合学习有许多相似之处。不过，联合数据库系统在交互过程 中不涉及任何隐私保护机制，所有数据库单元对管理系统都是完全可见的。此外，联合数据库系统的重点在于数据的基本操作，包括插入、删除、搜索、合并等，而联合学习的目的是在保护数据隐私的前提下，为每个数据拥有者建立联合模型，让数据所蕴含的各种价值和规律更好地为我们服务。

4 申请

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。

以智能零售为例。其目的是利用机器学习技术为客户提供个性化服务，主要包括产品推荐和销售服务。智慧零售业务涉及的数据特征主要包括用户购买力、用户个人偏好和产品特征。在实际应用中，这三个数据特征很可能分散在三个不同的部门或企业中。例如，用户的购买力可以从其银行存款中推断出来，用户的个人偏好可以从其社交网络中分析出来，而产品特征则由电子商店记录下来。在这种情况下，我们面临两个问题。首先，为了保护数据隐私和数据安全，银行、社交网站和电子购物网站之间的数据壁垒很难打破。因此，无法直接汇总数据来训练模型。其次，三方存储的数据通常是异构的，传统的机器学习模型无法直接处理异构数据。目前，传统的机器学习方法还不能有效解决这些问题，阻碍了人工智能在更多领域的推广和应用。

联盟学习和迁移学习是解决这些问题的关键。首先，利用联盟学习的特点，我们可以在不输出企业数据的情况下，为三方建立机器学习模型，既充分保护了数据隐私和数据安全，又能为客户提供个性化、有针对性的服务，实现互利共赢。同时，我们可以利用迁移学习来解决数据异构问题，突破传统人工智能技术的局限。因此，联盟学习为我们构建跨企业、跨数据、跨领域的大数据和人工智能生态圈提供了良好的技术支撑。

我们可以使用联合学习框架进行多方数据库查询，而无需暴露数据。例如，假设在金融应用中，我们有兴趣检测多 方 借贷，这一直是银行业的一个主要风险因素。当某些用户恶意从一家银行借款以支付另一家银行的贷款时，就会发生这种情况。多方借贷对金融稳定构成威胁，因为大量此类非法行为可能导致整个金融系统崩溃。为了找到这类用户，而又不在 A 银行和 B 银行之间互相暴露用户列表，我们可以利用联合学习框架。具体来说，我们可以利用联合学习的加密机制，在每一方对用户列表进行加密，然后取加密列表在联盟中的交集。解密后的最终结果就是多方借贷者名单，而不会将其他 "好 "用户暴露给对方。我们将在下文中看到，这一操作与垂直联合学习框架相对应。

智能医疗是另一个领域，我们预计联合学习技术的兴起将使该领域受益匪浅。疾病症状、基因序列、医疗报告等医疗数据非常敏感和私密，但医疗数据难以收集，且存在于孤立的医疗中心和医院中。数据源的不足和标签的缺乏导致机器学习模型的性能不尽如人意，成为当前智慧医疗的 瓶颈。我们设想，如果所有医疗机构联合起来，共享数据，形成一个大型医疗数据集，那么在该大型医疗数据集上训练的机器学习模型的性能将得到显著提高。联合学习与迁移学习相结合是实现这一愿景的主要途径。迁移学习可用于填补缺失的标签，从而扩大可用数据的规模，进一步提高训练模型的性能。因此，联合迁

移学习将在智能医疗的发展中发挥举足轻重的作用，并有可能将人类的医疗保健提升到一个全新的水平。

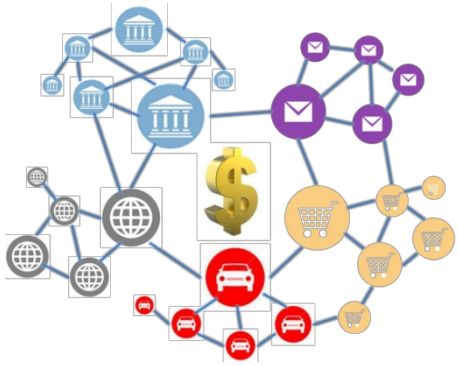


图 5.数据联盟在区块链上分配利益

5 企业联合学习和数据联盟

联盟学习不仅是一种技术标准，也是一种商业模式。当人们意识到大数据的作用时，首先想到的是将数据汇总在一起，通过远程处理器计算模型，然后下载结果供进一步使用。在这种需求下，云计算应运而生。然而，随着数据隐私和数据安全越来越重要，公司利润与数据之间的关系越来越密切，云计算模式受到了挑战。然而，联合学习的商业模式为大数据的应用提供了一种新的范式。当每个机构所占据的孤立数据无法产生理想的模型时，联合学习的机制使得机构和企业无需交换数据就能共享一个统一的模型。此外，联盟学习还可以借助区块链技术的共识机制，制定公平的利益分配规则。数据拥有者无论数据规模大小，都会有动力加入数据联盟，实现自身盈利。我们认为，数据联盟的商业模式和联盟学习的技术机制应该一并建立。我们还将制定各领域的联盟学习标准，使其尽快投入使用。

6 结论与展望

近年来，数据的孤立和对数据隐私的重视正在成为人工智能面临的下一个挑战，但联合学习给我们带来了新的希望。它可以在保护本地数据的同时，建立多企业联合模式，以数据安全为前提，实现企业共赢。本文总体介绍了联盟学习的基本概念、架构和技术，并讨论了其在各种应用中的潜力。预计在不久的将来，联盟学习将打破行业间的壁垒，建立一个数据和知识可以安全共享的社区，并根据每个参与者的贡献公平分配利益。人工智能的红利终将惠及我们生活的每一个角落。

参考文献

[1] Martin Abadi、Andy Chu、Ian Goodfellow、H. Brendan McMahan、Ilya Mironov、Kunal Talwar 和 Li Zhang。

ACM Trans.Intell.Syst.技术》，第 10 卷，第 2 期，第 12 条。出版日期：2019 年 2 月。

2016.具有差异隐私的深度学习。In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*.ACM, New York, NY, USA, 308-318. https://doi.org/10.1145/2976749.2978318

[2] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti.2018.同态加密方案概览》：理论与实施。*ACM Comput.Surv.*51, 4, Article 79 (July 2018), 35 pages. https://doi.org/10.1145/3214303

[3] Rakesh Agrawal 和 Ramakrishnan Srikant。2000.隐私保护数据挖掘》。In *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (SIGMOD '00)*.ACM, New York, NY, USA, 439-450. https://doi.org/10.1145/342009.335438

[4] Yoshinori Aono、Takuya Hayashi、Le Trieu Phong 和 Lihua Wang.2016.通过同态加密实现可扩展的安全逻辑回归。In *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy (CODASPY '16)*.ACM, New York, NY, USA, 142-144. https://doi.org/10.1145/2857705.2857731

[5] Toshinori Araki、Jun Furukawa、Yehuda Lindell、Ariel Nof 和 Kazuma Ohara。2016.具有诚实多数的高吞吐量半诚实安全三方计算》（High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority.In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*.ACM, New York, NY, USA, 805-817. https://doi.org/10.1145/2976749.2978331

[6] Eugene Bagdasaryan、Andreas Veit、Yiqing Hua、Deborah Estrin 和 Vitaly Shmatikov。2018.如何后门 联合学习。arXiv:cs.CR/1807.00459

[7] 拉德-巴马尼、曼努埃尔-巴尔博萨、费迪南德-布拉瑟、贝尔纳多-波尔特拉、艾哈迈德-雷扎-萨德吉、纪尧姆-斯凯里和博格丹-沃林斯基。2017.来自 SGX 的安全多方计算。*金融密码学与数据安全 - 第 21 届国际会议，FC 2017，马耳他斯利马，2017 年 4 月 3-7 日，修订选编论文*。477-497. https://doi.org/10.1007/978-3-319-70972-7_27

[8] Dan Bogdanov、Sven Laur 和 Jan Willemson。2008.Sharemind：快速隐私保护计算框架。*第 13 届欧洲计算机安全研究研讨会论文集：计算机安全（ESORICS '08）*。Springer-Verlag, Berlin, Heidelberg, 192-206. https://doi.org/10.1007/978-3-540-88313-5_13

[9] Keith Bonawitz、Vladimir Ivanov、Ben Kreuter、Antonio Marcedone、H. Brendan McMahan、Sarvar Patel、Daniel Ramage、Aaron Segal 和 Karn Seth。2017.保护隐私的机器学习的实用安全聚合。In *Proceedings 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

[10] Florian Bourse、Michele Minelli、Matthias Minihold 和 Pascal Paillier。2017.深度 离散化神经网络的快速同态评估。*IACR Cryptology ePrint Archive* 2017 (2017)，1114.

[11] Hervé Chabanne、Amaury de Wargny、Jonathan Milgram、Constance Morel 和 Emmanuel Prouff。2017.深度神经网络的隐私保护分类（Preserving Classification on Deep Neural Network）。*IACR Cryptology ePrint Archive* 2017 (2017)，35.

[12] Kamalika Chaudhuri and Claire Monteleoni.2009.隐私保护逻辑回归。*神经信息处理系统进展 21*》，D. Koller、D. Schuurmans、Y. Bengio 和 L. Bottou（编辑）。Curran Associates, Inc., 289-296. http://papers.nips.cc/paper/3486-privacy-preserving-logistic-regression.pdf

[13] 陈飞、董振华、李振国、何秀强。2018.用于推荐的联合元学习。*CoRR* abs/1802.07876 (2018). arXiv:1802.07876 http://arxiv.org/abs/1802.07876

[14] Nathan Dowlin、Ran Gilad-Bachrach、Kim Laine、Kristin Lauter、Michael Naehrig 和 John Wernsing。2016. *CryptoNets: Applying Neural Networks to Encrypted Data with High Through-put and Accuracy*. 技术报告。https://www.microsoft.com/en-us/research/publication/Cryptonets-applying-neural-networks-to-encrypted-data-with-high-throughput-and-accuracy/

[15] W.Du and M. Atallah.2001. 隐私保护合作统计分析》。In *Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC '01)*.IEEE Computer Society, Washington, DC, USA, 102-. http：//dl.acm.org/citation.cfm?id=872016.872181

[16] Wenliang Du, Yunghsiang Sam Han, and Shigang Chen.2004.保护隐私的多元统计分析：线性回归与分类》。在 *SDM*.

[17] Wenliang Du and Zhijun Zhan.2002.在隐私数据上构建决策树分类器》。*电气和电子工程师学会隐私、安全和数据挖掘国际会议论文集-第 14 卷（CRPIT '14）*。澳大利亚计算机协会、Inc., Darlinghurst, Australia, Australia, 1-8. http://dl.acm.org/citation.cfm?id=850782.850784

[18] Cynthia Dwork.2008.Differential Privacy：成果概览》。In *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation (TAMC'08)*. Springer-Verlag, Berlin, Heidelberg, 1-19.Springer-Verlag, Berlin, Heidelberg, 1-19. http：//dl.acm.org/citation.cfm?id=1791834.1791836

[19] 欧盟。2016.欧洲议会和欧盟理事会关于保护关于个人数据处理和此类数据自由流动的第 95/46/EC 号指令，并废除第 95/46/EC 号指令（《一般数据保护条例》）。*见：https://eur-lex. europa. eu/legal-content/EN/TXT* (2016)。

[20] 博伊-法尔廷斯、戈兰-拉达诺维奇、罗纳德-布拉赫曼。2017.*数据科学的博弈论：获取真实信息》*。摩根克莱普尔出版社。

[21] Jun Furukawa、Yehuda Lindell、Ariel Nof 和 Or Weinstein。2016.恶意对手和诚实多数的 高吞吐量安全三方计算。密码学电子图书档案，2016/944 号报告。https://eprint.iacr.

org/2016/944。

[22] Adrià Gascón、Phillipp Schoppmann、Borja Balle、Mariana Raykova、Jack Doerner、Samee Zahur 和 David Evans。2016.垂直分区数据集上的安全线性回归。*IACR Cryptology ePrint Archive* 2016 (2016)，892.

[23] Robin C. Geyer, Tassilo Klein, and Moin Nabi.2017.差异化私人联合学习：客户级视角》。*CoRR* abs/1712.07557 (2017). arXiv:1712.07557 http://arxiv.org/abs/1712.07557

[24] Irene Giacomelli, Somesh Jha, Marc Joye, C. David Page, and Kyonghwan Yoon.2017.仅使用线性同构加密的隐私保护岭回归。Cryptology ePrint Archive, Report 2017/979. https：//eprint.iacr.org/2017/979.

[25] O.Goldreich, S. Micali, and A. Wigderson.1987.How to Play ANY Mental Game.In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC '87)*. ACM, New York, NY, USA, 218-229.ACM, New York, NY, USA, 218-229. https://doi.org/10.1145/28395.28420

[26] Rob Hall、Stephen E. Fienberg 和 Yuval Nardi。2011.基于同态 加密的安全多元线性回归。*官方统计期刊》* 27，4 (2011)，669-691。

[27] 斯蒂芬-哈迪、威尔科-亨内卡、哈米什-伊维-洛、理查德-诺克、乔治-帕特里尼、纪尧姆-史密斯和布莱恩-索恩。2017.通过实体解析和加性同态 加密对垂直分区数据进行私有联合学习。*CoRR* abs/1711.10677 (2017).

[28] Ehsan Hesamifard、Hassan Takabi 和 Mehdi Ghasemi。2017.CryptoDL：加密数据上的深度神经网络。*CoRR* abs/1711.05189 (2017). arXiv:1711.05189 http://arxiv.org/abs/1711.05189

[29] Briland Hitaj、Giuseppe Ateniese 和 Fernando Pérez-Cruz.2017.GAN下的深度模型：协作深度学习的信息泄露。*CoRR* abs/1702.07464 (2017).

[30] Qirong Ho, James Cipar, Henggang Cui, Jin Kyu Kim, Seunghak Lee, Phillip B. Gibbons, Garth A. Gibson, Gregory R. Ganger, and Eric P. Xing.2013.通过陈旧的同步并行参数服务器实现更有效的分布式 ML。*第 26 届神经信息处理系统国际会议论文集 - 第 1 卷（NIPS'13）*。Curran Associates Inc., USA, 1223-1231. http://dl.acm.org/citation.cfm?id=2999611.2999748

[31] Murat Kantarcioglu and Chris Clifton.2004.水平分区数据上关联规则的隐私保护分布式挖掘》。*IEEE Trans. on Knowl.*16, 9 (Sept. 2004), 1026-1037. https://doi.org/10.1109/TKDE.2004.45

[32] Alan F. Karr, X. Sheldon Lin, Ashish P. Sanil, and Jerome P. Reiter.2004.使用安全矩阵产品对垂直 分区数据进行隐私保护分析》。

[33] Niki Kilbertus、Adria Gascon、Matt Kusner、Michael Veale、Krishna Gummadi 和 Adrian Weller。2018.盲目正义：加密敏感属性的公平性。*第 35 届机器学习国际会议论文集》（Proceedings of the 35th International Conference on Machine Learning (Proceedings of Machine Learning Research)）*，Jennifer Dy 和 Andreas Krause（编辑），第 80 卷。PMLR, Stockholmsmässan、瑞典斯德哥尔摩，2630-2639。http://proceedings.mlr.press/v80/kilbertus18a.html

[34] Hyesung Kim、Jihong Park、Mehdi Bennis 和 Seong-Lyun Kim。2018.通过区块链进行的设备上 Federated Learning 及其延迟分析。arXiv:cs.IT/1808.03949

[35] Miran Kim、Yongsoo Song、Shuang Wang、Yuhou Xia 和 Xiaoqian Jiang.2018.基于同态加密的安全逻辑回归：设计与评估.*JMIR Med Inform* 6, 2 (17 Apr 2018), e19. https://doi.org/10.2196/ medinform.8805

[36] Jakub Konecný、H. Brendan McMahan、Daniel Ramage 和 Peter Richtárik。2016.联合优化：面向设备智能的分布式机器学习。*CoRR* abs/1610.02527 (2016). arXiv:1610.02527 http://arxiv.org/abs/1610.02527

[37] Jakub Konecný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave

Bacon.2016.Federated Learning ： 提 高 交 流 效 率 的 策 略 》 。 *CoRR* abs/1610.05492 (2016). arXiv:1610.05492 http://arxiv.org/abs/1610.05492

[38] Gang Liang and Sudarshan S Chawathe.2004.保护隐私的数据库间操作。*情报与安全信息学国际会议*。Springer, 66-82.

[39] Yujun Lin, Song Han, Huizi Mao, Yu Wang, and William J. Dally.2017.深度梯度压缩：降低分布式训练的通信带宽。*CoRR* abs/1712.01887 (2017). arXiv:1712.01887 http：//arxiv.org/abs/1712.01887

[40] Jian Liu, Mika Juuti, Yao Lu, and N. Asokan.2017.通过 MiniONN 变换实现遗忘神经网络预测。In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*.ACM, New York, NY, USA, 619-631. https://doi.org/10.1145/3133956.3134056

[41] H.Brendan McMahan、Eider Moore、Daniel Ramage 和 Blaise Agüera y Arcas。2016.使用模型平均化进行深度网络的联合学习。*CoRR* abs/1602.05629 (2016). arXiv:1602.05629 http://arxiv.org/abs/1602.05629

[42] H.Brendan McMahan、Daniel Ramage、Kunal Talwar 和 Li Zhang。2017.学习差异私有语言模型而不损失准确性。*CoRR* abs/1710.06963 (2017).

[43] 卢卡-梅利斯、宋拥政、埃米利亚诺-德-克里斯托法罗和维塔利-什马蒂科夫。2018.针对协作 rative Learning 的推理攻击。*CoRR* abs/1805.04049 (2018). arXiv:1805.04049 http://arxiv.org/abs/1805.04049

[44] Payman Mohassel 和 Peter Rindal.2018.ABY3：机器学习的混合协议框架。In *Proceedings o f the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*.ACM, New York, NY, USA, 35-52. https://doi.org/10.1145/3243734.3243760

[45] Payman Mohassel、Mike Rosulek 和 Ye Zhang。2015.快速安全的三方计算：乱码电路方法》。*第 22 届 ACM SIGSAC 计算机与通信安全会议（CCS '15）论文集*》。ACM, New York, NY, USA, 591-602. https://doi.org/10.1145/2810103.2813705

[46] Payman Mohassel 和 Yupeng Zhang.2017.SecureML：可扩展的隐私保护机器学习系统。*IEEE 安全与隐私研讨会*。IEEE 计算机协会，19-38。

[47] Payman Mohassel 和 Yupeng Zhang.2017.SecureML：可扩展的隐私保护机器学习系统。*IACR Cryptology ePrint Archive* 2017 (2017)，396。

[48] Valeria Nikolaenko、Udi Weinsberg、Stratis Ioannidis、Marc Joye、Dan Boneh 和 Nina Taft。2013.上亿记录的隐私保护岭回归。2013 *年 IEEE 安全与 隐私研讨会 (SP '13) 论文集*。IEEE 计算机学会，美国华盛顿特区，334-348。https://doi.org/10.1109/SP.2013.30。

[49] 理查德-诺克、斯蒂芬-哈迪、威尔科-亨内卡、哈米什-伊维-劳、乔治-帕特里尼、纪尧姆-史密斯和布莱恩-索恩。2018. 实体解析与联合学习获得联合解析。*CoRR* abs/1803.04035 (2018). arXiv:1803.04035 http://arxiv.org/abs/1803.04035

[50] Sinno Jialin Pan and Qiang Yang.2010. 迁移学习概览》。22, 10 (Oct. 2010), 1345-1359. https://doi.org/10.1109/TKDE.2009.191

[51] Le Trieu Phong、Yoshinori Aono、Takuya Hayashi、Lihua Wang 和 Shiho Moriai。2018.通过加性同态加密保护隐私的深度学习。*IEEE Trans.Information Forensics and Security* 13, 5 (2018), 1333-1345.

[52] M.Sadegh Riazi、Christian Weinert、Oleksandr Tkachenko、Ebrahim M. Songhori、Thomas Schneider 和 Farinaz Koushanfar。2018.变色龙：机器学习应用的混合安全计算框架。*CoRR* abs/1801.03239 (2018).

[53] R L Rivest、L Adleman 和 M L Dertouzos。1978.On Data Banks and Privacy Homomorphisms.*安全 计算基础》，学术出版社*（1978 年），169-179。

[54] Bita Darvish Rouhani、M. Sadegh Riazi 和 Farinaz Koushanfar。2017.DeepSecure：可扩展的可证明安全的深度学习。*CoRR* abs/1705.08963 (2017). arXiv:1705.08963 http://arxiv.org/abs/1705.08963

[55] Ashish P. Sanil, Alan F. Karr, Xiaodong Lin, and Jerome P. Reiter.2004.通过分布式计算进行隐私保护回归建模。In *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '04)*. ACM, New York NY, 2009.ACM, New York, NY, USA, 677-682. https://doi.org/10.1145/1014052.1014139

[56] Monica Scannapieco、Ilya Figotin、Elisa Bertino 和 Ahmed K. Elmagarmid。2007.隐私保护模式与数据匹配》。*2007 年 ACM SIGMOD 数据管理国际会议论文集（SIGMOD '07）*。ACM, New York, NY, USA, 653-664. https://doi.org/10.1145/1247480.1247553

[57] Amit P. Sheth and James A. Larson.1990.用于管理分布式、异构和 自主数据库的联合数据库系统》（Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases.*ACM Comput.Surv.*22, 3 (Sept. 1990), 183-236. https://doi.org/10.1145/96602.96604

[58] Reza Shokri 和 Vitaly Shmatikov.2015.隐私保护深度学习》。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

[59] 戴维-西尔弗、黄雅、克里斯托弗-J-麦迪逊、阿瑟-格兹、洛朗-西弗尔、乔治-范登-德里舍、 朱利安- 施里特威瑟、伊万尼斯-安东诺格鲁、维达-潘内谢尔万、马克-兰克托、桑德尔-迪埃勒曼、多米尼克-格雷维、约翰-纳 姆 、 纳尔-卡尔奇布伦纳、伊利亚-苏茨克沃尔、蒂莫西-利利克拉普、马德琳-利奇、科雷-卡武库奥卢、托雷-格拉佩尔和德米斯-哈萨比斯。2016.用深度神经网络和树搜索掌握围棋。*自然》* 529 (2016), 484-503. http://www.nature.com/nature/journal/v529/n7587/full/nature16961.html

[60] Virginia Smith、Chao-Kai Chiang、Maziar Sanjabi 和 Ameet S Talwalkar。2017.联合多任务学习》。In *Advances in Neural Information Processing Systems 30*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett (Eds.).Curran Associates, Inc., 4424-4434. http://papers.nips.cc/paper/7029-federated-multi-task-learning.pdf

[61] Shuang Song, Kamalika Chaudhuri, and Anand D. Sarwate.2013.随机梯度下降与差异化私有 更新。*2013 IEEE 信号与信息处理全球会议*（2013），245-248。

[62] Lili Su and Jiaming Xu.2018.确保高维度分布式机器学习的安全。*CoRR* abs/1804.10140 (2018). arXiv:1804.10140 http://arxiv.org/abs/1804.10140

[63] Latanya Sweeney.2002.K-anonymity：保护隐私的模式》。*Int. J. Uncertain.J. Uncertain.Fuzziness Knowl.-Based Syst.* 10, 5 (Oct. 2002), 557-570. https://doi.org/10.1142/S0218488502001648

[64] Jaideep Vaidya 和 Chris Clifton.[n.d.]。针对垂直分区数据的隐私保护 Naive Bayes 分类器。在 *第四届 SIAM 数据挖掘会议论文集》，2004 年*。330-334.

[65] Jaideep Vaidya and Chris Clifton.2002.垂直分区数据中的隐私保护关联规则挖掘。在 *第八届 ACM SIGKDD 知识发现与数据挖掘国际会议 (KDD '02) 论文集*。ACM, New York, NY, USA, 639-644. https://doi.org/10.1145/775047.775142

[66] Jaideep Vaidya and Chris Clifton.2003.垂直分区数据上的隐私保护 K 均值聚类。在 *第九届 ACM SIGKDD 知识发现与数据挖掘国际会议 (KDD '03) 论文集*。ACM, New York, NY, USA, 206-215. https://doi.org/10.1145/956750.956776

[67] Jaideep Vaidya and Chris Clifton.2005.垂直分区数据上的隐私保护决策树》。In *Data and Applications Security XIX*, Sushil Jajodia and Duminda Wijesekera (Eds.).Springer Berlin Heidelberg, Berlin, Heidelberg, 139-152.

[68] Li Wan, Wee Keong Ng, Shuguo Han, and Vincent C. S. Lee.2007.梯度下降方法的隐私保护。*第 13 届 ACM SIGKDD 知识发现与数据挖掘国际会议（KDD '07）论文集*。ACM, New York, NY, USA, 775-783. https://doi.org/10.1145/1281192.1281275

[69] Shiqiang Wang, Tiffany Tuor, Theodoros Salonidis, Kin K. Leung, Christian Makaya, Ting He, and Kevin Chan.2018.当边缘遇到学习：资源受限分布式机器学习的自适应控制。*CoRR* abs/1804.05271 (2018). arXiv:1804.05271 http://arxiv.org/abs/1804.05271

[70] 维基百科。2018. https://en.wikipedia.org/wiki/Facebook-Cambridge_Analytica_data_scandal.

[71] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong.2018.Federated Learning.*CCF Communications* 14, 11 (2018), 49-55.

[72] Andrew C. Yao.1982.安全计算协议》。In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS '82)*.IEEE 计算机学会，美国华盛顿特区，160-164。http://dl.acm.org/citation.cfm?id=1382436.1382751

[73] Hwanjo Yu, Xiaoqian Jiang, and Jaideep Vaidya.2006.在水平分割数据上使用非线性核的隐私保护 SVM。2006 *年 ACM 应用计算研讨会（SAC '06）论文集》*。ACM, New York, NY、美国，603-610。https://doi.org/10.1145/1141277.1141415

[74] Hwanjo Yu, Jaideep Vaidya, and Xiaoqian Jiang.2006.垂直分区数据上的隐私保护 SVM 分类。*第 10 届太平洋-亚洲知识发现与数据挖掘进展会议（PAKDD'06）论文集*》。Springer-Verlag, Berlin, Heidelberg, 647-656. https://doi.org/10.1007/11731139_74

[75] Jiawei Yuan and Shucheng Yu.2014.利用云计算实现隐私保护的反向传播神经网络学习。*IEEE Trans.Parallel Distrib.Syst.*25, 1 (Jan. 2014), 212-221. https://doi.org/10.1109/TPDS.2013.18

[76] Qingchen Zhang, Laurence T. Yang, and Zhikui Chen.2016.用于大数据特征学习的云上隐私保护深度计算模型。*IEEE Trans.Comput.*65, 5 (May 2016), 1351-1362. https://doi.org/10.1109/TC.2015.2470255

[77] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, and Vikas Chandra.2018.非 IID 数据的联合学习。arXiv:cs.LG/1806.00582