Federated Machine Learning: Concept and Applications

QIANG YANG, Hong Kong University of Science and Technology, Hong Kong
YANG LIU, Webank, China
TIANJIAN CHEN, Webank, China
YONGXIN TONG, Beihang University, China

Today's AI still faces two major challenges. One is that in most industries, data exists in the form of isolated islands. The other is the strengthening of data privacy and security. We propose a possible solution to these challenges: secure federated learning. Beyond the federated learning framework first proposed by Google in 2016, we introduce a comprehensive secure federated learning framework, which includes horizontal federated learning, vertical federated learning and federated transfer learning. We provide definitions, architectures and applications for the federated learning framework, and provide a comprehensive survey of existing works on this subject. In addition, we propose building data networks among organizations based on federated mechanisms as an effective solution to allow knowledge to be shared without compromising user privacy.

CCS Concepts: • **Security and privacy**; • **Computing methodologies** → **Artificial intelligence**; **Machine learning**; *Supervised learning*;

Additional Key Words and Phrases: federated learning, GDPR, transfer learning

ACM Reference Format:
Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated Machine Learning: Concept and Applications. *ACM Trans. Intell. Syst. Technol.* 10, 2, Article 12 (February 2019), 19 pages. https://doi.org/0000001.0000001

1 INTRODUCTION

2016 is the year when artificial intelligence (AI) came of age. With AlphaGo[59] defeating the top human Go players, we have truly witnessed the huge potential in artificial intelligence (AI), and have began to expect more complex, cutting-edge AI technology in many applications, including driverless cars, medical care, finance, etc. Today, AI technology is showing its strengths in almost every industry and walks of life. However, when we look back at the development of AI, it is inevitable that the development of AI has experienced several ups and downs. Will there be a next down turn for AI? When will it appear and because of what factors? The current public interest in AI is partly driven by Big Data availability: AlphaGo in 2016 used a total of 300,000 games as training data to achieve the excellent results.

With AlphaGo's success, people naturally hope that the big data-driven AI like AlphaGo will be realized soon in all aspects of our lives. However, the real world situations are somewhat disappointing: with the exception of few industries, most fields have only limited data or poor

Authors' addresses: Qiang Yang, Hong Kong University of Science and Technology, Hong Kong, China; email: qyang@cse.ust.hk; Yang Liu, Webank, Shenzhen, China; email: yangliu@webank.com; Tianjian Chen, Webank, Shenzhen, China; email: tobychen@webank.com; Yongxin Tong (corresponding author), Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China; email: yxtong@buaa.edu.cn.

2157-6904/2019/2-ART12 $15.00
https://doi.org/0000001.0000001

联邦机器学习：概念与应用

杨强，香港科技大学，香港刘洋，微众银行，中国

TIANJIAN CHEN，微众银行，中国
中国北京航空航天大学童永新

今天的AI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。二是加强数据隐私和安全。我们提出了一个可能的解决方案来应对这些挑战：安全的联邦学习。除了Google 在2016 年首次提出的联邦学习框架之外，我们还介绍了一个全面的安全联邦学习框架，包括水平联邦学习，垂直联邦学习和联邦迁移学习。我们提供了联邦学习框架的定义，架构和应用程序，并提供了一个全面的调查现有的工作在这个问题上。此外，我们建议建立基于联合机制的组织之间的数据网络作为一个有效的解决方案，让知识共享，而不损害用户隐私。

CCS概念：·安全和隐私; ·计算方法→人工智能;机器学习;监督学习;

其他关键词和短语：联邦学习，GDPR，迁移学习

ACM参考格式：
杨强，刘扬，陈天健，童永新。2019 .联邦机器学习：概念与应用美国计算机学会翻译中心系统技术10，2，第12条（2019 年2月），19 页。https ://doi .org /0000001.0000001

12

1引言

2016 年是人工智能（AI）成熟的一年。随着AlphaGo [59]击败人类顶级围棋选手，我们真正见证了人工智能（AI）的巨大潜力，并开始期待更多复杂、前沿的AI技术在许多应用中的应用，包括无人驾驶汽车、医疗、金融等。然而，当我们回顾AI的发展时，难免会发现AI的发展经历了几次大起大唐斯。AI会有下一个下降趋势吗？什么时候会出现，又是出于什么因素？目前公众对人工智能的兴趣部分是由大数据驱动的：AlphaGo 在2016 年使用了总共30 万场比赛作为训练数据，以取得优异的成绩。

随着AlphaGo 的成功，人们自然希望像AlphaGo 这样的大数据驱动的AI能够很快在我们生活的各个方面实现。然而，真实的世界情况却有些令人失望：除了少数行业外，大多数领域的数据都很有限或很差

作者tobychen @webank .com yangliu @webank .com qyang @cse .ust .hk

quality data, making the realization of AI technology more difficult than we thought. Would it be possible to fuse the data together in a common site, by transporting the data across organizations? In fact, it is very difficult, if not impossible, in many situations to break the barriers between data sources. In general, the data required in any AI project involves multiple types. For example, in an AI-driven product recommendation service, the product seller has information about the product, data of the user's purchase, but not the data that describe user's purchasing ability and payment habits. In most industries, data exists in the form of isolated islands. Due to industry competition, privacy security, and complicated administrative procedures, even data integration between different departments of the same company faces heavy resistance. It is almost impossible to integrate the data scattered around the country and institutions, or the cost is prohibited.

At the same time, with the increasing awareness of large companies compromising on data security and user privacy, the emphasis on data privacy and security has become a worldwide major issue. News about leaks on public data are causing great concerns in public media and governments. For example, the recent data breach by Facebook has caused a wide range of protests [70]. In response, states across the world are strengthening laws in protection of data security and privacy. An example is the General Data Protection Regulation (GDPR)[19] enforced by the European Union on May 25, 2018. GDPR (Figure 1) aims to protect users' personal privacy and data security. It requires businesses to use clear and plain languages for their user agreement and grants users the "right to be forgotten", that is, users can have their personal data deleted or withdrawn. Companies violating the bill will face stiff fine. Similar acts of privacy and security are being enacted in the US and China. For example, China's Cyber Security Law and the General Principles of the Civil Law, enacted in 2017, require that Internet businesses must not leak or tamper with the personal information that they collect and that, when conducting data transactions with third parties, they need to ensure that the proposed contract follow legal data protection obligations. The establishment of these regulations will clearly help build a more civil society, but will also pose new challenges to the data transaction procedures commonly used today in AI.

To be more specific, traditional data processing models in AI often involves simple data transactions models, with one party collecting and transferring data to another party, and this other party will be responsible for cleaning and fusing the data. Finally a third party will take the integrated data and build models for still other parties to use. The models are usually the final products that are sold as a service. This traditional procedure face challenges with the above new data regulations and laws. As well, since users may be unclear about the future uses of the models, the transactions violate laws such as the GDPR. As a result, we face a dilemma that our data is in the form of isolated islands, but we are forbidden in many situations to collect, fuse and use the data to different places for AI processing. How to legally solve the problem of data fragmentation and isolation is a major challenge for AI researchers and practitioners today.

In this article, we give an overview of a new approach known as *federated learning*, which is a possible solution for these challenges. We survey existing works on federated learning, and propose definitions, categorizations and applications for a comprehensive secure federated learning framework. We discuss how the federated learning framework can be applied to various businesses successfully. In promoting federated learning, we hope to shift the focus of AI development from improving model performance, which is what most of the AI field is currently doing, to investigating methods for data integration that is compliant with data privacy and security laws.

2 AN OVERVIEW OF FEDERATED LEARNING

The concept of federated learning is proposed by Google recently [36, 37, 41]. Their main idea is to build machine learning models based on data sets that are distributed across multiple devices while preventing data leakage. Recent improvements have been focusing on overcoming the

高质量的数据，使得AI技术的实现比我们想象的要困难。是否有可能通过跨组织传输数据，将数据融合在一个公共站点中？事实上，在许多情况下，打破数据源之间的障碍是非常困难的，如果不是不可能的话。一般来说，任何AI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，产品销售者拥有产品的信息，用户购买的数据，但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，数据以孤岛的形式存在。由于行业竞争、隐私安全和复杂的行政程序，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。几乎不可能整合分散在全国各地和机构的数据，或者成本被禁止。

与此同时，随着大公司对数据安全和用户隐私的妥协意识越来越强，对数据隐私和安全的重视已成为全球性的重大问题。有关公共数据泄露的新闻引起了公共媒体和政府的极大关注。例如，Facebook 最近的数据泄露事件引起了广泛的抗议[70]。作为回应，世界各国正在加强保护数据安全和隐私的法律。一个例子是欧盟于2018 年5月25 日实施的通用数据保护条例（GDPR ）[19]。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明了的语言，并赠款用户“被遗忘权”，即用户可以删除或撤回其个人数据。违反该法案的公司将面临严厉的罚款。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《民法通则》要求互联网企业不得泄露或篡改其收集的个人信息，并且在与第三方进行数据交易时，他们需要确保拟议合同遵循法律的数据保护义务。这些法规的建立显然有助于建立一个更加公民的社会，但也将对人工智能中目前常用的数据交易程序提出新的挑战。

更具体地说，人工智能中的传统数据处理模型通常涉及简单的数据交易模型，一方收集数据并将数据传输给另一方，另一方将负责清理和融合数据。最后，第三方将获得整合后的数据，并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。这一传统程序面临上述新数据法规和法律的挑战。此外，由于用户可能不清楚这些模型的未来用途，因此这些交易违反了GDPR 等法律。因此，我们面临着一个困境，我们的数据是孤岛的形式，但我们在许多情况下被禁止收集，融合和使用数据到不同的地方进行人工智能处理。如何合法地解决数据碎片化和隔离问题，是当今人工智能研究者和从业者面临的重大挑战。

在本文中，我们给予一个新的方法称为联邦学习，这是一个可能的解决方案，这些挑战的概述。我们调查现有的工作，联邦学习，并提出了一个全面的安全的联邦学习框架的定义，分类和应用。我们将讨论如何将联邦学习框架成功应用于各种业务。在促进联邦学习的过程中，我们希望将人工智能开发的重点从提高模型性能（这是大多数人工智能领域目前正在做的事情）转移到研究符合数据隐私和安全法律的数据集成方法。

第二章联邦学习概述

联邦学习的概念是由Google 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构建机器学习模型，同时防止数据泄露。最近的改进一直集中在克服

Fig. 1. GDPR: EU regulation on data protection

statistical challenges [60, 77] and improving security [9, 23] in federated learning. There are also research efforts to make federated learning more personalizable [13, 60]. The above works all focus on on-device federated learning where distributed mobile user interactions are involved and communication cost in massive distribution, unbalanced data distribution and device reliability are some of the major factors for optimization. In addition, data are partitioned by user Ids or device Ids, therefore, *horizontally* in the data space. This line of work is very related to privacy-preserving machine learning such as [58] because it also considers data privacy in a decentralized collaborative learning setting. To extend the concept of federated learning to cover collaborative learning scenarios among organizations, we extend the original "federated learning" to a general concept for all privacy-preserving decentralized collaborative machine learning techniques. In [71], we have given a preliminary overview of the federated learning and federated transfer learning technique. In this article, we further survey the relevant security foundations and explore the relationship with several other related areas, such as multiagent theory and privacy-preserving data mining. In this section, we provide a more comprehensive definition of federated learning which considers data partitions, security and applications. We also describe a workflow and system architecture for the federated learning system.

2.1 Definition of Federated Learning

Define N data owners $\{\mathcal{F}_1, ...\mathcal{F}_N\}$, all of whom wish to train a machine learning model by consolidating their respective data $\{\mathcal{D}_1, ...\mathcal{D}_N\}$. A conventional method is to put all data together and use $\mathcal{D} = \mathcal{D}_1 \cup ... \cup \mathcal{D}_N$ to train a model $\mathcal{M}_{SUM}$. A federated learning system is a learning process in which the data owners collaboratively train a model $\mathcal{M}_{FED}$, in which process any data owner $\mathcal{F}_i$ does not expose its data $\mathcal{D}_i$ to others [1]. In addition, the accuracy of $\mathcal{M}_{FED}$, denoted as $\mathcal{V}_{FED}$ should be very close to the performance of $\mathcal{M}_{SUM}$, $\mathcal{V}_{SUM}$. Formally, let δ be a non-negative real number, if

$$| \mathcal{V}_{FED} - \mathcal{V}_{SUM} | < \delta \tag{1}$$

we say the federated learning algorithm has δ-accuracy loss.

2.2 Privacy of Federated Learning

Privacy is one of the essential properties of federated learning. This requires security models and analysis to provide meaningful privacy guarantees. In this section, we briefly review and compare different privacy techniques for federated learning, and identify approaches and potential challenges for preventing indirect leakage.

[1]Definition of data security may differ in different scenarios, but is required to provide meaning privacy guarantees. We demonstrate examples of security definitions in section 2.3

Fig. 1. GDPR： 欧盟数据保护法规

统计挑战[60，77]和提高联合学习的安全性[9，23]。也有研究努力使联邦学习更加个性化[13，60]。上述工作都集中在设备上的联邦学习，其中涉及分布式移动的用户交互，大规模分布中的通信成本，不平衡的数据分布和设备可靠性是优化的一些主要因素。此外，数据通过用户ID或设备ID在数据空间中水平地划分。这一领域的工作与隐私保护机器学习（如[58]）非常相关，因为它也考虑了去中心化协作学习环境中的数据隐私。为了扩展联邦学习的概念以覆盖组织之间的协作学习场景，我们将原始的“联邦学习”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，我们对联邦学习和联邦迁移学习技术进行了初步概述。在这篇文章中，我们进一步调查相关的安全基础，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，我们提供了一个更全面的联邦学习定义，其中考虑了数据分区，安全性和应用程序。我们还描述了联邦学习系统的工作流程和系统架构。

2.1 Federated Learning的定义

定义N个数据所有者{F，. F}，所有这些人都希望通过合并他们各自的数据{D，. D}。传统的方法是将所有数据放在一起，并使用D = D...训练一个模型M.联邦学习系统是一个学习过程，其中数据所有者协作训练模型M，在该过程中，任何数据所有者F都不会将其数据D暴露给其他人。此外，M的精度，记为V，应该非常接近M的性能，V。形式上，设δ是非负的真实的数，如果

| V− V| < δ（1）我们说联邦学习算法有δ -精度损失。

2.2 联邦学习的隐私

隐私是联邦学习的基本属性之一。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，我们简要回顾和比较了用于联邦学习的不同隐私技术，并确定了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的场景中可能会有所不同，但需要提供有意义的隐私保证。我们在2.3 节中演示了安全定义的示例

Secure Multi-party Computation (SMC). SMC security models naturally involve multiple parties, and provide security proof in a well-defined simulation framework to guarantee complete zero knowledge, that is, each party knows nothing except its input and output. Zero knowledge is very desirable, but this desired property usually requires complicated computation protocols and may not be achieved efficiently. In certain scenarios, partial knowledge disclosure may be considered acceptable if security guarantees are provided. It is possible to build a security model with SMC under lower security requirement in exchange for efficiency [16]. Recently, studies [46] used SMC framework for training machine learning models with two servers and semi-honest assumptions. Ref [33] uses MPC protocols for model training and verification without users revealing sensitive data. One of the state-of-the-art SMC framework is Sharemind [8]. Ref [44] proposed a 3PC model [5, 21, 45] with an honest majority and consider security in both semi-honest and malicious assumptions. These works require participants' data to be secretly-shared among non-colluding servers.

Differential Privacy. Another line of work use techniques Differential Privacy [18] or k-Anonymity [63] for data privacy protection [1, 12, 42, 61]. The methods of differential privacy, k-anonymity, and diversification [3] involve in adding noise to the data, or using generalization methods to obscure certain sensitive attributes until the third party cannot distinguish the individual, thereby making the data impossible to be restore to protect user privacy. However, the root of these methods still require that the data are transmitted elsewhere and these work usually involve a trade-off between accuracy and privacy. In [23], authors introduced a differential privacy approach to federated learning in order to add protection to client-side data by hiding client's contributions during training.

Homomorphic Encryption. Homomorphic Encryption [53] is also adopted to protect user data privacy through parameter exchange under the encryption mechanism during machine learning [24, 26, 48]. Unlike differential privacy protection, the data and the model itself are not transmitted, nor can they be guessed by the other party's data. Therefore, there is little possibility of leakage at the raw data level. Recent works adopted homomorphic encryption for centralizing and training data on cloud [75, 76]. In practice, Additively Homomorphic Encryption [2] are widely used and polynomial approximations need to be made to evaluate non-linear functions in machine learn algorithms, resulting in the trade-offs between accuracy and privacy [4, 35].

2.2.1 Indirect information leakage. Pioneer works of federated learning exposes intermediate results such as parameter updates from an optimization algorithm like Stochastic Gradient Descent (SGD) [41, 58], however no security guarantee is provided and the leakage of these gradients may actually leak important data information [51] when exposed together with data structure such as in the case of image pixels. Researchers have considered the situation when one of the members of a federated learning system maliciously attacks others by allowing a backdoor to be inserted to learn others' data. In [6], the authors demonstrate that it is possible to insert hidden backdoors into a joint global model and propose a new "constrain-and-scale" model-poisoning methodology to reduce the data poisoning. In [43], researchers identified potential loopholes in collaborative machine learning systems, where the training data used by different parties in collaborative learning is vulnerable to inference attacks. They showed that an adversarial participant can infer membership as well as properties associated with a subset of the training data. They also discussed possible defenses against these attacks.In [62], authors expose a potential security issue associated with gradient exchanges between different parties, and propose a secured variant of the gradient descent method and show that it tolerates up to a constant fraction of Byzantine workers.

安全多方计算（SMC ）。SMC 安全模型自然涉及多方，并在一个定义良好的仿真框架中提供安全证明，以保证完全零知识，即各方除了输入和输出之外什么都不知道。零知识是非常理想的，但这种理想的属性通常需要复杂的计算协议，可能无法有效地实现。在某些情况下，如果提供了安全保证，部分知识披露可能被认为是可以接受的。可以在较低的安全需求下使用SMC 构建安全模型，以换取效率[16]。最近，研究[46]使用SMC 框架来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]，其中大多数是诚实的，并在半诚实和恶意假设中考虑安全性。这些作品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。另一项工作使用差分隐私[18]或k-匿名[63]技术来保护数据隐私[1，12，42，61]。差分隐私、k-匿名和多样化的方法[3]涉及在数据中添加噪声，或使用泛化方法来掩盖某些敏感属性，直到第三方无法区分个体，从而使数据无法恢复以保护用户隐私。然而，这些方法的根源仍然需要将数据传输到其他地方，这些工作通常涉及准确性和隐私性之间的权衡。在[23]中，作者介绍了一种用于联邦学习的差分隐私方法，以便通过在训练期间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]也被用于在机器学习期间通过加密机制下的参数交换来保护用户数据隐私[24，26，48]。与差异隐私保护不同，数据和模型本身是不传输的，也不能被对方的数据猜到。因此，在原始数据层面泄露的可能性很小。最近的工作采用同态加密来集中和训练云上的数据[7 5，7 6]。在实践中，加性同态加密[2]被广泛使用，并且需要进行多项式近似来评估机器学习算法中的非线性函数，从而导致准确性和隐私性之间的权衡[4，35]。

2.2.1 间接信息泄露。联邦学习的先驱工作公开了中间结果，例如来自随机梯度下降（SGD ）[4 1，5 8]等优化算法的参数更新，但是没有提供安全保证，并且当与数据结构一起暴露时，这些梯度的泄漏实际上可能会泄漏重要的数据信息[51]，例如在图像像素的情况下。研究人员考虑了联邦学习系统的一个成员通过允许插入后门来学习其他人的数据来恶意攻击其他人的情况。在[6]中，作者证明了可以将隐藏的后门插入到联合全局模型中，并提出了一种新的“约束和缩放”模型中毒方法来减少数据中毒。 在[43]中，研究人员发现了协作机器学习系统中的潜在漏洞，其中协作学习中不同方使用的训练数据容易受到推理攻击。他们表明，对抗性参与者可以推断成员资格以及与训练数据子集相关的属性。在[62]中，作者揭示了与不同方之间的梯度交换相关的潜在安全问题，并提出了梯度下降方法的安全变体，并表明它可以容忍恒定比例的拜占庭工人。

Researchers have also started to consider blockchain as a platform for facilitating federated learning. In [34], researchers have considered a block-chained federated learning (BlockFL) architecture, where mobile devices' local learning model updates are exchanged and verified by leveraging blockchain. They have considered an optimal block generation, network scalability and robustness issues.

2.3 A Categorization of Federated Learning

In this section we discuss how to categorize federated learning based on the distribution characteristics of the data.

Let matrix $\mathcal{D}_i$ denotes the data held by each data owner i. Each row of the matrix represents a sample, and each column represents a feature. At the same time, some data sets may also contain label data. We denote the features space as $\mathcal{X}$, the label space as $\mathcal{Y}$ and we use $\mathcal{I}$ to denote the sample ID space. For example, in the financial field labels may be users' credit; in the marketing field labels may be the user's purchase desire; in the education field, $\mathcal{Y}$ may be the degree of the students. The feature $\mathcal{X}$, label $\mathcal{Y}$ and sample Ids $\mathcal{I}$ constitutes the complete training dataset $(\mathcal{I}, \mathcal{X}, \mathcal{Y})$. The feature and sample space of the data parties may not be identical, and we classify federated learning into horizontally federated learning, vertically federated learning and federated transfer learning based on how data is distributed among various parties in the feature and sample ID space. Figure 2 shows the various federated learning frameworks for a two-party scenario .

2.3.1 Horizontal Federated Learning. Horizontal federated learning, or sample-based federated learning, is introduced in the scenarios that data sets share the same feature space but different in samples (Figure 2a). For example, two regional banks may have very different user groups from their respective regions, and the intersection set of their users is very small. However, their business is very similar, so the feature spaces are the same. Ref [58] proposed a collaboratively deep learning scheme where participants train independently and share only subsets of updates of parameters. In 2017, Google proposed a horizontal federated learning solution for Android phone model updates [41]. In that framework, a single user using an Android phone updates the model parameters locally and uploads the parameters to the Android cloud, thus jointly training the centralized model together with other data owners. A secure aggregation scheme to protect the privacy of aggregated user updates under their federated learning framework is also introduced [9]. Ref [51] uses additively homomorphic encryption for model paramter aggregation to provide security against the central server.

In [60], a multi-task style federated learning system is proposed to allow multiple sites to complete separate tasks, while sharing knowledge and preserving security. Their proposed multi-task learning model can in addition address high communication costs, stragglers, and fault tolerance issues. In [41], the authors proposed to build a secure client-server structure where the federated learning system partitions data by users, and allow models built at client devices to collaborate at the server site to build a global federated model. The process of model building ensures that there is no data leakage. Likewise, in [36], the authors proposed methods to improve the communication cost to facilitate the training of centralized models based on data distributed over mobile clients. Recently, a compression approach called Deep Gradient Compression [39] is proposed to greatly reduce the communication bandwidth in large-scale distributed training.

We summarize horizontal federated learning as:

$$\mathcal{X}_i = \mathcal{X}_j, \quad \mathcal{Y}_i = \mathcal{Y}_j, \quad I_i \neq I_j, \quad \forall \mathcal{D}_i, \mathcal{D}_j, i \neq j \tag{2}$$

Security Definition. A horizontal federated learning system typically assumes honest participants and security against a honest-but-curious server [9, 51]. That is, only the server can compromise

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[34]中，研究人员考虑了区块链联邦学习（BlockFL ）架构，其中移动的设备的本地学习模型更新通过利用区块链进行交换和验证。他们考虑了最佳块生成，网络可扩展性和鲁棒性问题。

2.3 联邦学习的分类

在本节中，我们将讨论如何根据数据的分布特征对联邦学习进行分类。

令矩阵D表示由每个数据所有者i持有的数据。矩阵的每一行代表一个样本，每一列代表一个特征。同时，某些数据集还可能包含标签数据。我们将特征空间表示为X，将标签空间表示为Y，并使用I表示样本ID空间。例如，在金融领域，标签可以是用户的信用;在营销领域，标签可以是用户的购买欲望;在教育领域，Y可以是学生的学位。特征X、标签Y和样本Ids I构成完整的训练数据集（I，X，Y）。数据方的特征和样本空间可能不相同，我们根据数据在特征和样本ID空间中如何分布在各方之间，将联邦学习分为水平联邦学习，垂直联邦学习和联邦迁移学习。图2显示了两方场景的各种联邦学习框架。

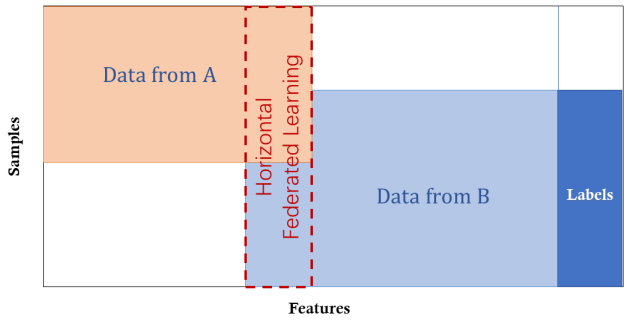
2.3.1 水平联邦学习水平联邦学习或基于样本的联邦学习是在数据集共享相同特征空间但样本不同的场景中引入的（图2a ）。例如，两个区域银行可能具有与其各自区域非常不同的用户组，并且其用户的交集非常小。然而，它们的业务非常相似，因此特征空间是相同的。参考文献[58]提出了一种协作式深度学习方案，其中参与者独立训练，仅共享参数更新的子集。2017 年，谷歌提出了一种用于Android 手机型号更新的水平联邦学习解决方案[41]。在该框架中，使用Android 手机的单个用户在本地更新模型参数并将参数上传到Android 云，从而与其他数据所有者一起联合训练集中式模型。 还介绍了一种安全的聚合方案，以保护其联邦学习框架下聚合用户更新的隐私[9]。参考文献[51]使用加法同态加密进行模型参数聚合，以提供针对中央服务器的安全性。

在[60]中，提出了一种多任务风格的联合学习系统，允许多个站点完成单独的任务，同时共享知识并保持安全性。他们提出的多任务学习模型还可以解决高通信成本、落伍者和容错问题。在[41]中，作者提出构建一个安全的客户端-服务器结构，其中联合学习系统按用户划分数据，并允许在客户端设备上构建的模型在服务器站点上协作以构建全局联合模型。模型构建过程确保没有数据泄漏。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的客户端上的数据的集中式模型的训练。最近，提出了一种称为深度梯度压缩的压缩方法[39]，以大大降低大规模分布式训练中的通信带宽。

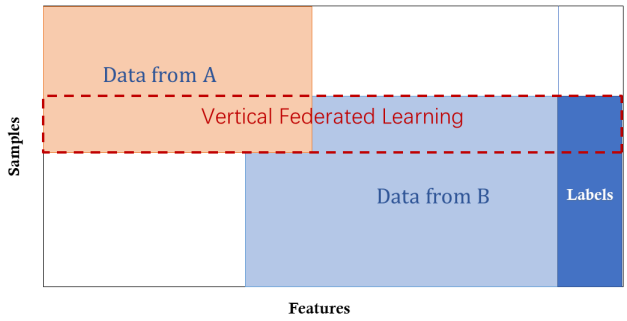
我们将水平联邦学习总结为：

$$X= X，Y= Y，I，I，D，D，i，j \quad (2)$$

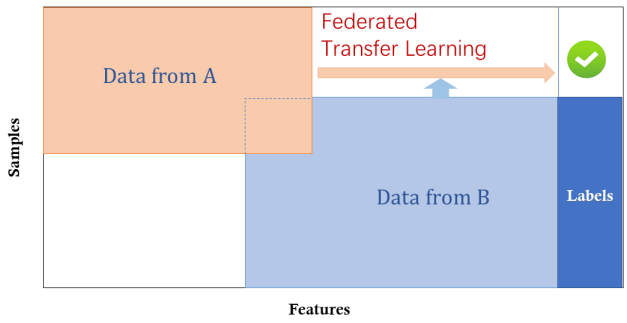
安全定义。水平联邦学习系统通常假设诚实的参与者和诚实但好奇的服务器的安全性[9，51]。也就是说，只有服务器可以妥协



(a) Horizontal Federated Learning

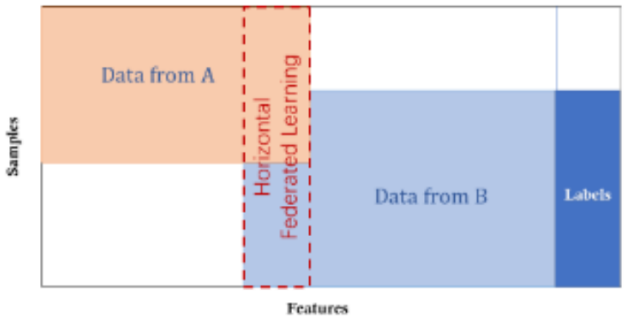


(b) Vertical Federated Learning

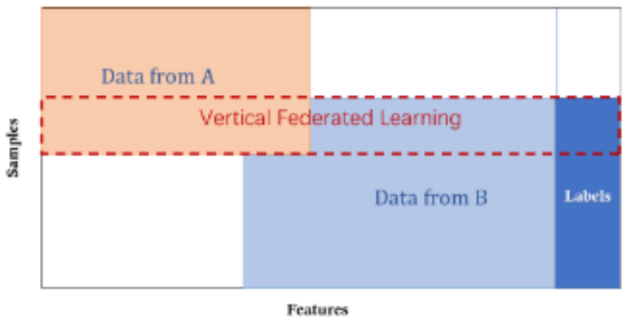


(c) Federated Transfer Learning

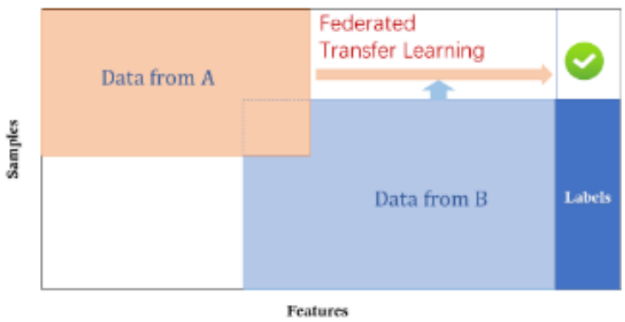
Fig. 2. Categorization of Federated Learning



(a)水平联合学习



(b)垂直联合学习



(c)联邦迁移学习

图2.联邦学习的分类

the privacy of data participants. Security proof has been provided in these works. Recently another security model considering malicious user [29] is also proposed, posing additional privacy challenges. At the end of the training, the universal model and the entire model parameters are exposed to all participants.

2.3.2 Vertical Federated Learning. Privacy-preserving machine learning algorithms have been proposed for vertically partitioned data, including Cooperative Statistical Analysis [15], association rule mining [65], secure linear regression [22, 32, 55], classification [16] and gradient descent [68]. Recently, Ref [27, 49] proposed a vertical federated learning scheme to train a privacy-preserving logistic regression model. The authors studied the effect of entity resolution on the learning performance and applied Taylor approximation to the loss and gradient functions so that homomorphic encryption can be adopted for privacy-preserving computations.

Vertical federated learning or feature-based federated learning (Figure 2b) is applicable to the cases that two data sets share the same sample ID space but differ in feature space. For example, consider two different companies in the same city, one is a bank, and the other is an e-commerce company. Their user sets are likely to contain most of the residents of the area, so the intersection of their user space is large. However, since the bank records the user's revenue and expenditure behavior and credit rating, and the e-commerce retains the user's browsing and purchasing history, their feature spaces are very different. Suppose that we want both parties to have a prediction model for product purchase based on user and product information.

Vertically federated learning is the process of aggregating these different features and computing the training loss and gradients in a privacy-preserving manner to build a model with data from both parties collaboratively. Under such a federal mechanism, the identity and the status of each participating party is the same, and the federal system helps everyone establish a "common wealth" strategy, which is why this system is called "federated learning.". Therefore, in such a system, we have:

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

Security Definition. A vertical federated learning system typically assumes honest-but-curious participants. In a two-party case, for example, the two parties are non-colluding and at most one of them are compromised by an adversary. The security definition is that the adversary can only learn data from the client that it corrupted but not data from the other client beyond what is revealed by the input and output. To facilitate the secure computations between the two parties, sometimes a Semi-honest Third Party (STP) is introduced, in which case it is assumed that STP does not collude with either party. SMC provides formal privacy proof for these protocols [25]. At the end of learning, each party only holds the model parameters associated to its own features, therefore at inference time, the two parties also need to collaborate to generate output.

2.3.3 Federated Transfer Learning (FTL). Federated Transfer Learning applies to the scenarios that the two data sets differ not only in samples but also in feature space. Consider two institutions, one is a bank located in China, and the other is an e-commerce company located in the United States. Due to geographical restrictions, the user groups of the two institutions have a small intersection. On the other hand, due to the different businesses, only a small portion of the feature space from both parties overlaps. In this case, transfer learning [50] techniques can be applied to provide solutions for the entire sample and feature space under a federation (Figure2c). Specially, a common representation between the two feature space is learned using the limited common sample sets and later applied to obtain predictions for samples with only one-side features. FTL is an important extension to the existing federated learning systems because it deals with problems exceeding the

数据参与者的隐私。在这些工作中提供了安全证明。最近，另一个考虑恶意用户的安全模型[29]也被提出，带来了额外的隐私挑战。在训练结束时，通用模型和整个模型参数将暴露给所有参与者。

2.3.2 垂直联邦学习隐私保护机器学习算法已被提出用于垂直分区数据，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]提出了一种垂直联邦学习方案来训练隐私保护逻辑回归模型。作者研究了实体分辨率对学习性能的影响，并将泰勒近似应用于损失和梯度函数，以便可以采用同态加密进行隐私保护计算。

垂直联邦学习或基于特征的联邦学习（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。他们的用户集很可能包含了该地区的大部分居民，因此他们的用户空间交集很大。但是，由于银行记录的是用户的收支行为和信用评级，而电商保留的是用户的浏览和购买历史，因此它们的特征空间有很大的不同。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。

垂直联邦学习是聚合这些不同特征并以隐私保护的方式计算训练损失和梯度的过程，以利用来自双方的数据协作构建模型。在这样的联邦机制下，每个参与方的身份和地位都是相同的，而联邦系统帮助每个人建立“共同财富”战略，这就是为什么这个系统被称为“联邦学习”。 “.因此，在这样的系统中，我们有：

$$X，X，Y，Y，I= I D，D，i，j \quad (3)$$

安全定义。垂直联邦学习系统通常假设诚实但好奇的参与者。例如，在两方当事人的案件中，两方当事人是非串通的，最多其中一方被对手妥协。安全性定义是，攻击者只能从被破坏的客户端学习数据，而不能从其他客户端学习数据，而不是输入和输出所揭示的数据。为了促进双方之间的安全计算，有时会引入半诚实第三方（STP ），在这种情况下，假设STP 不与任何一方勾结。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，双方还需要协作生成输出。

2.3.3 联邦迁移学习（FTL）。联合迁移学习适用于两个数据集不仅样本不同而且特征空间不同的情况。考虑两个机构，一个是位于中国的银行，另一个是位于美国的电子商务公司。由于地域限制，两家机构的用户群体交集不大。另一方面，由于业务不同，双方只有一小部分特征空间重叠。在这种情况下，可以应用迁移学习[50]技术为联邦下的整个样本和特征空间提供解决方案（图2c ）。特别地，使用有限的公共样本集学习两个特征空间之间的公共表示，然后应用于获得仅具有单侧特征的样本的预测。FTL是对现有联邦学习系统的重要扩展，因为它处理的问题超出了

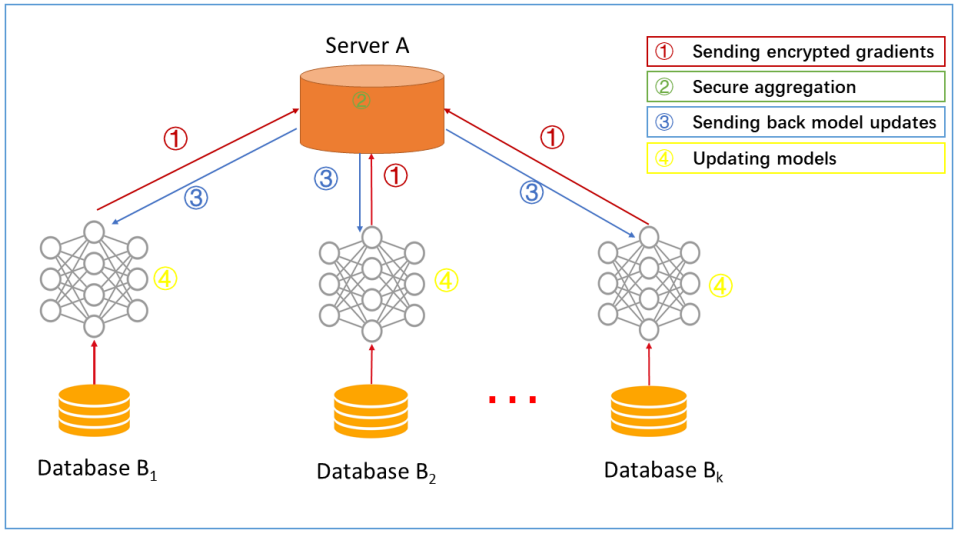


Fig. 3. Architecture for a horizontal federated learning system

scope of existing federated learning algorithms:

$$\mathcal{X}_i \neq \mathcal{X}_j, \quad \mathcal{Y}_i \neq \mathcal{Y}_j, \quad I_i \neq I_j \quad \forall \mathcal{D}_i, \mathcal{D}_j, i \neq j \tag{4}$$

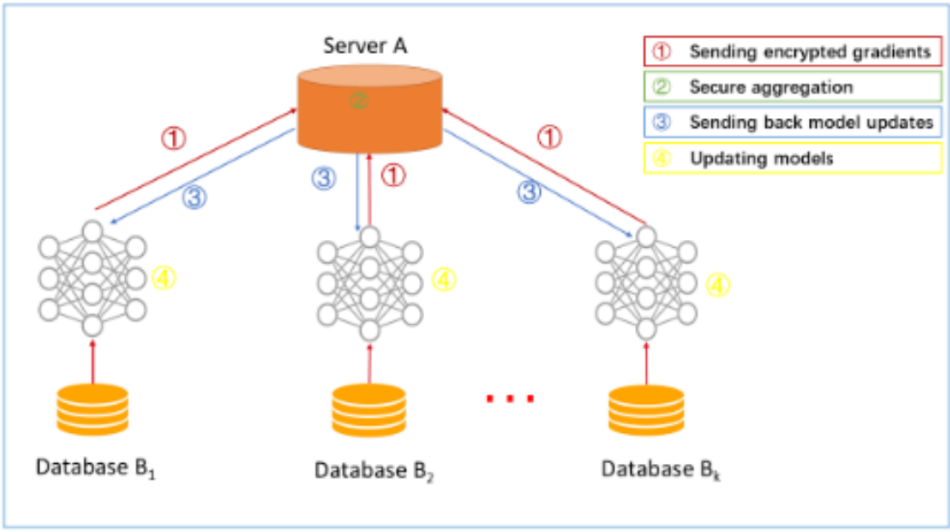
Security Definition. A federated transfer learning system typically involves two parties. As will be shown in the next section, its protocols are similar to the ones in vertical federated learning, in which case the security definition for vertical federated learning can be extended here.

2.4 Architecture for a federated learning system

In this section, we illustrate examples of general architectures for a federated learning system. Note that the architectures of horizontal and vertical federated learning systems are quite different by design, and we will introduce them separately.

2.4.1 Horizontal Federated Learning. A typical architecture for a horizontal federated learning system is shown in Figure 3. In this system, k participants with the same data structure collaboratively learn a machine learning model with the help of a parameter or cloud server. A typical assumption is that the participants are honest whereas the server is honest-but-curious, therefore no leakage of information from any participants to the server is allowed [51]. The training process of such a system usually contain the following four steps:

- **Step 1**: participants locally compute training gradients, mask a selection of gradients with encryption [51], differential privacy [58] or secret sharing [9] techniques, and send masked results to server;
- **Step 2**: Server performs secure aggregation without learning information about any participant;
- **Step 3**: Server send back the aggregated results to participants;
- **Step 4**: Participants update their respective model with the decrypted gradients.



图三.水平联邦学习系统的体系结构

现有联邦学习算法的范围：

$$X, X, Y, Y, I, ID, D, i, j \quad (4)$$

安全定义。联合迁移学习系统通常涉及两方。正如下一节所示，它的协议类似于垂直联邦学习中的协议，在这种情况下，垂直联邦学习的安全定义可以在这里扩展。

2.4 联邦学习系统的体系结构

在本节中，我们将举例说明联邦学习系统的一般架构。请注意，水平和垂直联邦学习系统的架构在设计上有很大的不同，我们将分别介绍它们。

2.4.1 水平联邦学习图3显示了水平联邦学习系统的典型架构。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露信息[51]。这种系统的训练过程通常包括以下四个步骤：

- 第一步：参与者在本地计算训练梯度，使用加密[51]，差分隐私[58]或秘密共享[9]技术屏蔽梯度的选择，并将屏蔽结果发送到服务器;
- 步骤2：服务器执行安全聚合，而不学习关于任何参与者的信息;
- 步骤3：服务器将聚合结果发送回参与者;
- 步骤4：参与者用解密的梯度更新他们各自的模型。

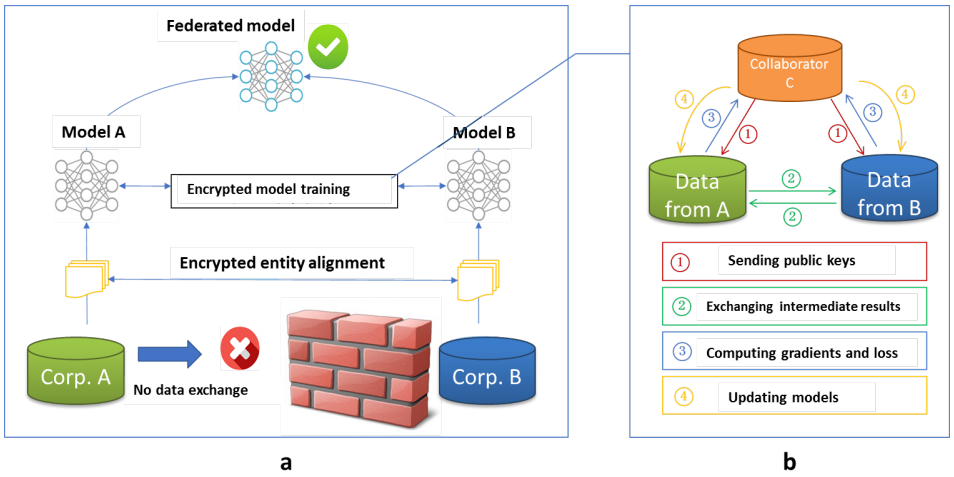


Fig. 4. Architecture for a vertical federated learning system

Iterations through the above steps continue until the loss function converges, thus completing the entire training process. This architecture is independent of specific machine learning algorithms (logistic regression, DNN etc) and all participants will share the final model parameters.

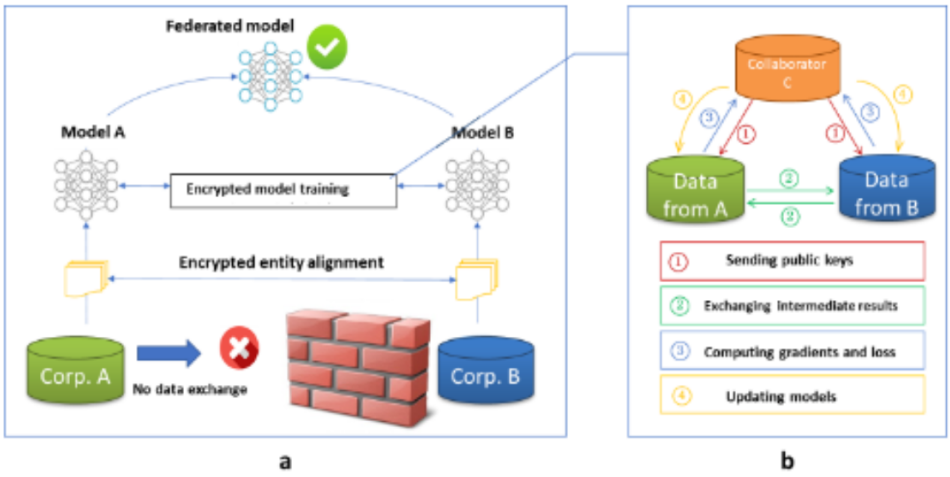
Security Analysis. The above architecture is proved to protect data leakage against the semi-honest server, if gradients aggregation is done with SMC [9] or Homomorphic Encryption [51]. But it may be subject to attack in another security model by a malicious participant training a Generative Adversarial Network (GAN) in the collaborative learning process [29].

2.4.2 Vertical Federated Learning. Suppose that companies A and B would like to jointly train a machine learning model, and their business systems each have their own data. In addition, Company B also has label data that the model needs to predict. For data privacy and security reasons, A and B cannot directly exchange data. In order to ensure the confidentiality of the data during the training process, a third-party collaborator C is involved. Here we assume the collaborator C is honest and does not collude with A or B, but party A and B are honest-but-curious to each other. A trusted third party C a reasonable assumption since party C can be played by authorities such as governments or replaced by secure computing node such as Intel Software Guard Extensions (SGX) [7]. The federated learning system consists of two parts, as shown in Figure 4.

Part 1. Encrypted entity alignment. Since the user groups of the two companies are not the same, the system uses the encryption-based user ID alignment techniques such as [38, 56] to confirm the common users of both parties without A and B exposing their respective data. During the entity alignment, the system does not expose users that do not overlap with each other.

Part 2. Encrypted model training. After determining the common entities, we can use these common entities' data to train the machine learning model. The training process can be divided into the following four steps (as shown in Figure 4):

- **Step 1**: collaborator C creates encryption pairs, send public key to A and B;
- **Step 2**: A and B encrypt and exchange the intermediate results for gradient and loss calculations;



见图4。垂直联邦学习系统的体系结构

通过上述步骤的迭代继续，直到损失函数收敛，从而完成整个训练过程。该架构独立于特定的机器学习算法（逻辑回归，DNN 等），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，则上述架构被证明可以防止半诚实服务器的数据泄漏。但是，它可能会受到另一种安全模型中的恶意参与者在协作学习过程中训练生成对抗网络（GAN）的攻击[29]。

2.4.2 垂直联邦学习假设公司A和B希望联合训练机器学习模型，并且他们的业务系统都有自己的数据。此外，公司B还有模型需要预测的标签数据。出于数据隐私和安全原因，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，第三方合作者C参与其中。在这里，我们假设合作者C是诚实的，不与A或B勾结，但A和B彼此诚实但好奇。可信的第三方C是一个合理的假设，因为C方可以由政府等权威机构扮演，也可以由英特尔软件保护扩展（SGX）等安全计算节点取代[7]。联邦学习系统由两部分组成，如图4所示。

部分1.加密实体对齐。由于两家公司的用户群不一样，系统采用了[38，56]等基于验证的用户ID比对技术，在不暴露A、B各自数据的情况下，确认双方的共同用户。在实体对齐期间，系统不会公开彼此不重叠的用户。

部分2.加密模型训练。在确定公共实体之后，我们可以使用这些公共实体的数据来训练机器学习模型。培训过程可分为以下四个步骤（如图4所示）：

- 步骤1：协作者C创建加密对，将公钥发送给A和B;
- 第二步：A和B加密并交换中间结果进行梯度和损失计算;

- **Step 3**: A and B computes encrypted gradients and adds *additional mask*, respectively,and B also computes encrypted loss; A and B send encrypted values to C;
- **Step 4**: C decrypts and send the decrypted gradients and loss back to A and B; A and B unmask the gradients, update the model parameters accordingly.

Here we illustrate the training process using linear regression and homomorphic encryption as an example. To train a linear regression model with gradient descent methods, we need secure computations of its loss and gradients. Assuming learning rate η, regularization parameter λ, data set $\{x_i^A\}_{i\in\mathcal{D}_A}$, $\{x_i^B, y_i\}_{i\in\mathcal{D}_B}$, and model paramters Θ_A, Θ_B corresponding to the feature space of x_i^A, x_i^B respectively, the training objective is:

$$\min_{\Theta_A,\Theta_B} \sum_i ||\Theta_A x_i^A + \Theta_B x_i^B - y_i||^2 + \frac{\lambda}{2}(||\Theta_A||^2 + ||\Theta_B||^2) \tag{5}$$

let $u_i^A = \Theta_A x_i^A$, $u_i^B = \Theta_B x_i^B$, the encrypted loss is:

$$[[\mathcal{L}]] = [[\sum_i ((u_i^A + u_i^B - y_i))^2 + \frac{\lambda}{2}(||\Theta_A||^2 + ||\Theta_B||^2)]] \tag{6}$$

where additive homomorphic encryption is denoted as $[[\cdot]]$. Let $[[\mathcal{L}_A]] = [[\sum_i ((u_i^A)^2) + \frac{\lambda}{2}\Theta_A^2]]$, $[[\mathcal{L}_B]] = [[\sum_i ((u_i^B - y_i)^2) + \frac{\lambda}{2}\Theta_B^2]]$, and $[[\mathcal{L}_{AB}]] = 2\sum_i ([[u_i^A]](u_i^B - y_i))$, then

$$[[\mathcal{L}]] = [[\mathcal{L}_A]] + [[\mathcal{L}_B]] + [[\mathcal{L}_{AB}]] \tag{7}$$

Similarly, let $[[d_i]] = [[u_i^A]] + [[u_i^B - y_i]]$, then gradients are:

$$[[\frac{\partial \mathcal{L}}{\partial \Theta_A}]] = \sum_i [[d_i]] x_i^A + [[\lambda \Theta_A]] \tag{8}$$

$$[[\frac{\partial \mathcal{L}}{\partial \Theta_B}]] = \sum_i [[d_i]] x_i^B + [[\lambda \Theta_B]] \tag{9}$$

Table 1. Training Steps for Vertical Federated Learning : Linear Regression

	party A	party B	party C
step 1	initialize Θ_A	initialize Θ_B	create an encryption key pair, send public key to A and B;
step 2	compute $[[u_i^A]]$,$[[\mathcal{L}_A]]$ and send to B;	compute $[[u_i^B]]$,$[[d_i^B]]$,$[[\mathcal{L}]]$, send $[[d_i^B]]$ to A, send $[[\mathcal{L}]]$ to C;	
step 3	initialize R_A, compute $[[\frac{\partial \mathcal{L}}{\partial \Theta_A}]]$+$[[R_A]]$ and send to C;	initialize R_B, compute $[[\frac{\partial \mathcal{L}}{\partial \Theta_B}]]$+$[[R_B]]$ and send to C;	C decrypt $\mathcal{L}$, send $\frac{\partial \mathcal{L}}{\partial \Theta_A} + R_A$ to A, $\frac{\partial \mathcal{L}}{\partial \Theta_B} + R_B$ to B;
step 4	update Θ_A	update Θ_B	
what is obtained	Θ_A	Θ_B	

- 第三步：A和B分别计算加密梯度并添加额外掩码，B还计算加密损失; A和B将加密值发送给C;
- 步骤4：C解密并将解密的梯度和损失发送回A和B; A和B对梯度进行解密，相应地更新模型参数。

在这里，我们使用线性回归和同态加密作为示例来说明训练过程。为了使用梯度下降方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，数据集{x}，{x，y}，模型参数Θ，Θ分别对应于x，x的特征空间，训练目标为：

$$\min_{\Theta,\Theta} \sum_i ||\mathcal{X} + \mathcal{X} - \mathcal{Y}|| + \frac{\lambda}{2} (||\mathrm{Te}|| + ||\mathrm{Te}||) \quad (五)$$

令u = Θx，u = Θx，加密损失为：

$$[[\mathcal{L}]] = [[\sum_i ((u + (y)) + \frac{\lambda}{2} (||\mathrm{Te}|| + ||\mathrm{Te}||]] \quad (6)$$

其中，加性同态加密表示为[[·]]。令[[L]] = [[$\sum_i$ ((u)) + Θ]]，[[L]] = [[$\sum_i$ ((u - y)) + Θ]]，且[[L]] = [[$\sum_i$ ((u - y))，则[[$\mathcal{L}$]] = [[$\mathcal{L}$]] + [[$\mathcal{L}$]] + [[$\mathcal{L}$]] (7)

同样，令[[d]] = [[u]] + [[u − y]]，则梯度为：

$$[[\frac{\partial \mathcal{L}}{\partial \Theta}]] = \sum_i [[d]]x + [[\lambda\Theta]] \quad (8)$$

$$[[\frac{\partial \mathcal{L}}{\partial \Theta}]] = \sum_i [[d]]x + [[\lambda\Theta]] \quad (9)$$

表1.垂直联邦学习的训练步骤：线性回归

A方	B方	C方	
步骤1	初始化Θ	初始化Θ	创建加密密钥对，将公钥发送给A和B;
步骤2	计算[[u]]，[[L]]并发送给B;	计算[[u]]、[[d]]、[[$\mathcal{L}$]]、[d]发送到A，发送[[$\mathcal{L}$]]到C;	
步骤3	初始化R，计算[[$\frac{\partial \mathcal{L}}{\partial \Theta}$]]+[[R]]并发送到C;	初始化R，计算机[[$\frac{\partial \mathcal{L}}{\partial \Theta}$]]+[[R]]并发送到C;	C解密L，发送 $\frac{\partial}{\partial \Theta}$ + Rto A， $\frac{\partial}{\partial \Theta}$ + Rto B;
步骤4	更新Θ	更新θ	
是什么获得	ΘΘ		

Table 2. Evaluation Steps for Vertical Federated Learning : Linear Regression

	party A	party B	inquisitor C
step 0			send user ID i to A and B;
step 1	compute u_i^A and send to C	compute u_i^B and send to C;	get result $u_i^A + u_i^B$;

See Table 1 and 2 for the detailed steps. During entity alignment and model training, the data of A and B are kept locally, and the data interaction in training does not lead to data privacy leakage. Note potential information leakage to C may or may not be considered to be privacy violation. To further prevent C to learn information from A or B in this case, A and B can further hide their gradients from C by adding encrypted random masks. Therefore, the two parties achieve training a common model cooperatively with the help of federated learning. Because during the training, the loss and gradients each party receives are exactly the same as the loss and gradients they would receive if jointly building a model with data gathered at one place without privacy constraints, that is, this model is lossless. The efficiency of the model depends on the communication cost and computation cost of encrypted data. In each iteration the information sent between A and B scales with the number of overlapping samples. Therefore the efficiency of this algorithm can be further improved by adopting distributed parallel computing techniques.

Security Analysis. The training protocol shown in Table 1 does not reveal any information to C, because all C learns are the masked gradients and the randomness and secrecy of the masked matrix are guaranteed [16]. In the above protocol, party A learns its gradient at each step, but this is not enough for A to learn any information from B according to equation 8, because the security of scalar product protocol is well-established based on the inability of solving n equations in more than n unknowns [16, 65]. Here we assume the number of samples N_A is much greater than n_A, where n_A is the number of features. Similarly, party B can not learn any information from A. Therefore the security of the protocol is proved. Note we have assumed that both parties are semi-honest. If a party is malicious and cheats the system by faking its input, for example, party A submits only one non-zero input with only one non-zero feature, it can tell the value of u_i^B for that feature of that sample. It still can not tell x_i^B or Θ_B though, and the deviation will distort results for the next iteration, alarming the other party who will terminate the learning process. At the end of the training process, each party (A or B) remains oblivious to the data structure of the other party, and it obtains the model parameters associated only with its own features. At inference time, the two parties need to collaboratively compute the prediction results, with the steps shown in Table 2, which still do not lead to information leakage.

2.4.3 Federated Transfer Learning. Suppose in the above vertical federated learning example, party A and B only have a very small set of overlapping samples and we are interested in learning the labels for all the data set in party A. The architecture described in the above section so far only works for the overlapping data set. To extend its coverage to the entire sample space, we introduce transfer learning. This does not change the overall architecture shown in Figure 4 but the details of the intermediate results that are exchanged between party A and party B. Specifically, transfer learning typically involves in learning a common representation between the features of party A and B, and minimizing the errors in predicting the labels for the target-domain party by leveraging the labels in the source-domain party (B in this case). Therefore the gradient computations for

表2.垂直联邦学习的评估步骤：线性回归

	当事人A当事人B调查员C		
步骤0			将用户ID i发送到A，B;
步骤1计算u并发送到	C	计算并发送到C;	得到结果u + u;

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的数据都保存在本地，训练中的数据交互不会导致数据隐私泄露。请注意，潜在的信息泄漏到C可能会或可能不会被视为侵犯隐私。在这种情况下，为了进一步防止C从A或B学习信息，A和B可以通过添加加密的随机掩码来进一步向C隐藏它们的梯度。因此，双方在联邦学习的帮助下合作训练一个共同的模型。因为在训练过程中，每一方接收到的损失和梯度与他们在没有隐私约束的情况下使用在一个地方收集的数据联合构建模型时接收到的损失和梯度完全相同，也就是说，这个模型是无损的。该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之间发送的信息与重叠样本的数量成比例。因此，采用分布式并行计算技术可以进一步提高算法的效率。

安全分析。表1所示的训练协议不会向C透露任何信息，因为所有C学习都是掩码梯度，并且掩码矩阵的随机性和保密性得到了保证[16]。在上述协议中，A方在每一步都学习其梯度，但这不足以让A根据等式8从B学习任何信息，因为标量积协议的安全性是基于无法在多于n个未知数中求解n个等式而建立的[16，65]。这里我们假设样本数N远大于n，其中n是特征数。同样，B方也无法从A方获知任何信息。从而证明了协议的安全性。注意，我们假设双方都是半诚实的。如果一方是恶意的，并且通过伪造其输入来欺骗系统，例如，A方仅提交一个非零输入，只有一个非零特征，它可以告诉该样本的该特征的u值。 它仍然不能告诉xor θ，并且偏差将扭曲下一次迭代的结果，警告将终止学习过程的另一方。在训练过程结束时，每一方（A或B）保持不注意另一方的数据结构，并且它获得仅与其自身特征相关联的模型参数。在推理时，双方需要协同计算预测结果，步骤如表2所示，仍然不会导致信息泄露。

2.4.3 联邦迁移学习。假设在上面的垂直联邦学习示例中，A方和B方只有一个非常小的重叠样本集，我们对学习A方中所有数据集的标签感兴趣。到目前为止，上一节中描述的架构仅适用于重叠数据集。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。这不会改变图4所示的整体架构，但会改变在A方和B方之间交换的中间结果的细节。具体来说，迁移学习通常涉及学习A方和B方的特征之间的公共表示，并通过利用源域方（在这种情况下为B方）中的标签来最小化预测目标域方的标签的错误。因此，

party A and party B are different from that in the vertical federated learning scenario. At inference time, it still requires both parties to compute the prediction results.

2.4.4 Incentives Mechanism. In order to fully commercialize federated learning among different organizations, a fair platform and incentive mechanisms needs to be developed [20]. After the model is built, the performance of the model will be manifested in the actual applications and this performance can be recorded in a permanent data recording mechanism (such as Blockchain). Organizations that provide more data will be better off, and the model's effectiveness depends on the data provider's contribution to the system. The effectiveness of these models are distributed to parties based on federated mechanisms and continue to motivate more organizations to join the data federation.

The implementation of the above architecture not only considers the privacy protection and effectiveness of collaboratively-modeling among multiple organizations, but also considers how to reward organizations that contribute more data, and how to implement incentives with a consensus mechanism. Therefore, federated learning is a "closed-loop" learning mechanism.

3 RELATED WORKS

Federated learning enables multiple parties to collaboratively construct a machine learning model while keeping their private training data private. As a novel technology, federated learning has several threads of originality, some of which are rooted on existing fields. Below we explain the relationship between federated learning and other related concepts from multiple perspectives.

3.1 Privacy-preserving machine learning

Federated learning can be considered as privacy-preserving decentralized collaborative machine learning, therefore it is tightly related to multi-party privacy-preserving machine learning. Many research efforts have been devoted to this area in the past. For example, Ref [17, 67] proposed algorithms for secure multi-party decision tree for vertically partitioned data. Vaidya and Clifton proposed secure association mining rules [65], secure k-means [66], Naive Bayes classifier [64] for vertically partitioned data. Ref [31] proposed an algorithm for association rules on horizontally partitioned data. Secure Support Vector Machines algorithms are developed for vertically partitioned data [73] and horizontally partitioned data [74]. Ref [16] proposed secure protocols for multi-party linear regression and classification. Ref [68] proposed secure multi-party gradient descent methods. The above works all used secure multi-party computation (SMC) [25, 72] for privacy guarantees.

Nikolaenko et al.[48] implemented a privacy-preserving protocol for linear regression on horizontally partitioned data using homomorphic encryption and Yao's garbled circuits and Ref [22, 24] proposed a linear regression approach for vertically partitioned data. These systems solved the linear regression problem directly. Ref [47] approached the problem with Stochastic Gradient Descent (SGD) and they also proposed privacy-preserving protocols for logistic regression and neural networks. Recently, a follow-up work with a three-server model is proposed [44]. Aono et al.[4] proposed a secure logistic regression protocol using homomorphic encryption. Shokri and Shmatikov [58] proposed training of neural networks for horizontally partitioned data with exchanges of updated parameters. Ref [51] used the additively homomorphic encryption to preserve the privacy of gradients and enhance the security of the system. With the recent advances in deep learning, privacy-preserving neural networks inference is also receiving a lot of research interests[10, 11, 14, 28, 40, 52, 54].

A方和B方与垂直联合学习场景中的不同。在推理时，仍然需要双方计算预测结果。

2.4.4 激励机制为了在不同组织之间充分商业化联合学习，需要开发公平的平台和激励机制[20]。在模型建立之后，模型的性能将在实际应用中表现出来，并且这种性能可以记录在永久的数据记录机制（如区块链）中。提供更多数据的组织会更好，模型的有效性取决于数据提供者对系统的贡献。这些模型的有效性基于联邦机制分发给各方，并继续激励更多的组织加入数据联邦。

上述架构的实现不仅考虑了隐私保护和多组织间协同建模的有效性，还考虑了如何奖励贡献更多数据的组织，以及如何通过共识机制实现激励。因此，联邦学习是一种“闭环”学习机制。

3相关作品

联合学习使多方能够协作构建机器学习模型，同时保持其私人训练数据的私密性。作为一种新技术，联邦学习有几个原创性的线索，其中一些是植根于现有领域。下面我们从多个角度解释联邦学习和其他相关概念之间的关系。

3.1隐私保护机器学习

联邦学习可以被认为是隐私保护的分散协作机器学习，因此它与多方隐私保护机器学习密切相关。过去，许多研究工作都致力于这一领域。例如，参考文献[17，67]提出了垂直分区数据的安全多方决策树算法。Vaidya 和克利夫顿提出了安全关联挖掘规则[65]，安全k均值[66]，朴素贝叶斯分类器[64]用于垂直分区数据。参考文献[31]提出了一种水平分区数据上的关联规则算法。安全支持向量机算法是针对垂直分区数据[73]和水平分区数据[74]开发的。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]提出了安全多方梯度下降方法。

上述作品都使用了安全多方计算（SMC ）[25，72]来保证隐私。
Nikolaenko 等人[48]使用同态加密和Yao的乱码电路实现了水平分区数据上线性回归的隐私保护协议，参考文献[22，24]提出了垂直分区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（SGD ）解决了这个问题，他们还提出了逻辑回归和神经网络的隐私保护协议。最近，提出了一个三服务器模型的后续工作[44]。Aono 等人[4]提出了一种基于同态加密的安全逻辑回归协议。Shokri 和Shmatikov [58]提出了对水平分区数据进行神经网络训练，并交换更新的参数。参考文献[51]使用加法同态加密来保护梯度的隐私并增强系统的安全性。 随着深度学习的最新进展，隐私保护神经网络推理也受到了很多研究兴趣[10，11，14，28，40，52，54]。

3.2 Federated Learning vs Distributed Machine Learning

Horizontal federated learning at first sight is somewhat similar to Distributed Machine Learning. Distributed machine learning covers many aspects, including distributed storage of training data, distributed operation of computing tasks, distributed distribution of model results, etc. Parameter Server [30] is a typical element in distributed machine learning. As a tool to accelerate the training process, the parameter server stores data on distributed working nodes, allocates data and computing resources through a central scheduling node, so as to train the model more efficiently. For horizontally federated learning, the working node represents the data owner. It has full autonomy for the local data, and can decide when and how to join the federated learning. In the parameter server, the central node always takes the control, so federated learning is faced with a more complex learning environment. Secondly, federated learning emphasizes the data privacy protection of the data owner during the model training process. Effective measures to protect data privacy can better cope with the increasingly stringent data privacy and data security regulatory environment in the future.

Like in distributed machine learning settings, federated learning will also need to address Non-IID data. In [77] showed that with non-iid local data, performance can be greatly reduced for federated learning. The authors in response supplied a new method to address the issue similar to transfer learning.

3.3 Federated Learning vs Edge Computing

Federated learning can be seen as an operating system for edge computing, as it provides the learning protocol for coordination and security. In [69], authors considered generic class of machine learning models that are trained using gradient-descent based approaches. They analyze the convergence bound of distributed gradient descent from a theoretical point of view, based on which they propose a control algorithm that determines the best trade-off between local update and global parameter aggregation to minimize the loss function under a given resource budget.

3.4 Federated Learning vs Federated Database Systems

Federated Database Systems [57] are systems that integrate multiple database units and manage the integrated system as a whole. The federated database concept is proposed to achieve interoperability with multiple independent databases. A federated database system often uses distributed storage for database units, and in practice the data in each database unit is heterogeneous. Therefore, it has many similarities with federated learning in terms of the type and storage of data. However, the federated database system does not involve any privacy protection mechanism in the process of interacting with each other, and all database units are completely visible to the management system. In addition, the focus of the federated database system is on the basic operations of data including inserting, deleting, searching, and merging, etc., while the purpose of federated learning is to establish a joint model for each data owner under the premise of protecting data privacy, so that the various values and laws the data contain serve us better.

4 APPLICATIONS

As an innovative modeling mechanism that could train a united model on data from multiple parties without compromising privacy and security of those data, federated learning has a promising application in sales, financial, and many other industries, in which data cannot be directly aggregated for training machine learning models due to factors such as intellectual property rights, privacy protection, and data security.

3.2 联合学习与分布式机器学习

乍一看，水平联邦学习有点类似于分布式机器学习。分布式机器学习涵盖了很多方面，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]是分布式机器学习中的典型元素。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，通过中央调度节点分配数据和计算资源，从而更高效地训练模型。对于水平联合学习，工作节点代表数据所有者。它对本地数据具有完全的自主性，可以决定何时以及如何加入联邦学习。在参数服务器中，中心节点始终处于控制地位，因此联邦学习面临着更加复杂的学习环境。 其次，联邦学习强调模型训练过程中数据所有者的数据隐私保护。采取有效措施保护数据隐私，可以更好地科普未来日益严格的数据隐私和数据安全监管环境。

与分布式机器学习设置一样，联邦学习也需要处理非IID数据。在[77]中表明，对于非iid本地数据，联邦学习的性能可能会大大降低。作为回应，作者提供了一种新的方法来解决类似于迁移学习的问题。

3.3 联合学习与边缘计算

联邦学习可以被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。他们从理论的角度分析了分布式梯度下降的收敛界，在此基础上，他们提出了一种控制算法，该算法确定了局部更新和全局参数聚合之间的最佳权衡，以在给定的资源预算下最小化损失函数。

3.4 联邦学习与联邦数据库系统

联邦数据库系统[57]是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。联邦数据库的概念是为了实现与多个独立数据库的互操作性而提出的。联邦数据库系统通常对数据库单元使用分布式存储，并且实际上每个数据库单元中的数据是异构的。因此，它在数据类型和存储方面与联邦学习有许多相似之处。但是，联邦数据库系统在相互交互的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完全可见。此外，联邦数据库系统的重点是数据的基本操作，包括插入、删除、搜索和合并等。而联邦学习的目的是在保护数据隐私的前提下，为每个数据所有者建立联合模型，让数据所蕴含的各种价值和规律更好地为我们服务。

4 应用程序

作为一种创新的建模机制，可以在不损害这些数据的隐私和安全性的情况下，对来自多方的数据进行统一模型的训练，联邦学习在销售，金融和许多其他行业中具有很好的应用前景，其中由于知识产权，隐私保护和数据安全等因素，数据无法直接聚合用于训练机器学习模型。

Take the smart retail as an example. Its purpose is to use machine learning techniques to provide customers with personalized services, mainly including product recommendation and sales services. The data features involved in the smart retail business mainly include user purchasing power, user personal preference, and product characteristics. In practical applications, these three data features are likely to be scattered among three different departments or enterprises. For example, a user's purchasing power can be inferred from her bank savings and her personal preference can be analyzed from her social networks, while the characteristics of products are recorded by an e-shop. In this scenario, we are facing two problems. First, for the protection of data privacy and data security, data barriers between banks, social networking sites, and e-shopping sites are difficult to break. As a result, data cannot be directly aggregated to train a model. Second, the data stored in the three parties are usually heterogeneous, and traditional machine learning models cannot directly work on heterogeneous data. For now, these problems have not been effectively solved with traditional machine learning methods, which hinder the popularization and application of artificial intelligence in more fields.

Federated learning and transfer learning are the key to solving these problems. First, by exploiting the characteristics of federated learning, we can build a machine learning model for the three parties without exporting the enterprise data, which not only fully protects data privacy and data security, but also provides customers with personalized and targeted services and thereby achieves mutual benefits. Meanwhile, we can leverage transfer learning to address the data heterogeneity problem and break through the limitations of traditional artificial intelligence techniques. Therefore federated learning provides a good technical support for us to build a cross-enterprise, cross-data, and cross-domain ecosphere for big data and artificial intelligence.

One can use federated learning framework for multi-party database querying without exposing the data. For example, supposed in a finance application we are interested in detecting multi-party borrowing, which has been a major risk factor in the banking industry. This happens when certain users maliciously borrows from one bank to pay for the loan at another bank. Multi-party borrowing is a threat to financial stability as a large number of such illegal actions may cause the entire financial system to collapse. To find such users without exposing the user list to each other between banks A and B, we can exploit a federated learning framework. In particular, we can use the encryption mechanism of federated learning and encrypt the user list at each party, and then take the intersection of the encrypted list in the federation. The decryption of the final result gives the list of multi-party borrowers, without exposing the other "good" users to the other party. As we will see below, this operation corresponds to the vertical federated learning framework.

Smart healthcare is another domain which we expect will greatly benefit from the rising of federated learning techniques. Medical data such as disease symptoms, gene sequences, medical reports are very sensitive and private, yet medical data are difficult to collect and they exist in isolated medical centers and hospitals. The insufficiency of data sources and the lack of labels have led to an unsatisfactory performance of machine learning models, which becomes the bottleneck of current smart healthcare. We envisage that if all medical institutions are united and share their data to form a large medical dataset, then the performance of machine learning models trained on that large medical dataset would be significantly improved. Federated learning combining with transfer learning is the main way to achieve this vision. Transfer learning could be applied to fill the missing labels thereby expanding the scale of the available data and further improving the performance of a trained model. Therefore, federated transfer learning would play a pivotal role in the development of smart healthcare and it may be able to take human health care to a whole new level.

以智慧零售为例。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、产品特征等。在实际应用中，这三种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她的银行储蓄中推断出来，她的个人偏好可以从她的社交网络中分析出来，而产品的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，对于数据隐私和数据安全的保护，银行、社交网站、电子购物网站之间的数据壁垒难以打破。因此，无法直接聚合数据来训练模型。 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作用于异构数据。就目前而言，这些问题还没有用传统的机器学习方法得到有效解决，阻碍了人工智能在更多领域的推广和应用。

联邦学习和迁移学习是解决这些问题的关键。首先，利用联邦学习的特点，在不导出企业数据的情况下，为三方构建机器学习模型，既充分保护数据隐私和数据安全，又能为客户提供个性化、针对性的服务，从而实现互利共赢。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性。因此，联邦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。

人们可以使用联邦学习框架进行多方数据库查询，而不会暴露数据。例如，假设在一个金融应用程序中，我们对检测多方借贷感兴趣，这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。多方借贷是对金融稳定的威胁，因为大量此类非法行为可能导致整个金融体系崩溃。为了在银行A和银行B之间找到这样的用户而不向彼此暴露用户列表，我们可以利用联邦学习框架。特别地，我们可以使用联邦学习的加密机制，在每一方加密用户列表，然后在联邦中取加密列表的交集。最终结果的解密给出了多方借款人的名单，而不会将其他“好”用户暴露给对方。 正如我们将在下面看到的，这个操作对应于垂直联邦学习框架。

智能医疗是另一个领域，我们预计它将从联邦学习技术的兴起中受益匪浅。疾病症状、基因序列、医疗报告等医疗数据是非常敏感和私密的，但医疗数据很难收集，而且它们存在于孤立的医疗中心和医院。数据源的不足和标签的缺乏导致机器学习模型的性能不理想，成为当前智能医疗的瓶颈。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。联邦学习与迁移学习相结合是实现这一愿景的主要途径。迁移学习可以用来填补缺失的标签，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，联邦迁移学习将在智能医疗保健的发展中发挥关键作用，它可能将人类医疗保健提升到一个全新的水平。

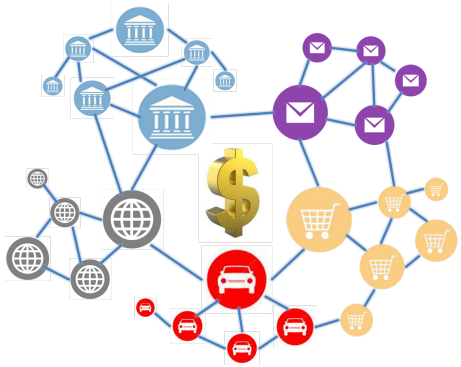


Fig. 5. Data Alliance Allocates the Benefits on Blockchain

5 FEDERATED LEARNING AND DATA ALLIANCE OF ENTERPRISES

Federated learning is not only a technology standard but also a business model. When people realize the effects of big data, the first thought that occurs to them is to aggregate the data together, compute the models through a remote processor and then download the results for further use. Cloud computing comes into being under such demands. However, with the increasing importance of data privacy and data security and a closer relationship between a company's profits and its data, the cloud computing model has been challenged. However, the business model of federated learning has provided a new paradigm for applications of big data. When the isolated data occupied by each institution fails to produce an ideal model, the mechanism of federated learning makes it possible for institutions and enterprises to share a united model without data exchange. Furthermore, federated learning could make equitable rules for profits allocation with the help of consensus mechanism from blockchain techniques. The data possessors, regardless of the scale of data they have, will be motivated to join in the data alliance and make their own profits. We believe that the establishment of the business model for data alliance and the technical mechanism for federated learning should be carried out together. We would also make standards for federated learning in various fields to put it into use as soon as possible.

6 CONCLUSIONS AND PROSPECTS

In recent years, the isolation of data and the emphasis on data privacy are becoming the next challenges for artificial intelligence, but federated learning has brought us new hope. It could establish a united model for multiple enterprises while the local data is protected, so that enterprises could win together taking the data security as premise. This article generally introduces the basic concept, architecture and techniques of federated learning, and discusses its potential in various applications. It is expected that in the near future, federated learning would break the barriers between industries and establish a community where data and knowledge could be shared together with safety, and the benefits would be fairly distributed according to the contribution of each participant. The bonus of artificial intelligence would finally be brought to every corner of our lives.

REFERENCES

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep Learning with Differential Privacy. 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

图五.数据联盟在区块链上分配利益

5企业的联合学习和数据联盟

联邦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影响时，他们的第一个想法是将数据聚合在一起，通过远程处理器计算模型，然后下载结果以供进一步使用。云计算正是在这样的需求下应运而生的。然而，随着数据隐私和数据安全的重要性越来越高，以及公司利润与数据之间的关系越来越紧密，云计算模式受到了挑战。然而，联邦学习的商业模式为大数据的应用提供了新的范式。当各机构所占用的孤立数据无法产生理想模型时，联邦学习机制使机构和企业无需进行数据交换就可以共享一个统一的模型。 此外，联邦学习可以在区块链技术的共识机制的帮助下制定公平的利润分配规则。数据拥有者，无论他们拥有的数据规模如何，都将有动力加入数据联盟并获得自己的利润。我们认为，数据联盟的商业模式的建立和联邦学习的技术机制应该一起进行。我们还将制定各个领域的联邦学习标准，以便尽快投入使用。

6结论与展望

近年来，数据的隔离和对数据隐私的重视正在成为人工智能的下一个挑战，但联邦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，为多个企业建立一个统一的模型，使企业在数据安全的前提下共赢。本文介绍了联邦学习的基本概念、体系结构和技术，并讨论了其在各种应用中的潜力。预计在不久的将来，联邦学习将打破行业之间的壁垒，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。人工智能的红利最终将被带到我们生活的每个角落。

引用

[1]马丁阿巴迪，朱安迪，伊恩古德费罗，H。布伦丹·麦克马汉、伊利亚·米罗诺夫、库纳尔·塔尔瓦尔和李章。2016 .深学习不同的隐私。*2016* 年*ACM SIGSAC* 计算机与通信会议论文集

安全（CCS '16 ）。ACM，纽约，NY，美国，308 -318 。https ://doi .org /10.1145 /2976749.2978318

[2] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. 2018. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Comput. Surv.* 51, 4, Article 79 (July 2018), 35 pages. https://doi.org/10.1145/3214303

[3] Rakesh Agrawal and Ramakrishnan Srikant. 2000. Privacy-preserving Data Mining. 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, and Lihua Wang. 2016. Scalable and Secure Logistic Regression via Homomorphic Encryption. 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, and Kazuma Ohara. 2016. 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, and Vitaly Shmatikov. 2018. How To Backdoor Federated Learning. arXiv:cs.CR/1807.00459

[7] Raad Bahmani, Manuel Barbosa, Ferdinand Brasser, Bernardo Portela, Ahmad-Reza Sadeghi, Guillaume Scerri, and Bogdan Warinschi. 2017. Secure Multiparty Computation from SGX. In *Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*. 477–497. https://doi.org/10.1007/978-3-319-70972-7_27

[8] Dan Bogdanov, Sven Laur, and Jan Willemson. 2008. Sharemind: A Framework for Fast Privacy-Preserving Computations. In *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security (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, and Karn Seth. 2017. Practical Secure Aggregation for Privacy-Preserving Machine Learning. 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, and Pascal Paillier. 2017. Fast Homomorphic Evaluation of Deep Discretized Neural Networks. *IACR Cryptology ePrint Archive* 2017 (2017), 1114.

[11] Hervé Chabanne, Amaury de Wargny, Jonathan Milgram, Constance Morel, and Emmanuel Prouff. 2017. Privacy-Preserving Classification on Deep Neural Network. *IACR Cryptology ePrint Archive* 2017 (2017), 35.

[12] Kamalika Chaudhuri and Claire Monteleoni. 2009. Privacy-preserving logistic regression. In *Advances in Neural Information Processing Systems 21*, D. Koller, D. Schuurmans, Y. Bengio, and L. Bottou (Eds.). Curran Associates, Inc., 289–296. http://papers.nips.cc/paper/3486-privacy-preserving-logistic-regression.pdf

[13] Fei Chen, Zhenhua Dong, Zhenguo Li, and Xiuqiang He. 2018. Federated Meta-Learning for Recommendation. *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, and John Wernsing. 2016. *CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy*. Technical Report. 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. Privacy-Preserving Cooperative Statistical Analysis. 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. Privacy-Preserving Multivariate Statistical Analysis: Linear Regression and Classification. In *SDM*.

[17] Wenliang Du and Zhijun Zhan. 2002. Building Decision Tree Classifier on Private Data. In *Proceedings of the IEEE International Conference on Privacy, Security and Data Mining - Volume 14 (CRPIT '14)*. Australian Computer Society, Inc., Darlinghurst, Australia, Australia, 1–8. http://dl.acm.org/citation.cfm?id=850782.850784

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

[19] EU. 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Available at: https://eur-lex. europa. eu/legal-content/EN/TXT* (2016).

[20] Boi Faltings, Goran Radanovic, and Ronald Brachman. 2017. *Game Theory for Data Science: Eliciting Truthful Information*. Morgan & Claypool Publishers.

[21] Jun Furukawa, Yehuda Lindell, Ariel Nof, and Or Weinstein. 2016. High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority. Cryptology ePrint Archive, Report 2016/944. https://eprint.iacr.

[2]Abbas Acar 、Hidayet 阿克苏、A.塞尔丘克·乌卢加克和毛罗·孔蒂2018 .同态加密方案的理论与实现综述。ACM 计算监视器51，4 ，第79 条（2018 年7月），35 页。https ://doi .org /10.1145 /3214303 Rakesh Agrawal 和Ramakrishnan Srikant . 2000 . 隐私保护数据挖掘。在2000 年的会议记录中

ACM SIGMOD 数据管理国际会议（*SIGMOD '00* ）。*ACM* ，纽约，*NY* ，美国，*439 -450* 。

https ://doi .org /10.1145 /342009.335438 Yoshinori Aono ，Takuya Hayashi ，Le Trieu Phong ，and Lihua Wang . 2016 . 可扩展和安全的Logistic 回归，通过

同态加密第六届ACM 数据和应用程序安全与隐私会议（CODASPY '16 ）。ACM ，纽约，NY ，美国，142 -144 。https ://doi .org /10.1145 /2857705.2857731

[5]Toshinori Araki 、Jun Furukawa 、Yehuda Lindell 、Ariel Nof 和Kazuma 大原。2016 .具有诚实多数的高精度半诚实安全三方计算。2016 年ACM SIGSAC 计算机和通信安全会议（CCS '16 ）。ACM ，纽约，NY ，美国，805 -817 。https ://doi .org /10.1145 /2976749 .

2978331 [6]尤金·巴格达萨良，安德烈亚斯·维特，华毅青，黛博拉·埃斯特林，维塔利·什马提科夫. 2018 .如何后门联邦学习。[7]Raad Bahmani ，Manuel 巴博萨，Ferdinand Brasser ，Bernardo Portela ，Ahmad -Reza Sadeghi ，Guillaume Scerri ，and Bogdan Warinschi . 2017 .来自SGX 的安全多方计算。In Financial Cryptography and Data Security

- 第*21* 届国际会议，*FC 2017* ，斯莱马，马耳他，*2017* 年*4*月*3*日至*7*日，修订的选定论文。*477 -497 . http* ：

//doi .org /10.1007 /978 -3 -319 -70972 -7_27 Dan Bogdanov ，Sven Laur ，and Jan Willemson . 2008 . Sharemind ：一个快速隐私保护计算框架

tions 。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* 出版社，柏林，海德堡，*192 —206* 。*https ://doi .org /10.1007 /978 -3 -540 -88313 -5_13*

[9]放大图片作者：基思博纳维茨，弗拉基米尔伊万诺夫，本克罗伊特，安东尼奥Marcedone ，H.布兰登·麦克马汉，萨瓦尔·帕特尔，丹尼尔·拉米奇，亚伦·西格尔，卡恩·赛斯。2017 .隐私保护机器学习的实用安全聚合。在

2017 年*ACM SIGSAC* 计算机和通信安全会议（*CCS '17* ）。*ACM* ，纽约，

美国纽约，1175 -1191 。https ://doi .org /10.1145 /3133956.3133982 Florian Bourse ，Michele Minelli ，Matthias Minihold ，and Pascal Paillier . 2017 .深度离散神经网络的快速同态求值。IACR Cryptology ePrint Archive 2017 （2017 ），1114 . [11]Hervé Chabanne 、Amaury de Wargny 、Jonathan Milgram 、Constance Morel 和Emmanuel Prouff 。2017 .深度神经网络上的隐私保护分类。IACR Cryptology ePrint Archive 2017 （2017 ），35 . [12]卡玛丽卡·乔杜里和克莱尔·蒙特莱奥尼2009 .隐私保护逻辑回归In Advances in Neural

信息处理系统21 ，D。Koller ，D. Schuurmans ，Y. Bengio 和L. Bottou （编辑）.柯兰联营公司289 -296 . http ://papers .nips .cc /paper /3486 -privacy -preserving -logistic -regression .pdf Fei Chen ，Zhenhua Dong ，Zhenguo Li，and Xiuqiang He . 2018 .联邦元学习推荐。Corr

abs /1802.07876 （2018 ）。http ://arxiv .org /abs /1802.07876 [14] Nathan Dowlin ，Ran Gilad -Bachrach ，Kim Laine ，Kristin 劳特，Michael Naehrig ，and John

韦恩辛*2016* . *CryptoNets* ：将神经网络应用于高穿透率的加密数据

放和准确性。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 和M .阿塔拉2001 .隐私保护合作统计分析。在第17 届年度会议上，

计算机安全应用会议（ACSAC '01 ）。IEEE计算机协会，华盛顿，美国，102 -。http ：//dl .acm .org /citation .cfm ?id = 872016.872181 [16]杜文良，韩永祥，陈世刚. 2004 .隐私保护多元统计分析：线性回归和分类。在SDM 中。[17]杜文良，詹志军。2002 .在私有数据上构造决策树分类器。在Proceedings of the IEEE

隐私，安全和数据挖掘国际会议-第*14* 卷（*CRPIT '14* ）。澳大利亚计算机协会，

股份有限公司、达令赫斯特，澳大利亚，澳大利亚，1 -8 。http ://dl .acm .org /citation .cfm ? [18]第十八话2008 .差异隐私：结果调查。第五届国际会议论文集

计算模型的理论与应用（TAMC'08 ）。Springer -Verlag ，柏林，海德堡，1 -19 。http ：//dl .acm .org /citation .cfm ?1791834.1791836 （微信同号）

[19]EU. 2016 .欧洲议会和理事会关于保护的法规（EU）2016 /679

关于自然人个人数据处理和此类数据自由流动的法律，并废除第95 /46 /EC 号指令（通用数据保护条例）。网址：https ：//eur -lex 。Europa . eu /legal -content /EN/TXT（2016 ）.

[20]博伊·费廷斯，戈兰·拉达诺维奇，还有罗纳德·布莱克曼. 2017 .数据科学博弈论：获取真实信息

出版社：Morgan & Claypool Publishers

[21]Jun Furukawa ，Yehuda Lindell ，Ariel Nof 和Or Weinstein 。2016 .高吞吐量的安全三方计算

恶意的对手和诚实的大多数。Cryptology ePrint Archive ，Report 2016 /944 . https ://eprint .iacr .

org/2016/944.
[22] Adrià Gascón, Phillipp Schoppmann, Borja Balle, Mariana Raykova, Jack Doerner, Samee Zahur, and David Evans. 2016. Secure Linear Regression on Vertically Partitioned Datasets. *IACR Cryptology ePrint Archive* 2016 (2016), 892.
[23] Robin C. Geyer, Tassilo Klein, and Moin Nabi. 2017. Differentially Private Federated Learning: A Client Level Perspective. *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. Privacy-Preserving Ridge Regression with only Linearly-Homomorphic Encryption. 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. https://doi.org/10.1145/28395.28420
[26] Rob Hall, Stephen E. Fienberg, and Yuval Nardi. 2011. Secure multiple linear regression based on homomorphic encryption. *Journal of Official Statistics* 27, 4 (2011), 669–691.
[27] Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Richard Nock, Giorgio Patrini, Guillaume Smith, and Brian Thorne. 2017. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. *CoRR* abs/1711.10677 (2017).
[28] Ehsan Hesamifard, Hassan Takabi, and Mehdi Ghasemi. 2017. CryptoDL: Deep Neural Networks over Encrypted Data. *CoRR* abs/1711.05189 (2017). arXiv:1711.05189 http://arxiv.org/abs/1711.05189
[29] Briland Hitaj, Giuseppe Ateniese, and Fernando Pérez-Cruz. 2017. Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning. *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. More Effective Distributed ML via a Stale Synchronous Parallel Parameter Server. In *Proceedings of the 26th International Conference on Neural Information Processing Systems - Volume 1 (NIPS'13)*. Curran Associates Inc., USA, 1223–1231. http://dl.acm.org/citation.cfm?id=2999611.2999748
[31] Murat Kantarcioglu and Chris Clifton. 2004. Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data. *IEEE Trans. on Knowl. and Data Eng.* 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. Privacy-Preserving Analysis of Vertically Partitioned Data Using Secure Matrix Products.
[33] Niki Kilbertus, Adria Gascon, Matt Kusner, Michael Veale, Krishna Gummadi, and Adrian Weller. 2018. Blind Justice: Fairness with Encrypted Sensitive Attributes. In *Proceedings of the 35th International Conference on Machine Learning (Proceedings of Machine Learning Research)*, Jennifer Dy and Andreas Krause (Eds.), Vol. 80. PMLR, Stockholmsmässan, Stockholm Sweden, 2630–2639. http://proceedings.mlr.press/v80/kilbertus18a.html
[34] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. 2018. On-Device Federated Learning via Blockchain and its Latency Analysis. arXiv:cs.IT/1808.03949
[35] Miran Kim, Yongsoo Song, Shuang Wang, Yuhou Xia, and Xiaoqian Jiang. 2018. Secure Logistic Regression Based on Homomorphic Encryption: Design and Evaluation. *JMIR Med Inform* 6, 2 (17 Apr 2018), e19. https://doi.org/10.2196/medinform.8805
[36] Jakub Konecný, H. Brendan McMahan, Daniel Ramage, and Peter Richtárik. 2016. Federated Optimization: Distributed Machine Learning for On-Device Intelligence. *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: Strategies for Improving Communication Efficiency. *CoRR* abs/1610.05492 (2016). arXiv:1610.05492 http://arxiv.org/abs/1610.05492
[38] Gang Liang and Sudarshan S Chawathe. 2004. Privacy-preserving inter-database operations. In *International Conference on Intelligence and Security Informatics*. Springer, 66–82.
[39] Yujun Lin, Song Han, Huizi Mao, Yu Wang, and William J. Dally. 2017. Deep Gradient Compression: Reducing the Communication Bandwidth for Distributed Training. *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. Oblivious Neural Network Predictions via MiniONN Transformations. 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, and Blaise Agüera y Arcas. 2016. Federated Learning of Deep Networks using Model Averaging. *CoRR* abs/1602.05629 (2016). arXiv:1602.05629 http://arxiv.org/abs/1602.05629
[42] H. Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. 2017. Learning Differentially Private Language Models Without Losing Accuracy. *CoRR* abs/1710.06963 (2017).

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]罗宾·C盖耶，塔西洛·克莱因，莫因·纳比。2017 .差异化私人联合学习：客户层面的视角。

CoRR abs / 1712.07557 （2017 ）。arXiv： 1712.07557 http ://arxiv .org / abs / 1712.07557 [24] Irene Giacomelli , Somesh Jha , Marc Joye , C 大卫佩奇和丹克焕 2017 .隐私保护岭

仅使用线性同态加密的回归。Cryptology ePrint Archive , Report 2017 / 979 . https ： //eprint .iacr .org / 2017 / 979 .

[25]O. Goldreich , S. Micali 和A.威格德森1987 .如何玩心理游戏在第十九届会议上，

ACM Symposium on Theory of Computing （英语：ACM Symposium on Theory of Computing ）ACM , 纽约，NY , 美国，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。Journal of Official Statistics 27 , 4 （2011 ） , 669 -691 .

[27]斯蒂芬哈代，威尔科·赫内卡，哈米什·艾维·劳，理查德·诺克，乔治·帕特里尼，纪尧姆·史密斯和布赖恩·索恩。

2017 .通过实体解析和加法同态加密对垂直分区数据进行私有联邦学习。CoRR abs / 1711.10677 （2017 ）。

[28]Ehsan Hesamifard , 哈桑Takabi , 和Mehdi Ghasemi 。2017 . CryptoDL ： 加密数据上的深度神经网络。

CoRR abs / 1711.05189 （2017 ）。http ://arxiv .org / abs / 1711.05189 [29] Briland Hitaj , Giuseppe Ateniese , and Fernando Pérez -Cruz . 2017 . GAN 下的深度模型：协作深度学习的信息泄漏。CoRR abs / 1702.07464 （2017 ）。

[30]Qirong Ho , James Cipar , Henggang Cui , Jin Kyu Kim , Seunghak Lee , 菲利普B.作者：Gibbons , A.作者：吉布森

Ganger , and Eric P. Xing . 2013 .更有效的分布式ML 通过一个陈旧的同步并行参数服务器。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 ? 2019 - 09 - 29 00： 00： 00

[31]穆拉特坎塔奇奥卢和克里斯克利夫顿。2004 .水平方向上隐私保护的分布式关联规则挖掘

分区数据。IEEE Trans . on Knowl . and Data Eng . 16 , 9 （Sept . 2004 ） , 1026 -1037 。https ://doi .org / 10.1109 / TKDE. 2004.45 [32] Alan F. Karr , X.谢尔顿·林、阿希什·P·萨尼尔和杰罗姆·P·赖特。2004 .使用安全矩阵乘积的垂直分区数据隐私保护分析。[33]Niki Kilbertus , Adria Gascon , Matt Kusner , Michael Veale , Krishna Gummadi 和Adrian Weller 。2018 .盲目的正义：

加密敏感属性的公平性。第*35* 届机器学习国际会议论文集

（《机器学习研究学报》） , 詹妮弗·迪和安德烈亚斯·克劳斯（编） , 卷。80 . PMLR , 斯德哥尔斯梅桑，斯德哥尔摩瑞典，2630 -2639 。http ://proceedings .mlr .press / v80 / kilbertus18a .html [34]Hyesung Kim , Jihong Park , Mehdi Bennis 和 Seong -Lyun Kim 。2018 .通过区块链实现的设备上联邦学习

及其延迟分析。[35] Miran Kim , Yongsoo Song , Shuang Wang , Yuhou Xia , and Xiaoqian Jiang . 2018 .安全的 Logistic 回归

同态加密：设计与评估。JMIR Med Inform 6 , 2 （2018 年4月17 日） , e19 。
https ://doi .org / 10.2196 / www .example .com

[36]Jakub Konecnanjung , H.布兰登·麦克马汉，丹尼尔·拉梅奇，彼得·里奇塔里克。2016 .联合优化：分布式
用于设备智能的机器学习。CoRR abs / 1610.02527 （2016 ）。arXiv： 1610.02527 http ://arxiv .org / abs / 1610 。02527

[37]Konecnyi , H。布兰登·麦克马汉，Felix X. Yu , Peter Richtárik , Ananda Theertha Suresh , 和Dave Bacon 。2016 .

联合学习：提高沟通效率的策略。CoRR abs / 1610.05492 （2016 ）。arXiv： 1610.05492 http ://arxiv .org / abs / 1610.05492
[38] Gang Liang and Sudarshan S Chawathe . 2004 .隐私保护数据库间操作。在情报和安全信息学国际会议上。斯普林格，66 -82 。[39]Yujun Lin , Song Han , Huizi Mao , Yu Wang , and William J. Dally . 2017 .深度梯度压缩：减少

分布式训练的通信带宽。CoRR abs / 1712.01887 （2017 ）。网址： http ： //arxiv .org / abs / 1712.01887

[40]Jian Liu , Mika Juuti , Yao Lu , and N.阿索坎2017 .通过MiniONN 变换的不经意神经网络预测。

2017 年ACM SIGSAC 计算机和通信安全会议（CCS '17 ）。ACM , 纽约，NY , 美国，619 -631 。
https ://doi .org / 10.1145 / 3133956.3134056 的网站上。Brendan McMahan , Eider 摩尔，丹尼尔拉梅奇，Blaise Agüera y Arcas . 2016 .使用模型平均的深度网络联合学习。CoRR abs / 1602.05629 （2016 ）。[42]第四十二章
http ://arxiv .org / abs / 1602.05629 Brendan McMahan 、丹尼尔·拉梅奇、Kunal Talwar和张立。2017 .学习不同的私人语言模型，而不会失去准确性。CoRR abs / 1710.06963 （2017 ）。

[43] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. 2018. Inference Attacks Against Collaborative Learning. *CoRR* abs/1805.04049 (2018). arXiv:1805.04049 http://arxiv.org/abs/1805.04049

[44] Payman Mohassel and Peter Rindal. 2018. ABY3: A Mixed Protocol Framework for Machine Learning. In *Proceedings of 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, and Ye Zhang. 2015. Fast and Secure Three-party Computation: The Garbled Circuit Approach. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. ACM, New York, NY, USA, 591–602. https://doi.org/10.1145/2810103.2813705

[46] Payman Mohassel and Yupeng Zhang. 2017. SecureML: A System for Scalable Privacy-Preserving Machine Learning. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 19–38.

[47] Payman Mohassel and Yupeng Zhang. 2017. SecureML: A System for Scalable Privacy-Preserving Machine Learning. *IACR Cryptology ePrint Archive* 2017 (2017), 396.

[48] Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh, and Nina Taft. 2013. Privacy-Preserving Ridge Regression on Hundreds of Millions of Records. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP '13)*. IEEE Computer Society, Washington, DC, USA, 334–348. https://doi.org/10.1109/SP.2013.30

[49] Richard Nock, Stephen Hardy, Wilko Henecka, Hamish Ivey-Law, Giorgio Patrini, Guillaume Smith, and Brian Thorne. 2018. Entity Resolution and Federated Learning get a Federated Resolution. *CoRR* abs/1803.04035 (2018). arXiv:1803.04035 http://arxiv.org/abs/1803.04035

[50] 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

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

[52] M. Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M. Songhori, Thomas Schneider, and Farinaz Koushanfar. 2018. Chameleon: A Hybrid Secure Computation Framework for Machine Learning Applications. *CoRR* abs/1801.03239 (2018).

[53] R L Rivest, L Adleman, and M L Dertouzos. 1978. On Data Banks and Privacy Homomorphisms. *Foundations of Secure Computation, Academia Press* (1978), 169–179.

[54] Bita Darvish Rouhani, M. Sadegh Riazi, and Farinaz Koushanfar. 2017. DeepSecure: Scalable Provably-Secure Deep Learning. *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. Privacy Preserving Regression Modelling via Distributed Computation. In *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '04)*. ACM, New York, NY, USA, 677–682. https://doi.org/10.1145/1014052.1014139

[56] 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

[57] Amit P. Sheth and James A. Larson. 1990. 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 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

[59] David Silver, Aja Huang, Christopher J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot, Sander Dieleman, Dominik Grewe, John Nham, Nal Kalchbrenner, Ilya Sutskever, Timothy Lillicrap, Madeleine Leach, Koray Kavukcuoglu, Thore Graepel, and Demis Hassabis. 2016. Mastering the game of Go with deep neural networks and tree search. *Nature* 529 (2016), 484–503. http://www.nature.com/nature/journal/v529/n7587/full/nature16961.html

[60] Virginia Smith, Chao-Kai Chiang, Maziar Sanjabi, and Ameet S Talwalkar. 2017. Federated Multi-Task Learning. 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. Stochastic gradient descent with differentially private updates. *2013 IEEE Global Conference on Signal and Information Processing* (2013), 245–248.

[62] Lili Su and Jiaming Xu. 2018. Securing Distributed Machine Learning in High Dimensions. *CoRR* abs/1804.10140 (2018). arXiv:1804.10140 http://arxiv.org/abs/1804.10140

[63] Latanya Sweeney. 2002. K-anonymity: A Model for Protecting Privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* 10, 5 (Oct. 2002), 557–570. https://doi.org/10.1142/S0218488502001648

[43]Luca Melis , Congzheng Song , Emiliano De Cristofaro , and Vitaly Shmatikov . 2018 .对Collabo 的推理攻击

迭代学习CoRR abs / 1805.04049 （2018 ）。arXiv： 1805.04049 http ://arxiv .org / abs / 1805.04049 [44] Payman Mohassel and Peter Rindal . 2018 . ABY 3 : 机器学习的混合协议框架 . 法律程序中

2018 年*ACM SIGSAC* 计算机和通信安全会议（*CCS '18* ）。美国纽约州纽约*ACM* ，

35 - 52 . https ://doi .org / 10.1145 / 3243734.3243760 Payman Mohassel , Mike Rosulek , and Ye Zhang . 2015 .快速安全的三方计算： 乱码电路

Approach .第*22* 届*ACM SIGSAC* 计算机与通信安全会议（*CCS '15* ）

ACM ，纽约，NY ，美国，591 - 602 。https ://doi .org / 10.1145 / 2810103.2813705 Payman Mohassel 和Yupeng Zhang . 2017 . SecureML ： 可扩展的隐私保护机器学习系统。

*IEEE Symposium on Security and Privacy . IEEE*计算机学会，*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 .隐私保护Privacy Preserving 岭回归在数亿条记录上的应用在2013 年IEEE安全与隐私研讨会（SP '13 ）的会议记录中。IEEE计算机学会，华盛顿，美国，334 - 348 。https ://doi .org / 10.1109 / SP .2013.30

[49]理查德·诺克、斯蒂芬·哈代、威尔科·赫内茨卡、哈米什·艾维-劳、乔治·帕特里尼、纪尧姆·史密斯和布赖恩

索恩2018 . Entity Resolution 和Federated Learning 得到一个Federated Resolution 。CoRR abs / 1803.04035 （2018 ）。arXiv： 1803.04035 http ://arxiv .org / abs / 1803.04035 [50] Sinno Jialin Pan and Qiang Yang . 2010 .迁移学习研究综述。IEEE Trans . on Knowl . and Data Eng . 22 , 10

(Oct . 2010 ） , 1345 - 1359 . https ://doi .org / 10.1109 / TKDE.2009.191 Le Trieu Phong , Yoshinori Aono , Takuya Hayashi ,

通过加法同态加密学习。IEEE Trans .信息取证和安全13 , 5 （2018 ） , 1333 - 1345 。

[52]M .放大图片作者： Sadegh Riazi , Christian Weinert , Oleksandr Tkachenko , Ebrahim M . Songhori 、托马斯施耐德和Farinaz 库尚法尔2018 . Chameleon ： 一个用于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 .关于数据银行和隐私同态。安全计算的基础，Academia Press （1978 ） , 169 - 179 。[54]Bita Darvish Rouhani , M .沙代·里亚兹和法里纳兹·库尚法尔2017 . DeepSecure ： 可扩展的可证明安全的深度

学习CoRR abs / 1705.08963 （2017 ）。http ://arxiv .org / abs / 1705.08963 [55]第一章： 第二章： 第三章： 第一章： 第二章： 第一章： 第二章： 第三章： 第一章： 第二章： 第一Karr , Xiaodong Lin , and 杰罗姆P. Reiter . 2004 .隐私保护回归建模通过

分布式计算第十届*ACM SIGKDD* 知识发现国际会议论文集

数据挖掘（KDD '04 ）ACM , 纽约，NY ，美国，677 - 682 。https ://doi .org / 10.1145 / 1014052.1014139 Monica Scannapieco , Ilya Figotin , Elisa Bertino , and Ahmed K. Elmagarmid 。2007 .隐私保护模式和

数据匹配。2007 年ACM SIGMOD 数据管理国际会议（SIGMOD '07 ）。ACM , 纽约，NY ，美国，653 - 664 。https ://doi .org / 10.1145 / 1247480.1247553 Amit P. Sheth 和James A.拉森1990 .用于管理分布式、异构和

自治数据库。ACM 计算监视器22 、3 （Sept . 1990 ） , 183 - 236 . https ://doi .org / 10.1145 / 96602.96604 Reza Shokri 和 Vitaly Shmatikov . 2015 .隐私保护深度学习第22 届ACM SIGSAC 会议论文集

计算机和通信安全会议（CCS '15 ）。ACM , 纽约，NY , 美国，1310 - 1321 。网址： //doi .org / 10.1145 / 2810103.2813687

[59]David Silver , Aja Huang , Christopher J. Maddison , Arthur Guez , Laurent Sifre , George van den Driesche , Julian 步 行者 , Ioannis Antonoglou , Veda Panneershelvam , Marc Lanctot , Sander Dieleman , Dominik Grewe , John Nham , Nal Kalchbrenner , Ilya Sutskever , Timothy Lillicrap , Madeleine Leach , Koray Kavukcuoglu , Thore Graepel , 和 Demis Hassabis 。2016 .利用 深度 神经 网络 和 树 搜索 掌握 围棋 游戏 。Nature 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 . Federated Multi Task Learning 多任务 联合 学习

神经 信息 处理 系统 的 研究 进展 （ Advances in Neural Information Processing Systems , 30 ） Guyon , 美国V. Luxburg , S 。本 , H 。沃尔克 , R 。费格斯 , S 。Vishwanathan , 和 R . Garnett （ EDS 。Curran Associates , Inc . 公司 简介4424 - 4434 . http ://papers .nips .cc / paper / 7029 - federated - multi - task - learning .pdf [61] Shuang Song , Kamalika Chaudhuri , 和 Anand D . Sarwade 。2013 . Stochastic gradient descent with differentially private updates . 随机 梯度 变化 与 私人 更新 。2013 年 IEEE 全球 信号 与 信息 处理 会议 （ 2013 ） , 第 245 - 248 页 。

[62]苏丽丽和徐家明。2018 .在高维度中保护分布式机器学习。CoRR abs / 1804.10140 （2018 ）。

10 , 5 （2002 年10 月） , 557 - 570 。https ://doi .org / 10.1142 / S0218488502001648

[64] Jaideep Vaidya and Chris Clifton. [n. d.]. Privacy Preserving Naive Bayes Classifier for Vertically Partitioned Data. In *in Proceedings of the fourth SIAM Conference on Data Mining, 2004*. 330–334.

[65] Jaideep Vaidya and Chris Clifton. 2002. Privacy Preserving Association Rule Mining in Vertically Partitioned Data. In *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '02)*. ACM, New York, NY, USA, 639–644. https://doi.org/10.1145/775047.775142

[66] Jaideep Vaidya and Chris Clifton. 2003. Privacy-preserving K-means Clustering over Vertically Partitioned Data. In *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '03)*. ACM, New York, NY, USA, 206–215. https://doi.org/10.1145/956750.956776

[67] Jaideep Vaidya and Chris Clifton. 2005. Privacy-Preserving Decision Trees over Vertically Partitioned Data. 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. Privacy-preservation for Gradient Descent Methods. In *Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '07)*. 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. When Edge Meets Learning: Adaptive Control for Resource-Constrained Distributed Machine Learning. *CoRR* abs/1804.05271 (2018). arXiv:1804.05271 http://arxiv.org/abs/1804.05271

[70] Wikipedia. 2018. https://en.wikipedia.org/wiki/Facebook-Cambridge_Analytica_data_scandal.

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

[72] Andrew C. Yao. 1982. Protocols for Secure Computations. In *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS '82)*. IEEE Computer Society, Washington, DC, USA, 160–164. http://dl.acm.org/citation.cfm?id=1382436.1382751

[73] Hwanjo Yu, Xiaoqian Jiang, and Jaideep Vaidya. 2006. Privacy-preserving SVM Using Nonlinear Kernels on Horizontally Partitioned Data. In *Proceedings of the 2006 ACM Symposium on Applied Computing (SAC '06)*. ACM, New York, NY, USA, 603–610. https://doi.org/10.1145/1141277.1141415

[74] Hwanjo Yu, Jaideep Vaidya, and Xiaoqian Jiang. 2006. Privacy-Preserving SVM Classification on Vertically Partitioned Data. In *Proceedings of the 10th Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining (PAKDD'06)*. Springer-Verlag, Berlin, Heidelberg, 647–656. https://doi.org/10.1007/11731139_74

[75] Jiawei Yuan and Shucheng Yu. 2014. Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing. *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. Privacy Preserving Deep Computation Model on Cloud for Big Data Feature Learning. *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. Federated Learning with Non-IID Data. arXiv:cs.LG/1806.00582

[64]贾迪普·瓦迪亚和克里斯·克利夫顿。[n. d.]。垂直分割数据的隐私保护朴素贝叶斯分类器。2004 年第四届SIAM 数据挖掘会议论文集。330 -334 . [65]贾迪普·瓦迪亚和克里斯·克利夫顿。2002 .垂直分割数据中隐私保护关联规则挖掘。在

第八届*ACM SIGKDD* 知识发现和数据挖掘国际会议（*KDD '02* ）。*ACM* ，纽约，*NY* ，美国，*639 -644* 。
https ://doi .org /10.1145 /775047.775142

[66]贾迪普·瓦迪亚和克里斯·克利夫顿。2003 .垂直分区数据的隐私保护K-means 聚类。在
第九届*ACM SIGKDD* 知识发现和数据挖掘国际会议（*KDD '03* ）。*ACM* ，纽约，*NY* ，美国，*206 -215* 。
https ://doi .org /10.1145 /956750.956776

[67]贾迪普·瓦迪亚和克里斯·克利夫顿。2005 .垂直分割数据上的隐私保护决策树。的数据和
应用安全XIX，Sushil Jajodia 和Duminda Wijesekera （编辑。Springer Berlin Heidelberg ，柏林，海德堡，139 —152 .

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

[69]王世强，Tiffany Tuor ，Theodoros Salonidis ，Kin K。梁，克里斯蒂安·马卡亚，婷和，还有陈凯文。

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 ）。
http ://arxiv .org /abs /1804.05271 [70]维基百科，自由的百科全书。2018 . https ://en .wikipedia .org /wiki/Facebook -Cambridge_Analytica_data_scandal . [71]杨强，刘扬，陈天健，童永新。2018 .联邦学习CCF通信14，11 （2018 ），49 -55 。
[72]Andrew C.耀1982 .安全计算协议。第23 届基金会年会论文集

计算机科学（SFCS '82 ）。IEEE计算机学会，华盛顿，美国，160 -164 。http ://dl.acm .org /citation . cfm？（单位：立方英尺）联系电话：1382436.1382751

[73]Hwanjo Yu，Xiaoqian Jiang ，and Jaideep Vaidya . 2006 .水平非线性核的隐私保护SVM
分区数据。*2006* 年*ACM Symposium on Applied Computing* （*SAC '06* ）*ACM* ，纽约，纽约州，

USA ， 603 -610 . https ://doi .org /10.1145 /1141277.1141415 Yu，Jaideep Vaidya ，and Xiaoqian Jiang . 2006 .基于垂直分块的隐私保护SVM 分类
数据第*10* 届亚太知识发现与数据挖掘进展会议（*PAKDD '06* ）。

Springer -Verlag ，柏林，海德堡，647 -656 。https ://doi .org /10.1007 /11731139_74 Jiawei Yuan and Shucheng Yu. 2014 .隐私保护反向传播神经网络学习实用化

与云计算。IEEE Trans .并行分布25，1 （2014 年1月），212 -221 。https ://doi .org /10.1109 /TPDS .2013.18 张清晨，劳伦斯T. Yang ， and Zhikui Chen . 2016 .基于云的隐私保护深度计算模型

大数据特征学习IEEE Trans . Comput . 65，5 （2016 年5月），1351 -1362 . https ://doi .org /10.1109 /TC.2015.2470255
Yue Zhao ， Meng Li ，Liangzhen Lai ，Naveen 苏达 ，Damon Civin ，and Vikas Chandra . 2018 .联合学习
非IID数据。arXiv： cs .LG/1806.00582