联邦学习
白皮书 V1.0

深圳前海微众银行股份有限公司

发布：微众银行 AI 项目组

编制：微众银行 AI 项目组

2018 年 9 月

目录

第一章 联邦学习背景和重要性 5
1.1 人工智能发展概况 5
1.2 GDPR 与人工智能新挑战 6
1.3 联邦学习成为可行的解决方案 6
第二章 联邦学习的定义和范围 7
2.1 联邦学习概述 7
2.2 联邦学习的定义 7
第三章 联邦学习的分类 9
3.1 横向联邦学习 9
3.2 纵向联邦学习 10
3.3 联邦迁移学习 10
3.4 联邦学习的系统架构 10
第四章 联邦学习与现有研究的区别 12
4.1 联邦学习与差分隐私理论的区别 12
4.2 联邦学习与分布式机器学习的区别 12
4.3 联邦学习与联邦数据库的关系 12
第五章 联邦学习的应用实例 14
5.1 智慧金融 14
5.2 智慧医疗 14
5.3 联邦学习和“企业数据联盟” 15
第六章 联邦学习的发展路径 16
6.1 建立联邦学习国内外标准 16
6.2 建立行业垂直领域应用示例 16
6.3 全面展开建立联邦数据联盟 16
第七章 总结展望 18
参考文献 19

第一章 联邦学习背景和重要性

1.1 人工智能发展概况

从 1955 年达特茅斯会议开始，人工智能经过两起两落的发展，迎来了第三个高峰期。第一个高峰期的出现是因为人们看到了 AI 的希望，也就是自动化算法对提高效率的希望，但是受算法能力的限制，机器不能完成大规模数据训练和复杂任务，AI 进入了第一个低谷。第二个高峰来自于霍普菲尔特神经网络的提出，以及 BP 算法实现了神经网络训练的突破，使得大规模神经网络训练成为可能。但是这时却发现算力和数据不够，专家系统的设计跟不上工业的成长需求，引发了 AI 的第二个低谷。2006 年，深度学习神经网络被提出，加上近年来算法和算力的巨大提升和大数据的出现，人工智能迎来了第三个高峰。2016 年的 AlphaGo，其总计使用了 30 万盘棋局作为训练数据并且接连战胜两位人类职业围棋选手，我们真正看到了人工智能迸发出的巨大潜力，也更加憧憬人工智能技术可以在无人车、医疗、金融等更多、更复杂、更前沿的领域施展拳脚。

AlphaGo 的巨大成功使得人们自然而然的希望像这种大数据驱动的人工智能会在各行各业得以实现。但是真实的情况却让人非常失望：除了有限的几个行业，更多领域存在着数据有限且质量较差的问题，不足以支撑人工智能技术的实现。更多的应用领域有的只是小数据，或者质量很差的数据。 这种“人工智能到处可用”的错误的认知会导致很严重的商业后果。一个案例是 IBM 的沃森，一个非常有名的问答（QA）系统，即给一个问题 Q，它能很精准找到答案 A。沃森可以用一个高维的表示来表达这个问题 Q，这种表示可以比喻为成物理学里的光谱，棱镜把一束光分解成不同频率的光，形成光谱。有了这个光谱以后，可以和答案库里对应答案，概率相应高的就是可能的答案。整个流程应该说非常简单，但问题就是要有一个很健全的答案库。IBM 在电视大赛上取得了成功之后，就把这个应用在一些听起来比较好的垂直领域——医疗领域。然而，最近在一个美国的癌症治疗中心，发现这个应用非常不理想，从而导致了这个项目的失败。我们可以看一看在医疗领域，这些领域里的问题和答案来自哪里？比如输入有病症、基因序列、病理报告、各种各样的检测、各种论文，沃森的任务是利用这些数据来做诊断，帮助医生。但是，经过一段时间的实践发现，这些数据的来源远远不够，导致了系统效果很差。医疗领域需要非常多的标注数据，而医生的时间却非常宝贵，不能像其他的一些计算机视觉应用一样，可以由大众普通人来完成数据标注。所以在医疗这样的专业领域，这种标注的数据非常有限。有人估计，把医疗数据放在第三方公司标注，需要动用 1 万人用长达 10 年的时间才能收集到有效的数据。这就说明，在这些领域，即使动用很多人来做标注，数据也不够。这就是我们面临的现实。

同时数据源之间存在着难以打破的壁垒，一般情况下人工智能的所需要的数据会涉及多个领域，例如在基于人工智能的产品推荐服务中，产品销售方拥有产品的数据、用户购买商品的数据，但是没有用户购买能力和支付习惯的数据。在大多数行业中，数据是以孤岛的形式存在的，由于行业竞争、隐私安全、行政手续复杂等问题，即使是在同一个公司的不同部门之间实现数据整合也面临着重重阻力，在现实中想要将分散在各地、各个机构的数据进行整合几乎是不可能的，或者说所需的成本是巨大的。

1.2 GDPR 与人工智能新挑战

另一方面，随着大数据的进一步发展，重视数据隐私和安全已经成为了世界性的趋势。每一次公众数据的泄露都会引起媒体和公众的极大关注，例如最近 Facebook 的数据泄露事件就引起了大范围的抗议行动。同时各国都在加强对数据安全和隐私的保护，欧盟最近引入的新法案《通用数据保护条例》（General Data Protection Regulation, GDPR）[11]表明，对用户数据隐私和安全管理的日趋严格将是世界趋势。这给人工智能领域带来了前所未有的挑战，研究界和企业界目前的情况是收集数据的一方通常不是使用数据的一方，如 A 方收集数据，转移到 B 方清洗，再转移到 C 方建模，最后将模型卖给 D 方使用。这种数据在实体间转移，交换和交易的形式违反了 GDPR，并可能遭到法案严厉的惩罚。同样，中国在 2017 年起实施的《中华人民共和国网络安全法》[12]和《中华人民共和国民法总则》[13]中也指出网络运营者不得泄露、篡改、毁坏其收集的个人信息，并且与第三方进行数据交易时需确保拟定的合同明确约定拟交易数据的范围和数据保护义务。这些法规的建立在不同程度上对人工智能传统的数据处理模式提出了新的挑战。在这个问题上，人工智能的学界和企业界，目前并无较好的解决方案来应对这些挑战。

1.3 联邦学习成为可行的解决方案

要解决大数据的困境，仅仅靠传统的方法已经出现瓶颈。 两个公司简单的交换数据在很多法规包括 GDPR 是不允许的。用户是原始数据的拥有者，在用户没有批准的情况下，公司间是不能交换数据的。 其次，数据建模使用的目的，在用户认可前也不可以改变。所以，过去的许多数据交换的尝试，例如数据交易所，也需要巨大的改变才能合规。 同时，商业公司所拥有的数据往往都有巨大的潜在价值。两个公司甚至公司间的部门都要考虑利益的交换，在这个前提下，往往这些部门不会把数据与其他部门做简单的聚合。导致即使在同一个公司内，数据也往往以孤岛形式出现。

如何在满足数据隐私、安全和监管要求的前提下，设计一个机器学习框架，让人工智能系统能够更加高效、准确的共同使用各自的数据，是当前人工智能发展的一个重要课题。我们倡议把研究的重点转移到如何解决数据孤岛的问题。我们提出一个满足隐私保护和数据安全的一个可行的解决方案，叫做联邦学习[14-15]。

联邦学习是：

- 各方数据都保留在本地，不泄露隐私也不违反法规；
- 多个参与者联合数据建立虚拟的共有模型，并且共同获益的体系；
- 在联邦学习的体系下，各个参与者的身份和地位相同；
- 联邦学习的建模效果和将整个数据集放在一处建模的效果相同，或相差不大 （在各个数据的用户对齐（user alignment）或特征（feature alignment）对齐的条件下）；
- 迁移学习是在用户或特征不对齐的情况下，也可以在数据间通过交换加密参数达到知识迁移的效果。

联邦学习使得两方或多方的数据使用实体在合作当中数据不出本地也能共同使用，解决数据孤岛问题。

第二章 联邦学习的定义和范围

2.1 联邦学习概述

什么是联邦学习呢？举例来说，假设有两个不同的企业 A 和 B，它们拥有不同数据。比如，企业 A 有用户特征数据；企业 B 有产品特征数据和标注数据。这两个企业按照上述 GDPR 准则是不能粗暴地把双方数据加以合并的，因为数据的原始提供者，即他们各自的用户并没有机会来同意这样做。假设双方各自建立一个任务模型，每个任务可以是分类或预测，而这些任务也已经在获得数据时有各自用户的认可。那现在的问题是如何在 A 和 B 各端建立高质量的模型。但是，由于数据不完整（例如企业 A 缺少标签数据，企业 B 缺少特征数据），或者数据不充分 （数据量不足以建立好的模型），那么，在各端的模型有可能无法建立或效果并不理想。 联邦学习是要解决这个问题： 它希望做到各个企业的自有数据不出本地，而后联邦系统可以通过加密机制下的参数交换方式，即在不违反数据隐私法规情况下，建立一个虚拟的共有模型。这个虚拟模型就好像大家把数据聚合在一起建立的最优模型一样。但是在建立虚拟模型的时候，数据本身不移动，也不泄露隐私和影响数据合规。这样，建好的模型在各自的区域仅为本地的目标服务。在这样一个联邦机制下，各个参与者的身份和地位相同，而联邦系统帮助大家建立了“共同富裕”的策略。 这就是为什么这个体系叫做“联邦学习”。

上述实例阐述了联邦学习的基本思想，下文将规范联邦学习的定义，并进一步依据孤岛数据的分布特点对联邦学习进行分类，最后描述联邦学习系统的工作流程与系统构架。

2.2 联邦学习的定义

为了进一步准确地阐述联邦学习的思想，我们将其定义如下：

当多个数据拥有方（例如企业）F_i, i=1…N 想要联合他们各自的数据 D_i 训练机器学习模型时，传统做法是把数据整合到一方并利用数据 D={Di, i=1…N}进行训练并得到模型 M_sum。然而，该方案由于其涉及到的隐私和数据安全等法律问题通常难以实施。为解决这一问题，我们提出联邦学习。联邦学习是指使得这些数据拥有方 F_i 在不用给出己方数据 D_i 的情况下也可进行模型训练并得到模型 M_FED 的计算过程，并能够保证模型 M_FED 的效果 V_FED 与模型 M_SUM 的效果 V_SUM 间的差距足够小,即：

|V_FED-V_SUM |＜δ， 这里 δ 是任意小的一个正量值。

联邦学习的出处是金融机构的痛点，尤其是像“微众银行”这样的互联网银行。一个实用的例子是检测多方借贷。这在银行业，尤其是互联网金融一直是很头疼的一个问题。多方借贷是指某不良用户在一个金融机构借贷后还钱给另一个借贷机构,这种非法行为会让整个金融系统崩溃。要发现这样的用户，传统的做法是金融机构去某中心数据库查询用户信息，而各个机构必须上传他们所有用户,但这样做等于暴露金融机构的所有重要用户隐私和数据安全，这在 GDPR 下就不被允许。 在联邦学习的条件下，没有必要建立一个中心数据库，而任何参与联邦学习的金融机构可以利用联邦机制向联邦内的其他机构发出新用户的查询,其

他机构在不知道这个用户具体信息的前提下，回答在本地借贷的提问。这样做既能保护已有用户在各个金融机构的隐私和数据完整性，同时也能完成查询多头借贷的这个重要问题。

第三章 联邦学习的分类

上述对联邦学习的定义并没有讨论如何具体地设计一种联邦学习的实施方案。在实际中，孤岛数据具有不同分布特点，根据这些特点，我们可以提出相对应的联邦学习方案。下面，我们将以孤岛数据的分布特点为依据对联邦学习进行分类。

考虑有多个数据拥有方，每个数据拥有方各自所持有的数据集 D_i 可以用一个矩阵来表示。矩阵的每一行代表一个用户，每一列代表一种用户特征。同时，某些数据集可能还包含标签数据。如果要对用户行为建立预测模型，就必须要有标签数据。我们可以把用户特征叫做 X，把标签特征叫做 Y。比如，在金融领域，用户的信用是需要被预测的标签 Y；在营销领域，标签是用户的购买愿望 Y；在教育领域，则是学生掌握知识的程度等。用户特征 X 加标签 Y 构成了完整的训练数据（X， Y）。但是，在现实中，往往会遇到这样的情况：各个数据集的用户不完全相同，或用户特征不完全相同。具体而言，以包含两个数据拥有方的联邦学习为例，数据分布可以分为以下三种情况：

- 两个数据集的用户特征（X1,X2,…）重叠部分较大，而用户(U1, U2…)重叠部分较小；
- 两个数据集的用户(U1, U2…)重叠部分较大，而用户特征（X1,X2,…）重叠部分较小；
- 两个数据集的用户(U1, U2…)与用户特征重叠（X1,X2,…）部分都比较小。

为了应对以上三种数据分布情况，我们把联邦学习分为**横向联邦学习、纵向联邦学习与联邦迁移学习**（如图 1）。

横向联邦学习　　纵向联邦学习　　联邦迁移学习

图 1 联邦学习的分类

3.1 横向联邦学习

在两个数据集的用户特征重叠较多而用户重叠较少的情况下，我们把数据集按照横向(即用户维度)切分，并取出双方用户特征相同而用户不完全相同的那部分数据进行训练。这种方法叫做横向联邦学习。比如有两家不同地区银行，它们的用户群体分别来自各自所在的地区，相互的交集很小。但是，它们的业务很相似，因此，记录的用户特征是相同的。此时，就可以使用横向联邦学习来构建联合模型。Google 在 2017 年提出了一个针对安卓手机模型更新的数据联合建模方案[6-7]：在单个用户使用安卓手机时，不断在本地更新模型参数并将参数上传到安卓云上，从而使特征维度相同的各数据拥有方建立联合模型的一种联邦学习方案。

3.2 纵向联邦学习

在两个数据集的用户重叠较多而用户特征重叠较少的情况下，我们把数据集按照纵向（即特征维度）切分，并取出双方用户相同而用户特征不完全相同的那部分数据进行训练。这种方法叫做纵向联邦学习。比如有两个不同机构，一家是某地的银行，另一家是同一个地方的电商。它们的用户群体很有可能包含该地的大部分居民，因此用户的交集较大。但是，由于银行记录的都是用户的收支行为与信用评级，而电商则保有用户的浏览与购买历史，因此它们的用户特征交集较小。纵向联邦学习就是将这些不同特征在加密的状态下加以聚合，以增强模型能力的联邦学习。目前，逻辑回归模型，树型结构模型和神经网络模型等众多机器学习模型已经逐渐被证实能够建立在这个联邦体系上。

3.3 联邦迁移学习

在两个数据集的用户与用户特征重叠都较少的情况下，我们不对数据进行切分，而可以利用迁移学习[9]来克服数据或标签不足的情况。这种方法叫做联邦迁移学习。

比如有两个不同机构，一家是位于中国的银行，另一家是位于美国的电商。由于受到地域限制，这两家机构的用户群体交集很小。同时，由于机构类型的不同，二者的数据特征也只有小部分重合。在这种情况下，要想进行有效的联邦学习，就必须引入迁移学习，来解决单边数据规模小和标签样本少的问题，从而提升模型的效果。

3.4 联邦学习的系统架构

在讨论了联邦学习的定义与分类之后，我们以纵向联邦学习为例深入介绍一下联邦学习系统的构架，从而理解其工作的流程与细节。

我们以包含两个数据拥有方（即企业 A 和 B）的场景为例来介绍联邦学习的系统构架，该构架可扩展至包含多个数据拥有方的场景。假设企业 A 和 B 想联合训练一个机器学习模型，它们的业务系统分别拥有各自用户的相关数据。此外，企业 B 还拥有模型需要预测的标签数据。出于数据隐私和安全考虑，A 和 B 无法直接进行数据交换。此时，可使用联邦学习系统建立模型，系统构架由两部分构成，如图 2a 所示。

第一部分：加密样本对齐。由于两家企业的用户群体并非完全重合，系统利用基于加密的用户样本对齐技术，在 A 和 B 不公开各自数据的前提下确认双方的共有用户，并且不暴露不互相重叠的用户。 以便联合这些用户的特征进行建模。

第二部分：加密模型训练。在确定共有用户群体后，就可以利用这些数据训练机器学习模型。为了保证训练过程中数据的保密性，需要借助第三方协作者 C 进行加密训练。以线性回归模型为例，训练过程可分为以下 4 步（如图 2b 所示）：

- 第①步：协作者 C 把公钥分发给 A 和 B，用以对训练过程中需要交换的数据进行加密；
- 第②步：A 和 B 之间以加密形式交互用于计算梯度的中间结果；
- 第③步：A 和 B 分别基于加密的梯度值进行计算，同时 B 根据其标签数据计算损失，并把这些结果汇总给 C。C 通过汇总结果计算总梯度并将其解密。
- 第④步：C 将解密后的梯度分别回传给 A 和 B；A 和 B 根据梯度更新各自模型的参数。

迭代上述步骤直至损失函数收敛，这样就完成了整个训练过程。在样本对齐及模型训练过程中，A 和 B 各自的数据均保留在本地，且训练中的数据交互也不会导致数据隐私泄露。因此，双方在联邦学习的帮助下得以实现合作训练模型。

第三部分： 效果激励。联邦学习的一大特点就是它解决了为什么不同机构要加入联邦共同建模的问题， 即建立模型以后模型的效果会在实际应用中表现出来，并记录在永久数据记录机制（如区块链）上。 提供的数据多的机构会看到模型的效果也更好，这体现在对自己机构的贡献和对他人的贡献。这些模型对他人效果在联邦机制上以分给各个机构反馈，并继续激励更多机构加入这一数据联邦。

以上三个步骤的实施，即考虑了在多个机构间共同建模的隐私保护和效果，有考虑了如何奖励贡献数据多的机构，以一个共识机制来实现。 所以， 联邦学习是一个“闭环”的学习机制。

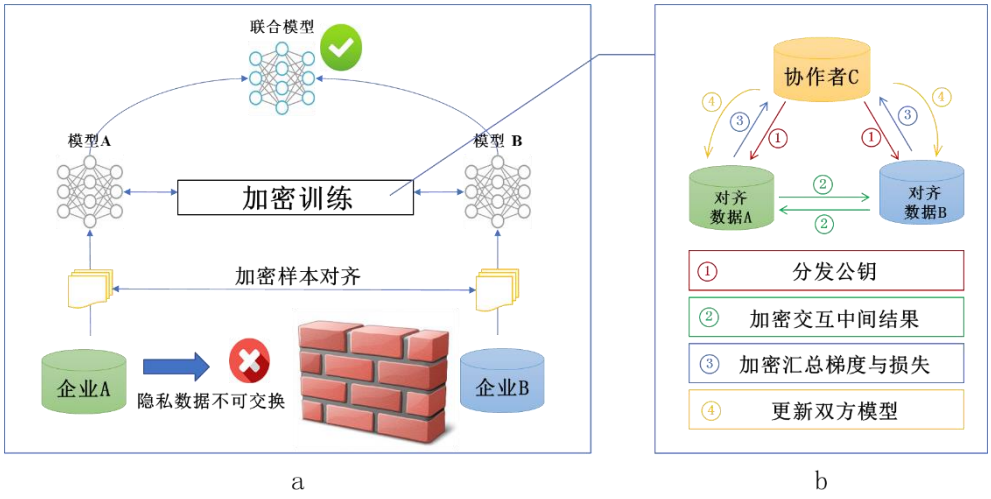

图 2 联邦学习系统构架

第四章 联邦学习与现有研究的区别

作为一种全新的技术，联邦学习在借鉴一些成熟技术的同时也具备了一定的独创性。下面我们就从多个角度来阐释联邦学习和其他相关概念之间的关系。

4.1 联邦学习与差分隐私理论的区别

联邦学习的特点使其可以被用来保护用户数据的隐私，但是它和大数据、数据挖掘领域中常用的隐私保护理论如差分隐私保护理论（Differential Privacy）[1]、k 匿名（k-Anonymity）[2]和 l 多样化（l-Diversity）[3]等方法还是有较大的差别的。首先联邦学习与传统隐私保护方法的原理不同，联邦学习通过加密机制下的参数交换方式保护用户数据隐私，加密手段包括同态加密[10]等。与 Differential Privacy 不同，其**数据和模型本身不会进行传输**，因此在数据层面上不存在泄露的可能，也不违反更严格的数据保护法案如 GDPR 等。而差分隐私理论、k 匿名和 l 多样化等方法是通过在数据里加噪音，或者采用概括化的方法模糊某些敏感属性，直到第三方不能区分个体为止，从而以较高的概率使数据无法被还原，以此来保护用户隐私。但是， 从本质上来说这些方法还是进行了原始数据的传输，存在着潜在被攻击的可能性，并且在 GDPR 等更严格的数据保护方案下这种数据隐私的保护方式可能不再适用。与之对应的，联邦学习是对用户数据隐私保护更为有力的手段。

4.2 联邦学习与分布式机器学习的区别

同时横向联邦学习中多方联合训练的方式与分布式机器学习（Distributed Machine Learning）有部分相似的地方。分布式机器学习涵盖了多个方面，包括把机器学习中的训练数据分布式存储、计算任务分布式运行、模型结果分布式发布等，参数服务器（Parameter Server）[4]是分布式机器学习中一个典型的例子。参数服务器作为加速机器学习模型训练过程的一种工具，它将数据存储在分布式的工作节点上，通过一个中心式的调度节点调配数据分布和分配计算资源，以便更高效的获得最终的训练模型。而对于联邦学习而言，首先在于横向联邦学习中的工作节点代表的是模型训练的数据拥有方，其对本地的数据具有完全的自治权限，可以自主决定何时加入联邦学习进行建模，相对地在参数服务器中，中心节点始终占据着主导地位，因此联邦学习面对的是一个更复杂的学习环境；其次，联邦学习则强调模型训练过程中对数据拥有方的数据隐私保护，是一种应对数据隐私保护的有效措施，能够更好地应对未来愈加严格的数据隐私和数据安全监管环境。

4.3 联邦学习与联邦数据库的关系

联邦数据库系统（Federated Database System）[5]是将多个不同的单元数据库进行集成，并对集成后的整体进行管理的系统。它的提出是为了实现对多个独立的数据库进行相互操作。联邦数据库系统对单元数据库往往采用分布式存储的方式，并且在实际中各个单元数

据库中的数据是异构的，因此，它和联邦学习在数据的类型与存储方式上有很多相似之处。但是，联邦数据库系统在各个单元数据库交互的过程中不涉及任何隐私保护机制，所有单元数据库对管理系统都是完全可见的。此外，联邦数据库系统的工作重心在包括插入、删除、查找、合并等各种数据库基本操作上面，而联邦学习的目的是在保护数据隐私的前提下对各个数据建立一个联合模型，使数据中蕴含的各种模式与规律更好地为我们服务。

第五章 联邦学习的应用实例

联邦学习是否有价值，取决于联邦学习的关键应用场景。只有通过联邦学习的应用实例化，才能发现联邦学习在发展中所遇到的各种挑战和机遇。下文我们将介绍两个联邦学习的典型应用场景。

5.1 智慧金融

联邦学习作为一种保障数据安全的建模方法，在销售、金融等行业中拥有巨大的应用前景。在这些行业中，受到知识产权、隐私保护、数据安全等诸多因素影响，数据无法被直接聚合来进行机器学习模型训练。此时，就需要借助联邦学习来训练一个联合模型。

以智慧零售业务为例，它的目的是利用机器学习技术为用户带来个性化的产品服务，主要包括产品推荐与销售服务。智慧零售业务中涉及到的数据特征主要包含用户购买能力，用户个人偏好，以及产品特点三部分，但是在实际应用中，这三种数据特征很可能分散在三个不同的部门或企业。例如，银行拥有用户购买能力的特征，社交网站拥有用户个人偏好特征，而购物网站则拥有产品特点的特征。这种情况下，我们面临两大难题：首先，出于保护用户隐私以及企业数据安全等原因，银行、社交网站和购物网站三方之间的数据壁垒是很难被打破的。因此，智慧零售的业务部门无法直接把数据进行聚合并建模；其次，这三方的用户和用户特征数据通常是异构的，传统的机器学习模型无法直接在异构数据上进行学习。目前，这些问题在传统的机器学习方法上都没有得到切实有效的解决，它们阻碍着人工智能技术在社会更多领域中的普及与应用。

而联邦学习正是解决这些问题的关键。设想一下，在智慧零售的业务场景中，我们使用联邦学习与迁移学习对三方的数据进行联合建模。首先，利用联邦学习的特性，我们不用导出企业的数据，就能够为三方联合构建机器学习模型，既充分保护了用户隐私和数据安全，又为用户提供了个性化，针对性的产品服务，从而实现了多方共同受益。同时，我们可以借鉴迁移学习的思想来应对用户和用户特征数据异构的问题。迁移学习能够挖掘数据间的共同知识并加以利用，从而突破传统人工智能技术的局限性。可以说，联邦学习为我们建立一个跨企业、跨数据、跨领域的大数据 AI 生态提供了良好的技术支持。

5.2 智慧医疗

如今，智慧医疗也在成为一个与人工智能相结合的热门领域。然而，目前的智慧医疗水平还远没有达到真正“智慧”的程度。下面，我们将通过 IBM“沃森”的例子探讨目前智慧医疗的不足之处，并提出一种利用联邦迁移学习提高智慧医疗水平的构想。

IBM 的超级电脑“沃森”是人工智能在医疗领域最出名的应用之一。在医疗领域，沃森被中国、美国等多个国家的医疗机构用于自动诊断，主攻对多种癌症疾病的确诊以及提供医疗建议。然而，沃森也在不断遭受着外界的质疑。最近曝光的一份文件显示，沃森曾经在一次模拟训练中错误地开出了可能会导致患者死亡的药物。沃森医疗项目也因此备受打击。那么沃森为何会做出错误的诊断呢？我们发现，沃森使用的训练数据本应包括病症、基因序列、

病理报告、检测结果、医学论文等数据特征。但是在实际中，这些数据的来源却远远不够，并且大量数据面临着标注缺失的问题。有人估计，把医疗数据放在第三方公司标注，需要动用 1 万人用长达 10 年的时间才能收集到有效的数据。数据的不足与标签的缺失导致了机器学习模型训练效果的不理想，这成为了目前智慧医疗的瓶颈所在。

那么，如何才能突破这一瓶颈呢？我们设想，如果所有的医疗机构都联合起来，贡献出各自那一部分数据，那将会汇集成为一份足够庞大的数据，而对应的机器学习模型的训练效果也能得到质的突破。实现这一构想的主要途径便是联邦学习与迁移学习。它适用的原因有以下两个方面：第一，各个医疗机构的数据必然有很大的隐私性，直接进行数据交换并不可行，联邦学习则能保证不进行数据交换的同时进行模型训练。第二，数据仍然存在着标签缺失严重的问题，而迁移学习则可以用来对标签进行补全，从而扩大可用数据的规模，进一步提高模型效果。因此，联邦迁移学习必将在智能医疗的发展道路上扮演弥足轻重的角色。在未来，如果所有的医疗机构能建立一个联邦迁移学习联盟，那或许可以使人类的医疗卫生事业迈上一个全新的台阶。

5.3 联邦学习和“企业数据联盟”

联邦学习即是一个技术规范，也是一个商业模式。当大家意识到大数据的作用时，首先想到的是把各自的数据聚到一起，通过远程的处理能力来产生结果，再把结果下载到本地加以使用。云计算在这一需求中应运而生。但是，在隐私和数据安全的重要性，以及公司利益和数据绑定越来越紧密的时候，这一模式遭到挑战。

联邦学习的商业方式为大数据使用提供了一个新的范式。当各自的数据不足以建立理想的预测模型时，联邦学习的机制使得参与的机构和企业可以不交换数据，同时可以共同建模。如果利用区块链等共识机制，联邦学习的利益分配机制又可以合理建立，使得数据拥有方，无论大小，都有动力加入数据联邦，并得到应有的好处。我们认为，建立数据联邦的商业机制要和联邦学习的技术机制一同展开，我们也会在国内国际建立各种行业的联邦学习标准和规范，使得联邦学习能尽快落地。

第六章 联邦学习的发展路径

结合人工智能与大数据的发展环境，行业痛点与需求的实际情况，建议通过以下三个阶段来发展联邦学习：

6.1 建立联邦学习国内外标准

国内、国际上都在加速人工智能标准体系和相关标准的建设。国际标准化组织于 2017 年 10 月成立人工智能分技术委员会（ISO/IEC JTC 1/SC 42），美国、德国等国家提出了人工智能术语、参考模型标准项目提案。国内于 2018 年 1 月，在国标委和工信部的高度重视和指导支持下，成立了国家人工智能标准化总体组成立，集合国内在人工智能领域的重要企业和科研院所，推动我国人工智能标准体系的建设。

通过研制和建立联邦学习的国内标准（如团体标准和国家标准）与国际标准（如 IEEE 企业标准），制定联邦学习的算法框架规范，使用模式和使用规范，可帮助不同类别的企业在合作过程中合法合规的共同使用数据，在用户的隐私和数据安全的情况下，不同的数据实体合作共赢，建立更准确的数据模型。也给人工智能在不同产业的实际落地中或将遇到的问题，提供可行性依据。

6.2 建立行业垂直领域应用示例

联邦学习在产业场景中的实际落地，将给算法研究提供切实有效的支撑。应用场景可分为同构场景和异构场景。同构场景指的是两个企业属于相同或相近的领域，所拥有的数据性质相似，特征相近，但是样本不同。如在银行和金融机构间的合作，双方拥有的不同的用户样本，但是样本属性同质，这种场景下使用横向联邦学习，可达到将双方样本放到一起的建模效果。异构场景指的是两个企业分属不同的领域，所拥有的数据性质不同，特征不同，但是有重叠的样本 ID。比如银行与互联网公司之间的合作，双方有重叠的用户 ID，但是企业间各自拥有用户不同的特征，如银行有用户的收入和交易行为，互联网公司有用户的社交或出行行为，这种场景下使用纵向联邦学习建模，可达到特征增加的建模效果。两种场景下的应用均可使得比数据在本地单方建模更好。

推动联邦学习在行业垂直领域的应用尤其是异构场景下的应用，将建立一个基于联邦学习的新的数据商业模式和共同成长的大数据生态。

6.3 全面展开建立联邦数据联盟

联邦学习的新商业模式，需要一个商业联盟。这样的联盟应该有 N 个实体，加入联盟的实体，可以像朋友圈一样能够利用各自的数据联合建立模型。联邦数据联盟鼓励各方参与，联盟成员一方面进行垂直领域的合作，另一方面，联盟有明确的在不同场景下的激励机制和权益分享，可以使用区块链技术建立一个让参与各方都满意的一个共识机制来估计大家的贡献，以此奖励对联盟有作用的机构。既有共识机制，又有底层的联邦学习技术支撑，这样可

以设计出多个垂直领域的联邦学习联盟。比如，金融机构合作就有一个金融联邦联盟；而医疗领域的合作，可以建立一个医药联邦学习联盟。

第七章 总结展望

近年来，数据的孤岛分布以及对数据隐私监管力度的加强正在逐渐成为人工智能的下一个挑战，联邦学习的产生为人工智能打破数据屏障和进一步发展提供了新的思路。它实现了在保护本地数据的前提下让多个数据拥有方联合建立共有的模型，从而实现了以保护隐私和数据安全为前提的互利共赢。本文概括性地介绍了联邦学习的基本概念、构架与技术原理，并且尝试在一些应用场景中探讨联邦学习对人工智能发展的巨大助力。期待在不远的将来，联邦学习能够帮助打破各领域、各行业的数据壁垒，在保护数据隐私和安全的前提下形成一个数据与知识共享的共同体，并同时解决了奖励对联盟做出贡献机构的共识机制，必将能为人工智能带来的红利落实到社会的各个角落。

参考文献

[1] Dwork C. Differential privacy: A survey of results[C]//International Conference on Theory and Applications of Models of Computation. Springer, Berlin, Heidelberg, 2008: 1-19.
[2] Sweeney L. k-anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(05): 557-570.
[3] Li N, Li T, Venkatasubramanian S. t-closeness: Privacy beyond k-anonymity and l-diversity[C]//Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on. IEEE, 2007: 106-115.
[4] Ho Q, Cipar J, Cui H, et al. More effective distributed ml via a stale synchronous parallel parameter server[C]//Advances in neural information processing systems. 2013: 1223-1231.
[5] Sheth A P, Larson J A. Federated database systems for managing distributed, heterogeneous, and autonomous databases[J]. ACM Computing Surveys (CSUR), 1990, 22(3): 183-236.
[6] Konečný J, McMahan H B, Yu F X, et al. Federated learning: Strategies for improving communication efficiency[J]. arXiv preprint arXiv:1610.05492, 2016.
[7] McMahan H B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[J]. arXiv preprint arXiv:1602.05629, 2016.
[8] Hardy S, Henecka W, Ivey-Law H, et al. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption[J]. arXiv preprint arXiv:1711.10677, 2017.
[9] Pan S J, Yang Q. A survey on transfer learning[J]. IEEE Transactions on knowledge and data engineering, 2010, 22(10): 1345-1359.
[10] Hesamifard E, Takabi H, Ghasemi M. CryptoDL: Deep Neural Networks over Encrypted Data[J]. arXiv preprint arXiv:1711.05189, 2017.
[11] https://www.eugdpr.org
[12] http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm
[13] http://www.npc.gov.cn/npc/xinwen/2017-03/15/content_2018907.htm
[14] https://zhuanlan.zhihu.com/p/42646278 杨强：GDPR 对 AI 的挑战和基于联邦迁移学习的对策
[15] https://zhuanlan.zhihu.com/p/41052548 机器之心专访杨强教授：联邦迁移学习与金融领域的 AI 落地