知识联邦白皮书

打造数据安全的人工智能生态系统

同盾科技人工智能研究院

2020 年 5 月

同盾科技
www.tongdun.cn

同盾科技有限公司

目录

同盾科技有限公司

同盾科技有限公司

第1章 知识联邦背景

互联网时代出现了两种普遍的现象，一个是数据孤岛现象，一个是隐私换便利现象。而随着数据安全合规的监管日益严格，突破这两种现象造成的壁垒必然需要技术的创新。这一章将首先介绍这两种互联网时代的现象，然后进一步分析并提出相应的解决办法。

1.1 数据孤岛现象

随着信息化和互联网应用的发展，数据孤岛已经成为一个全球普遍存在的问题。企业发展到一定阶段，会出现多个子公司或分公司，每个子公司都有各自数据，部门之间的数据往往都各自存储，各自定义。每个部门的数据就像一个个孤岛一样无法(或者极其困难)和企业内部的其他数据进行连接互动。这就是数据孤岛。数据孤岛的类型有很多，不仅企业内各部门或环节存在着数据孤岛，企业或机构间也存在数据孤岛。甚至政府机关之间也存在数据孤岛，在很多地方，有多少个委、办、局就有多少个信息系统，每个系统都有自己的数据库，相互之间完全独立。

数据孤岛不仅仅是物理上的，还有更多是逻辑上的孤岛。每家企业都会有业务数据的产生，有对数据保存和使用的需要，不同企业对数据的定义和使用可能存在比较大的差异，所以各企业之间的数据在逻辑上就不能互通。

数据孤岛的存在所带来的弊端是显而易见的。首先是不同部门间的数据信息不能共享，数据出现脱节，势必给企业带来重复多次采集、数据冗余的问题，甚至数据一致性和正确性也可能无法保证。其次在涉及多工作模块数据时不能有效共享互动，会导致数据的价值不能得到真正体现，以致对企业的决策支持只能流于空谈。

数据孤岛产生的数据割裂也严重制约了人工智能的发展，人工智能应用需要大量的数据。发展人工智能需要消除数据孤岛，不仅是内部消除孤岛，还要消除外部孤岛，最终形成智能化应用的闭环。未来大数据的发展是要消除各行业的数据孤岛现象，创造出各种渠道、模式让数据协作的更好。

1.2 隐私换便利现象

移动互联网时代，不少企业强制用户开放与其提供的服务毫不相关的各种手机权限，不同意就不能用——手电筒软件为什么要知道我在哪里，天气软件打探我的通讯录做什么？我们在享受互联网软件提供便利的同时，不得不牺牲一些个人隐私，这就是隐私换便利。

隐私换便利不是新鲜事——“你向医生袒露身体的隐私，以换取健康的保证；你向邮局公开住所的隐私，以换取信报邮包的及时送达”。与互联网软件获取用户隐私不同的是，这两个例中消费者是在知情的情况下自愿适度让渡隐私换取必要的服务。“知情”“自愿”“适度”“必要”等限制性要素缺一不可，突破限制就会走向反面。而用户在与互联网软件交互中显然多数不是自愿的，而且也不是在适度必要的原则下提供数据，更没有对自己数据使用的知情权、更正权和退出权等。

网络服务提供者大量收集用户数据后，导致用户毫无隐私地赤裸裸地暴露在网络服务提供者面前。而有些不法人员也趁机把个人隐私在网上被当成商品买卖，造成大量的用户数据泄露，甚至还形成了产业链条，催生了变现途径。据调研问卷分析，70%以上的社会公众对当前个人信息环境缺乏安全感。未来在隐私性和便利性之间，通过技术创新寻求一个平衡点是至关重要的一环。

1.3 数据安全与隐私保护新挑战

随着越来越多的数据产生，用户隐私保护日益成为关注热点，而同时打破数据孤岛进行数据共享和交换也会面临数据安全的问题。尤其是近年来数据泄漏事故频发，数据安全和隐私保护问题引起了全球的关注。2016 年 11 月，我国通过了《中华人民共和国网络安全法》，旨在通过多项举措加强个人信息和数据保护。2018 年 5 月在欧盟生效的《通用数据保护条例》（GDPR）[1]规定用户可以要求经营者删除其个人数据并且停止利用其数据进行建模，而违背该条例的企业将会面临巨额罚款。在 GDPR 正式实施一个月后，美国加利福尼亚州颁布了《2018 年加州消费者隐私法案》（CCPA）[2]，加强消费者隐私权和数据安全保护。2019 年 5 月 28 日，我国国家互联网信息办公室发布了《数据安全管理办法（征求意见稿）》[3]，提出了收集重要数据的备案制以及向第三方提供重要数据的批准制的新要求。中国人民银行近期正式发布了《个人金融信息保护技术规范》[4]，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。而随着 2020 年《信息安全技术 个人信息安全规范》修订版[5]正式获批发布，数据安全和隐私保护将迎来新时代。

1.3.1 相关概念

参照相关标准，这里给出数据安全和隐私保护相关术语的统一定义：

- 数据安全：以数据为中心的安全，保护数据的可用性、完整性和机密性。
- 数据交换：数据供方和需方以数据商品作为交易对象，以货币或者数据商品交换。数据商品包括原始数据或加工处理后的数据衍生产品[6]。
- 个人信息：即隐私。能单独或结合识别特定自然人身份或反映其活动情况的各种信息。个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。关于个人信息的判定方法和类型参见《信息安全技术 个人信息安全规范》[5]。
- 数据共享：数据控制者向其他控制者提供数据，且双方分别对数据拥有独立控制权的过程。
- 数据有用性：数据对于应用有着具体含义、具有使用意义的特性。每种应用将要求数据具有某些特性以达到应用目的，因此在数据去标识化、脱敏或加密后，需要保证对这些特性的保留。

1.3.2 数据可用不可见的趋势

大数据时代，数据已经成为个人或企业的核心资产，数据资产化趋势明显。尤其是个人数据资产，在不久之后的未来，我们会看到一个与真实的物理世界平行的虚拟世界里，所有的个人信息资产包括房产、存款、汽车、保单等会成为信贷或各种交易的依据。简单直接共享这些数据资产无法保护用户隐私，显然是不安全的，如果数据不对外共享，可以保证数据对外不可见，但也不利于数据经济价值的发掘。把数据资产根据场景提取有用的知识，把知识开放共享才是保证数据可用的一种合理解决方案，这就是资产知识化。从数据资产化和资产知识化可以看出一种数据应用的新趋势——数据可用不可见。

1.4 知识联邦应运而生

1.4.1 大数据、人工智能与密码学交叉融合

最近几年，学术界和工业界都已经开始在数据安全和隐私保护方向的探索。尤其是在大数据、人工智能和密码学等领域，出现了安全多方计算、隐私计算、联邦学习、可信执行环境等多个方向，都在研究如何在保证数据安全的前提下打破数据孤岛，实现数据可用。具体解决方案基本上沿着两个方向在演化：

- 中心化向分布式或去中心化过渡。现有的大数据平台基本上都是中心化的，对数据进行集中的存储、管理、分发等操作。中心化方式的缺点是数据存储在第三方平台，脱离数据提供方的控制，违背了数据隐私保护的规定。同时，随着数据规模的不断变大，直接在中心服务器上计算或学习的压力也会不断增加。为了减轻这种压力，计算或学习过程需要分散到数据提供方或终端设备上进行，这种分布式计算或学习的过程则是人工智能领域更关心的问题。而如果没有中心节点的存在，这种智能化的过程则变为去中心化的形式。这时的数据是分而治之，各自为数据所有者控制，每个节点上的数据相对只是小数据，但是由于可以触达更多的数据，其性能甚至会超越有限数据的中心化聚集方式。
- 数据向知识化升级。为了保护节点数据安全和隐私，直接共享使用显然是不可行的，要做到数据对外不可见才是关键，这就需要密码学。通过加密方法（如：哈希编码、同态加密等）对数据脱敏和去标识化，让数据转化成为安全的信息或者知识，再对分散的信息计算或知识聚合，来保证数据不直接共享但是可用的。

多学科多领域的交叉融合发展是大势所趋。大数据、人工智能和密码学的交叉融合可以将大数据分解成小数据，确保参与各方数据的独立性，同时用加密技术保证参与数据的安全，解决参与方互不信任的问题，最终通过在小数据生成的信息或知识的基础上联邦实现大智能。

1.4.2 知识联邦开创数据可用不可见新局面

数据可用不可见的目标是实现数据智能化利用同时又保证数据安全与隐私保护。其核心有两层含义：

1）数据可用性，也就是数据开放性。目前的人工智能本质上是数据智能，也就是用大数据来训练计算模型支撑业务应用。但是现实中数据是各机构或个人的核心资产，数据孤岛现象普遍存在。如何充分利用各方的数据，让数据对外开放，进行智能化服务，这是数据可用关心的重点。

2）数据不可见性，也就是数据不共享。不共享数据，也就是数据不离开各机构或个人，可以保证数据对外不可见，自然也就可以保护数据隐私了。但这也会导致数据孤岛现象更加严重，智能化发展受到更大制约。

数据不可见性可以采用加密技术解决，但是针对数据可用性则需要考虑数据的应用场景，常见的应用包括查询、计算、学习、推理等。为此，同盾科技提出了“知识联邦”的理论框架体系，它是人工智能、大数据和密码学交叉融合的产物。知识联邦首先将数据转化成信息、模型、认知或知识，满足数据不可见，再通过联邦的方式实现数据可用，打造安全的人工智能。

知识联邦是一个国产原创、自主可控、全球引领的技术体系，该体系在解决了数据割裂和隐私保护问题的同时，可以进一步开展跨源跨域的知识发现、表示、归纳、推理和演绎，为人工智能 3.0 奠定了坚强的基石。

1.4.3 知识联邦的历史新机遇

在智能时代，数据将成为驱动技术革命和重新定义人类社会未来的新动力。2020 年 4 月 9 日，中共中央国务院出台了《关于构建更加完善的要素市场化配置体制机制的意见》[7]，首次明确将数据纳入生产要素，与土地、劳动力、资本、技术等传统要素并列。意见强调要从三个方面加快培育数据要素市场：

1） 推进政府数据开放共享，加快推动各地区各部门间数据共享交换。
2） 提升社会数据资源价值，培育数字经济新产业、新业态和新模式。
3） 加强数据资源整合和安全保护，尤其是对政务数据、企业商业秘密和个人数据的保护。

作为一种安全的数据和知识交换框架体系，知识联邦有助于打破数据孤岛，推动各地区各部门间数据共享交换，充分挖掘社会数据资源价值。

数据作为一种新型生产要素，必将成为智慧城市建设的有力抓手。社会数据的应用场景也日益丰富，可以促进 5G、大数据中心、工业互联网、人工智能等新型基础设施建设，进而提升全社会数字化水平。这正是知识联邦迎来的一个历史新机遇。我们也相信知识联邦打造的数据安全的人工智能生态系统能够为新基建国家级战略规划贡献一份力量。

第2章 知识联邦概念

2.1 知识联邦概述

知识联邦从字面上理解可以看成是“知识”和“联邦”两个概念的结合，下面分别进行介绍。

2.1.1 知识

我们身边充满了各种各样的数据，有数字、文字、图像、符号等，在没有被处理之前，这些数据并没有什么潜在的意义，也不会有什么价值。当通过某种方式对数据进行组织和分析时，数据的意义才显示出来，从而演变为信息。信息具有一定的价值，可以对某些简单的问题给予解答，譬如：谁？什么？哪里？知识是在对信息进行了筛选、综合、分析等过程之后提炼融合出来的。它不是信息的简单累加，往往还需要加入基于常识和相关知识及上下文所作的判断。因此，知识可以解决较为复杂的问题，可以回答和解释“如何”、“为什么”、“如果不”（反事实的，Counterfactual）的问题[8]，能够积极地指导任务的执行和管理，进行决策，并最终形成智慧。从数据到智慧[9]是要经历多个层级的，而知识正是将数据转变成为智慧的关键一环。

为了更有效地对数据、信息和知识进行比较分析，我们在这里分别给出如下的定义：

- 数据是对客观事物的数量、属性、位置及其相互关系进行抽象表示。
- 信息是经过加工处理具有逻辑关系的数据，它对决策是有价值的。
- 知识是对信息进行归纳、演绎后，沉淀下来的有价值的信息，与决策相关。

事实上，数据是没有对错的，但得到的信息可能会是错的，可能无法反映真实的情况。特别是在噪声比较强的环境下的数据，更容易使信息出错。各种信息来源参差不齐，真正有价值的信息往往被裹挟在大量冗余、错误且一直呈爆炸性增长的信息之中。而知识具有去伪存真、去粗存精的作用，它可以从信息中提炼出有价值的信息，形成规则策略，用于指导后续的行动或决策。

在实际应用中，数据、信息和知识三者之间的区别并非泾渭分明，常常被混用，主要是因为数据、信息和知识的界定是与实际使用者和应用场景相关的。某个经过加工的数据对某个人来说是信息，而对另外一个人来说则可能是数据；一个系统或一次处理所输出的信息，可能是另一个系统或另一次处理的原始数据。同时，在某个语境下是知识的内容，在另外的语境中，可能就是信息，甚至是无意义的数据。

2.1.2 联邦

联邦常用于政府的组织形式中，是一种协约。依据这种协约，几个独立的政治单元联合起来，构成一个有机整体。联邦国家作为一个整体有自己的立法、司法和行政机关，联邦成员各也有自己相对独立的立法、司法和行政机关，有较大的自主权。联邦成员之间是平等的，新成员加入后联邦会不断扩大。

解决数据孤岛难题同样可以采用联邦的方式，联邦连通了每个数据孤岛所属的机构。此时，每个机构就像一个个独立的政治单元，他们自行管理自己的数据，是自治的；但

是机构之间会通过一种协议联合起来，共同参与组成一个整体作为联邦机构，所有参与成员共同赋予联邦机构一定的权利由其统一行使。因此，知识联邦中的联邦在本质上是一种数据和知识安全交换协议。

2.1.3 从数据联邦到知识联邦

数据联邦是一种数据集成方法，将多个不同的来源的的数据库进行集成，比如联邦数据库系统[10]。数据联邦是为了实现对多个独立的数据库进行相互操作，它只是提供了一种为数据提供抽象的数据接口的能力，而数据消费者不需要知道数据的物理位置、数据结构和保存方式。数据联邦在一定程度上解决了数据孤岛的难题，但是在交互过程中不涉及任何隐私保护机制，因此存在监管合规的问题。

知识驱动的联邦技术则是在联邦的理念上进一步升华，有了新的飞跃。知识的提炼和生成需要人工智能和大数据技术的有机结合，知识的升级和扩展则离不开密码学支撑的多方安全联邦技术。知识联邦可以打破数据孤岛困境，并保护数据隐私，符合法规监管的要求。而且，知识联邦除了能用于进行数据查找、合并等基本操作外，还可以进行安全多方计算或者多方联合学习建模，充分利用多方数据中蕴含的知识，提供更好的决策服务。

2.2 知识联邦定义

知识联邦的基本内涵 [11]包括：

- 基于**数据安全交换协议**，来利用**多个参与方**的数据；
- 基于多方数据进行安全的**知识共创、共享和推理，**实现数据可用不可见；
- **支持统一的多层次的知识联邦生态**：信息层、模型层、认知层和知识层；
- **管理知识安全联邦的全生命周期**：统计查询、训练、学习、表示、预测和推理及其监管、仲裁和评价。

简单地讲，知识联邦是将散落在不同机构或个人的数据联合起来转换成有价值的知识，同时在联合过程中采用安全协议来保护数据隐私。知识联邦不是一种单一的技术方法，它是一套理论框架体系，是人工智能、大数据、密码学等几个领域交叉融合的产物。

知识联邦是一个支持安全多方检索、安全多方计算、安全多方学习、安全多方推理的统一框架，为打造安全的知识融合、管理、使用的生态系统提供设计指南和标准。它可以用于涉及到数据安全和隐私保护诸多领域，尤其是在金融、保险、医疗或政务等行业中有非常大的应用潜力。

知识联邦是一个国产原创、自主可控、全球引领的技术体系，该体系在解决了数据割裂和数据安全问题的同时，可以进一步开展跨源跨域的知识发现、表示、归纳、推理和演绎，为人工智能 3.0 奠定了坚强的基石。

2.3 知识联邦与相关技术

表 1. 弱中心化与强中心化、去中心化对比

分项	强中心化	分布式	
		去中心化	弱中心化
数据安全	中心节点归集所有数据 参与方数据失去控制权 安全性低	参与节点存储所有数据 数据访问需共识授权 安全性中	参与节点存储本地数据 不对外共享本地数据 安全性高
计算效率	中心节点计算所有数据 效率适中	本地计算所有数据 效率低	本地计算本地数据 效率高
网络通信	一次性传输 效率高	多方相互通信 效率低	通过中心节点通信 效率适中

在实践中，知识联邦采用的是**弱中心化**的分布式方法，这与传统的强中心化和完全的去中心化还是有很大差别的，如表 1 所示。强中心化模式下，中心节点（也称作第三方）会聚集并保存所有参与方的数据，所有的计算和学习都是在中心节点完成，强中心化方式有数据安全隐患，隐私保护方面也很难合规。去中心化模式没有中心节点，需要所有参与方互联互通。去中心化以区块链为代表，通常会在节点中保存完整数据或者保存区块头来索引相应区块，同时通过多方共识机制进行数据访问授权，当节点规模较大时，通信成本很高，达成共识效率低下。而弱中心化模式中原始数据是保留在本地，并且不会离开本地的，计算和学习仍然发生在本地，中心节点仅对参与方模型知识进行安全的聚集。弱中心化模式达成了效率和安全之间的平衡，是一种更切实可行的安全多方应用解决方案。这种模式尤其适合在强监管行业应用，有助于监管部门开展合规监管工作。

表 2. 知识联邦与相关技术

技术领域	关注点	数据控制	实现方式	与知识联邦关系
联邦学习	模型训练学习	参与节点控制自有数据	弱中心化	是知识联邦的子集
区块链	分布式记账系统	参与节点存储所有数据	去中心化	可结合使用
隐私计算	全生命周期的隐私信息保护和计算	参与节点控制自有数据	去中心化	与知识联邦中的联邦计算部分相似
安全多方计算	多参与方的统计分析计算	参与节点控制自有数据	去中心化 弱中心化	是知识联邦的子集
可信执行环境	隔离的执行环境	参与节点控制自有数据	硬件实现	知识联邦的硬件化实现方式
分布式机器学习	模型训练学习	中心节点控制数据	强中心化	与知识联邦中的跨样本联邦部分相似
知识联邦	安全多方查询、计算、学习和推理	参与节点控制自有数据	弱中心化	/

知识联邦是一个统一的安全多方应用框架，它支持安全多方查询、安全多方计算、安全多方学习、安全多方推理等多种联邦应用。知识联邦在借鉴一些相关技术的同时，也具备一定的独创性，尤其是在认知层和知识层联邦都是自主创新的。知识联邦与其它技术领域，如联邦学习、区块链、隐私计算、安全多方计算等，都有着紧密的关系。表 2 简单概括了它们之间的关系，下面我们将从多个角度进行详细阐述。

2.3.1 知识联邦与联邦学习的关系

联邦学习[12],[13],[14]更关注的是联合建模训练过程，最初的联邦学习是面向用户客户端解决跨样例联邦问题的。在这种情况下，数据特征在每个用户端保持一致，如何通过安全联邦的方式训练模型成为关键，而至于模型训练好之后的预测基本不用考虑，因为每个训练好的模型只依赖当前用户端的数据，预测时不需要数据交换。在机构间进行跨特征联邦时，建模完成后的预测过程中仍然需要进行联邦。

知识联邦关注的是通过联邦提取有用的知识，其联邦的目的可能是建模、预测、计算、推理。知识联邦不仅仅是面向学习，还包括安全的多方计算和知识推理。联邦学习更多是知识联邦中模型层联邦，而知识联邦除了包括模型层联邦外，还包括信息层、认知层和知识层等几个层级的联邦。因此，联邦学习是知识联邦的一个子集，专注于数据分布的联合建模，详细讨论参见章节 3.4.3。知识联邦关注的是安全的数据到知识的全生命周期的知识创造、管理和使用及其监管，设计目标是面向生产环境的完整知识联邦生态系统，致力于推动下一代人工智能，不仅仅是一个安全的联合建模。

2.3.2 知识联邦与区块链、隐私计算的关系

区块链本质上是一个去中心化的数据库，它通过共识机制创造信任保证数据一致性。知识联邦更多是介于去中心化和强中心化中之间的一种弱中心化的模式，第三方在其中作为一个协调和仲裁的角色出现，它不会像强中心节点一样保存所有的数据，更多是对参与方知识进行聚集，并对参与方数据质量和贡献进行仲裁。在数据存储中，区块链的节点会保存完整数据或者保存区块头来索引相应区块。这与知识联邦在本质上是不同的，知识联邦中原始数据是保留在本地，并且不会离开本地的。区块链中常用非对称加密和授权技术保证账户身份信息的数据安全和个人隐私，而知识联邦则是通过数据知识化后进行加密联邦。当然知识联邦也可以与区块链技术相结合，利用区块链的去中心化的信任和共识机制。

隐私计算是从数据的产生、收集、保存、分析、利用、销毁等环节中对隐私进行保护，是面向隐私信息全生命周期的。隐私计算本质上是一类在保证数据提供方不泄露敏感数据的前提下，对数据进行计算并能验证计算结果的技术。同样是关注隐私保护，隐私计算是关注隐私数据全流程中的保护问题，其分析也更侧重于计算，不涉及训练学习，与知识联邦的联邦计算（参见章节 3.4.2）有较多相似；知识联邦更关心数据分析和利用过程中的隐私保护，也不局限于计算分析还包括模型和知识的学习、预测、推理等。隐私计算常与区块链结合，以去中心化形式落地；知识联邦更多会是以一种弱中心化的方式呈现，更切实可行。

2.3.3 知识联邦与安全多方计算的关系

安全多方计算（MPC）[15]是一种在无可信第三方的情况下，安全地计算一个约定函数的方式。MPC 中各参与方可以在本地数据不被归集、隐私数据不被泄露的前提下，共同执行既定逻辑的运算，获取共同想要的数据分析结果。计算参与方只需参与计算协议，无需依赖第三方就能完成数据计算，并且各参与方拿到计算结果后也无法推断出原始数据。

理想状态下的 MPC 是不依赖于第三方的，也就是一种去中心化的模式，但是 MPC 只会在本地数据上进行计算。理想的 MPC 在多方参与时通信交互会非常复杂，效率低下。如果 MPC 也采用弱中心化的方式，那么它就和知识联邦中的联邦计算是等价的了，也就成为知识联邦的一个子集，关于联邦计算的介绍可以参见章节 3.4.2。MPC 更关注数据计算层面的问题，但是知识联邦除了多方联合计算之外，还会关注多方联合建模、多方联合预测和多方联合推理等应用。

2.3.4 知识联邦与可信执行环境的关系

可信执行环境（TEE）提供一个隔离的执行环境，提供的安全特征包含：隔离执行、可信应用的完整性、可信数据的机密性、安全存储等。主要思路是在计算机硬件平台上引入安全芯片架构，通过提供的安全特性来提高终端系统的安全性。TEE 是一种数据安全和隐私保护的硬件实现方式；知识联邦则对硬件执行环境没有特定的要求，是一种更便捷的实现方式。知识联邦也可以与 TEE 相结合，在联邦节点上采用 TEE 实现以提升数据安全性，构建更可信的知识联邦。

2.3.5 知识联邦与分布式机器学习的关系

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，参数服务器是分布式机器学习中一个典型的例子。分布式机器学习强调如何加速模型训练过程，不关注数据安全和隐私问题。而对于知识联邦而言，首先采用弱中心化的计算模式，不像分布式机器学习那样有强中心节点主导；其次知识联邦中的参与方是数据拥有方，对数据有独立控制权，而分布式机器学习中数据的拥有者和控制权都是中心节点；最后，知识联邦在进行多方计算和学习过程中更关注参与方数据安全和隐私保护，目的是在打破各方数据割据的同时又能达到安全合规要求。

2.3.6 知识联邦与差分隐私的关系

差分隐私[16]是密码学中的一种实现隐私保护的技术手段，旨在提供一种当从统计数据库查询时，减少泄漏数据库中具体记录所属主体的身份的机会。差分隐私是一个概率概念，它通过加扰在统计数据的准确性和隐私参数之间进行权衡，实现准确性与隐私的均衡。差分隐私是实现安全知识联邦的一种技术手段。在联邦过程中同样需要用到这

些传统的隐私保护和加密技术，即便是在模型层、认知层和知识层联邦时，虽然传输数据已经被加工处理过，但仍需要采用这些技术来保护数据隐私。

同盾科技有限公司

第3章 知识联邦分类

知识联邦的分类可以有很多种方式，可以按联邦阶段、数据特点、参与对象类型和应用目的进行划分，如图 1 所示，下面分别进行介绍。

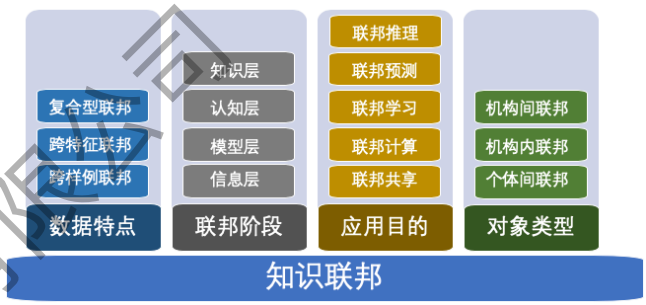

图1. 知识联邦分类

3.1 按联邦阶段分类

知识联邦按照联邦发生的阶段可以分为四个层级：信息层、模型层、认知层和知识层，其整体层级结构如图 2 所示。

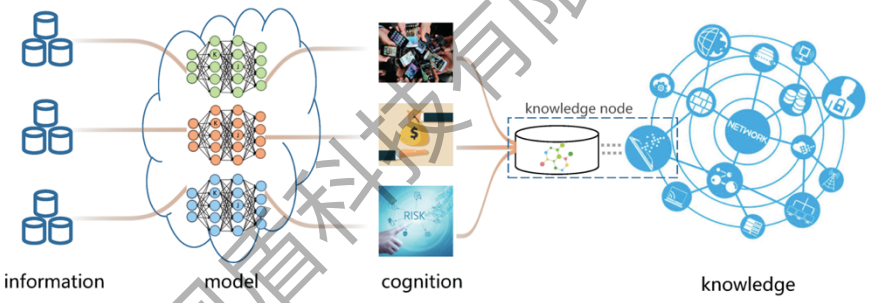

图2. 知识联邦的层级

3.1.1 信息层

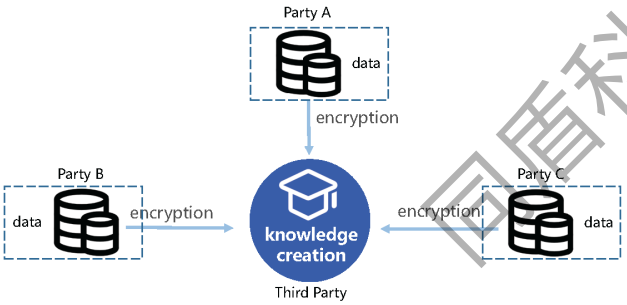

图3. 信息层联邦

信息层联邦是指在将原始数据汇聚到第三方服务器之前，必须对参与方数据进行清洗、转换和加密，让数据变成有价值的密文信息，如图 3 所示。值得注意的是，这里的

加密要求是非常严格的，不允许密文信息在第三方服务器中解密后运算，通常需要采用同态加密技术。知识创造过程发生在第三方服务器上，它直接对密文信息进行计算或学习，不能解密。信息层联邦的优势是联邦过程是一次性通信，通信开销小，但缺点在于对于加密方法要求较高，而且在密文信息上的训练学习也比较困难。

信息层联邦和隐私计算和安全多方计算有很多相似之处，但信息层联邦不仅仅局限于计算应用，还可以在密文上进行安全的学习和推理。比如 Aslett 等人[17]在 2015 就采用完全同态加密方法进行隐私保护的机器学习。随后，Dowlin 等人[18]又提出了第一个基于密文信息的神经网络 CryptoNets 做隐私保护的深度学习。信息层联邦常用于多头共债、黑名单查询、用户对齐等应用中。

3.1.2 模型层

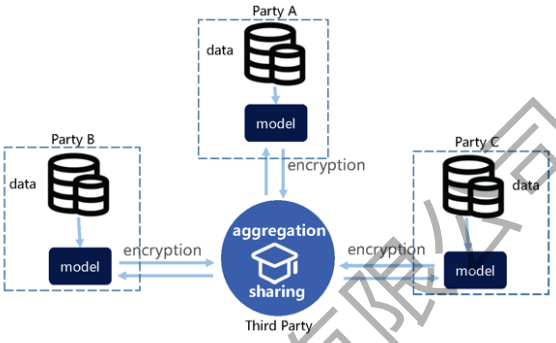

图4. 模型层联邦

模型层联邦主要发生在模型训练过程中。基本思想是首先在各个参与方分别利用自身数据训练学习一个初步模型；然后将模型更新的模型参数加密后上传至第三方服务器进行聚合；聚合后的更新参数再分发给各个参与方用于各参与方本地模型的参数更新；模型迭代后再进行聚合，如此重复多次直到模型收敛，如图 4 所示。这里知识提取过程发生在参与方内部，局部知识聚集后可以有效平衡各方的数据偏差，形成更鲁棒的全局知识。

模型层联邦与现在热门的联邦学习在本质上是一致的。模型层联邦的优势是训练学习是分布式的，即模型的训练、优化发生在各个参与方，第三方只进行聚合，计算开销小。但其最大劣势是联邦过程需要频繁地进行模型参数的上传和分发，通信成本高。尤其是对网络安全要求较高的金融机构，通常会将内外网隔离，如果是在内网训练，多方只能在外网定时联通聚合，必然会导致训练周期变长。此外，由于模型参数中蕴含着数据隐私信息，所以在上传聚合前同样也需要同态加密或差分隐私等方法进行安全处理。

3.1.3 认知层

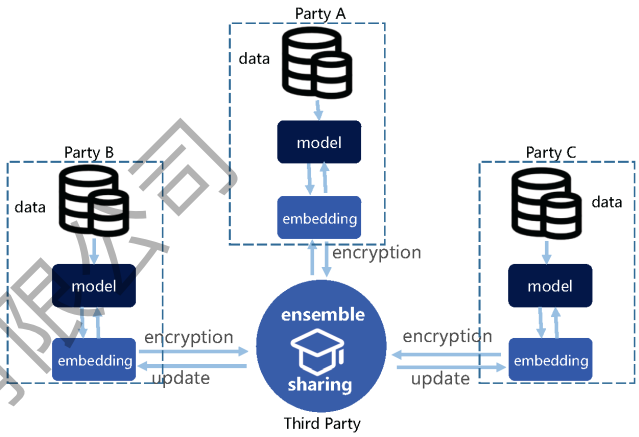

图5. 认知层联邦

认知层和模型层的显著区别在于，是用嵌套特征而不是模型更新进行联邦。嵌套特征可以是深度神经网络中的全连接层，也可以是特征提取后得到的高层语义特征或局部认知结果。在第三方联邦时，会基于局部嵌套特征再训练或学习一个独立模型，训练过程也会与各参与方交互并迭代至收敛。具体如图 5 所示，联邦前先用本地数据提取嵌套特征，然后再加密发送到第三方服务器进行联邦知识发现。局部嵌套特征可以看作是元知识，联邦集成后创造的知识时一种综合知识。

认知层联邦如果是应用在各联邦节点上数据同构但样本不同的场景下，理论上与集成学习的核心思想一致。事实上，认知层联邦更经常遇到的场景是在各联邦节点上数据异构的情况，比如在分布式的多模态学习中，需要融合图像、声音、视频、文字等信息进行综合认证，以降低金融交易环节中的风险。

3.1.4 知识层

一旦初始知识以某种方式构建并保存在知识库中，联邦将进入一个更高级的阶段，即知识层联邦。在该阶段，多个知识库中的知识相互协作进一步演绎出更重要的知识。为了能让知识不同知识源之间自由流动，需要将每个知识库当作一个知识节点连接起来构建一个知识网络。值得强调的是，知识网络与知识图谱完全不同，但又密切相关。后者主要描述实体及其相互关系，以图表形式组织。知识网络是建立在知识图谱之上的一种网络，它是由与多个特定领域知识组成的网络。

简单地说，知识层联邦实际上是通过知识融合或推理，让知识在知识网络中自由流动，以创造或挖掘出更全面、更有价值的知识，这对管理决策有很大帮助。知识推理和演绎相关技术在分布式环境下的扩展，是知识层联邦落地的一种解决方案。

3.2 按数据特点分类

参与联邦的各方数据分布有时是相同的，有时又有很大差异。根据数据分布的差异，可以将知识联邦划分为：跨样本联邦、跨特征联邦和复合型联邦。

3.2.1 跨样本联邦

跨样本联邦是指每个联邦参与方的数据具有相同的特征分布，但各方的样本（或用户）是独立的，而且每个参与方都有与自己样本对应的标签数据。联邦的目的就是要充分利用数据持有者的样本和标签数据，让各个参与方利用自由数据在本地进行训练或知识化提取，然后在通过模型知识聚合方式不断更新模型知识。

由于本地标签只是用于监督本地模型训练，所以跨样本联邦不需要在不同参与方之间传输标签数据，降低了联合训练的难度。跨样本联邦的模型在训练和预测中都仅仅利用自有数据，因此也避免了在模型预测时需要联合预测。跨样本联邦最典型应用就是，Google 提出的在手机输入法中根据用户输入习惯预测下一个可能出现的单词。

跨样本联邦在联邦学习中也称作横向联邦学习[13], [14]，但是跨样本联邦不仅仅可以用于联邦学习建模，还可以用于联邦计算分析。在实际应用中，由于不同机构中样本数据特征分布很难保持一致，因此跨样本联邦应用场景也有很大的局限性。

3.2.2 跨特征联邦

联邦应用的一个目的就是利用其他参与方的数据弥补自身数据不足，以计算或学习更好的模型知识。尤其是在机构间，数据特征分布不同，但不同参与方之间有很多共同的用户样本，那么融合这些交集样本的独立特征将有助于模型知识的优化，这就是跨特征联邦。跨特征联邦要比跨样本复杂，因为此时的参与方可能只有一家是有标签数据的，训练过程中不仅仅要保证特征数据的安全，还要防止标签数据的泄漏。由于模型需要用多方数据才能训练，模型预测时也同样需要多方数据才能完成，这也就意味着在生产环境也需要联合预测。

跨特征联邦在联邦学习中也称作纵向联邦学习[13], [14]，但是跨样本联邦并不局限于学习建模，还可以用于联邦计算或推理。跨特征联邦在金融行业中有非常广泛的应用需求，不管是信用评估还是反欺诈，都需要联合多方数据进行跨特征联邦才能有效解决。

3.2.3 复合型联邦

除跨样本和跨特征联邦之外，还有一种更复杂的场景，其中只有一小部分样本或特征集是参与各方的交集，其余数据无论是特征分布还是样本分布都不相同。这种场景下，涉及跨样本和跨特征的组合，因此我们称之为复合型联邦。复合型联邦尽管复杂，但也有很多可行的解决方案，比如可以采用元学习、迁移学习或知识蒸馏 [14][19][20]等方法提取不同领域知识并自适应到目标领域。这种联邦在实际应用中更为常见。比如有两个机构，一个是位于甲城市的且面向当地客户的保险公司，另一个是位于乙城市的服务于周边居民的地方医院。显然，由于地理区域不同，双方共同用户群体很少；而业务上的差异也决定了两个机构之间的数据特征是异构的。如果保险公司想在乙城市开展业务，并期望利用医院数据来进行当地客户风险评估，这时复合型联邦将派上用场。

3.3 按对象类型分类

知识联邦按照联邦参与对象类型分为三种：个体间联邦、机构内联邦、机构间联邦。

3.3.1 个体间联邦

个体间联邦，是面向个人终端用户的，这种场景下要求每个用户数据都不离开个人终端，以保证用户隐私不受侵犯；同时希望利用每个用户的数据，通过大量用户数据提炼一个稳定可靠的通用模型。在通用模型的基础上，每个用户还可以根据自己的行为特征定制个性化服务。个体间联邦采用的数据特征属性是一致的，因此通常都属于跨样本联邦。

比如，在用户浏览习惯分析中，由于用户浏览细节会涉及个人隐私，这些数据不能直接对外共享，要利用这些数据就只能直接在个人终端上计算，再将每个个体上得到的模型知识进行联邦。通过个体间联邦，可以让终端设备更懂用户让应用服务更贴心，同时由于数据对外不可见，用户隐私数据也不会发生泄漏。

3.3.2 机构内联邦

机构内联邦常常发生在大型企业集团内部。不同分公司所处地区不同，面向的客户群体也不相同，而各子公司因为业务类型不同也产生的数据特征不尽相同。比如有些保险公司在国内和东南亚地区都有业务，但是东南亚地区客户数据量较少，国内数据较多，公司希望在东南亚应用的营销模型或风险控制模型可以利用国内数据。由于数据出境合规性要求，不能直接将双方数据聚集在一起使用。那么这时就可以采用机构内联邦的方式，在保证数据安全同时，双方联合训练模型，以适应业务的需求。

3.3.3 机构间联邦

机构间联邦会出现在政府部门或企业之间。比如在疫情期间，要分析感染人群的行为轨迹和跟踪密切接触人群，就需要联合运营商、社交、交通和社区等部门的数据。各机构的数据字段属性不同，但可以起到互补作用，充分利用每一方的数据可以进行有效分析进而深度挖掘潜在的风险人群。但是，由于涉及到很多用户的隐私信息，数据直接对外共享，这时就可以采用机构间的知识联邦，从各部门数据中提取有用知识，通过知识共享和推理的方式解决这个问题。

3.4 按应用目的分类

联邦是一种数据和知识安全交换协议，按照联邦应用目的的不同，可以细分为联邦共享、联邦计算、联邦学习、联邦预测和联邦推理。因为联邦本身就是解决安全多方问题的，所以这些术语也可以称作：安全多方共享、安全多方计算、安全多方学习、安全

多方预测和安全多方推理。这些应用与信息层、模型层、认知层和知识层联邦有潜在的对应关系，具体如表 3 所示。

表 3. 联邦应用与联邦阶段对应关系

联邦应用	别名	关注重点	联邦阶段
联邦共享	安全多方共享	数据查询检索	信息层
联邦计算	安全多方计算	线性统计分析	信息层
联邦学习	安全多方学习	复杂模型训练学习	模型层、认知层
联邦预测	安全多方预测	模型预测使用	信息层、模型层
联邦推理	安全多方推理	知识推理和演绎	认知层、知识层

3.4.1 联邦共享

联邦共享不是简单的数据共享，它是在联邦的基础上，也就是在满足数据和知识安全交换协议的基础上，进行数据或知识的共享。而且，这里的共享并不会将数据控制权转移给其他参与方，数据拥有者依然独立保持对数据的控制权。在某种程度上，联邦共享类似于数据联邦，但前者会更关心数据安全和隐私保护。联邦共享的核心在于参与方之间的数据保留在本地，分别经过分类分级脱敏后与其他参与方数据形成虚拟的动态数据仓库对外提供服务。

联邦共享主要用于多方数据安全查询和检索。在打通政务数据开展一网通办业务中，可以采用联邦共享的方法破解横向数据共享交互的难题，这也是未来新基建中建设大数据中心的基础。

3.4.2 联邦计算

实际应用中有许多先验知识可以直接利用，这种先验知识可能是从实践中积累生活常识，也可能是在理论上已经验证过的领域知识，它们共同的特点就是已经经过验证不需要再从大量数据中挖掘学习。基于已有的规则性知识，利用各参与方数据进行联合计算，得到统计分析结果，这就是联邦计算。联邦计算通常会直接在密文数据上进行计算分析。

安全多方计算可能是在工业界和学术界使用更多的一个术语。理想的安全多方计算常以去中心化的方式实现，而联邦计算会采用一种弱中心化的方式实施。安全多方计算与联邦计算其实本质上是一致的，都是利用多方数据安全地进行统计分析或线性计算。如果安全多方计算也采用弱中心化方式实现，那么它与联邦计算就是完全等价的了。

3.4.3 联邦学习

联邦学习，也称作联邦建模或联邦训练，其主要目的是联合多个参与方的数据进行模型训练学习，这个过程主要对应模型层和认知层联邦。在利用参与方现有的数据时，保证数据不离开本地，同时能够形成一个更全面的模型知识。简单地讲，联邦学习就是将传统的联合建模过程分布式线上完成。但是传统的联合建模常用于异构数据的跨特征联邦，显然联邦学并不局限于传统的联合建模，它还包括同构数据的跨样本联合训练。

跨特征联邦学习在金融行业合作中常有应用，跨样本联邦学习在用户个性化产品定制或智能化运维中经常会用到。

3.4.4 联邦预测

联邦学习生成的模型在使用过程中还会遇到另一个问题，那就是模型预测。跨样本联邦学习相对比较简单，因为模型训练发布后不会再涉及多方数据协作进行预测。而跨特征联邦学习在训练模型过程中需要各方数据同时训练，所以模型预测阶段也同样需要各方数据参与才能完成预测。如何保证参与方用户数据隐私的情况下，利用各方数据完成预测，就是联邦预测要解决的问题。

跨特征联邦学习在训练前通常需要进行批量用户样本对齐，安全的用户对齐是希望对齐过程中能保护各方数据不为其他参与方所见。相比之下，联邦预测不需要批量用户对齐，它只需要对单个用户进行查询检索。联邦预测过程中的安全用户查询也希望被查询的用户数据不会被其他参与方知道。

3.4.5 联邦推理

联邦推理是在知识库和知识图谱形成之后，在多个跨领域跨机构的知识库之间进行知识推理和演绎的过程。联邦推理涉及到知识表达规范化、知识融合、知识演绎等 [21]，主要发生在知识层联邦中。例如机构 A 和机构 B 分别侦测到的可能的欺诈团伙关系图谱 G_a 和 G_b，通过知识联邦推理，可以相互增强判断、分类和打分。企业或个人信用评分，也可以通过知识联邦来利用各个机构已经创建的知识，辅助以人工知识及各自的约束条件或目标，进行联邦推理得出并提供可解释性。

第4章 知识联邦平台——智邦

知识联邦平台化核心需要考虑三个要素：数据隐私安全性、模型知识开放性、平台功能实用性。智邦平台（iBond）是同盾科技基于知识联邦理论体系打造的工业级应用产品，是知识联邦的参考实现，构建数据安全的人工智能生态系统。

4.1 平台开放生态

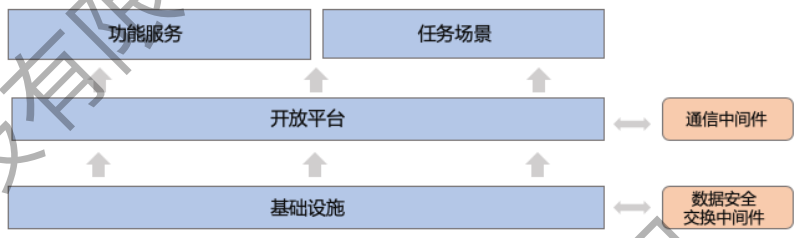

图6.智邦平台生态

如图 6 所示，智邦平台包括四大核心模块和两个中间件。核心模块包括：

- 功能服务模块：主要提供实际应用中需要的诸如账户管理、配置管理、费用统计、测试分析、模型发布等服务
- 任务场景模块：面向需求场景设计模型策略知识，开展学习、计算、检索等任务。比如：信用分、欺诈分、多头贷等
- 开放平台模块：主要完成算法联邦化的实现，支持数据加密解密、计算或学习、知识归集等功能。
- 基础设施模块：提供底层的公共设施，包括：离线/实时任务调度监控、计算环境、资源调度、数据/知识存储。

中间件具体如下：

- 通信中间件：支持内外部网络通信，对接生产/预发环境以及其他参与方。
- 数据安全交换中间件：对接多源异构数据，实现数据标准化和分类分级脱敏加密等。

4.2 平台参与者角色定位

联邦环境中存在多种不同的角色参与其中，具体可以分为：

- 数据提供者，参与联邦计算或学习等行为的数据拥有者。数据提供者通过联邦的方式对外进行安全数据交换，但是数据不离开本地，数据提供者仍旧拥有数据控制权。
- 模型设计者，依托联邦平台设计联邦化模型策略的人员。模型设计者不用关心数据提供者如何进行通信或数据交换，也不需要过多关心模型如何联邦化实施，只需要关心如何利用参与方数据特征设计高性能可解释的模型或依托常识来设计某种策略进行多方计算。

- 模型使用者，使用联邦平台提供的模型策略的用户。这些用户不需要关心模型是如何联邦，调用了哪些参与方的数据，他们只需要利用这些模型开启应用或服务即可。
- 平台运营方，即联邦平台的运营管理者。平台运营方会设计平台运营收费模式，制定相应的利润分配规则，以及平台的发展规划。
- 平台提供方，即联邦平台的开发和维护升级的技术提供方。平台运营方通常会委托平台提供方开发和维护平台，双方保持紧密合作关系。
- 第三方，也称仲裁方或协调方。第三方只承担模型知识的归集工作，不像传统的强中心化模式种的第三方，这里的第三方只是一个协调者，不会解密信息，存储数据。

4.3 平台实施的挑战

4.3.1 可信第三方

在知识联邦中，第三方的存在只是一个协调者和监管者作用，不会触碰参与方的原始数据。事实上，第三方可以是虚拟的，只是一个可审计和可追溯的机器。在数据参与方都达成共识的情况下，虚拟第三方可以部署在更担心数据安全的一方的私有云上，也可以部署在都认可的公有云或专有云上。第三方也可以是实体机构，一般是一个中立的、可信的机构。

可信第三方要保证在任何情况下都不会撒谎，也不会泄露任何不该泄露的信息。可信第三方的选择一般是基于任务场景的，不同联邦任务可能会选择不同的第三方机构。一个有公信力的平台运营方也常常会承担可信第三方的职责。

4.3.2 数据提供者公平性

联邦平台中的数据提供者，尽管在理想状况下会作为诚实参与者严格遵守安全协议执行。但是在实际应用中，也会遇到半诚实参与者和恶意参与者。

- 半诚实参与者：在协议的执行过程中会按照协议要求忠实地履行协议，执行协议后，除了协议的执行结果外没有任何信息泄露。但他们可能会记录下协议执行过程中收集到的所有信息，并试图根据收集到的信息推算出其他参与者的输入信息。所以，半诚实参与者又称为诚实但好奇参与者。
- 恶意参与者：不遵循协议，采取任意的行为获取他方的隐私。常见的恶意行为包括中途退出协议、替换自己真实的输入以及拒绝执行协议等。

针对联邦平台中的半诚实和恶意参与者，还需要探索高效合理的方法来智能监测和识别，以保证参与者之间的公平性和数据安全性。

4.3.3 数据质量和贡献评估

数据质量是数据衍生类产品产生价值的关键，低质量的数据很难创建有价值的模型知识，而数据质量的高低往往又是很难评判的。与大数据平台建设中的数据质量评

价不同，联邦过程中的数据质量评价是面向模型知识应用的。其数据质量的高低主要取决于参与训练学习的数据对模型性能提升的贡献，贡献大质量就高，贡献小质量就低。因此在联邦训练前，一般会分别进行数据特征选择，然后再联邦过程中再进行一次多方数据特征选择，并按照单方模型性能与多方联邦后性能做性能提升效果分析，分别计算出各方在模型中的贡献分。模型贡献分将作为后续利润分配的依据。

4.3.4 平台参与各方的激励方式

事实上，各方参与联邦的动机不同，所以对应可以采取的激励措施是不同的。对于模型使用者，其参与联邦平台的目的是为了借助已有的联邦模型，安全合规地利用多个数据提供者的数据，提升其业务核心竞争力和行业影响力。这种参与方有对联邦模型和数据的刚需，属于模型知识购买方。只要平台提供有效的模型知识，就会积极参与，无需太多激励。

数据提供者通常会有很多自有授权的数据，在数据交易合规要求日益严格的情况下，也需要探索新的数据价值变现方式。数据提供者是利润分配的主体，也有数据合规变现的潜在需求。

其他参与方，包括平台运营方、平台提供方、模型设计者和第三方都是通过提供联邦过程中的相应服务获取利润分配的，是有潜在动力的。

4.3.5 平台数据安全性的证明

联邦的核心是要保证各参与方的数据安全并实现隐私保护。联邦平台的数据安全性可以从数据完整的过程域进行评估，包括数据导入、数据存储、数据处理、数据传输、数据共享、数据溯源、数据销毁。隐私安全性评估可以根据个人信息的类型、敏感程度、处理方式等对个人信息进行分类，分别进行影响分析和风险评价。目前还没有一个类似等保认证的国家级标准规范可以用于联邦平台数据安全和隐私保护评估，这也是需要各方努力共同推进的。

4.4 平台发展路径

4.4.1 建立联邦数据安全交换标准

近两年，在国内外学术界和工业界，掀起了一股联邦学习热潮。这股技术热潮主要是由于隐私保护的合规性要求带来的。但是，目前真正制约联邦（尤其是跨特征联邦）实施应用的难点主要包括：

- 数据异构问题。参与方之间数据异构主要体现在两个方面，一是数据库类型不同，有的采用关系型数据库如 MySQL，DB2 等，有的采用的是非关系型数据库如 MongoDB、Redis 等，还有些采用分布式数据库；二是数据字段描述和数值表示方式不同，同样是出生日期字段不同数据库里可能会采用不同形式描述也可能用不同格式记录。因此，需要在联邦时必须先对各参与方数据进行标准化，让各家参与方数据达成一致。

- 数据一致性问题。实际应用数据有很多种类型，有些属于业务数据，有些属于个人信息，各自敏感级不同。此外，不同数据字段敏感级不同。因此需要对数据进行严格的分类分级，然后分别进行去标识化和脱敏，并要保证去标识化和脱敏后的各方数据具有一致性，这对后续联邦应用是非常重要的。
- 安全交换问题。不论是在联邦计算还是联邦训练中，都会涉及到数据或模型知识与第三方的交互，在交互前必须对这些数据进行加密处理，具体加密方法取决于不同的应用场景。在传输过程中，也需要对传输通道进行加密处理以进一步保证数据安全性。

针对上述问题，亟需形成一套完整的联邦数据安全交换的标准，让参与方在选择使用联邦平台时有规范可依，可以不用担心数据安全和用户隐私的合规问题。标准的建立也有益于推进联邦在各行各业的应用落地。

4.4.2 存量模型联邦化

联邦平台会提供常用的深度网络模型和传统机器学习模型。模型设计者可以更多关注特征选择和指标设计，也可以采用学习流方式设计自己的算法。

此外，有些机构有很多过去通过线下联合建模方式得到的模型，这些模型在应用中相对稳定性能也能满足要求。这些机构希望能够将现有的这些存量模型能够快速的转换成为联邦化的模型，这就是存量模型联邦化的问题。受制于应用场景的限制，联合建模中产生的模型差异很大，也涉及各种不同参与方，所以存量模型目前还无法自动联邦化，但这将是联邦平台进一步演化升级的方向。

4.4.3 打造任务联盟维持开放生态

联邦平台可以解决不同应用场景需求，一个场景就是一类任务，不同类任务之间需要的数据特征也完全不同，相应的参与方也自然不同。比如在个人信用风险评估时，可能会需要个人的收入情况、消费能力、贷款情况以及其它信息，而这些信息可能分布在不同的机构中。根据任务不同，联合相关机构参与任务，建立相应的任务联盟是一件非常有意义的工作。尤其是那些中小微企业，自由数据量少，需要借助外部数据才能开展业务，通过联邦平台建立小范围的任务联盟就可以有效解决这个难题。

联邦平台将会是一个开放的生态。开放主要体现在三个层面：

- 任务联盟是开放的。基于联邦平台，每个机构可以参与多个任务联盟，在不同联盟中也可以开放不同的数据。
- 模型设计是开放的。有兴趣和能力参与模型设计的人员可以开放的加入到联邦平台，并在不同的任务联盟中针对任务需要设计模型。一个模型设计者可以参与多个任务，每个任务也可以有多个模型设计者设计不同的模型。
- 模型使用是开放的。每个任务对应的模型性能效果是对外开放的，可供使用者查询。模型使用者可以根据业务需求选择合适的模型，也可以将不同任务场景下的模型连通起来形成业务闭环。

第5章 知识联邦的应用场景

知识联邦通过安全的数据交换实现知识共创和共享，是打破部门数据割裂，同时确保数据安全和隐私保护的关键，在金融、保险、政务和医疗行业有很大应用潜力，也是实现智慧金融、智慧政务和智慧医疗的基础。

5.1 智慧金融

智慧金融领域中所有需要多方参与建模、知识共享的场景都可以应用知识联邦，尤其是在贷前风险防控，联合营销和多头共债中，可以很好提升企业的核心竞争力和行业影响力。在风控评分中又可以细分为个体信用评估和企业信用评估，具体联邦建模的形式完全取决于参与方之间数据的特点。由于不同机构间含有各种不同维度客户特征，常以跨特征联邦为主。

在现实场景中，金融机构之间、金融机构与政府部门之间，普遍存在基于多方联邦进行安全查询和安全计算的场景。有些是基于高频高并发的非明文加密查询，有些是基于数据可用不可见的建模增益。金融行业普遍存在的多头共债问题，可以采用联邦计算的方式解决，保证多方的信贷数据不共享的同时降低信贷的风险。

联合营销则是可以利用流量渠道的数据与金融机构的数据进行有针对性的精准投放，实现用户增长或默客激活，同时保护各参与方数据不会外流，另外在联合营销的过程中，需求投放方希望核心投放用户数据在三方渠道处是不可细数的，既能满足拉新需求又能保证核心资产安全。

随着互联网银行（也称虚拟银行）的不断发展，智能 KYC 成为客户审核的关键一环，如何在保证客户隐私的同时，能综合利用客户的生物特征信息，如：人脸、声纹、语音，和客户的有效证件信息全方位认识客户，是一个有挑战性的难题，认知层联邦是一个有效的解决方案。

在保险领域，保险产品的定价往往取决于各方面的因素，风控的难度就在于信息的不对称，才会频频出现骗保或薅羊毛事件。在健康险和寿险领域，保险公司和医院数据联邦，可以在保证病人隐私的前提下，健全人、病、医、药、保的全方位知识。这可以通过知识层联邦实现，不仅能加速保险理赔的流程，同时让保单定价更人性化，扩大营收降低风险，真正做到降本增效。同样，在车险、航空延误险或其它财产险中，知识联邦也有相应的发挥空间。

未来开放银行的发展和可持续深化给用户带来了极大的便利，也给银行和金融科技带来新的挑战。在开放银行的场景下，知识联邦将成为刚需，各个机构间各种复杂业务场景下，需要安全交换各种要素，应用场景覆盖了知识联邦的全部四个层次。

很多地方政府为了盘活地方中小微经济，组织了不少面向产业链或者供应链的撮合平台，一方面撮合上下游产业供给，一方面对接银行资金。这类中小微融资扶持平台跨智慧金融和智慧政务场景，需要打通政务、税务、银行、企业及个人等安全和隐私要求差异较大的异构数据，采用知识联邦的方式对信息/流程进行安全串联。知识联邦可以提供强有力的支撑平台和监管等安全和监管标准工具，满足复杂的多层次需求。

5.2 智慧政务

政务数据通常会分散在各个部门里面，每家机构的数据独立存储，独立维护，彼此间相互鼓励。政府部门间数据共享不足、开放利用不够、质量标准不一，这是一个普遍存在的现象。现在地方政府在打造大数据中心也是希望能够破解数据割裂的问题，但在实践过程中，横向数据共享交互仍存在困难，税务、民航、通信管理等垂管部门系统相对独立、数据无法接入地方共享平台。

知识联邦是一种很好的解决方案，因为联邦的本质就是一种数据安全交换协议。通过知识联邦可以帮助政府实现安全的数据虚拟融合，实现数据联邦检索，在保护个人信息的情况下，建立政府数据向社会开放的安全渠道；同时可以为各部门行政审批事项梳理和业务流程再造提供支持。

基于各部门数据进行建模分析，地方政府可以进一步加强安全管控和预警预判。比如在疫情期间，通过多部门数据协作，尤其是人群运动和迁徙轨迹和社交关系分析，可以快速筛选出来与确诊病例紧密接触的潜在风险人群。

5.3 智慧医疗

知识联邦在医疗领域有广泛的应用前景，常见的应用包括医药发现、智能影像分析、疾病知识推理等。医药发现主要是通过疾病诊疗变化和个人用药情况综合分析药品对疾病治疗的效果，进而探索和发现新的药物。通过联邦的方式，可以在保护个人的疾病信息的同时，进行大范围的药品临床效果分析。

在医疗影像分析中，普遍面临的一个问题是影像打标，医疗影像需要专业人员才能完成打标，而这些人员时间有限，影像数据又分散在各家医院里无法对外共享，采用联邦可以有效破解这个难题。

疾病知识推理则是利用各家医疗诊断数据建立知识图谱中，然后在知识库上进行知识推理发现疾病之间的潜在关系，采用联邦的方式可以在保护各家知识库的前提下深度挖掘疾病关联性，可以采取更有效的措施治疗。

5.4 智慧城市

在智慧城市建设发展中，知识联邦同样可以发挥重要的作用。在车联网，通过知识联邦可以保护车主行为习惯的前提，让每辆车辆与周边车辆保持安全的信息交流，为自动驾驶形成助力。在城市交通中，交通信号灯可以根据不同方向车流人流量智能调整。这种基于知识联邦智能控制信号灯方式，不会泄漏行人或车辆的隐私，同时可以避免目前固定间隔方式导致有的方向交通拥堵，而有的方向则是没有车辆通过。而在社区监控或智能门禁中，利用知识联邦可以将区域或家庭监控系统与公安的犯罪嫌疑人数据库连通，通过本地计算分析，在保护过往行人的隐私情况下，对发现的潜质嫌疑人及时报警。

第6章 知识联邦与人工智能 3.0

知识联邦致力于打造数据安全的人工智能生态系统。知识联邦的设计理念受到了人工智能发展历史的启发和影响，也希望成为推动下一代人工智能发展突破的一个关键环节。

6.1 人工智能的发展阶段

表 4. 人工智能与计算平台的发展阶段

年代	人工智能	计算平台
1950s	AI 0.1：萌芽；感知机	第一代：大型机 Mainframe
1980s	AI 1.0：有知识，规则；专家系统，浅层模型	第二代：个人电脑 PC/Client/Server
2010s	AI 2.0：有感知，模式识别；深度学习，强化学习	第三代：云计算大数据 SMAC
2040s	AI 3.0：很有知识、很有感觉、擅长推理决策	第四代：智能平台 （量子计算机、智能芯片及超算）

人工智能的几个关键发展阶段简单概括如表 4 所示。 1950 年代，AI 0.1 阶段带来了 AI 的启蒙，以感知机为典型代表。1980 年代，AI 1.0 阶段带来了知识，以专家系统和浅层模型为代表。2010 年代，我们目前所处的 AI 2.0 阶段带来了强大的感知能力、模式识别，以深度学习和强化学习为典型代表，获得了及其广泛的应用和社会影响力，比如在视觉、语音、翻译、自然语言处理、游戏、无人驾驶、生物医学、科学及工程、金融商务等上面的突破。我们观察到两个现象：（1）人工智能与计算平台的发展阶段有相当的巧合。（2）各个阶段的飞跃间隔大约 30 年。由此我们推测 AI 3.0 将在 2040 年代获得极大突破，进一步逼近强人工智能。目前 AI 2.0 突破的前提是大数据、云计算、GPU/TPU 等的极大提升（统称 SMAC - Social, Mobile, Analytics, and Cloud），以及深度学习等一系列人工智能等理论和技术的巨大突破。AI 3.0 的突破的前提预计会是新一代计算平台（我们暂时称为智能平台）的突破和人工智能理论和技术的突破。

人工智能的发展历史可谓波澜壮阔，从最初萌芽阶段的豪言壮语，历经两次寒冬的巨大打击，而终于在最近 10 年崛起并全面落地，影响了我们社会的方方面面，仍在发挥巨大的影响力，成为各个国家必争的技术高地。率先突破 AI 3.0 的国家必然拥有强大的先发优势，引领下一代工业革命 。

6.2 知识联邦为人工智能 3.0 奠定基石

虽然目前还没有完备的理论突破来实现 AI 3.0，学术界和工业界也没有统一的看法。如表 4 所示，AI 3.0 预计会融合前面近百年的人工智能技术达到很有知识、很有感觉、擅长推理决策。我们相信知识的智能发现、归纳、演绎和推理决策是通向 AI 3.0 的必经之路。

知识联邦倡导统一的多层次的安全联邦，从信息层、模型层、认知层到知识层。AI 3.0 也必须解决数据安全、个人隐私以及社会安全、人类安全等核心问题。知识联邦的安全人工智能生态系统为 AI 3.0 奠定了坚实的基石。知识联邦的理论、算法和智邦平台的实现机制，支持从数据到知识的发现、融合、归纳、推理及演绎的各个层面，为走向 AI 3.0 铺平道路。作为知识联邦生态的重要组成部分，监管、仲裁和评价机制也为未来 AI 3.0 的社会安全保障提供理论支撑和实践经验。

作为国产原创、自主可控、国际领先的技术，我们相信知识联邦的理论体系以及智邦平台的实践必将为中国率先突破 AI 3.0 做出微薄的贡献。我们也希望知识联邦和智邦平台抛砖引玉，得到国内同行的大力支持、发展和应用，并建立起强有力的社区联盟，群策群力，共同推进知识联邦的发展、推广并形成行业标准。

同盾科技有限公司

参考文献

[1] Mugabi, Ivan. GDPR: General Data Protection Regulation. [OL],2018 10.13140/RG. 2.2.31039.41122.

[2] CCPA: California Consumer Privacy Act, [OL],2018, https://www.caprivacy.org/

[3] 《数据安全管理办法(征求意见稿)》,[OL],2019,http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm

[4] JR/T 0171-2020《个人金融信息保护技术规范》[S], 2020，中国人民银行

[5] GB/T 35273-2020《信息安全技术 个人信息安全规范》[S],2020

[6] GB/T 37932-2019《信息安全技术 数据交易服务安全要求》[S],2019

[7] 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》[OL],2020, http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm

[8] Pearl, Judea, and Dana Mackenzie. The book of why: the new science of cause and effect. [B] Basic Books, 2018.

[9] Ackhoff, R. From Data to Wisdom. Journal of Applied Systems Analysis, [J], 1989. 16. 3-9.

[10] Sheth, A.P., & Larson, J.A., Federated database systems for managing distributed, heterogeneous, and autonomous databases, [J],1990, ACM Computing Surveys, 22(3), 183-236.

[11] Hongyu Li, Dan Meng, Hong Wang, and Xiaolin Li, Knowledge Federation: A Unified and Hierarchical Privacy-Preserving AI Framework, [J], 2020 IEEE International Conference on Knowledge Graph (ICKG), Nanjing, China, 2020, pp. 84-91.

[12] Konen, J., Mcmahan, H.B., Yu, F.X., Richtárik, Peter, Suresh, A.T., & Bacon, D. Federated learning: strategies for improving communication efficiency, [J],2016, arXiv:1610.05492.

[13] Yang, Q.,Liu, Y.,Chen, T.,Tong, Y. Federated machine learning: concept and applications,[J],2019,ACM Transactions on Intelligent Systems, 10(2), 12.1-12.

[14] Kairouz, Peter, H. Brendan McMahan, et al, Advances and Open Problems in Federated Learning. ArXiv abs/1912.04977 (2019).

[15] Goldreich, Oded. Secure Multi-Party Computation. Manuscript, [B],1999. Preliminary Version.

[16] Cynthia Dwork, Differential Privacy: A Survey of Results, [C], International Conference on Theory and Applications of Models of Computation, pp:1-19, 2008

[17] Louis Aslett, Pedro Esperança, and Chris Holmes. Encrypted statistical machine learning: new privacy preserving methods [J], 2015, arXiv:1508.06845.

[18] Dowlin, Nathan & Gilad-Bachrach, Ran & Laine, Kim & Lauter, Kristin & Naehrig, Michael & Wernsing, John, CryptoNets: Applying Neural Networks

to Encrypted Data with High Throughput and Accuracy, [TR],2016. MSR-TR-2016-3,1-12.

[19] Finn, Chelsea & Abbeel, Pieter & Levine, Sergey, Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks, [J],2017, arXiv:1703.03400

[20] Hinton, Geoffrey & Dean, Jeff & Vinyals, Oriol. Distilling the Knowledge in a Neural Network, [C], 2014.NIPS,1-9.

[21] Liwei Chen, Yansong Feng, Songfang Huang, Bingfeng Luo, Dongyan Zhao: Encoding implicit relation requirements for relation extraction: A joint inference approach. Artif. Intell. 265: 45-66 (2018)

同盾科技有限公司