腾讯安全
Tencent Security

腾讯安全

联邦学习应用服务白皮书

2020 年 4 月 17 日

目录

第一章 联邦学习发展概况

1.1 联邦学习从何而来

随着云计算和大数据技术的不断发展，无论是机构还是个人，每天都会源源不断地产生大量数据；与此同时，随着人工智能技术〔Artificial Intelligence，AI〕和数据处理能力的提升，不断产生的海量数据能够被实时地进行计算、分析与挖掘。理论上，大数据与人工智能技术的完美结合，能够充分挖掘和释放数据的价值。然而，现实中，由于数据中包含大量个人隐私、商业机密等，数据隐私安全的问题也广泛受到世界各国重视，相继出台了欧盟《通用数据保护条例》〔GDPR〕、美国《美国加州消费者隐私法》〔CCPA〕、新加坡修订《个人数据保护法案》、中国《信息安全技术网络安全等级保护基本要求》等。现实中的"数据壁垒"形成了大量的"数据孤岛"，导致大数据与人工智能的结合并不完美，数据价值并未被充分挖掘和释放。

针对隐私保护的问题，"联邦学习"的概念最早于 2016 年由谷歌研究科学家 H.Brendan McMahan 等提出[1]。它是指多个客户〔如移动设备、机构、组织等〕在一个或多个中央服务器协作下协同进行去中心化机器学习〔Decentralized Machine Learning〕的设置。在去中心化机器学习的过程中，联邦学习能够保证每个客户的隐私数据不出本地，从而降低了传统中心化机器学习〔Centralized Machine Learning〕带来的隐私泄露风险和因数据泄露带来的相应成本。随后，围绕着"联邦学习"这一主题，越来越多学术研究成果开始出现。典型的成果包括如何实现多方的数据加密和应用、如何实现分布式去中心化机器学习、如何在利用多方隐私数据的前提下保证人工智能的效果等。相关研究成果组成了"联邦学习"的整体解决方案。

换言之，是隐私保护的需求与传统中心化机器学习在隐私保护方面的局限与挑战，催生了"联邦学习"。从技术角度，"联邦学习"是一种跨学科的解决方案，集合了机器学习、统计学、加密学、分布式、系统、安全等学科的技术。这种跨学科的合作，让很多领域的技术可以有机地结合在一起，创造出有趣的可能性，同时也提出新的挑战。

在利用人工智能进一步挖掘大数据潜在价值的大趋势下，"联邦学习"已经实质上成

为了当下以及未来一段时间内，推动人工智能和机器学习商业落地的关键能力之一。

1.2 人工智能与数据现状

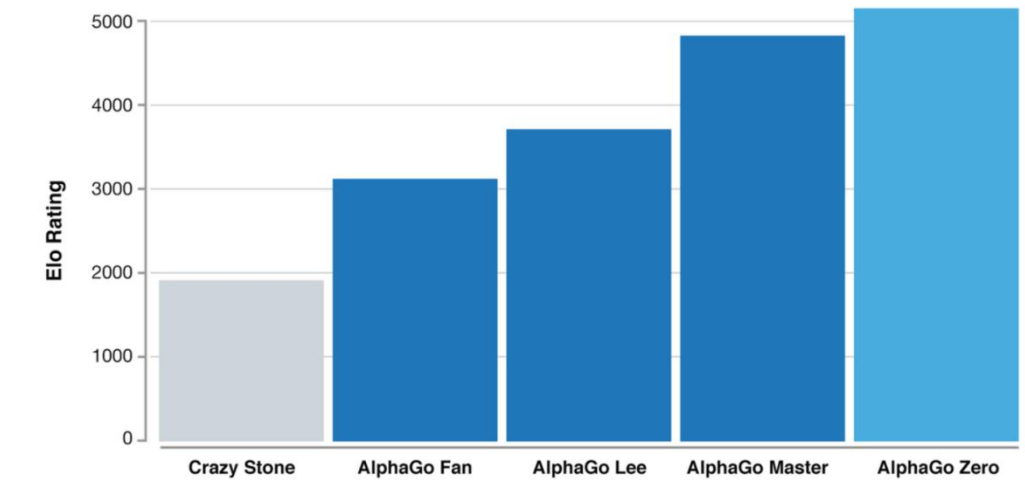
人工智能的本质，是制造出一种能够与人类智能相仿的具有独立处理事件或者思考能力的智能机器。

截至目前人工智能取得最大突破的机器学习，可以归纳出一个流程：

- 人类参考自身的神经元结构和功能，设计出数字化的节点模型；
- 人类参考自身神经元之间的互相作用、协作规律，设计出多种由节点组成的神经网络模型；
- 针对特定的场景和已有数据，人类设定、调成出特定的神经网络模型；
- 将标记好的大量数据，提供给计算机，让计算机根据这些数据进一步迭代神经网络模型，直到这个神经网络模型能够完美适应这些数据；
- 将训练之后的神经网络变成一个固定的“工具”，然后只需要将新的数据导入，就能够得到人工智能计算的结果。

这个流程好比造剑：设计神经网络节点、设计神经网络分别就是挑选基础的材料、铸造剑的毛坯；如何在毛坯之上塑造成剑最终的形状、如何给剑烤蓝防止氧化、如何磨出最锋利的剑刃，其实都是通过数据来“锤炼”。

以 2015 年的 AlphaGo 为例，它在围棋这个项目上实现了对人类的超越，间接带动了新一波的人工智能浪潮。聚焦到 AlphaGo 从最初立项时略弱于人类一般职业选手，到超越人类最顶尖职业选手的整个过程，它经过了包括神经网络、产品实现逻辑在内的数次升级。数据是这个升级过程中的唯一主轴，一开始 AlphaGo 所能使用的是 16 万盘人类棋谱，到最后已经能自我对弈，生成无穷无尽的新棋谱进行学习。



〔图 1：AlphaGo 版本迭代，围棋实力不断提升〕

不可否认的是，围棋是一个极度理想化的存在，有限的棋盘位置上，只有黑白子。现实中的问题，远不像围棋这样清晰而理想化，在应用人工智能的过程中，就对数据产生了更大的要求。

〔图 2：腾讯自动驾驶 TAD Sim 仿真平台〕

以自动驾驶为例，在大规模的真车实际道路测试的同时，包括腾讯在内的许多公司都专

门构建了用于模拟真实场景的系统，用以生成更多可用于训练自动驾驶的数据。但目前我们仍未能实现超越人类驾驶水平的自动驾驶。

回归到人工智能的发展趋势上，显然需要从自动驾驶这样仍需时日的应用转向更加实际、商用化的思路，即深入到各个已经数字化的场景中去，用最短的时间、最低的成本、最有效的人工智能算法，进一步挖掘潜藏的数据价值，带来切实的经济利益。

第二章 我们为何需要联邦学习

2.1 数据的现实状况

现实世界中，人工智能所需的数据，大多都会以“数据孤岛”的方式分布。这种物理和逻辑层面的障碍，直接影响了人工智能应用中的表现：各个“数据孤岛”之间的数据难以融合，无法以整体训练人工智能；若以单个“孤岛”的数据对人工智能训练，最终人工智能的效率又相当有限。

“数据孤岛”的产生难以避免，现实中国家、企业、组织都会出于安全的考虑，将大部分自己的数据保存在特定的物理空间中；其次是逻辑上，不同数据生成方的数据规范也存在不同，即便想要融合数据也无法轻易完成。

2.2 数据法规的新挑战

重视数据隐私和安全，近年来已经成为数据领域的最重要趋势。2018 年中，欧盟带头建立新法案《通用数据保护条例》(General Data Protection Regulation, GDPR)[2]，其中对企业使用用户数据进行了仔细而全面的规定。随之而来的，是对于企业的实际处罚。

截止至 2019 年 9 月 24 日，22 家欧洲数据监管机构对共 87 件案件作出了总计 3.7 亿欧元的行政处罚决定。从被罚款金额最大的英国航空 50 万乘客信息泄露案，到对公民在自家门窗安装过多摄像头的象征性处罚。

中国在 2017 年起实施《中华人民共和国网络安全法》[3]和《中华人民共和国民法总则》，明确了网络运营者不得泄露、篡改、毁坏其收集的个人信息。同时，新的《个人信息保护法》、《数据安全法》也在从草案落实成法案的过程中，届时，用户数据隐私和安全管理将会更加严格，这也对人工智能数据的收集与使用造成了直接的影响。

2.3 联邦学习的核心思路

假如我们将多方拥有的、具有利用人工智能挖掘价值潜力的数据看作“起点”，最终生成的可应用于单独一方原始数据的神经网络看作“终点”，保证两点之间的数据安全，显然需要的是一个整体方案。严格来说，它已经不是一个“纯粹”的机器学习，而是一个以机器学习为核心，分别对接“起点”和“终点”的框架。

再进一步，为了要实现数据安全、隐私的绝对保障，同时也是为了符合当下及未来全球的数据法规，各方的原始数据不可以上传汇总，只应该留存在“本地”〔物理位置可以在云端〕。

因为数据不可以上传汇总，所以训练神经网络所需的资料，需要通过其他不危及数据安全、隐私的方式进行传递，最终的解决方法是用在本地训练出来的神经网络替代。

截至目前，机器学习虽然由人类参考自己的神经网络架构创造，目前仍旧是一个“黑盒子”模型，即人类目前仍很难解释神经网络的内部规律。背后原因主要有两点：一是人类对于生物神经系统、尤其是人类自己的大脑，仍知之甚少；二是计算机本身的整套二进制符号系统，与人类的图形、文字符号系统不完全对应。

通过上传本地训练的神经网络，本地数据的相关特征被留存在网络当中，但同时，神经网络中不包含原始数据、且无法直接还原原始数据，数据的安全、隐私性得以确保。

保障了数据，最终的应用效果就成为另外一个关键：数据上传汇总进行机器学习，是最简单而且能确保效果的；为了实现“额外”的数据保障，最终的机器学习架构必须变得更加“复杂而曲折”。

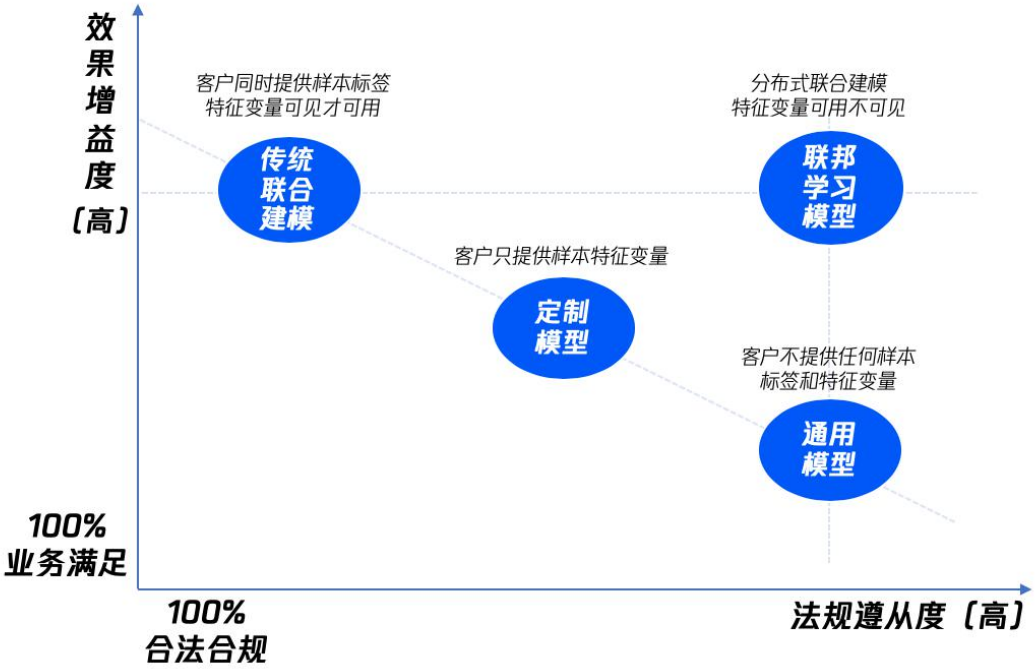
以上面提到的用本地训练的神经网络传递数据特征这个环节为例，不同参与方的本地数据机器学习过程也必须“协调而统一”，否则即便上传了也无法进行整合。然后是最终的效果，本地训练的神经网络中的特征如何完整地提取、整合到最终的模型当中，能够实现接近甚至等同于传统集中机器学习的效果，也是一个考验。

总结起来，联邦学习的核心思路其实可以这样概括：在人工智能取得长足进展的背景下，树立并且坚持严格的数据保障要求，利用消耗更多的计算机资源，来实现人工智能时代的“保护隐私前提下的数据挖掘”。多方共赢的机器学习方式，有助于打破数据孤岛、提升 AI 的应用效率，在市场监管、跨部门合作、数据隐私保护等领域，有着非常广阔的应用前景。

第三章 腾讯安全联邦学习应用服务产品介绍

3.1 关于腾讯安全联邦学习

腾讯安全联邦学习应用服务通过低成本快速迭代的联合建模服务，能够在保护所有参与方隐私的同时，有效释放出各方大数据生产力，广泛适用于业务创新的应用场景。

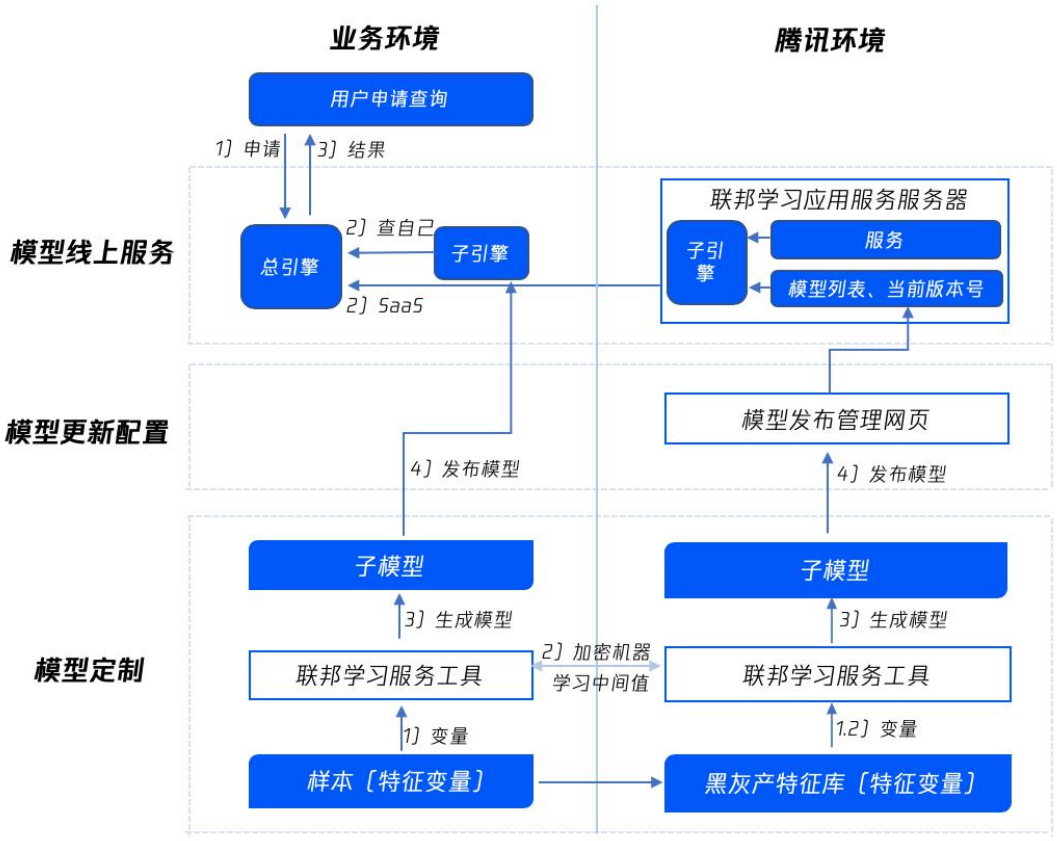


〔图 3：腾讯安全联邦学习应用服务综合优势〕

不论何种联合建模方式，都是在满足了现有的合规和业务需求的条件下，对于降本增效的追求。与传统的联合建模相比，联邦学习建模采用加密交换机器学习的中间结果完成联合建模，在保持效果增益的情况下，对法规的遵从度更高。

根据具体应用场景下数据的组织和使用形式不同，腾讯安全联邦学习应用服务技术分为“纵向”[4]和“横向”两种。

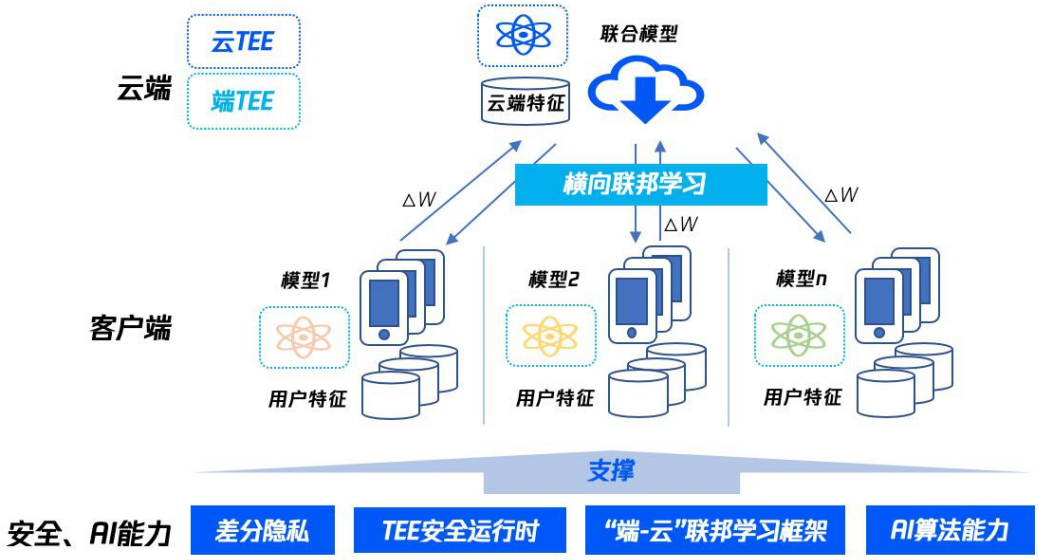
3.2 腾讯安全纵向联邦学习应用服务



〔图 4：腾讯安全纵向联邦学习应用服务架构〕

主要针对拥有异构数据的机构，如银行、电商等，通过融合多个机构对相同样本的不同观察进行 AI 联合建模。腾讯安全联邦学习应用服务目前聚焦银行、消金、互金等金融机构的信贷审批难题，提供安全、合规、高效的联合建模服务，下一步会延展到其他行业业务创新服务。

3.3 腾讯安全横向联邦学习应用服务



〔图 5：腾讯安全横向联邦学习应用服务架构〕

横向联邦学习应用服务主要针对拥有同构数据的大量终端用户，如互联网 APP 用户，通过融合终端用户对相同设备或应用的不同体验进行 AI 联合建模。在经用户授权后，联合建模过程中，用户的个人隐私均不出个人终端设备〔如：手机、平板〕，从而保证了个人隐私安全。腾讯安全支持海量互联网用户参与对用户有价值的联合建模，基于腾讯安全自研的可实际部署在移动设备〔如：安卓手机、平板、IoT 设备等〕上商用的“端-云”横向联邦学习应用服务框架，提供对用户有价值的应用服务。

3.4 腾讯安全联邦学习应用服务的优势

3.4.1 保护隐私、大数据分析能力强、接入便捷，模型高效

作为“PaaS+SaaS 级”联邦学习产品，腾讯安全联邦学习应用服务具备安全性高、大数据分析能力强、接入便捷、高效率和成本低的四大优势：

- 充分满足企业机构隐私保护和数据安全的需求；
- 助力客户充分挖掘大数据生产力。腾讯安全 20 余年来累积了大量的黑灰产库，

形成了包含百亿点、千亿边的黑灰产知识图谱，安全服务已经覆盖中国 99% 的网民，形成了独有的优势；

- 便捷接入，聚焦业务场景所需的联合建模功能，支持容器化便携安装部署，轻量易用；
- 腾讯安全联邦学习在联合建模过程中的通信、稳定性上具有优势。通过通信次数优化、中间结果压缩，减少了联合建模过程中需要传输的数据量，提高效率；另外对于网络环境造成的传输中断，专门打造了模型的断点备份功能，即便数据传输中断也能断点重启，而无需再从零开始。此外，无需外派专业人员出差，通过远程操作、低成本快速迭代的方式完成模型训练。

3.4.2 开放合作，协同性高

腾讯是国内最早倡导“联邦学习”的企业之一，其联邦学习技术已覆盖 PaaS 级和 SaaS 级领域，形成产业链协同互补关系，从而提升腾讯安全联邦学习技术的附加值。

〔图 6：腾讯公司联邦学习技术协同〕

在 PaaS 级层面，腾讯微众银行〔WeBank〕提出了工业级别联邦学习框架——联邦学习开源项目 Federated AI Technology Enabler(简称 FATE)；腾讯 TEG 数据平台部基于自研分布式机器学习平台 Angel，设计了一种“去中心化”的联邦学习框架 PowerFL，并研发了 FM、神经网络等联邦学习算法。腾讯安全对这两种计算框架进行了云化部署，形成了 PaaS 级联邦学习服务。

在 SaaS 级层面，腾讯安全联邦学习应用服务基于自身海量安全大数据，提供安全、合规、高效的联合建模服务，并通过部署在云端的 SaaS 服务进行输出，帮助企业机构用户快速应用联邦学习技术成果；同时支持海量互联网用户参与对用户有价值的联合建模，在个人隐私数据均不出个人终端设备的情况下实现有价值的数据应用。

第四章 腾讯安全联邦学习应用服务案例

目前，腾讯安全联邦学习应用服务适用于金融风控、营销风控、智能终端等领域。

4.1 金融风控领域应用

场景ID	场景名称	适用对象
1	通用	数据驱动型业务均可适用
2	银行	银行风控、大数据等部门
3	信用卡	金融机构信用卡中心
4	消费分期	消费金融公司、持牌互金平台
5	信用贷	消费金融公司、持牌互金平台

〔图 7：腾讯安全联邦学习应用服务在金融风控领域应用场景〕

4.1.1 行业痛点

在金融风险识别过程中，金融机构引入第三方大数据能力当前普遍采用的方法是接入第三方通用模型进行辅助判断。而通用模型普遍存在对业务匹配度不高，效果不理想的情况。信用卡在实现智能化管理的过程中也面临同样问题。

4.1.2 江苏银行合作

江苏银行不仅是第一家通过联邦学习实现融合腾讯安全黑灰产库的银行，也是第一家借力腾讯业务环境，实现信用卡智能化管理、助力信用卡盈利规模化的银行。2020 年 4 月，双方联合共建“智能化信用卡管理联合实验室”，围绕联邦学习开展深入合作，推动 AI 技术与信贷风控结合，开启信用卡智能化经营之路。

早在 2015 年，江苏银行就与腾讯公司探索开展联合贷款业务，并逐步建立战略合作伙伴关系。在联邦学习领域，双方再次携手，联合共建‘智能化信用卡管理联合实验室’，运用联邦学习技术这一先进的加密算法确保数据安全，将腾讯生态特征变量与江苏银行信用卡特征变量进行融合，实现双向赋能。

此前，江苏银行与腾讯安全基于联邦学习技术对智能化信用卡经营进行了联合开发和方案部署，在保障双方信息安全的前提下，在信用卡接入规模化、盈利规模化方向上取得技术突破，并于 2020 年 3 月 6 日国内首家上线。在联邦学习技术的支持下，双方共同进行金融风控模型训练，提升模型效果，既保障了数据资产的所有权，又实现了特征变量的共享。联邦学习技术还实现了合作双方建模人员线上分析与建模，有效节约人力成本与财务成本。江苏银行与腾讯安全的联邦学习建模仅用 3 天就完成部署，几个小时内完成远程模型训练，建模效率相比之前有较大提高，对互联网用户欺诈风险识别能力更强、覆盖面更广。

4.1.3 济宁银行、消金机构合作

腾讯安全协助济宁银行建设线上信贷业务系统，通过联邦学习技术在“数据不出域”的前提下联合构建反欺诈模型、画像模型，模型效果显著提升。在丰富银行的大数据信

贷风控能力同时实现优质客群优质定价，既满足了银行实际管理需求，资金又得到高效使用。

与湖北消金、玖富数科、嘉银金科等机构，腾讯安全通过联邦学习进行反欺诈模型的协同训练。数据始终没有离开各自本地，有效解决了在联合建模过程中各方面临的隐私保护问题；同时实现融合双方特征，让模型效果达到最佳；比起通用模型的测试结果，基于联邦学习的联合建模效果提升 20%。

4.1.4 行业应用优势

数据隐私保护：在整个联邦学习建模过程中，各方的特征变量均不出自己的私有域模型业务匹配度高：联邦学习继承了定制模型的优点，为具体业务进行模型定制。联邦学习训练出的模型对业务的适配度更高，效果更好。

总体成本低：利用联邦学习，金融业务可以更快速的迭代模型，因而能够更敏捷地适应市场变化，提升业务的竞争力。

复用性高：腾讯安全的联邦学习应用服务，集成了标准化的软件和工具，在训练阶段和生产阶段均采用容器化部署，同时支持在私有环境和公有云上部署。腾讯安全联邦学习应用服务的高复用性，使各种类型的金融机构都能方便快捷的接入。

4.2 营销风控领域应用

在营销风控领域，腾讯安全研发了航空票务营销风控场景联邦学习应用服务。

场景ID	场景名称	适用对象
1	航空票务营销风控	航空公司

〔图 8：腾讯安全联邦学习应用服务在营销风控领域应用场景〕

腾讯安全通过“联邦学习”为四川航空打造出全票务智能营销风控中台。在用户信息不出域的条件下，腾讯安全与四川航空实现模型差异梯度交换，完成黑产欺诈模型联合建模。建模后的票务欺诈模型有较好的欺诈识别效果，已经在四川航空的 APP、官网订票渠道中上线。

4.3 智能终端领域应用

在智能终端领域，腾讯安全通过自研的“端-云”横向联邦学习框架，成功将联邦学习应用服务拓展到互联网海量终端设备之上，从而形成一个以智能终端〔如：安卓手机、平板、IoT 设备〕为计算节点、大规模分布式联邦学习框架。目前，横向联邦学习能够支持个人相册类业务的精细化管理。

场景ID	场景名称	适用对象
1	个人相册类业务	个人相册类APP厂商

〔图 9：腾讯安全联邦学习应用服务在智能终端领域应用场景〕

以个人相册类业务为例，通过预测并展示用户可能喜爱的照片，能够提供更好的用户体验。基于腾讯安全的“端-云”横向联邦学习应用服务框架，业务 APP 可以在终端设备上根据用户的行为〔如：停留在每张照片上的时间、操作等〕对用户照片的喜好进行本地建模；通过将生成的不泄露用户隐私的中间结果进行加密传输，并在腾讯安全联邦学习后台安全聚合为统一模型，从而实现在不触及用户隐私的前提下对用户个性化喜好进行建模，模型准确率提升了约 10%。

在“合作共享、多方共赢”的开放原则下，腾讯安全将持续聚焦各个行业领域的实际需求，提供合规安全、高效便捷的联邦学习应用服务，携手合作伙伴，助力 AI 等数字化技术在更大范围内落地，从而助推数字产业的发展。

第五章 展望

放眼人工智能的整体发展趋势，2000 年后取得重大突破的机器学习，还将作为人工智能的主要“突破口”，数据也将扮演整个人工智能实现过程中的关键点。

在实际操作中，对数据要求少、能够本地完成训练的人工智能应用会优先落地。剩下的是需要联合才能够凑齐足够训练数据的，以及联合之后都凑不齐足够数据的。这三种类型的场景，大致的占比是一个从塔尖到底座的金字塔型。

换言之，通过应用联邦学习，这个链接分散、孤岛化原始数据，通过以机器学习为核心、数据管理、调用为辅的整体框架，最终生成最为高效神经网络的新发展思路，人工智能的应用推广很有希望再次迎来一波快速增长。

腾讯安全联邦学习应用服务的推出，正是顺应这一行业大趋势，同时也是为了满足客户的需求，通过低成本的联合建模服务，在保护隐私的同时，有效释放出大数据生产力。

对于最前沿人工智能应用技术的跟进，也是一次宝贵的、深入理解联邦学习思路的机会，尤其是如何跨学科解决人工智能问题，这种思路未来必然会生成新的人工智能解决能力，给未来的人工智能予以更多的启示。我们相信，通过应用和理解联邦学习能力，我们有能力进一步将人工智能的红利，更好地传递到客户以及现实用户手中。

参考文献

[1] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017.

[2] General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] 《中华人民共和国网络安全法》, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[4] 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. arXiv:1711.10677, 2017.

关注公众号
了解更多

腾讯安全
Tencent Security