CAICT 中国信通院

联邦学习场景应用研究报告

（2022 年）

中国信息通信研究院泰尔终端实验室

2022 年 2 月

版权声明

编制说明

本报告编写参与单位: 中国信息通信研究院、卓信大数据计划、开放星云计划、铸基计划、杭州锘崴信息科技有限公司、北京百度网讯科技有限公司、北京明略软件系统有限公司、第四范式(北京)技术有限公司、北京智慧易科技有限公司、深圳市洞见智慧科技有限公司、同盾科技有限公司、光之树（北京）科技有限公司、上海富数科技有限公司、零氪科技 (北京)有限公司、OASES 智能终端安全生态工作委员会。

前　言

数据作为数字经济和信息社会的核心资源，被认为是继土地、劳动力、资本、技术之后的又一个重要生产要素，其在企业数字化转型中发挥重要作用，并对国家治理能力、经济运行机制、社会生活方式等产生深刻影响。与此同时，数据安全的重要性愈发凸显。依法采取严密的监管措施，保障数据安全无虞，有利于为数字经济发展夯实安全基础，为国家安全和公共利益保驾护航。

2021年以来，《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》相继实施，个人隐私和产业机密数据保护日趋完善，在着重强调数据安全和个人信息保护的同时，完善了数据相关合规监管框架，为数据流通和使用进一步拓展了空间。

与此同时，以联邦学习技术为代表的隐私计算赛道产业生态逐渐丰富，互联网厂商、初创专精型厂商、人工智能厂商等各领域企业纷纷加入，在进一步加深技术研究的同时，相关垂直领域的行业应用也逐渐丰富，形成百花齐放的行业发展态势。

本报告在中国信息通信研究院前期对于联邦学习技术、产业的研究基础上，联合联邦学习产业链上下游企业，深入探讨联邦学习在政务、医疗、金融、广告、物流的应用价值，以期为数据应用价值的释放带来解读和参考。

目 录

图 目 录

表 目 录

一、联邦学习简介

(一) 数据隐私安全及孤岛问题

数据孤岛普遍存在于所有需要进行数据共享和交换的系统之间，包括不同部门之间的数据信息能不能共享、不同公司之间的数据信息能不能共享，以及不同产业之间的数据能不能共享等等。

在 2019 年中国互联网协会对外公布的《中国网民权益保护调查报告》显示，在 2019 年，七成左右的网民个人身份信息和个人网上活动信息均遭到泄露。78.2%的网民个人身份信息(姓名、学历、家庭住址、身份证号及工作单位等)被泄露；63.4%的网民个人网上活动信息(通话记录、网购记录、网站浏览痕迹、IP 地址、软件使用痕迹及地理位置等)被泄露。近半数的网民个人通讯信息(即时通讯记录、手机短信等)被泄露。2019 年因个人信息泄露导致诈骗信息、诈骗消息等原因，导致网民总体损失约 805 亿元。

2021年以来，关于用户隐私泄露、数据违规的负面事件频发，公众对于数据安全和隐私保护越发关注。《数据安全法》《个人信息保护法》等相关法律法规的颁布和实施也从法律层面为数据安全和个人隐私提供了根本保障，同时也促进了以联邦学习为代表的隐私行业的飞速发展。

(二) 联邦学习定义

联邦学习（Federated Learning）本质是一种分布式机器学习框架，它做到了在保障数据隐私安全及合法合规的基础上，实现数据共享，共同建模。它的核心思想是在多个数据源共同参与模型训练时，不需

要进行原始数据流转的前提下，仅通过交互模型中间参数进行模型联合训练，原始数据可以不出本地。这种方式实现数据隐私保护和数据共享分析的平衡，即“数据可用不可见”的数据应用模式。

（三）联邦学习主要作用

随着信息化社会的发展，各行业积累了大量的数据，这些数据掌握在不同的实体手中，受技术、安全和监管等的限制，无法有效的分享融合，形成一个个独立的数据孤岛；而互联网和移动互联网时代的发展，加速了数据的碎片化。数据里面蕴含着重要模式（Pattern），如人类生物特征、喜好、金融信用等等。通过机器学习技术可以挖掘数据中蕴藏的这些模式，这些经过大量数据训练出来的机器学习模型已经应用在各行各业，例如医疗行业的临床辅助诊断、新药物研发、精准医疗；安全行业的人像识别、声纹识别等等。在这些应用中，模型的精度至关重要，而模型的精度核心依靠训练数据，只有经过大量数据的训练，才可能获得好模型。

另一方面，由于法律政策监管、数据隐私安全等方面的顾虑，各数据所有者也不愿直接交换原始数据，导致数据无法有效汇聚，从而影响机器学习的效果，制约着 AI 模型的提高。联邦学习正是为了解决这一两难情况而出现的高效技术解决方案。

（四）联邦学习技术优势

传统的机器学习需要将数据汇聚到中心后才可以进行模型训练。在此过程中需要转移存储原始数据，随着数据量的增加，相对的成本也呈指数级增加；同时，在数据出域后，数据将变得不可控，从而导

致数据隐私泄露，埋下数据安全隐患。图 1 给出了传统机器学习和联邦学习的对比。联邦学习技术，可以实现多个机构间构建统一的数据安全、高效、合规的多源数据应用生态系统，实现跨机构的数据共享融合，通过系统扩大样本量、增加数据维度为大数据应用提供高精度模型构建的有力支撑，进而提供更丰富、高质量的大数据服务，为社会发展创造更多价值。

来源：中国信息通信研究院

图 1 传统机器学习和联邦学习的对比

二、联邦学习发展历程

(一) 传统隐私保护

传统的隐私保护手段包括数据脱敏、假名化、数据消隐等。数据脱敏是信息从原始环境向目标环境交换过程中，对数据中的某些敏感信息进行一定规则的数据变形，其核心是通过剔除数据中能识别出个体的所有特征，从而达到隐私保护的目的。在涉及商业机密和个人隐私数据时，在不违反相关规则的条件下，对原始数据进行改造后才可提供使用，如个人姓名、手机号、身份证号、企业财务数据、税务、

供应链等机密数据，都需要进行脱敏处理。数据脱敏常用方法有泛化技术、抑制技术、扰乱技术、有损技术等，目前，各企事业单位，尤其政府部门均建立健全了数据脱敏的规范，数据脱敏已成为数据处理的标准流程。

数据消隐和脱敏类似，但又与脱敏不同的是，数据消隐并不会直接剔除敏感的标识符或准标识符，而是通过泛化或抑制来消除数据中能够直接识别个体的部分，以避免隐私泄露。主流实现技术包括 K-匿名、L-多样性、T-亲密度以及近年发展起来的差分隐私。然而，大量研究表明，这些传统的数据保护技术其保护能力并不完善，并不能完全保证数据的隐私安全，仍然存在系统性的漏洞使其隐私保护能力大打折扣。此外，由于对原始数据的处理，在很多场景中处理后的数据并不能满足应用的需求。例如生物信息的基因数据，包含了独特的遗传标记，这些信息可用于家族血缘搜索，通过将脱敏后的受试者与身份已知的远亲联系起来，还是可以识别受试者身份。因此，基因数据脱敏不足以保护隐私，我们需要更完善高效的技术解决数据共享过程中的隐私安全问题。

(二) 联邦学习

为了让数据共享更简易，同时又能保障数据安全，出现联邦学习技术框架。它可以做到在数据不流动的前提下进行数据融合共享与价值挖掘。

联邦学习进行模型训练时，需要根据数据来源对任务进行分解，多个分中心在本地利用各自数据资源进行分布模型训练，相互独立又

彼此协作。它的技术理论基础可追溯到分布式数据库（distributed database）联合分析技术，Cheung 等人在 1996 年提出了分布式数据库中实现关联规则（Association Rules）挖掘。 因为联邦学习涉及到数据源分布形态的不同，比如有些联邦网络中数据源之间样本上的重叠度比较多，有些则在特征属性结构上比较一致。根据不同的数据源分布联邦学习采用的分布式算法逻辑也有差异。例如，2006 年，Yu 等人提出了带有隐私保护的分布式支持向量机建模，并支持处理横向和纵向分割的数据场景。联邦学习在与产业的融合上最先是医疗领域。2013 年，王爽教授团队首次发表全球第一篇联邦学习论文，正式提出了分布式隐私保护与在线学习等概念，解决了医疗领域多中心合作难题，其成果被应用于国家级生物医疗健康数据网络中，用于保护数十家医共体中的数千万病人的数据隐私。

之后，联邦学习在其它领域的应用也取得了显著性进展，如 2016 年起，谷歌在其安卓手机端实现带有隐私保护的横向联邦学习，用于保护手机用户数据隐私。此后，杨强教授在 2019 年通过将迁移强化学习与联邦学习进行结合，服务于自动驾驶场景。

（三）安全联邦学习

联邦学习虽然只传递中间计算结果，保障了原始数据的安全性。但在有些情况下，中间参数如果被攻击，还是能够还原出原始数据，因此也存在一定的安全隐患。

为了弥补普通联邦学习技术中存在的补足，学术界和工业界提出了安全联邦学习。分别采用了不同的解决方案。其中基于硬件的可信

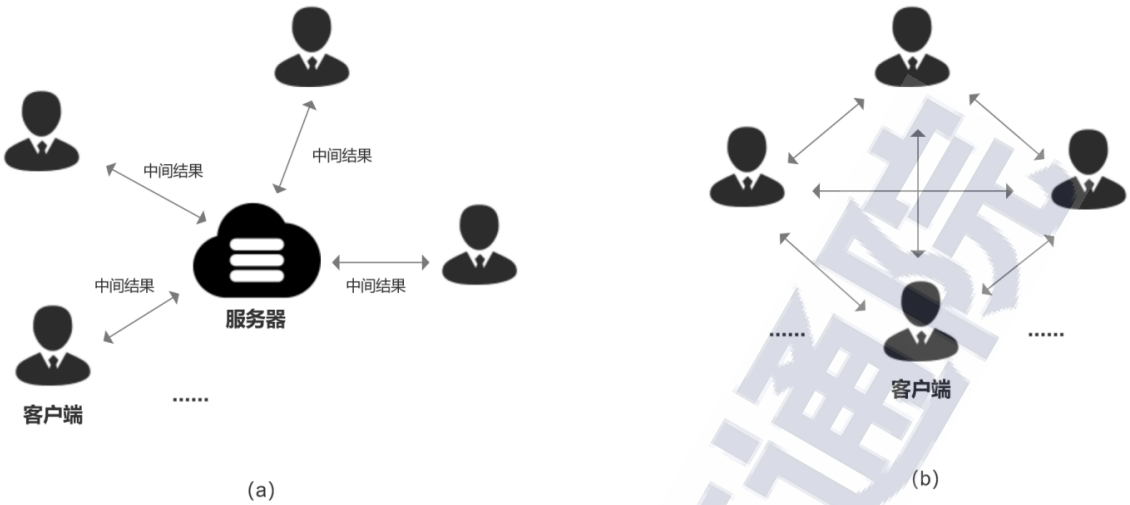
计算方案，可以保护整个计算过程安全可靠。基于同态加密或多方安全计算的密码学方案可以保障中间参数及结果发放不被攻击。而基于差分隐私的统计学方案则保证了过程与结果数据的安全性，但同时也引入了一定的计算误差。不同技术路线的保护能力、计算能力和安全信任模式也不尽相同。

安全联邦学习综合利用上述技术，可以补足普通联邦学习中对于计算过程和最后结果的隐私保护缺失，为数据流通全链路提供隐私保护。同时，经过算法优化，能够处理海量数据，满足特定业务场景的需求。

三、联邦学习进阶

(一) 主要技术原理

联邦学习是一种在计算过程中分享中间统计结果而不泄露原始数据的分布式算法框架，实现了数据在多中心协同计算中的隐私保护。其特点是在保护原始数据隐私安全的同时，又能保证计算结果准确性和精度。联邦学习一般认为有两种架构：客户端/服务器模式（图 2.a）和去中心化模式(图 2.b)。



来源：杭州锘崴信息科技有限公司

图 2 联邦学习的两种架构模式

客户端/服务器模式一般适用于预测全局模型参数和开展各种统计学检验。目前这种方式比较常见。它的本质是在中心节点的主导下，各节点协同分布式计算，在联邦学习的训练过程中，各个参与方拥有基于其本地数据生成的本地梯度，通过反复交换各参与方的本地梯度来实现全局模型参数的更新，并直到模型参数收敛，具体每一轮的迭代过程可分为如下几步：

a. 参与方在本地进行基于原始数据的隔离计算，各自使用本地样本完成模型的更新，发送加密的梯度到聚合服务器。

b. 聚合服务器对各方的梯度进行聚合，根据各个客户端的本地统计结果更新全局模型参数。

c. 聚合服务器把聚合更新后的梯度发送给各个参与方。

d. 各个参与方使用收到的新梯度更新本地模型参数。

这里示例中传递的是梯度，也可以是模型参数或者其它模型中间计算结果。设计合理的梯度的聚合方式和模型拆分方式不会影响最终的模型精确度。

去中心化模式使用于各种分布式算法，比如稀疏线性回归，主成分分析以及支持向量机等等。其特点在于不需要中心服务器，各个相邻的客户端不断交换本地计算的中间结果，进而得到进度可靠的全局计算结果。无论哪种架构，联邦学习实体之间只传输中间结果，中间结果不涉及任何原始数据信息，从而实现了敏感数据的隐私保护。

(二)联邦学习的分类

1.按数据本部模式

（1）横向联邦学习

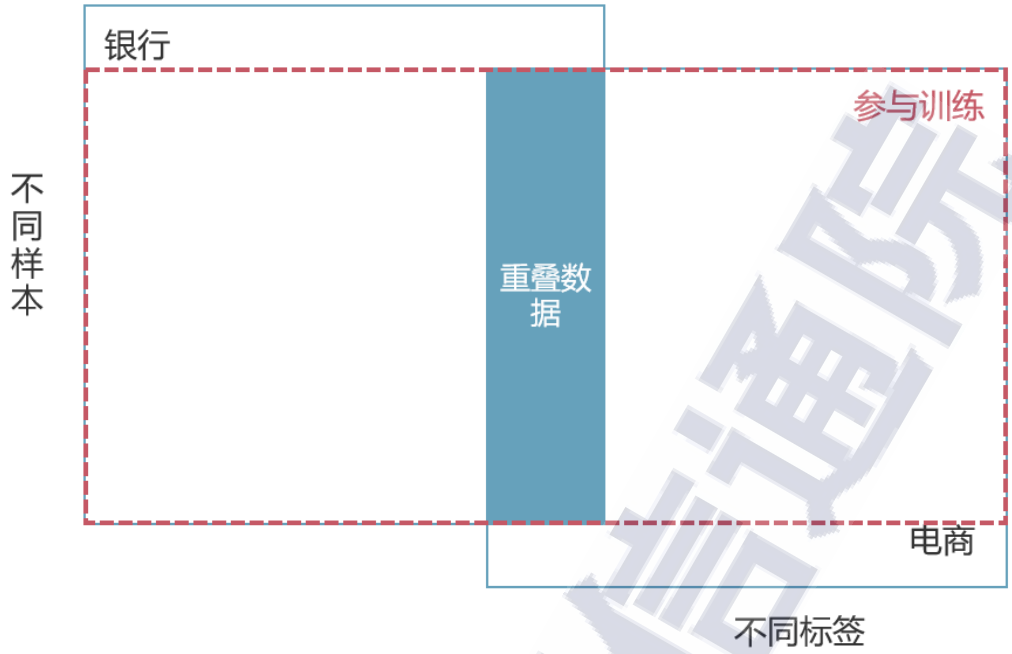
横向联邦学习的本质是样本的联合，适用于参与机构间业态相同但触达客户不同场景，这种情况往往特征重叠多，用户重叠少（如图 3 所示）。比如罕见病研究中，每个医院病例的数据维度基本一致，但它们分别有自己不同的病人，并且病例样本有限，通过联邦学习可以让这些来自不同机构的样本在保障隐私的前提下共享，提高模型训练的能力。又如，不同地区的银行间，他们的业务相似，但用户不同。

来源：中国信息通信研究院

图 3 横向联邦学习数据分割示例

（2）纵向联邦学习

纵向联邦学习的本质是特征的联合，适用于各参与机构间用户重叠多，特征重叠少的场景（如图 4 所示）。比如同一地区的银行、电商公司、运营商。他们的用户集可能包含该区域的大多数居民，但银行记录了用户的收支行为相关数据，电子商务保留了用户的购买行为相关数据，运营有用于的未知数据，所以其特征空间有很大的不同。假设我们希望基于用户的购买、收支、位置数据进行信用等级评估，需要融合三方数据做回归模型。纵向联邦学习是将这些不同的特征聚合在一起，以一种隐私保护的方式计算训练损失和梯度的过程，以便用双方的数据协作构建一个模型。

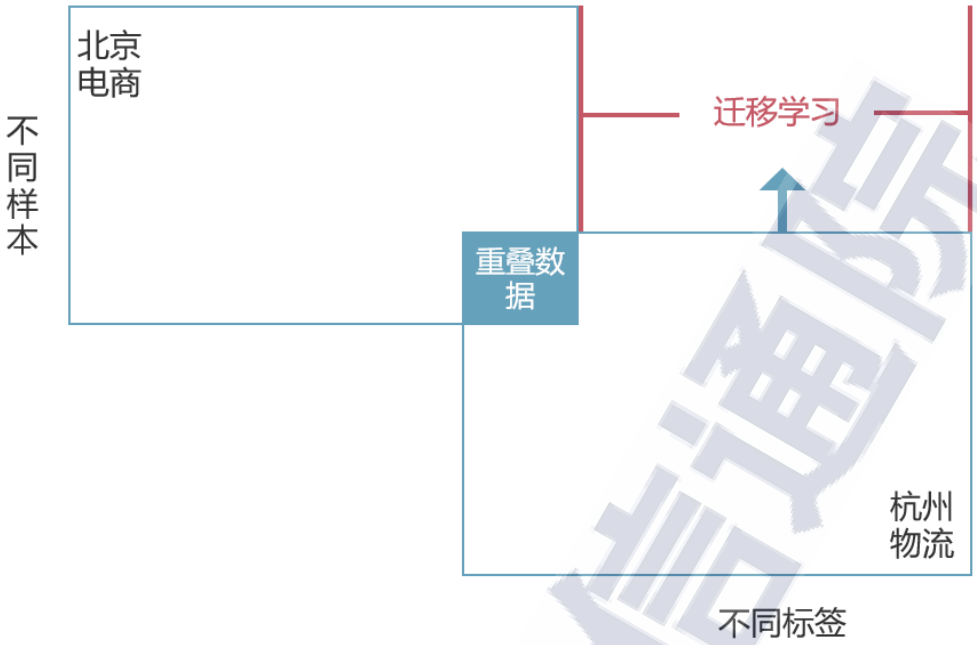


来源：中国信息通信研究院

图 4 纵向联邦学习数据分割示例

（3）迁移学习

迁移联邦学习适用于两个数据集的重叠较少，不仅样本不同，而且特征空间也有很大差异的场景下（如图 5 所示）。比如两个机构，一个是位于北京的电商平台，一个是位于杭州的物流公司。由于地域限制两个机构的用户群交叉点小，由于业务不同，双方的特征空间重叠也少。这种情况下可以利用迁移学习来克服数据与标签的不足，需要从公共样本获取公共表示，用于获取具有单侧特征的样本预测。迁移学习是对现有联邦学习的一个重要扩展。



来源：中国信息通信研究院

图 5 迁移学习数据分割示例

2.按拓扑结构

拓扑结构是指分布式系统中各个计算单元之间的物理或逻辑的互联关系。如图 6 所示，联邦学习按其参与方的数据网络结构主要可分为：星状结构、环状结构和点对点结构。

（1）星型结构

星型拓扑结构中，联邦学习网络的各参与者通过点到点的方式连接到一个中央节点上。该中央节点作为协调者与公信方向目标节点传送信息。中央节点执行通信控制策略，任何两个节点的通信都要经过中央节点。目前大部分联邦学习系统是基于星状网络结构进行部署，即包括本地计算节点和全局协同服务节点。它在联邦学习中的作用在

于全局协调本地节点，协助它们本地模型更新，进行计算任务分发以及最终模型结果的汇集。它有如下两点：

a. 控制简单。任何参与方只与中央节点通信，访问协议与介质访问控制方法都很简单。

b. 故障诊断与隔离都很容易。中央节点对地方节点可以逐一隔离进行故障检测，单个参与方故障不会影响全局。

问题主要是对中心节点的依赖太大，以及随着网络规模的扩大节点维护与协调成本线性增长。所以它比较适用于小型网络。

（2）环形结构

但是在有些情况下由于网络条件或者应用场景的限制，无法使用全局协同节点，环形联邦学习 [1]模式也被提出。环形结构是使用一个连续的环将每个节点连接在一起，没有中心节点。它能够保证一各节点上发送的信号可以被环上其他所有的节点都看到。环形结构的优势就是实现简单，对网络条件要求低，劣势就是使用场景有限，没法做复杂的协同任务。在简单的环形网中，网络中任何部件的损坏都将导致系统出现故障，这样将阻碍整个系统进行正常工作。而具有高级结构的环形网则在很大程度上改善了这一缺陷。

[1]J.-W. Lee, J. Oh, S. Lim, S.-Y. Yun, and J.-G. Lee, “TornadoAggregate: Accurate and Scalable Federated Learning via the Ring-Based Architecture,” arXiv [cs.LG], Dec. 06, 2020. [Online]. Available: http://arxiv.org/abs/2012.03214

（3）点对点

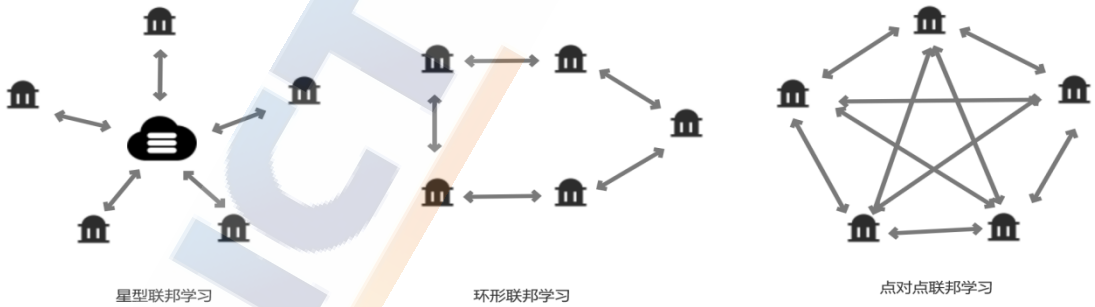
点对点联邦学习[2]跟环形结构一样实现了去中心化，联邦网络之间的各参与者都处于对等的地位，有相同的功能，无主次之分，一参与者既可作为业务方，发起建模和推理研究，也可作为特征方，提供数据源。它具有以下的优势:

a. 不需中央节点，可在网路的各个节点共享内容和资源。

b. 易于扩展，不受结构限制，也不存在增加中央节点的协调维护成本。

c. 参与方的资源和算例普遍不会有太大差别，资源利用率较高。

点对点联邦学习实现了去中心化的联邦学习范式，但是其也引入了很大的计算和通讯的成本，要想保证计算性能与客服安全隐患对结构性设计要求较高。比较使用于大型网络。



来源：杭州锘崴信息科技有限公司

图 6 联邦学习参与方的数据网络结构

[2] S. Warnat-Herresthal et al., “Swarm Learning for decentralized and confidential clinical machine learning,” Nature, vol. 594, no. 7862, pp. 265–270, Jun. 2021.

3.按模型精度

根据不同级别的模型精确度，联邦学习可以分为无损联邦学习和近似联邦学习。

（1）无损联邦学习

联邦学习的本质是各节点协同分布式计算，在联邦学习的训练过程中，各个参与方拥有基于其本地数据生成的本地梯度，通过反复交换各参与方的本地梯度来实现全局模型参数的更新，并直到模型参数收敛。根据梯度的聚合方式和模型拆分方式的不同会会影响最终不同的模型精确度。

其中无损联邦学习可以保证通过虚拟数据融合生成的全局模型完全等效于(比如，在模型参数和性能等各方面)数据汇总后的模型。目前在常用的机器学习算法中基本已经做到了无损联邦学习。

（2）近似联邦学习

近似联邦学习的目标是保证通过虚拟数据融合生成的全局在模型的某些性能上和数据汇总后的模型相当（比如在预测精度）[3]。造成联邦学习结果有损的大致原因有:

a. 在联邦学习模型融合的时候，没有采用严格的梯度交换进行模型迭代，而是直接在本地各自训练模型，然后再讲参数加权平均。这种方式在水平训练的时候可以得到比较精确的近似结果。

[3]P. Kairouz et al., “Advances and Open Problems in Federated Learning,” arXiv [cs.LG], Dec. 10, 2019. [Online]. Available: http://arxiv.org/abs/1912.04977

b. 在使用联邦学习的同时，加入了其它隐私计算安全保障技术，比如同态加密在做同态乘法规约时会造成计算误差，差分隐私在引入噪音时，也会造成不完全精准。

近似联邦学习也有它的使用场景，实际中，会根据需要在安全性、准确性、计算性能等方面做一定平衡。

(三)联邦学习模型

目前基本上各类常用的机器学习算法都可以采用联邦学习的方式进行模型训练，可分别支持结构化、文本、图像等类型数据源，可在样本分类、回归预测、图像识别、基因分析、自然语言等场景进行应用。

1.结构化数据

该场景下算法要处理的样本是结构化数据，比如可以以标准的格式存在数据库的二维表中，可用于分类与回归预测等分析。该类算法的数据源一般包括若干个特征变量及一个预测变量。常用的算法有感知器、逻辑回归、多元线性回归、随机森林、朴素贝叶斯、支持向量机等。其中多元线性回归可用来对样本预测值进行连续数值预测，比如根据用户的基本信息、历史消费记录等数据预测他的信贷信用值；其余可对样本进行分类，比如根据用户画像预测他是否某一产品的目标用户。根据数据来源的分布是垂直还是水平，以上每种算法又可分为同质、异质。比如逻辑回归有同质逻辑回归（水平逻辑回归）、异质逻辑回归（垂直分割逻辑回归）。

2.非结构化数据

该场景下算法要处理的样本是非结构化数据，比如文本、序列化二进制数据等数据。可在自然语言处理（NLP）、语音识别等场景应用。支持它的常用算法包括深度学习等,在实际计算过程中通常需要将非结构化数据通过词嵌入（word embedding）等方法进行向量化表示后进行相关统计分析。在该类算法的联邦学习中，根据数据源的分布特征同样可分为垂直跟水平学习两种。

3.基因数据

基因数据可用于全基因组关联分析等研究。比如从人类全基因组中找出序列的变异位点，即单核苷酸多态性 (Single Nucleotide Polymorphisms, SNPs)。通过对基因数据的研究分析可以找出与疾病相关的 SNPs，帮助进行疾病诊断和预防。基因数据在经过处理后也可转化为结构化数据，可以利用一系列统计学方法进行分析研究。在全基因组研究的联邦学习中，不同医疗机构或部门共同提供患者基因或其它健康指标相关的数据源，进行联合模型训练。

4.图像数据

图像数据可作为图像识别模型训练时的样本数据，所产生的模型广泛的应用于图像搜索、产品识别、自动驾驶、安防等不同领域。比如在使用卷积神经网络进行图像识别或目标检测时，用户只需要输入图片，系统利用卷积窗口计算出特征值，再对中间特征通过分类或回归计算进行图像分类与目标定位。该类算法的联邦学习一般采用水平分割的方式，在多模态场景理论上也支持垂直分割。

(四)联邦学习能力

联邦学习是一种在计算过程中分享中间统计结果而不泄露原始数据的分布式算法和框架。自王爽教授团队 2013 年发表后受到空前的重视，被认为是兼具隐私保护和跨机构数据共享的技术解决方案。通过联邦学习框架可以连接多个不同的数据源，实现数据的安全共享，其在数据共享过程中只交换加密的中间计算参数，而不需要交换原始数据，同时达到数据共享和隐私保护的双重目标。但是具体分析研究表明，普通的联邦学习还是存在一些风险和问题。

在没有加密计算的情况下，在联邦学习阶段，每次迭代时需要交换数据源方的中间统计信息，这些信息可用于推断来自数据源的敏感私有输入数据。例如，成员资格和重建攻击是针对联邦学习的热门攻击。研究结果表明，对攻击者可以通过分析中间结果推断数据源中是否存在确切的某个个体；而在联合图像处理中，交换的梯度可以用来获取部分原始图像信息。

另一方面，联邦学习本身无法支持许多数据预处理步骤，而这些对于后续步骤中的数据分析至关重要，例如重复数据消除、样本对齐、参数对齐、数据筛选等。传统的解决方案（如基于哈希的算法）容易受到字典和/或侧通道攻击，这些攻击可能会泄露敏感的输入和结果信息。

具体实践中联邦学习不支持模型评估阶段的隐私保护。模型评估阶段还包括许多敏感信息，如模型参数（如商业机密）、模型输入数据（例如用户信息）、模型结果（例如诊断结果）等。由于一般联邦

学习不提供模型评估过程中的隐私保护，上述敏感信息将会泄露给模型计算方。还有一点是联邦学习不能保护数据完整性，联合计算服务器可以在学习阶段伪造中间结果，并且其他参与者可能无法检测到。

简而言之，联邦学习是一种可以减少机器学习阶段交换的个体信息的有效参考技术框架，但是如果只单纯依赖联邦学习技术是无法确保在整个数据分析阶段最终保护敏感的私有数据。

（五）联邦学习流程

正如前文所说，联邦学习在狭义上仅指隐私保护下实现机器学习算法的模型训练，本身不包括数据预处理、特征工程等机器学习必要步骤。实际应用落地中的联邦学习通常会涉及样本对齐、联邦数据预处理，联邦特征工程，联邦模型训练，联邦在线推理等建模全流程。

1.样本对齐

根据联邦学习的分类模式，样本对齐可分为纵向联邦学习场景中的样本 ID 对齐和横向联邦学习场景中样本特征对齐。其主旨是在保护各自样本非交集的前提下，实现样本的求交，从而进行后续的建模流程。采用的主流技术包括基于哈希的算法、基于 RSA 等非对称加密技术、基于不经意传输（OT）等密码学协议等。

2.联邦特征工程

特征工程是机器学习中至关重要的步骤，好的特征工程往往可以达到事半功倍的效果，在联邦学习中同样适用。为保护各自数据隐私，联邦特征工程包括联邦特征分箱、联邦相关性分析、联邦特征选择等。除了支持对本地数据的直接特征预处理（如：异常值清洗、缺失值清

洗、特征无量纲化（标准化、归一化）、特征分箱、特征编码、特征衍生、特征变换、特征交叉等）、相关性分析（如 IV 值、woe 值，斯皮尔曼相关系数等）及基于特征工程的特征选择，还应包含跨资源的联邦场景下实现。

3.联邦模型训练

根据实际应用场景，构建联邦学习场景下的分类（如：逻辑回归、支持向量机、随机森林、朴素贝叶斯等）、回归（多元线性回归、广义线性回归等）、无监督（k-means、PCA、embedding 等）等联邦学习模型。

4.联邦在线推理

模型训练完成后，需要部署到实际的生产环境中，对实时样本进行推理，得到联邦学习的预测值。这一阶段，除了对安全性的考量外，对效率（如每秒相应的请求数（Query Per Second））也有很高的要求。

四、安全联邦学习

隐私计算是指在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合。它的目标是在完成计算任务的基础上，实现数据计算过程和数据计算结果的隐私保护。

联邦学习是隐私计算最常用的技术手段之一，普通联邦学习存在中间参数被攻击风险，在具体实践中也不支持模型评估阶段的隐私保护，在一些隐私保护要求比较高的场景下，还是需要更高级别的安全技术。

业界相关研究人员提出了安全联邦学习，是将传统联邦学习跟可信执行环境、多方安全计算、密码学等其它隐私计算技术相结合，根据场景侧重点发挥各技术路线各自优势，克服弊端，综合应用相关技术实现的解决方案。其中，TEE 有相对较高的执行效率、较高的处理能力。多方安全计算能够比较好的处理两方或三方数据问题，密码学技术用于协助进行数据管理、身份认证等内容，区块链用于协助实现业务流程管理、审计管理、计费等功能。通过综合利用上述技术，经过算法优化，能够处理海量数据，满足特定业务场景的需求。可实现在符合我国的数据安全法、个人信息保护法以及 GDPR、HIPAA 等严格隐私保护法律法规情况下的多中心多维度实时大数据分析计算。

(一) 可信计算环境

2006 年 OMTP 工作组智能终端的安全团队率先提出了一种双系统解决方案：即在同一个智能终端下，除了多媒体操作系统外再提供一个隔离的安全操作系统，这一运行在隔离的硬件之上的隔离安全操作系统专门处理敏感信息以保证信息的安全，该方案即可信执行环境的前身。可信执行环境(Trusted Execution Environment, TEE)通过软硬件方法在中央处理器中构建一个安全的区域，保证其内部加载的程序和数据在机密性和完整性上得到保护。TEE 技术将硬件和软件资源划分为安全和非安全两个区域，需要隐私保护的操作在安全区域，其余在非安全区域。

在联邦学习的执行过程中，可以通过将中心节点部署在可信执行环境中，通过设备中的芯片和硬件系统提供一个隔离的运行环境，有

效保证在整个计算过程，中间数据、结果数据免受其它环境的恶意行为。

（二）多方安全计算

1981 年 Rabin 等人首次提出不经意传输（Oblivious Transfer，OT）协议，奠定了多方安全计算的理论基础。1982 年华人图灵奖得主姚期智教授开创性提出的百万富翁问题，引入了多方安全计算概念。多方安全计算（Secure Multi-Party Computation，MPC）是指多个参与方共同参与计算一个目标任务，并且保证在参与方不串谋的前提下，每一方仅获取自己的计算结果，无法通过计算过程中的交互数据推测出其他任意一方的输入数据。MPC 主要基于混淆电路（Garbled Circuit）、秘密分享（Secret Sharing）与不经意传输（Oblivious Transfer）技术。例如，秘密分享技术是将数据以某种方式进行拆分，拆分后的数据分配给不同的计算参与者后完成联合计算。

多方安全计算跟联邦学习类似，都是保障多方数据合作时的数据隐私安全，都需要多个数据源的合作；但联邦学习侧重于于多方的机器学习场景，而 MPC 更侧重于多方的通用计算函数，两者可以形成一个互补。

（三）同态加密

1978 年 Ron Rivest、Leonard Adleman Michael L.Dertouzos 提出了同态加密的概念。同态加密（Homomorphic encryption，HE）是一种允许在加密之后的数据上直接进行密文计算的技术，。利用同态加密可以实现数据存储和计算的安全外包。同态加密技术可以实现让拥

有私钥一方获得最后的加密计算结果，但参与同态加密计算方没法获得任何明文数据，从而可以保障信息安全性。同态加密也可以跟可信执行环境结合，在数据预处理、模型评估/推理等环节对传统的联邦学习进行补充。

此外，同态加密分为部分同态、半同态和全同态三种模式，其中部分同态算法支持加密数据的加法或者乘法运算中的一种，半同态和全同态算法同时支持加密数据的加法或者乘法运算，但是半同态加密的数据对于密文数据的累计计算次数有一定限制。在安全性上，基于格子的同态加密算法能够有较高的抗量子攻击能力。

（四）差分隐私

差分隐私（Differential Privacy）是 Dwork 在 2006 年针对统计数据库的隐私泄露问题提出的一种新的隐私保护定义，主要是通过在统计结果中加入随机噪声来避免由于数据变化导致的结果差异而泄露数据中的个人隐私信息。通俗的来讲，差分隐私就是确保任意单个记录在数据集中的变化（添加、删除、修改等），对于查询结果的影响微乎其微。攻击者无法通过观察由于某一个记录的变化导致的查询结果的变化来推测出个体的信息。它基于严格的数据理论，并假设攻击者可以使用任何背景知识来进行攻击，因此提供了很强的隐私保护能力。

差分隐私也可以跟联邦学习、多方安全等其它技术路线结合使用，用以提高隐私计算的性能及局部数据的安全性。例如采用差分隐私与多方安全计算、同态加密、TEE 等集合，可以减少噪音的添加，增加

数据的可用性。差分隐私通过引入扰动或噪音实现对于数据隐私的保护，可以用在对联邦建模的过程中或者建模结果加入噪音，保证攻击者难以从建模过程中交换的统计信息或者建模的结果反推出敏感的样本信息。

（五）安全性

通过综合利用上述技术，可以补足普通联邦学习中对于计算过程和最后结果的隐私保护缺失，为数据流通全链路提供隐私保护，在处理海量数据问题上，可以满足更广泛的业务场景需求。但不同技术路线在安全性上的能力范围各有差异。

表 1 从计算过程保护、计算结果保护以及安全信任模式等不同角度分析了基于不同隐私保护技术下的安全性能。数据计算过程的隐私保护指参与方在整个计算过程中难以得到除计算结果以外的额外信息，数据计算结果的隐私保护指参与方难以基于计算结果逆推原始数据信息。

1.可信执行环境

隔离的执行环境，为受信任应用程序提供了比普通操作系统更高级别的安全性。但 TEE 信任链对硬件厂商的信任依赖较高。TEE 支持恶意模型假设（malicious attack model），即计算的参与方可能做出任何行为，例如背离约定好的计算协议同时尽其所能地去获得其他方的敏感隐私信息。

2.同态加密

对计算过程有比较好的保护，支持在加密数据上进行直接的密文计算，但是在多个数据源参与的情况下，私钥管理需要依赖共信第三方。同态加密通常支持半诚实模型（semi-honest model），即计算的各个参与方在计算过程中时候会严格遵守协议规范，但会尽其所能地去窥探其他参与方的敏感信息。

3.联邦学习

通过中间参数交互而非个体数据的分享进行多中心的合作计算，从而实现对于多中心合作中的数据保护，但计算过程中的中间结果的交互存在可以反推原始数据的风险。联邦学习通过结合其他隐私计算技术，演化而来的安全联邦学习，可以有效的解决传统联邦学中相关问题。

4.多方安全计算

其安全性有严格的密码理论证明，各方通过机密分享等方式在不分享明文数据的情况下实现多方的联合计算。但是，如果 MPC 参与方存在串谋的情况，多方的数据存在隐私风险，同时 MPC 对于网络通讯的带宽要求较高。大多数 MPC 解决方案采用半诚实模型。

5.差分隐私

可通过引入噪音来保护结果数据，有科学的统计学理论依据，结果有一定误差。但是由于加入噪音的幅度和数据集本身以及具体应用的敏感度相关，通常比较适用于大规模数据集保护。

表 1 不同隐私保护计算技术的安全能力范围

类别	计算过程保护	计算结果保护	安全信任模式
可信执行环境	很高	无	硬件制造商与提供商，恶意模型假设
同态加密	高	无	同态加密秘钥管理方（共信第三方），通常为半诚实模型假设
联邦学习	中	无	交换的统计信息不会泄漏敏感的数据源信息
多方安全计算	高	无	无串谋，通常为半诚实模型假设
差分隐私	低	有	统计概率边界内的输出信息的隐私保护
安全联邦学习	很高	有	综合利用不同隐私保护计算技术，支持恶意模型假设、保护计算过程和计算结果。

来源：中国信息通信研究院

(六)性能

从计算性能、计算精度、硬件依赖、理论支持场景、计算模式等维度对隐私保护的不同技术路线进行比较。

1.可信执行环境

支持绝大多数场景下的复杂计算，计算执行效率与处理能力较高，对硬件有依赖。

2.同态加密

支持同态加法和乘法运算，需要通过加法和乘法的组合实现更高级计算的支持，通常需要引入近似计算来代替复杂计算函数。

3.联邦学习

支持高性能的带有隐私保护的多中心机器学习。数据源相互配合进行梯度与权重交换，计算精度可以达到跟传统机器学习无差异。。

4.多方安全计算

支持多种隐私计算算子但是其通讯和计算性能问题是一大挑战。

5.差分隐私

可以高效的处理大规模数据计算结果中的隐私保护问题，但会在计算结果中引入噪音和摇动。

表 2 隐私保护的不同技术路线

类别	计算性能	计算精度	硬件依赖	支持场景	计算模型
可信执行环境	高	高	有	复杂计算	中心化/分布式
同态加密	低	中	无	加法和乘法计算	中心化/分布式
联邦学习	高	高	无	多中心机器学习	分布式
多方安全计算	低	中	无	基本算子计算	分布式
差分隐私	高	低	无	结果保护	中心化/分布式

来源：中国信息通信研究院

五、应用场景

(一) 政务开放

2020 年 12 月 30 日，中央全面深化改革委员会第十七次会议审议通过《关于建立健全政务数据共享协调机制加快推进数据有序共享的意见》，强调要全面构建政务数据共享安全制度体系、管理体系、技术防护体系，打破部门信息壁垒，推动数据共享对接更加精准顺畅。这是继 2020 年 4 月 9 日《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》将数据上升为新型生产要素后又一重磅政策文件。

政务大数据蕴含着巨大的经济与社会价值，其开放与共享对于促进政府自身转型、社会需求获取模式转型、打造智慧城市以及产业经济转型都具有重要意义。当前我国政务大数据开放与共享的障碍还有很多，除了相关法律法规较为滞后等因素外，数据安全共享技术也是制约因素之一。产品应用在政务大数据领域，可以为政务大数据安全共享提供有效的技术保障和平台支撑，助力政府实现安全、可控的数据开发体系。

在政务数据开放共享的过程中，由于缺乏可信的数据资产权利确认方案，导致政府部门不愿意共享数据。因缺乏有效的隐私安全保护技术，数据共享后无法限制数据用途，导致数据滥用和隐私泄露等问题，政府部门也不敢共享数据。产品可以与大数据开发组件集成，打破政府部门数据孤岛，实现跨部门、与社会数据等安全共享。除了提供“脱敏”、“审计”和“细粒度权限控制”等措施外，可以实现数

据资源的定向使用，防范申请权限获批后的数据滥用或二次分发等行为导致的隐私泄露问题。在数据授权的同时会限制数据的使用方式和使用范围，与此同时提供硬件级的技术方案保障数据使用行为强制执行，可有效减少数据泄露风险。

(二) 医疗应用

生物医疗大数据是现代医学研究、药物开发、公共卫生防疫以及临床医疗应用的重要基础性资源。信息技术在生物医疗领域的研究包括疾病预测、医学影像识别、药物发现、基因测序等场景。在多年的生物医学信息学研究积累过程中，很多技术可对电子病历数据、影像数据、基因数据等生物医疗大数据进行分析和挖掘。而基于生物医学的算法或统计研究需要大量的样本，单一数据源很难满足海量的数据需求。需要有一个多数据源医疗数据共享平台，在能够保证数据源隐私安全的情况下又能够实现数据价值的共享。

1.全基因组关联分析

人类的很多疾病跟基因突变有关，比如肿瘤的生物学基础是基因的异常，它的发生是多基因、多步骤突变的结果。目前已发现多种肿瘤驱动基因突变，比如 EGFR、KRAS、NRAS 等。进行全基因组关联分析有利于提前预防疾病。

全基因关联分析(Genome-Wide Association Study, GWAS)是指从人类全基因组范围内找出存在的序列变异，即单核苷酸多态性(Single Nucleotide Polymorphisms, SNPs)，并筛选出与疾病相关的SNPs。已广泛的应用于临床的早期疾病筛查、用药指导及辅助诊断

等领域。它常用于肿瘤、糖尿病和高血压等复杂疾病的研究，利用 GWAS 对遗传机制的研究有助于开发新药物、发展新疗法和开展预防工作。

然而，GWAS 技术对医疗大数据的依赖性一直是其应用中的一大挑战：一是数据安全方面。该技术需要的数据包含大量敏感的个人信息，一项研究发现基于几十个基因位点（SNPs）数据就可以基本确定一个个体的身份。如何合理的保护这些敏感信息，规避不必要的隐私泄露风险便成为了广泛推行生物医疗数据分享和联合分析，以及多元医疗数据融合中关键的挑战之一。二是 GWAS 非常依赖大量基因数据的积累，样本量不足是各项 GWAS 研究中最常见的问题和难点。近几年，得益于基因测序技术的发展，我国已经建立了多样化、多维度的基因数据库，其中基因数据的积累也正以前所未有的速度不断推进。但这些基因库中的基因数据大多独立存在，缺乏关联和交互方式，形成了一个个的“数据孤岛”，使这些数据无法发挥出其全部价值，产生高耗能、高成本的负担，变成了“食之无味，弃之可惜”的无用资源。

一篇发表在 Briefing in Bioinformatics 期刊上的论文介绍了一个联邦学习应用的具体案例。这篇论文的创作团队设计并开发了一个基于安全联邦学习的技术框架：iPRIVATES[4]，为全基因组关联研究提供隐私保护，以解决基因数据共享中的隐私安全问题。

[4] X. Wu et al., “A novel privacy-preserving federated genome-wide association study framework and its application in identifying potential risk variants in ankylosing spondylitis,” Brief. Bioinform., vol. 22, no. 3, May 2021, doi: 10.1093/bib/bbaa090.

iPRIVATES 的框架中利用安全联邦学习技术，使多个机构能够联合执行基于虚拟融合数据进行 GWAS 分析。由于在研究过程中只交换经过处理的非敏感中间计算结果，因而不会泄露患者级别的基因分型数据，保证了整个计算过程中及结果的数据安全性。研究以强制性脊柱炎（AS）作为切入点，使用 iPRIVATES 进行全基因组分析，以识别人类基因组中具有潜在风险——可能导致 AS 的基因型主要分布在人类白细胞抗原（HLA）区域。iPRIVATES 框架融合多种技术和算法，可以支持联邦 GWAS 分析的可配置管道，能够灵活地集成和配置不同的 GWAS，方便识别 SNPs 与许多不同类型的特征（如某些重大疾病）之间的关联。

此外，团队为了证实基于 iPRIVATES 框架进行联邦学习结果的准确性，进行了与传统分析方法就此项研究的对比实验。分别使用模拟实验与真实数据（真实环境下跨多家医院的数据）两种方式来评估 iPRIVATES 的性能。实验结果表明，联邦学习与传统的集中式计算结果一致，证明它在保护数据隐私的同时，还能保证计算效果。

这也意味着，这一框架和相关技术在推动不同疾病的协同基因组研究方面的巨大潜力。在另一项针对川崎病的研究中，研究团队也同样使用了安全联邦学习的隐私保护技术框架开发了 PRINCESS[5]框架，支持了一项跨国（英国、美国、新加坡）遗传数据分析。研究的结果显示，PRINCESS 不仅可以保护数据的隐私安全，还具有较高的计算效率。

[5]F. Chen et al., “PRINCESS: Privacy-protecting Rare disease International Network Collaboration via Encryption through Software guard extensionS,” Bioinformatics, vol. 33, no. 6, p. 871, Jan. 2017.

同样的技术还可以扩展到肿瘤突变基因检测与预防、药物代谢基因分析等领域的研究应用。

2.围术期静脉血栓栓塞症预防

静脉血栓栓塞症（venous thromboembolism, VTE）是外科手术术后常见的并发症之一，是病人非预期死忙的重要因素，严重影响着患者的生活质量和生存状态，成为恶性肿瘤患者死亡的第二大原因。

而研究表明，恶性肿瘤本身也是 VTE 发生的高危因素之一，它会通过使患者凝血机制异常，分泌过多促凝物质，术后破坏血管系统纤维蛋白沉淀与降解平衡等方式，使机体有高血栓形成的倾向。特别是围术期 VTE 发生率较高。因此，如何降低恶性肿瘤围术期 VTE 发生率是我国胸外科医生面临的严峻挑战。

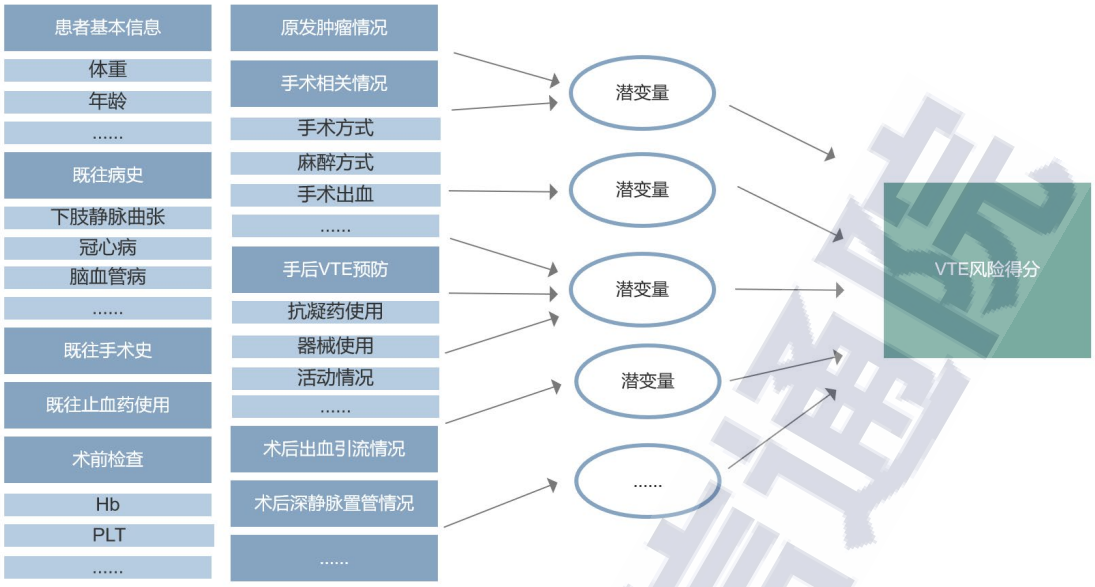
尽管国内外已有众多有关 VTE 防治的共识和指南，但针对恶性肿瘤围术期 VTE 预防的共识尚属空白。采用统计学及 AI 方法可以有效的研究 VTE 发生的相关因素，包括围术期和手术期两大部分高危因素，比如既往 VTE 史、创伤、卧床、高龄、内科基础、肥胖、吸烟、下肢静脉曲张、感染、药物使用等多方因素。进而总结原因，规范恶性肿瘤患者 VTE 预防的流程及方法，以期降低围术期 VTE 发生率。

有关这方面的研究已有一定成果，但针对特定疾病（比如肺癌、食管癌、结直肠癌等胸腹部恶性肿瘤）的围术期静脉血栓栓塞研究还需要进一步进行模型优化，以更有针对性的进行预防。然而这些研究需要大量的样本病例，特别是针对特定细分疾病的研究，单个医疗机

构没有足够的病例数据支撑研究得出科学的结论，而跨机构的数据融合共享，又在法律上存在极大的数据安全问题。基于加密技术的安全联邦学习成了当之无愧的解决方法。

在一项中国消化外科恶性肿瘤人群围术期 VTE 预防多中心队列研究中，基于类似 PRINCESS 框架，采用了安全联邦学习底层技术。多家三甲医院，联合多个科室将内部的病例数据在本地进行注册，数据源之间同时形成同构水平分割及机构垂直分割多种关系。终端节点分布式计算，中间参数加密后通过中心节点进行交换传输，完成了研究模型的联合训练。

如图 7 所示，该研究分别从患者基本信息、入院症状评估、既往病史、既往手术史、既往静脉血栓及预防情况、既往止血药使用情况、术前实验室检查情况、原发肿瘤情况、术中相关情况、术后预防用药情况、术后出血引流情况等多方面维度与 VTE 的最终发生情况进行了全方位相关性分析。最终得出了预测 VTE 发生的统计模型，可利用上述维度中可观测变量对 VTE 的发生概率进行了预估，从而平衡血栓栓塞发生风险与药物预防后大出血风险，根据实际情况做出精准判断，为实际决策提供指导意见。

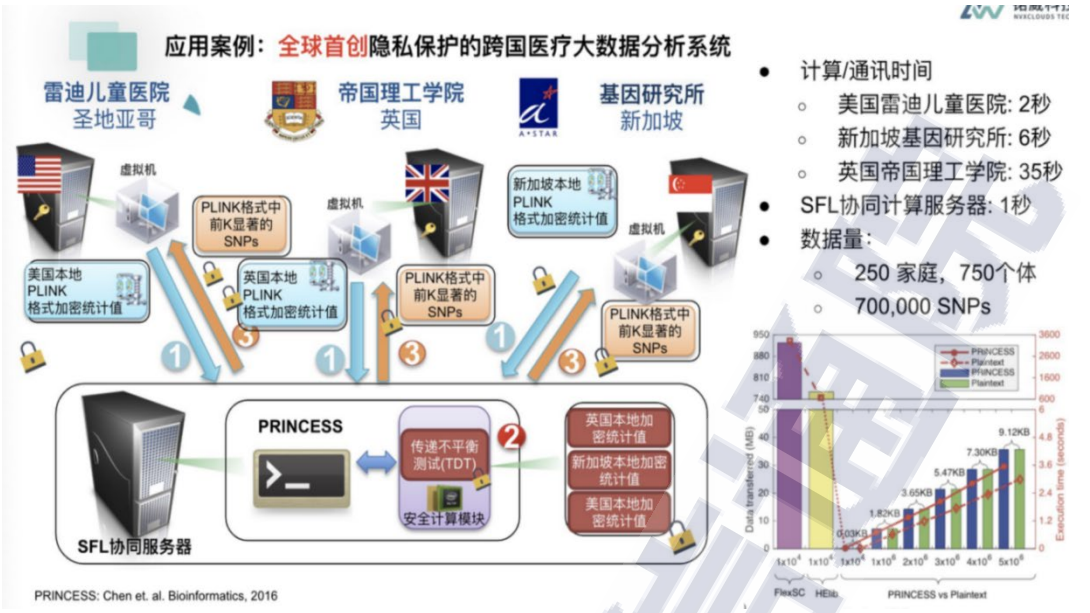


来源：杭州锘崴信息科技有限公司

图 7 VTE 数据分析示例

3.跨国川崎病联合研究

罕见疾病是医学研究中经常遇到的问题，但同一国家往往存在样本少，在不同医院分散等实际困难，极大的阻碍了相关研究，诊断治疗工作。针对罕见疾病（川崎病）的多中心国际研究中，通过采用王爽教授团队开发的基于 TEE 和安全联邦学习的 PRINCESS 隐私保护技术框架，支持全球首例跨国（英国、美国、新加坡）罕见病多中心遗传数据隐私保护分析。研究的结果显示，PRINCESS 不仅可以保护数据的隐私安全，还具有较高的计算效率。



来源：杭州锘崴信息科技有限公司

图 8 隐私保护的跨国川崎病研究

4.影像学深度分析引擎

健康医疗大数据时代，大量医疗数据被源源不断采集，并被使用到生物医学研究中。其中医学影像学数据是一个非常重要的组成部分。在医学影像实际问题中，人工智能模型精度和效果往往是由训练样本的数据量及其质量决定的。但是由于数据孤岛问题、传统数据脱敏的局限性带来的隐私问题、数据监管问题等，无法实现数据安全有效被利用。大数据分享和分析带来了信息隐私和模型保护两方面的挑战。

基于行业解决方案商提供的隐私保护计算平台和一体机打造的医学影像学深度分析引擎在医疗影像学中的应用覆盖智能辅助诊断疾病、智能勾画靶区、智能判断病理切片、影像设备的图像重建，以及其他智能辅助诊断方案。具体包括:

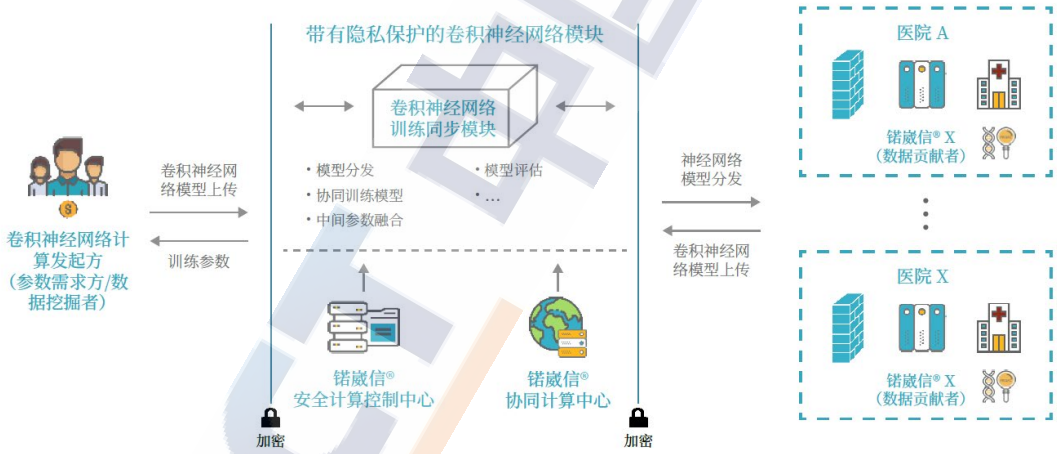
病灶识别：基于 AI 技术帮助医务工作者找出病灶区域，避免人工操作带来的失误，并且可以节约人力成本，为医生的诊断提供快速、可靠和精准的辅助诊断参考。

病灶分析：基于 AI 技术根据医学图像对病人病情作出初步判断和分析，为医生最后决策提供参考。

例如：

1) 诊断糖尿病性视网膜疾病——根据视网膜底的图片来识别糖尿病性视网膜病变程度，提高筛查效率。

2) 辅助诊断肺炎、结核病——根据病人胸部影像来快速准确的筛查出肺炎、结核病，医生可以在此基础上做进一步诊断。



来源：杭州锘崴信息科技有限公司

图 9 医学影像学深度分析引擎技术架构

5.电子病历结构化

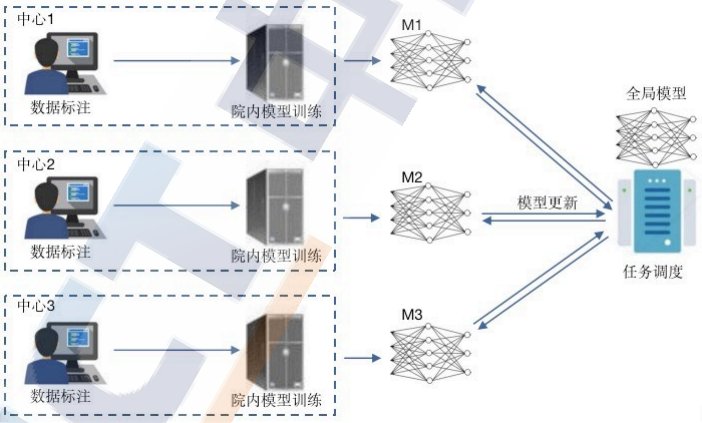
电子病历(EMR)包含了诊断、辅助检查、现病史、诊疗经过、病程记录等非结构化文本，也包含了医嘱、检验单、检查报告单等半结

构化数据，在基于 EMR 的下游应用研究中，往往需要进一步对 EMR 进行深度结构化，比如从诊断中结构化出疾病名称、发病部位和并发症等，从现病史和诊疗经过中结构化出患者的各种诊疗方案和疗效评价等信息。特别地在肿瘤领域科研中，对 EMR 的结构化要求更高，所需要的点位（医学实体）更多，结构化过程也更复杂。

电子病历结构化很大程度上依赖于医学文本的信息抽取，根据结构化医学模型的定义，对应地在信息抽取上需要定义不同粒度的医学事件或医学实体，然后构建信息抽取模型。典型的信息抽取范式为对原始文本进行编码，然后对编码进行实体解码，常用到的编码方式有 BiLSTM、预训练语言模型等，解码方式有 CRF、Pointer-net、Span 等，比如实体识别中的经典结构 BiLSTM+CRF，以及应用于句子级短语识别的 Bert+Span 模型。

构建信息抽取模型需要大量的标注数据，特别是使用深度学习的模型化方法，对数据的需求更是多多益善，这有助于增强模型的泛化性和鲁棒性。而在医疗领域，受限于信息安全和隐私保护等法律法规的合格性要求，电子病历是不能离院的，为实现电子病历的后结构化，通常的做法是院内数据治理，在院内进行数据标注、进行模型化训练和推断部署，这严重限制了多中心研究下数据间的彼此赋能。然而令人欣慰的是，联邦学习的出现则打破了这种局限，使得数据在合规的前提下依然能够彼此「共享」，在医疗领域多中心电子病历结构化上使用联邦学习，使得各中心间数据能力得以共享，各中心可持续利用「集体智慧」持续优化结构化能力。

围绕电子病历结构化，构建医学信息抽取横向联邦学习框架FedCIE，如下图所示（图 8），按预定规范使用实体&事件标注平台，各中心在院内完成自有数据的标注工作，然后在院内服务器上进行模型训练，FedCIE 控制中心负责在各中心间任务调度，主要是综合多中心训练的模型数据，进行全局模型的参数更新，然后再下发到各中心，继续进行模型训练，这一过程循环直至达到预设迭代次数。通过FedCIE，各中心数据不外露的情况下，同时使用了彼此的数据能力，间接丰富了数据的多样性，增强了信息抽取模型的泛化性和鲁棒性，在后续的迭代中，若一个中心标注数据有更新或增加，并进行了模型增量训练，这也将同时作用于其他中心，在 FedCIE 下所有参与者的所有数据信息都将被彼此利用，进而使得所有参与者都能从中收益。



来源：零氪科技(北京)有限公司

图 10 FedCIE:电子病历结构化联邦学习框架

（三）金融应用

1.信贷风控

近年来，风险控制能力越来越成为金融行业的隐形门槛。信息不对称，企业、个人用户信用记录缺失，信贷人工核验成本投入高且难以全覆盖核查，贷后预期逾期客户的风险识别困难等，都对金融机构进行风险控制带来了很大的挑战。特别是在近几年金融业务快速发展，恶意欺诈、过度消费、重复授信等乱象浮现，并且手段越来越专业化、产业化、隐蔽化、场景化。而传统风控手段维度单一、效率低下、范围受限越来越难以胜任复杂的场景应用需求。金融行业需要各个行业维度的数据去覆盖各类业务产品与风控需求，从而能够使业务人员及时准确的洞察不同来源与业务场景的风险行为变化。这些诉求使得大数据风控行业蓬勃发展。而大数据分析的风控手段又常常依赖于数据，但数据滥用又带来了数据隐私安全的问题。并且我们看到并不是有越多的数据补充，就能直接有效解决提升风控能力的问题。样本缺失，数据质量不足，有效数据维度欠缺等问题使得怎么挖掘数据价值来提升风控模型效果与怎么保证风控数据的可用率在双向平衡性中进退维谷。这些在金融行业内的智能风控领域是老生常谈的问题，而目前隐私计算正在成为这些问题在金融智能风控中一个有效的技术解。

一方面，隐私计算技术可以在保护用户信息不泄露的前提下将来自更多元，多维度的数据纳入联合风控模型中，从而实现更精细的洞察，构建更精准的风控模型。另一方面，各类金融机构也可基于隐私计算技术，利用多维度数据建立联合金融风险模型，共享黑名单与风

控应用等。在数据没有离开各自本地的情况下，扩充多方特征或样本，使模型效果不断提高。

借助隐匿查询、多方安全计算、联邦学习、机器学习、NLP 等领先人工智能与隐私计算技术，相关隐私计算服务商可在金融机构中针对企业端与个人端打造贯穿贷前、贷中、贷后的全流程新型的智能风控解决方案，端到端解决各类欺诈和信用风险问题。场景上，可覆盖小微企业融资风控、个人贷款申请信用评分、企业与个人贷款逾期预警，辅助智能催收等业务场景。隐私计算是一项融合了密码学、人工智能、大数据等综合学科的技术，在金融行业应用落地的过程中，各项技术均可与相应的风控业务流程结合，找到提升业务效果的价值点。从融合应用上，我们发现技术选型在实际落地中也有关联递进的关系，如以企业端风控举例：

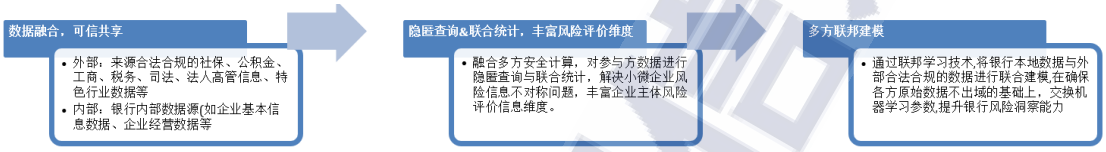
（1）企业端：贷前的企业准入与贷后的企业风险监控

以企业端为例，在实际落地中，场景应用可以分为三个阶段选型。

数据融合，可信共享：通过安全求交等隐私计算技术，金融机构可以依托内部本身对企业基本信息、提交信贷或其他业务数据的基础落盘，横向打通的数据包括税务、交通出行数据、水电燃气数据、公安数据、征信数据、其他关联经营交易数据，纵向针对不同的投向行业打通垂直领域的行业数据，从而实现企业端风控的基础信息补充。

隐匿查询&联合统计，丰富评价维度：利用多方安全计算与隐匿查询等技术，进一步针对参与方数据进行隐匿查询与联合统计，解决企业风险信息不对称问题，进一步丰富企业主体风险评价信息维度。

多方联邦建模，进一步提升数据价值：在数据维度补充和联合统计的基础上，通过有隐私保护的梯度下降机器学习，可以进一步提升数据价值，实现更细粒度的风险洞察和推测。通过联邦学习技术,将银行本地数据与外部合法合规的数据进行联合建模,在确保各方原始数据不出域的基础上打通跨行线上线下真实经营数据信息的评价，交换机器学习参数,提升对企业端信贷风险洞察能力。



来源：第四范式(北京)技术有限公司

图 11 全业务信贷风控流程示意图

（2）个人端：个人信贷的全流程风控

相比企业端，依赖于互联网及消费金融的发展，金融机构获客渠道日益丰富，线上成为主要业务来源，商业银行 C 端客户介入的信贷资产类型更加多样，涉及的消费场景、贷款金额、交易数量更加的多元不一。随着信贷客群逐渐下探，贷款申请数据维度饱和度低，大量客户没有征信数据。导致传统的风控策略无法覆盖所有的客群，逾期与不良风险普遍攀升。这时数据信息的补全对于 C 端客户的风控作用就显得尤为重要。然而过去几年大数据行业的野蛮生长使个人风控业务成为用户隐私泄露的重灾区。隐私计算技术目前也正在成为此问题的有效解法。

相关隐私计算企业可帮助某银行利用隐私计算与机器学习技术，在双方数据不出本地的前提下，对客户的申请信息、合同信息、人征信、身份、学历、消费、电信、航旅、公安司法、三方黑灰名单等数据价值进行充分挖掘，利用联邦学习建立了一套应用于零售客群和产品的申请信用评分与欺诈评分。通过对客户信用风险和欺诈风险两方面进行精细刻画，实现对每笔贷款的贷前风险做更精准的评估和打分。针对贷后进行了有效的风险管理和监控，帮助客户构建了良好的模型效果，辅助业务能更好的区分好坏客户，降低贷后呆坏账比例。同时在智能催收领域中，通过实现对入催客户进行精准刻画，提高了预测客户还款难度和自愈概率的准确率，帮助该行有效的配置贷后处置资源。

另外，通过隐匿查询、安全求交等方式，金融机构可联合运营商、政务机构、保险机构、支付机构等解决信贷业务中的多头借贷、共债、黑名单互通、电信诈骗、抵押估值、失联召回、保单贷款等场景，有效合规的解决风险信息不对称的问题。

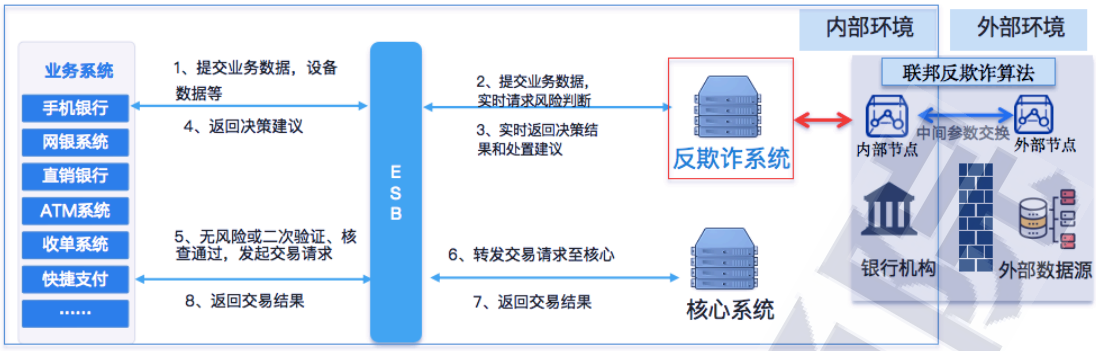
（3）基于联邦学习的联合反欺诈金融应用场景

人工智能技术在金融反欺诈的应用场景中迅速发展，并已取得显著成效，机器学习，知识图谱等多种技术被广泛应用，金融诈骗行为能够被有效识别。但在巨大的经济利益驱动下，金融诈骗手段层出不穷，传统基于单一企业的数据金融反欺诈模型逐渐难以应对不断升级的诈骗手段，无法进行有效防护和阻断，需要通过跨机构间的数据协作来构建更精准的金融反欺诈模型，然而由于数据安全、隐私保护等

监管要求日趋严厉，加剧了机构间数据合作的难度，“数据孤岛”问题普遍存在，迫切需要通过联邦学习等隐私计算技术打通企业间的数据孤岛，以“数据可用不可见”的方式安全合规地构建跨行业数据共享的反欺诈模型，挖掘出更深层次的金融欺诈风险，提升金融反欺诈的效率与精准性。

借助面向数据隐私保护的联邦学习技术，可以在保证用户隐私信息、企业的数据安全、企业的数据所有权与控制权的前提下，安全地融合银行机构、电商、运营商、互联网、政务等多元数据，实现跨行业、跨机构的反欺诈体系建设。通过金融机构的用户属性、收支行为、信贷行为、信用历史、资产情况等金融行为特征，融合外部的消费行为特征、通信行为特征、支付行为、社交行为特征等，采用联邦机器学习算法构建更为精准的金融反欺诈业务场景的模型，通过跨行业、跨机构的多样性欺诈数据特征互补，提升金融行业的整体反欺诈能力和效率。

以国内某商业银行为例，借助同盾科技的联邦学习技术，引入外部数据源，联合银行已有欺诈样本和行内金融特征构建联合反欺诈模型。首先通过隐私集合求交技术(PSI)进行跨机构间的样本安全对齐，确保参与方直接除了交集样本无法获知或反推其他参与方的非交集部分样本，然后利用纵向联邦学习算法进行反欺诈模型的构建，并与现有欺诈系统进行对接，具体应用如下图所示。



来源：同盾科技有限公司

图 12 银行联邦反欺诈方案示意图

基于联邦学习的金融反欺诈应用实践结果表明，通过联邦学习算法构建的跨机构反欺诈模型，对比仅基于行内数据构建的模型 KS 值、AUC 等模型评估指标均提升了 30%以上。模型结果表明基于联邦学习模型能够对用户欺诈行为进行有效识别，能够有效提升商业银行的风险防控能力。联邦学习技术将深刻影响金融大数据及金融反欺诈的应用场景的效能，解决了多方数据协作的合规性和安全性问题，挖掘出更大的数据潜能，并避免了数据在多方间的跨企业流动，有效保护数据的所有权和控制权，实现数据价值的安全共享和共创。

2.营销风控

项目背景：

在数字化的大背景下，银行机构希望能够打造一体化全流程反欺诈体系，建立集交易事前防范、事中监控及事后分析的风险监控体系，有效防范电信网络诈骗、银行卡欺诈、互联网交易欺诈等，全面提升反欺诈能力。因此对银行、证券、保险、互联网金融公司等多方数据

有很强的流通共享需求，应用到信贷领域，但需应对数据泄露、个人隐私泄露等顾虑。

风险及挑战:

数字化转型趋势下，单方数据已不能满足业务创新需要，需要合规融合多方数据，多方数据拥有方彼此不互信，缺乏数据融合共识，如何保证非互信机构之间进行数据安全融合？多方数据融合互补，缺少安全合规技术/平台，融合过程中如何保证数据全流程安全？多方异构数据融合，需要结合行业特定业务场景，进行联合分析和建模，如何提高现有模型准确性？

客户需求:

金融客户在营销反欺诈场景希望能够安全合规融合多方数据资源，提高现有 AI 风控模型准确率，同时降低人工审核成本，提高审核效率，进而提升用户体验。

解决方案:

搭建隐私计算平台，安全融合银行、借贷机构、保险机构、政府等多方数据进行数据核验、联合统计、模型训练，为跨机构多方联合风控提供安全数据流通解决方案。

来源：北京百度网讯科技有限公司

图 13 基于隐私计算的营销风控平台级解决方案

针对营销领域反欺诈场景，具体解决方案如下：

某银行客户信贷中心，希望能够针对白名单客户进行风控，通过引入外部合规数据资源，提高现有模型的效果，提高客户信贷审核效率同时降低信贷逾期风险。

采用联邦学习方案，在各个数据源域内搭建联邦学习平台，在网络联通的情况下，保证各方数据不出域的情况下汇聚多源历史数据进行联合建模，输出营销反欺诈模型。

当有新客户开展贷款业务时，通过部署上线的营销反欺诈模型进行模型预测，针对白名单客户输出风险分值，如风险值在 0-40 分证明该客户风险较低，可直接通过审核，发放贷款；风险值在 40-80 分，证明该客户中风险，根据客户贷款额度适当补充相关材料进行审核，审核通过后发放贷款；风险值大于 80 分，证明该客户属于高风险客户，有骗保可能，需要人工深度介入，重点筛查。

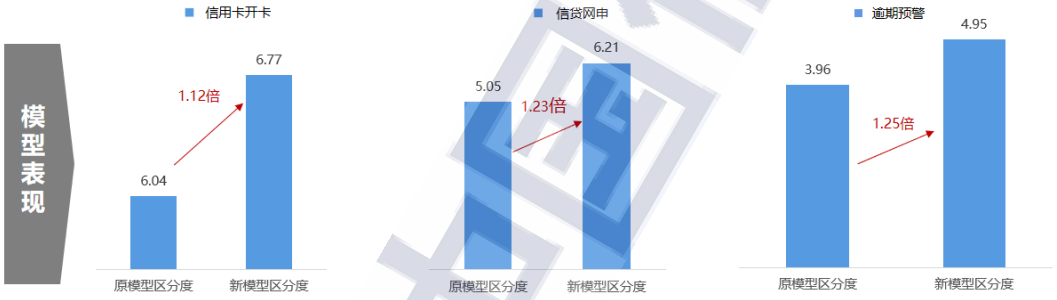
方案价值:

1）促进行业数据安全流通，充分释放数据价值

平台提升企业对数据全生命期的安全管理能力，促进企业内部和企业间的数据安全流通，在保证各方数据安全的前提下，充分释放数据价值，提升业务效能。

2）构建全流程风险防控体系，提升风控模型效果

实现多业务场景的统一风控管控，搭建稳定、动态的风险规则/模型库，让每一步风控决策都有据可依，有效识别交易风险。



来源：北京百度网讯科技有限公司

图 14 应用隐私计算后的营销风控场景表现 [6]

3.零售营销

在金融同业间竞争日益激烈与客户迁移成本越来越低的形势下，要保持领先与竞争优势针对如何把握每一个客户的产品需求，进行个性化的服务与客户留存是持续性命题，业内也均在不断的探索如何能够对客户进行更加精细化的运营。面向实现客户 MAU 与 AUM 的综合提升，产品的精准营销成为了一个重要的切入点。从业务价值提升的角度，金融机构希望通过精准营销的方式以最小的资源投入获得最

[6]模型的区分度KS值是指预测模型预测风险与实际风险的一致程度,是衡量模型预测绝对风险(Absolute risk)准确性的重要维度,模型区分度较差时将低估或高估事件发生风险。

大的业务收益。从客户体验的角度，在同业同质化竞争的趋势下，客户的切换成本是比较低的，金融机构希望避免过度或打扰性质的营销导致客户的流失。具体到各项产品精准营销的角度，金融机构希望做到的是在最佳的时间、以最佳的营销触达方式、结合最优的营销权益，为客户推荐最适合的产品以实现最优的业务转化。特别是在当前线上化业务发展所趋下，金融机构从线下发展到线上获客，对获取潜客的精准度也将直接影响客户触达与客户留存的成本与效率。

目前，针对金融机构已经积累了的大量基础零售客户群以及丰富的产品、内容、服务标的，隐私计算技术可以为其营销决策在保护数据安全的前提下提供更多维度的数据支撑。在联邦学习领域，金融机构可利用历史营销样本通过纵向联邦学习的方式与支付机构、运营商、互联网机构、政务部门等外部数据源进行联合建模来优化营销效果。如，首先可实现针对某项业务营销偏好用户的筛选场景，通过有效的补充特征，实现用户的多维的分层与分群，并基于这些分群的结果及用户的偏好，设计相关的营销策略；进而之后，可继续基于垂直业务的联邦学习建模，在面向内容、时间、权益、触达方式等多维度场景上，使每个维度相关的数据特征不断丰富，实现对客户的需求及偏好进一步深入的剖析和洞察。达到对客户需求的精准把握与度身定制，继续优化营销效果。

如我们在某银行在面向新客进行的进件营销上的场景中，由于银行在进件业务流程中的数据维度一般较为单一，不能较好的综合判断进件客户的价值潜力。我们在本行进件申请信息的基础上通过联邦学

习的方式，安全合规的联合外部数据源，在保证数据不出库的情况下，补充了征信类、通信类、终端类、行为偏好类数据特征进行纵向联邦建模，较大的提升了 APP 端进件营销的响应率。

在保险的场景中，某互联网保险机构自身拥有大量保险代理人与用户注册基本信息。利用其自身涵盖注册投保信息与样本，通过联邦学习的方式与外部运营商、支付、互联网等数据源进行联邦学习建模，更好的建立了对于健康险与车险的营销模型，并且后续基于注册用户的相似偏好行为，可及时发现潜在投保需求。

同时我们看到联邦学习技术对于长尾客群营销的场景也能发挥良好的效果。某银行拥有大量的零售客户群体，但受限于有限的营销资源，日常的营销活动更多的是覆盖和触达本行头部的一些客户，缺乏对本行长尾客户的关注。但长尾客户恰恰可能是高净值的潜力客户。如何能够精准的锁定具备业务转化潜力的客户，需要合规的了解客户的外部财富能力特征等信息。在该银行高潜力消费的客户挖掘案例中，我们在长尾客群中利用基本属性信息、流水与资产信息等行内数据和样本的基础上，通过联邦学习的方式引入外部数据源补充了跨行消费行为、资金流动性数据等信息，进行数据不出库下的联合建模，实现了本行优质高潜客户的挖掘。

不仅个人类场景，我们发现在面向小微企业的精准营销场景下联邦学习也能发挥相应作用。如某金融机构利用小微企业资质信息、行内对公账户历史资产、交易等信息，联合政务相关部门的税务、发票信息、企业主房贷信息等构建了纵向联邦学习模型。实现向小微企业

客户精准推荐指定贷款产品，通过联邦学习模型提升了现有基于白名单机制的营销响应率。

除联邦学习模型外，金融机构也可以利用隐私求交的技术，直接进行营销画像的补充，作用于营销决策规则的完善。如某信用卡中心能够根据客户的消费偏好与丰富后的客户画像进行对于不同客群推广不同的刷卡达标活动，在保护客户名单隐私的前提下根据外部数据源方的补充数据标签完成客群的划分。

相关企业的联邦学习方案为其提供了基于隐私保护求交的定向推广方案，通过隐私保护的求交方法，在不泄露非交集数据的情况下得到双方的交集。例如：针对刷卡达标的活动中的数码产品类活动、旅游产品活动、金融保险产品活动等，通过与数据方的隐私求交，生成数码爱好者’、‘旅游达人’、‘金融投资爱好者’三个交集返回给信用卡中心，从而实现对自身用户画像进行扩充，确定后续投放的活动类型。

针对基于联邦学习的银保营销金融应用场景，具体解决方案如下：

在保险的诸多主流分销渠道中，银保渠道是一个重要渠道，拥有海量客户基础和主账户关系的银行机构在保险业务的推广方面存在天然的优势，同时保险业务也是银行机构其重要业务组成的一部分。但目前银行在保险产品的营销和精准获客方面仍普遍存在获客转化率低、成本高等问题，主要是由于银行在寻找目标客户过程中，因客户画像不精准，导致获客转化率低；同时由于客户维度的缺失，导致银行营销人员对潜在客户的需求定位不清晰，难以挖掘其真实需求，

潜在价值没有得到充分的发挥；最后导致了获客转化率低，同时产品推介针对性不强，使得银行保险业务营销的整体 ROI 偏低，总获客成本居高不下。

要解决这些问题，首先需要打破银行与保险公司、与外部数据源之间的数据孤岛，通过联邦学习等隐私计算技术打通各个环节的数据割裂，以合规安全方式构建全流程的银保营销模型，并根据不同客群特性进行策略优化，从而降低保险机构的获客成本，更好满足银行客户的需求与用户体验，提升客户忠诚度。

以国内某商业银行为例，在代销保险业务中银行希望从数亿客群中挖掘出潜在的保险用户，并根据不同的用户分群分配不同的营销策略，进行银保交叉营销。在实施过程中，采用同盾科技的联邦学习技术，在保险公司与银行均部署同盾智邦（iBond）知识联邦平台，利用保险公司已有人群特征标签作为种子用户，并选用联邦推荐算法，构建多维、准确的联邦推荐模型，从而识别出更多潜在相似人群，同时优化营销渠道和方案，具体方案如下图所示。

来源：同盾科技有限公司

图 15 银保营销方案示意图

对模型运行结果及营销结果进行统计分析，实证结果表明，在转化率、ROI、长短期保险营销比例等方面，基于联邦学习的跨机构协同模型结果均原有的基于单边数据的规则银保营销模型有较为明显的提升，带来超过 50%的提升。

4.小微服务

场景金融可以理解为是互联网、传统行业以及金融三者的相互融合与渗透。场景金融利用新型的金融科学技术，将金融服务有机嵌入到已有场景活动中，以达到促使经济行为高效完成、金融服务得以更好地实践和展开的目的。

场景金融通过发掘客户的痛点，试图从使用者角度来分析问题、提供解决思路。从这个角度出发，场景金融需要为小微商户带来快速、便捷、精确等优质的客户体验，但金融的风险性决定了金融业务的成交是客户体验与金融机构风控不断平衡的结果，那么如何在为用户带来好的申请体验的同时，又能有效进行风险防控呢？这就需要充分利用场景中的各类数据，还原小微商户画像，在满足用户授权的前提下，在场景中通过隐私计算数据应用的方式来对小微商户的的经营情况在“可用不可见”的情况下进行判断。

然而小微商户在场景中期望得到的是类似“预授信”这类的明确的服务“邀约”，和“随用随取”的不确定经营资金的使用方式。小微商户并不希望通过填写复杂表单和不确定的经营隐私数据授权供金融机构进行通过率极低的风险审核。

这在传统风控上是个悖论，很显然没有数据的情况下无法判断客户风险情况，也就无法事前确认客户是否符合预授信要求，进而“邀约”相应的金融服务，但在隐私计算技术框架下，这个问题迎刃而解。

此时我们需要用到联邦学习技术，通过引入场景方和其他第三方数据能力，与金融机构自身样本资源结合，在各方数据或样本均不出本地的前提下，通过联邦学习构建金融机构在该场景下的风控筛选能力。

同时，场景方通过银行构建的多方安全计算策略进行风险筛选模型，进行小微商户的风险筛选，在合法合规的前提下筛选出符合银行风控“偏好”的小微商户，在这过程中模型筛选逻辑对场景方是“可用的”黑盒，而筛选出来的人群同样对银行也是不可见的，最大限度保护银行风控策略的保密性与场景用户的隐私。这样首先解决了一方选择问题，也就解决了原有的双向选择的不确定性问题。

最后对于筛选出来的小微金融商户来说，金融服务的可得性已经是确定的，此时再由场景方向这些用户进行具体的“邀约动作”，用户的转化显著高于传统的导流或者营销模式，且用户能够得到更好的金融服务体验。

对场景方来说，可以最小化触达客户但得到最大化转化，对金融机构来说，则将大幅提升业务运营效率、降低运营成本。

5.反洗钱监管

反洗钱，是指为了预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏

金融管理秩序犯罪等犯罪所得及其收益的来源和性质的洗钱活动。洗钱行为具有严重的社会危害性，损害了金融体系的安全和金融机构的信誉，乃至会扰乱正常的经济秩序和社会稳定。反洗钱对维护金融体系的稳健运行，维护社会公正和市场竞争，打击腐败等经济犯罪具有重大的意义。

在预防、监控洗钱活动方面，银行等金融机构以客户识别、大额交易、可疑交易报告以及记录保存等制度为核心内容为主，通过资金监测实现反洗钱工作目标，目前更多还是以经验规则手段作为反洗钱可疑交易提取的主要方式。然而，普遍的可疑交易监测规则一般是基于过去已发生的案例而设计的，这对于通过数据分析侦测洗钱行为造成了一些现实问题。一是该领域行为是低频的，一般没有标签，信息饱和度低，导致在该领域内数据样本少和数据质量较差是普遍存在的现象。二是交易明细是分析基础，而分析与交易量有直接关系。随着金融机构交易量的与日俱增，依靠事后规则的方式给反洗钱案件甄别增加了误判和低召回的可能性，上报率与预警准确率也亟待提高，间接影响后续的落盘的数据质量。三是，快速增加的交易量很多交易行为具有小额高频的特点。在样本少数据质量低，仅依靠人为总结经验的情况下，金融机构需要从海量交易中识别可疑交易乃至及时侦测到隐秘的新型作案手段会更加困难。四是，资金监测往往会涉及到跨机构，跨法人的协同，但此部分数据也是各机构内核心敏感数据，融合共享的趋向较慢。

五是特别针对于广大中小型金融机构而言，相比大型金融机构，样本更少，那相应的案例总结规则也会少，针对较为新型的洗钱手段滞后性也会加剧，形成了一个恶性循环。

相关企业发现隐私计算的技术在金融机构反洗钱侦测问题上也有比较好的作用效果。比如：通过多方安全计算技术，可以实现金融集团内部或者同业机构之间的黑名单等特殊客群信息安全融合与共享，提高合规反洗钱能力。特别是针对需要进行多家金融机构跨机构的资金追踪合作，还原资金链路的场景，提供了一个技术解。

同时，通过横向联邦学习，各个金融机构无需建立物理模型即可共享通用模型，这可以有效解决该领域样本少，数据质量低的问题。特别是针对中小金融机构而言，在不共享用户数据的前提下，通过与联合大型金融机构或联合多家金融机构，可以共同建立了横向联邦反洗钱模型提高侦测能力。同时，针对于在保证数据不出库的前提下，既能扩充样本，又能也扩充特征的方式，业内也在积极探索应用联邦迁移学习的方式探索。

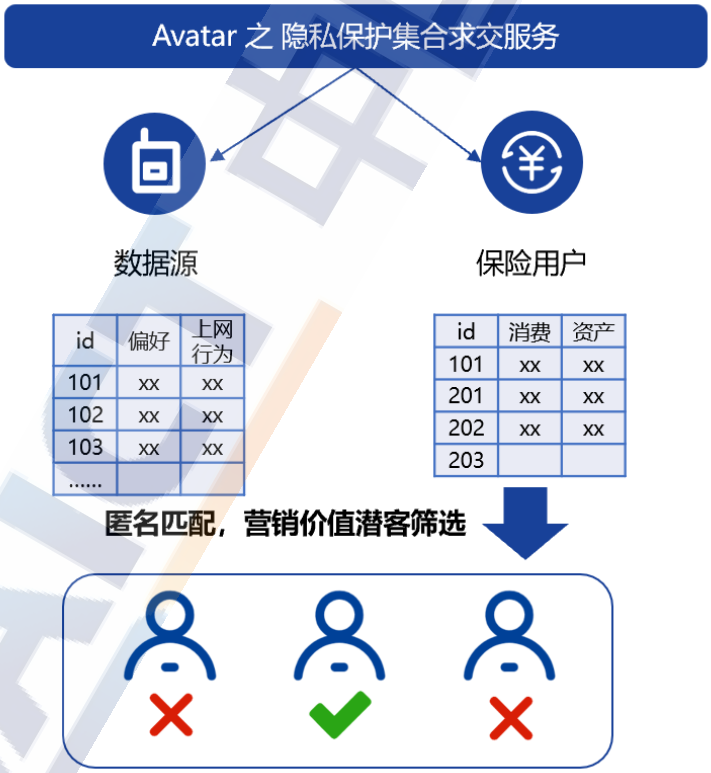
在多方安全计算与联邦学习等隐私计算技术的应用基础上，我们发现金融机构可继续将机器学习与图计算的能力应用，从而进一步去做侦测效果的提升。使可疑交易甄别从“经验主义”的模糊分析方式迈向“数据驱动”的精准治理方式，做到阈值自调整、性能自优化，加快监测模型的更新迭代，提高洗钱风险定位的精准性和及时性。

6.保险存量挖潜

保险公司在开展业务过程中，通常会通过赠险或其他短期小额险种积累大量的用户，但受限于自身数据匮乏，无法有效识别并运营这部分用户。在此场景下，保险公司可以利用安全求交或匿踪查询技术，在保护自身客户信息不泄露的前提下，安全引入外部数据资源，勾勒存量客户画像并对用户进行分群，提升营销激活效果。

解决方案 1：基于安全求交的实现方案

基于隐私保护集合求交技术，保险公司及合作数据源方共同进行数据集合的交集计算，最终得到集合交集，而双方交集之外的差集部分并不会暴露给任何一方。



来源：上海富数科技有限公司

图 16 银保营销方案示意图

解决方案 2：基于匿踪查询的实现方案

基于不经意传输及非对称加密技术，在保护保险客户信息不泄露的前提下，实现外部数据资源的安全查询，从而有效勾勒客户画像信息，提供营销决策依据。

（四）数字广告

一直以来，数字广告产业链的发展伴随着数据多而杂、应用不到位、数据使用安全性存疑等问题。随着移动设备的全面普及，用户及各个移动互联网参与环节制造出海量数据，在线营销领域的飞速发展，使得企业之间合法合规、安全高效地进行数据合作的诉求日益增多。然而，数字广告产业链复杂，涉及广告主、流量平台、消费者及其他第三方等多方参与，各行业、各企业的数据孤岛问题愈发严重，数据往往分布在不同的机构和个人形成的数据孤岛处。使用和聚合这些数据，都会受到用户隐私、商业安全、数据质量方面的挑战。

并行的，由于国家和行业对数据安全的密切关注和监管法律法规落实，数据孤岛和数据隐私问题共同制约着人工智能在广告营销行业的发展，利用大量数据只能进行很简单的小任务。这导致存在隐私安全风险的传统广告营销方法将面临法律、政策、监管的多重重大运营风险，基于“用户数据”为基础的互联网广告营销方式必须要做出变革，可预见地，它们将逐渐退出“移动营销黄金十年”的历史舞台。

在这样的背景下，隐私友好、合法合规、利用相对较少的数据基础上完成复杂任务的“联邦学习”(Federated Learning)将大放光彩。“联邦学习”能够通过设计一套 AI 系统较好的解决上述问题，既能

保护用户的数据隐私，同时又能更高效、准确地使用孤立的数据，最终学习到更好的模型。因此，可以在各互联网行业领域，尤其是数字广告产业链的智能营销中全面运用起来。

“联邦学习”是一种加密的分布式机器学习技术，其中的参与各方，如流量平台、广告主等均可以在不披露底层数据和底层数据的加密（混淆）形态的前提下共建模型。每个广告主业或者数据持有方不出本地，通过加密机制下的参数交换方式，就能在符合各项隐私安全法律、法规的情况下，建立出虚拟的共有模型，串联一个个“数据孤岛”。例如，在流量平台侧，为突破广告营销的效果瓶颈，进一步提升在线营销流量资源的商业价值，媒体平台公司通过推出隐私计算框架。以联邦学习为代表的隐私数据保护技术为基础，针对机器学习、数据分析等算法进行定制化的隐私保护改造，保证原始数据不出广告主本地即可快速完成隐私计算任务。结合联邦学习技术与广告推荐技术，保障数据安全的同时又能发挥数据最大价值；在广告主侧，以食品饮料、日用品、美妆为代表的企业也可以通过不断加速数字化转型，加快通过大数据和 AI 技术提升营销能力。

在流量平台侧，为突破广告营销的效果瓶颈，进一步提升在线营销流量资源的商业价值，已经陆续有大型媒体平台公司推出了隐私计算框架。以联邦学习为代表的隐私数据保护技术为基础，针对机器学习、数据分析等算法进行定制化的隐私保护改造，保证原始数据不出广告主本地即可快速完成隐私计算任务。结合联邦学习技术与广告推荐技术，保障数据安全的同时又能发挥数据最大价值。

在广告主侧，以食品饮料、日用品、美妆为代表的企业正不断加速数字化转型，加快通过大数据和 AI 技术提升营销能力。对整个在线营销行业而言，联邦学习的合作模式目前属于早期发展阶段，已经有部分行业头部广告主开展了基于多方联邦学习的广告营销实践。

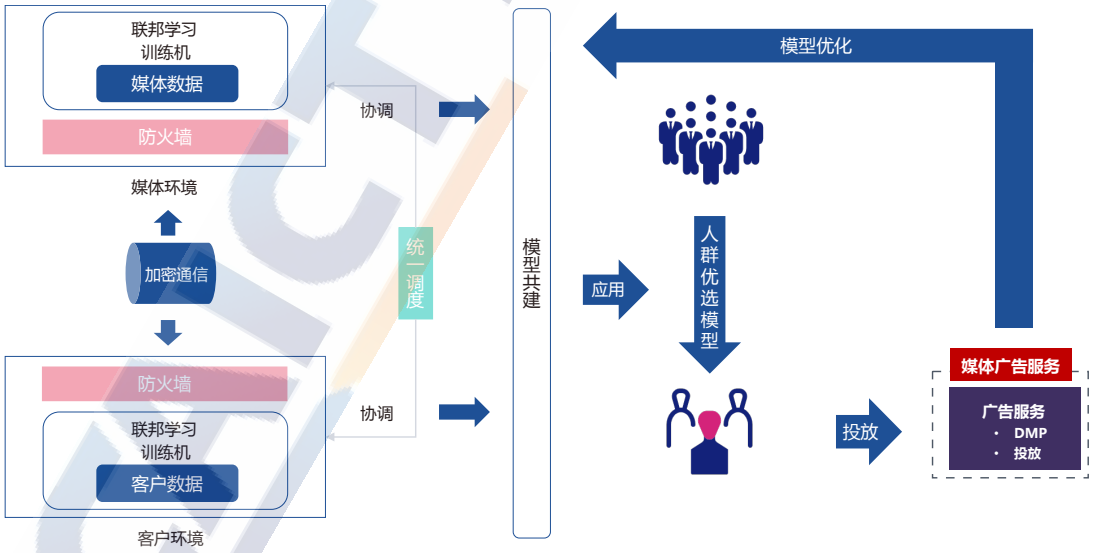
1.广告投放

在食品饮料、日用品、美妆等竞争日益激烈的行业，要如何保持竞争优势、如何让广告有效触达目标群体，并在保护数据安全的同时实现广告价值的高转化，是目前广告主最关注的问题。具备一定技术能力的广告主在人群定向策略的制定过程中，往往会面临数据安全的难题。如果想要实现更加个性化的策略，广告主通常需要上传一方数据到媒体平台的工具上进行洞察和分析，但出于行业特性或数据安全的考虑，往往只能止步。

为了能够让流量价值和转化效率最大化，媒体平台近几年陆续推出各自的联邦学习框架，以 AI 联合建模的方式与广告主共同探索数据价值。联邦学习主要解决数据跨域问题，保证数据不出域，也就是计算资源向数据资源靠拢，保证数据安全隐私和安全合规。在联邦学习技术出现之前，只能用来自媒体平台、广告主或第三方的单边数据进行建模，单边数据训练得出的模型在投放过程中可以支持某些场景，但会迅速遇到瓶颈，多方数据结合在一起的模型能力则会得到不同程度的增强。

在一个典型的 AI 联合建模场景中，数据参与方通常包括媒体平台方、广告主、第三方服务商，由媒体平台侧提供联邦学习的基础框

架和数据源特征库，例如消费者在媒体上的各类行为和兴趣特征，客户侧提供客户侧样本特征库，例如零售类企业已经积累的大量基础零售客户群信息以及丰富的产品和内容信息，第三方服务商可能会提供基于其他数据源的样本特征库。整体联邦学习联合建模的技术架构由底向上分为三层，分别是模型训练层、模型管理层和模型调用层。在模型训练层，广告主可以自建或与第三方服务商共建客户侧样本库，通过机器学习的方式实现与数据源特征库的联合建模。不同模型适用于不同的领域，例如广告推荐领域最常使用的模型之一神经网络训练模型，就已经有媒体实现了与广告主和第三方的联合建模。由于引入了分层级的模型加密，各方数据源特征库实现了可用不可见。在模型管理层，媒体平台侧对联邦学习的模型进行发布和管理。在模型调用层，媒体侧和客户侧分别研发引擎，用于各方权限内的申请查询模型结果，并将结果用于广告推荐场景。



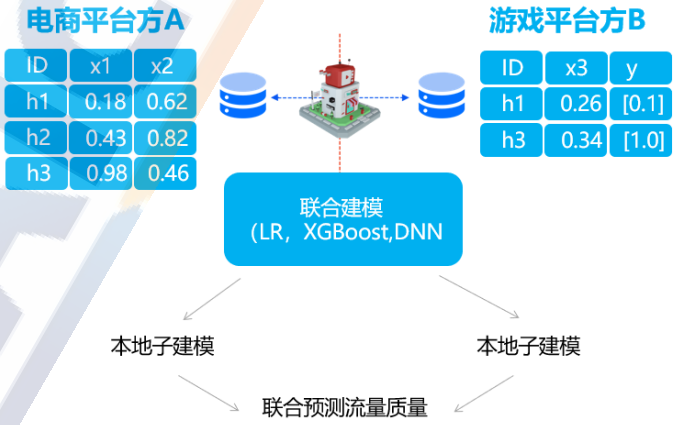
来源：北京明略软件系统有限公司

图 17 联邦学习 AI 联合建模应用于广告投放场景

2.流量反作弊

如今，用户对隐私问题空前关注，有关监管部门立法监管也愈发严谨，也在维护“数据安全”护航“数字经济”，于是，很多媒体平台、广告主、广告代理在互联网广告营销的反作弊环节，都采取了“联邦学习”的办法，高效并且合规、合法地识别流量质量。在流量反作弊的过程中，我们需要用各种各样的数据和标签来构建用户画像。数据越详尽，往往越有利于广告主做出正确的投放判断，捕捉正确的“场景”，找到对的“人”。

当前，数字广告产业链中使用的联邦学习分为跨样例和跨特征两种模式，跨样例模式更多的是同构数据，而跨特征模式则更多的是异构数据。举个例子：不同电商之间的数据相对是同构的，属于跨样例模式。而互联网媒体平台 A 与互联网媒体平台 B 之间的数据则是异构的，属于跨特征模式。对于流量反欺诈来说，跨特征的异构数据非常重要。联邦学习反作弊可以联合电商、游戏、大数据公司等多方数据共同构建反作弊模型。



来源：北京智慧易科技有限公司

图 18 多方数据融合反作弊模型

比如，某个用户在媒体 A 被判定为可疑用户也就是我们所说的“虚假流量”，广告主在媒体 B 投放广告时，是否对其进行广告曝光展示？尽管缺少该用户的相关数据，广告主可以通过联邦学习的方式进行建模，在无需查看用户隐私数据的条件下，对其进行多方计算，判断用户的真实情况，决定是否对其进行投放。从而实现流量反作弊，拒绝被黑产“薅羊毛”诈取营销预算。

3.联合归因

从用户洞察到广告创意，从智能投放到效果分析，AI 营销基于底层数据和机器学习，为广告营销业提供了自动化、个性化的智能解决方案。无论广告业态还是品牌行为，都在 AI 技术的驱动下发生了深刻变化。

过去在广告营销中比较常见的归因方法包括末次点击（last click）模型和均匀分配模型。比如一个用户看了 4 个广告，最终形成一次转化，末次点击模型将最后一次的广告贡献定为 100%，均匀分配模型则将 4 次广告的贡献率各分为 25%。而实际上，这两种归因方法并不科学，因为前 3 次广告对于最终转化是有贡献的，只不过贡献率各不相同。

基于丰富数据，联邦学习可以帮助广告做到多触点归因，准确识别每个用户触点的增益收益，在完备的经济学归因模型指导下，将广告贡献进行公平分配，实现准确评估各触点的真实贡献。这样的归因方式获得的分析结果可以为品牌广告资源配比提供重要参考，最大化提升整体营销收益。

通过媒体侧的用户兴趣标签，以及广告主的用户商业兴趣及商品标签数据，联邦学习平台可以优化广告的触发召回、CTR（点击通过率）、CVR（转化率）等模块，帮助媒体和广告主获得双赢的结果。

一直以来，数字广告产业链的发展伴随着数据多而杂、应用不到位、数据使用安全性存疑等问题。随着移动设备的全面普及，用户及各个移动互联网参与环节制造出海量数据，在线营销领域的飞速发展，使得企业之间合法合规、安全高效地进行数据合作的诉求日益增多。然而，数字广告产业链复杂，涉及广告主、流量平台、消费者及其他第三方等多方参与，各行业、各企业的数据孤岛问题愈发严重，数据往往分布在不同的机构和个人形成的数据孤岛处。使用和聚合这些数据，都会受到用户隐私、商业安全、数据质量方面的挑战。

（五）物流行业

经过长达 2 年的抗疫战，新冠传播态势有所好转，但仍有地方性区域偶有病例产生。这场抗疫持久战，对各行各业的发展都有一定的影响，尤其是对末端物流行业。为控制疫情蔓延，如何有效减少人与人之间接触，降低传播风险，让居民快件零接触、少接触的投递方式成为物流企业重点发展方向之一。

在防疫复工复产背景下，为满足零接触、少接触的寄件需要，对“先寄后付”模式的推广有强烈诉求。而在面对现有散客中，快递企业难以基于自有数据判断客户风险情况，需要快递员对“先寄后付模式”推广对象进行甄别，主观性较强，若快递员判断失误，容易造成

坏账风险，因此能够享受该服务的消费者范围较为有限，推广难度较大。

面对某头部物流企业现有客户，自有数据无法判断用户是否为低风险的“先寄后付”客户。通过运用隐私计算技术，帮助该物流企业引入了价值含量极高的散单客户真实跨行数据依据，在拥有散单客户基本信息的基础上，补充在金融业务中的个人信用相关行为变量等，通过建立低风险人群标准画像，从实际待推广客户数据中筛选符合标准的目标群体。

隐私计算技术在保障个人隐私的前提下，实现跨企业合作数据建模，能够降低先寄后付推广的坏账风险，同时提升客户服务质量，解决该企业目前业务痛点，可覆盖全国上亿消费者，让降本与增效并举，通过优质便捷的服务强化核心竞争力。在疫情期间，先寄后付简化派收件流程，最大程度上降低寄件过程中的人员接触，优化终端派收件环节，推动着快递业行业智能化发展。让日常高频的快递收送变得更加轻松、便捷、智能，优化消费者服务体验，助力打造多方安全的物流新模式。

六、展望

(一)政策引导、持续释放行业红利

当前，我国相关法律法规的颁布和实施，在加强数据安全和个人隐私保护的法律指引的同时，也一定程度上间接促进了以联邦学习为代表的隐私行业的蓬勃发展。联邦学习作为兼顾数据协同和安全隐私

的新型技术，是保障数据有序合规流通的基础激素，需要国家各主管部门不断完善政策，加强引导，有效激发和持续释放行业红利。

（二）凝聚共识、加速应用场景探索

当前，联邦学习及相关技术在政务、金融、广告、物流等多场景已经形成了典型应用。但行业仍对联邦学习的安全性、互联互通等方面抱有疑问。产业链上下游应凝聚共识，加强对于个人信息保护和数据安全的重视，积极探索联邦学习在垂直行业中的应用案例，形成行业示范，加速联邦学习行业应用场景的探索。

（三）标准建设、加强平台互联互通

当前，各联邦学习解决方案提供商还依托自身解决方案为行业提供服务。各平台之间的互联互通成为联邦学习应用进一步发展的阻碍。在2021年，联邦学习已正式进入互联互通阶段，产出标准化的框架和API 是行业的根本痛点。产业应在不断磨合和优化的过程中，推动联邦学习步入开放通用的阶段，共同打造联邦数据网络的生态。

中国信息通信研究院 泰尔终端实验室

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：13811959962

传真：010-62304364

网址：www.caict.ac.cn