隐私计算联盟
Privacy Preserving Computing Alliance

隐私计算应用研究报告

（2022 年）

隐私计算联盟

隐私计算联盟

2022 年 7 月

编写委员会

❖ **主要编写单位**（排名不分先后）：

隐私计算联盟、中国信息通信研究院云计算与大数据研究所、深圳市腾讯计算机系统有限公司、京东科技信息技术有限公司、杭州卷积云科技有限公司、北京百度网讯科技有限公司、杭州趣链科技有限公司、医渡云（北京）技术有限公司、北京安华金和科技有限公司、北京数牍科技有限公司、联易融数字科技集团有限公司、天冕信息技术（深圳）有限公司、同盾科技有限公司、深圳市洞见智慧科技有限公司

❖ **参与编写单位**（排名不分先后）：

腾讯云计算（北京）有限责任公司、杭州金智塔科技有限公司、优刻得科技股份有限公司、上海浦东发展银行股份有限公司、中国工商银行股份有限公司软件开发中心、西安交通大学、蚂蚁科技集团股份有限公司、京信数据科技有限公司、北京冲量在线科技有限公司、深圳致星科技有限公司（简称“星云Clustar”）、航天信息股份有限公司、上海富数科技有限公司、翼健（上海）信息科技有限公司、光之树(北京)科技有限公司

本报告的典型案例部分还得到了中国农业银行股份有限公司苏州分行、中国电信股份有限公司苏州分公司、天翼数智科技（北京）有限公司、中移动信息技术有限公司、中移动金融科技有限公司、中国移动通信集团四川有限公司、智慧齐鲁(山东)大数据科技有限公司、顺丰科技有限公司、国网四川省电力公司信息通信公司的支持。

❖ **编写组主要成员**（排名不分先后）：

贾　轩	闫　树	袁　博	白玉真
魏　凯	姜春宇	吕艾临	王思源
杨靖世	童锦瑞	刘嘉夕	马智华
李克鹏	程　勇	杨　博	孙中伟
杨树森	任雪斌	郭建领	周吉文
汪小益	徐　静	包仁义	畅绍政
杨　浩	霍仲春	金银玉	单进勇
陈　曦	李如先	吴焕明	许文彬
贾金龙	陈　涛	李　博	姚　明
刘站奇	王礼斌	陈超超	潘　榕
黄小芮	郑培钿	张晓蒙	高　靓
梁　孟	张亚申	王　寰	田　心
杨天雅	方　竞	张霖涛	陆诗晗

隐私计算联盟

前言

2020 年 4 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，将数据同土地、劳动力、资本、技术等传统生产要素并列，作为一种新型生产要素参与分配。2022 年 1 月，国务院办公厅印发的《要素市场化配置综合改革试点总体方案》中提出探索“原始数据不出域、数据可用不可见”的交易范式。作为释放要素价值的关键环节，数据资源的开放共享、交换流通成为重要趋势，市场需求日益增加。

隐私计算是在实现保护数据拥有者的权益安全及个人隐私的前提下，实现数据的流通及数据价值深度挖掘的一类重要方法。在政策驱动和市场需求同时作用下，隐私计算技术、产业、应用迅速发展，成为商业和资本竞争的热门赛道。随着隐私计算技术可用性的快速提升，市场由观望正在转向落地，金融、政务、通信、医疗、互联网等行业率先开展隐私计算应用。除以上传统场景外，隐私计算在能源、车联网等场景也开始探索性应用。

经过广泛调研征集和深入讨论，结合行业一线实践和关注焦点，隐私计算联盟联合中国信息通信研究院云计算与大数据研究所等单位共同完成了《隐私计算应用研究报告（2022 年）》。该报告系统梳理了隐私计算应用发展现状，深入剖析典型案例，并从项目管理角度详细阐述隐私计算在部署建设中遇到的应用难点及解决方案。该报告旨在为隐私计算参与各方提供应用参考，从而进一步推动隐私计算应用落地。

本研究报告亮点如下:

- 深度解读行业，洞察应用发展

围绕隐私计算应用行业占比、目的分布、技术路线等洞察应用发展需求和现状。

- 剖析典型案例，总结应用逻辑

凝聚业内专家的共识，全面系统梳理行业隐私计算应用全景现状，明确了场景名称及其常用流程，并完成经典应用逻辑梳理。

- 聚焦项目管理，梳理解决方案

从项目管理角度出发，以隐私计算项目建设部署前、中、后三个阶段进行划分，全面梳理项目常见难点并总结解决方案，为探索隐私计算项目可复制、可推广的实施路径和模式提供参考。

道阻且长，行则将至；行而不辍，未来可期。面对这个日新月异、快速发展的行业，我们期待与业界共同守正创新，推动隐私计算行业健康发展，让隐私计算在数据要素市场建设和数据流通过程中发挥更大的价值！

目录

隐私计算联盟

第一章

隐私计算应用背景

（一）隐私计算概述

隐私计算是“隐私保护计算”（Privacy-Preserving Computation）的简称，有时也被称为“隐私增强计算”（Privacy-Enhancing Computation），是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算，有效提取数据要素价值的一类信息技术，保障了数据在产生、存储、计算、应用、销毁等各个环节中的“可用不可见”。隐私计算交叉融合了人工智能、密码学、数据科学、计算机硬件等多个学科，并逐渐形成了以多方安全计算（Secure Multi-party Computation，MPC）、联邦学习（Federated Learning， FL）、可信执行环境 (Trusted Execution Environment，TEE)为代表的三大技术路线，以同态加密、差分隐私、零知识证明等其他密码学技术为辅助的成熟技术体系，能够在不泄露原始数据的前提下，对数据进行加工、分析处理、分析验证和联合建模等，为数据的开放共享与隐私保护提供丰富的解决方案。

目前主流隐私计算技术分为三大方向：第一类是以多方安全计算为代表的基于密码学的技术；第二类是以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术；第三类是以可信执行环境为代表的基于可信执行环境的技术。每种技术都解决了如何安全地使用保护中

的数据的问题，并具有相应的优点和缺点。

由于技术路径的不同，各类隐私计算技术均有其更加适用的场景，可满足不同的业务需求。多方安全计算是基于密码学的可证安全计算，具有高安全性，但对网络要求高，可应用在银行、政府等高安全要求场景。联邦学习效率高，适合数据量大的联合机器学习场景，针对梯度泄露风险，可结合差分隐私或者密码学等方式来提升安全性。可信执行环境属于数据加密后集中计算，具有高安全性、高精度等特点，但需要数据加密集中到第三方环境。相关技术的主要对比如表 1-1 所示。

表 1-1 隐私计算技术对比

技术	性能	通用性	安全性	可信方	整体描述	技术成熟度
多方安全计算（MPC）	低~中	高	高	不需要	通用性高、计算和通信开销大、安全性高，研究时间长，久经考验，性能不断提升	已达到技术成熟的预期峰值
可信执行环境（TEE）	高	高	中~高	需要	通用性高，性能强，开发和部署难度大，需要信任硬件厂商	快速增长的技术创新阶段
联邦学习（FL）	中	中	中	均可	综合运用 MPC、DP、HE 方法，主要用于模型训练和预测	快速增长的技术创新阶段
同态加密（HE）	低	中~高	高	不需要	计算开销大，通信开销小，安全性高，可用于联邦学习安全聚合、构造 MPC 协议	快速增长的技术创新阶段
零知识证明（ZKP）	低	低	高	不需要	广泛应用于各类安全协议设计，是各类认证协议的基础	快速增长的技术创新阶段

技术	性能	通用性	安全性	可信方	整体描述	技术成熟度
差分隐私（DP）	高	低	中	不需要	计算和通信性能与直接明文计算几乎无区别，安全性损失依赖于噪声大小	快速增长的技术创新阶段
区块链（BC）	低	中	中	不需要	基于带时间戳的块链式存储、智能合约、分布式共识等技术辅助隐私计算，保证原始数据、计算过程及结果可验证	逐渐接近技术成熟的预期峰值

（二）政策、需求推动隐私计算应用发展

数据作为新型生产要素已成为国家基础性的战略资源。为解决数据权属界定不清、要素流转无序、隐私保护不足等影响数据要素价值发挥的关键“命门”，随着政策与需求的双重推动，隐私计算已成为需求强烈的数据流通“技术解”之一。

我国在数据隐私保护领域已初步形成了由法律、法规规章、规范性文件及相关政策组成的多层次法律政策体系，为隐私计算技术的发展指明方向。自 2017 年《网络安全法》颁布以来，信息安全的立法进程逐步紧凑。我国第一部关于数据安全的法律《数据安全法》于 2021 年 9 月 1 日正式施行。《数据安全法》指出“国家建立数据分类分级保护制度”、“非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据“等数据安全相关法条。《数据安全法》、《网络安全法》以及《个人信息保护法》全面构筑中国数据安全领域的法律框架。

2020 年后，有利于推动隐私计算发展的政策加快布局落地。2020 年 12 月，《关于加快构建全国一体化大数据中心协同创新体系的指

导意见》提出，要“建立健全数据流通管理体制机制”，“试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式”，从技术层面为构建数据可信流通环境，提高数据流通效率提出了指导性意见。2022 年 1 月 12 日国务院发布并实施的《“十四五“数字经济发展规划》中明确指出，要进一步强化个人信息保护，规范身份信息、隐私信息、生物特征信息的采集、输出和使用，并且要求加强对收集使用个人信息的安全监管能力。2022 年 3 月，中央网信办、教育部、工业和信息化部、人力资源社会保障部联合印发《2022 年提升全民数字素养与技能工作要点》，多措并举提升全民数字素养与技能。

随着政策法规成为隐私计算发展和应用的重要基石，各行业出于数据流通的实际需求布局并应用隐私计算。自 2019 年起，隐私计算的落地需求呈逐递增趋势（见图 1-1），市场层面从落地初期验证阶段进入加速落地阶段，重点呈现出以下趋势：

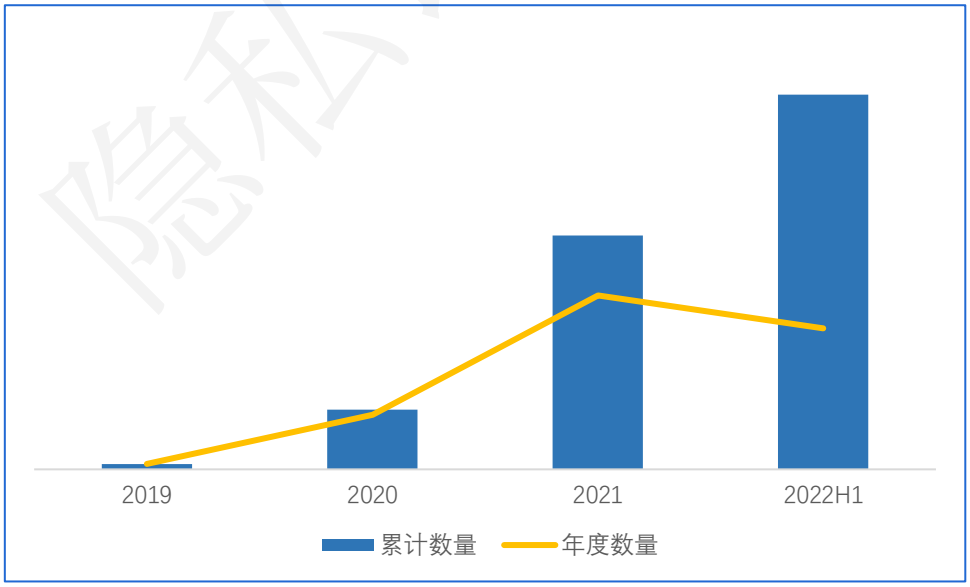


图 1-1 2019 年-2022 上半年隐私计算招标数量

一是隐私计算应用行业广泛，金融行业应用最多。根据 2019-2022

年政府公开招标项目整理，金融、通信、政务、医疗等行业均已进行隐私计算平台招标，且需求逐年增长（见图 1-2）。其中金融行业招标数量占比最高，为 53%，主要包含银行、金融科技、保险、证券等；通信行业招标数量占比为 17%，主要包含运营商；政务行业占比 13%，主要包含政府、政府部门、事业单位；医疗行业占比 9%，主要包含医院、医疗机构或研究所；互联网占比 5%，主要包含车联网类、网站类、信息科技类；能源占比 3%，主要包含电力。

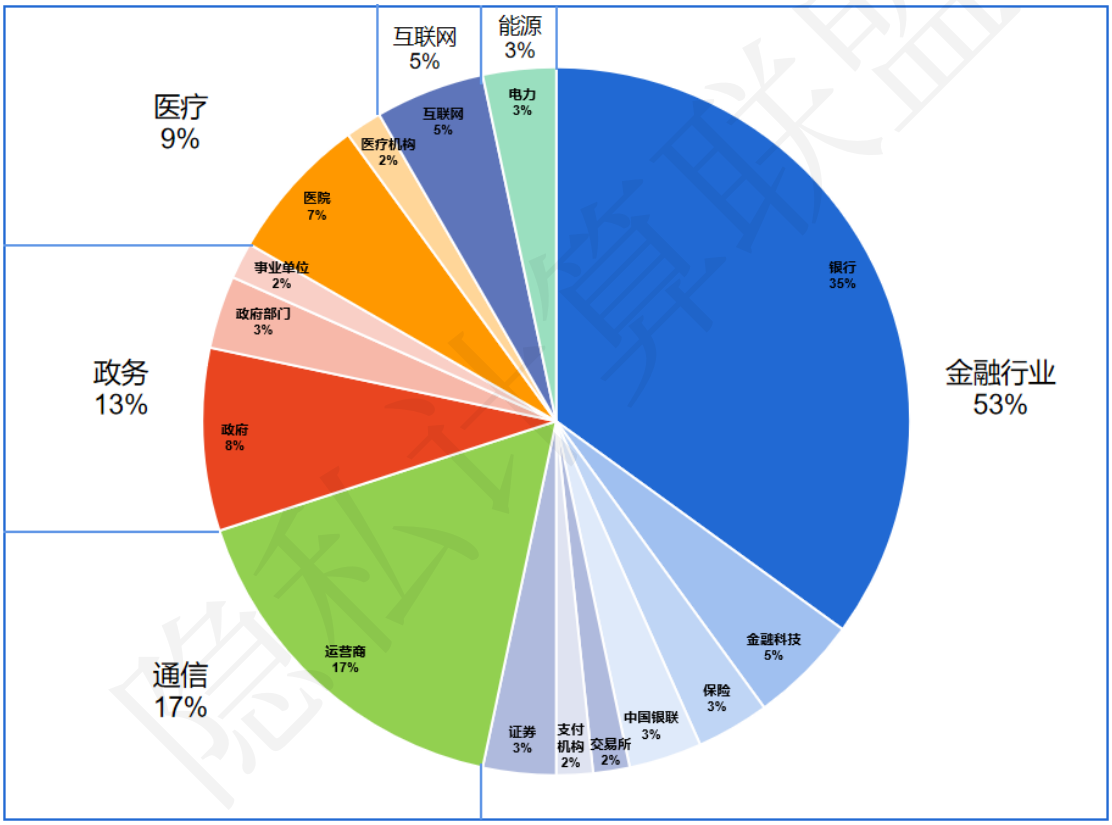


图 1-2　2019 年-2022 上半年隐私计算招标行业比例图

二是隐私计算不同行业间的招标目的分布不同。主要有对内赋能、对外赋能和双向赋能等形式。对内赋能指招标方通过隐私计算平台引入外部数据价值或能力提升内部业务效果，主要包含科研、数据应用，比如引入外部数据进行联合风控、联合营销等。对外赋能指招标方通

过隐私计算平台对外输出数据价值或能力，主要包含数据运营、数据服务，比如对外提供数据安全查询或对外输出联合建模能力等。双向赋能指招标方通过隐私计算平台同时对内、外赋能。

如图 1-3 所示，金融行业 55%的招标项目目的为对内赋能；互联网、通信、医疗、能源行业对外赋能占比均超 50%；政务行业双向赋能占比较高。分析其背后产生的原因：首先，金融领域具有高度数字化的特点，具备隐私计算试点的良好条件。同时，金融领域也有大量的隐私计算需求，金融业务中重要的联合风控、联合营销、反欺诈等应用场景，也是隐私计算技术重点支撑场景。其次，通信运营商的数据包括个人实名信息、上网信息、通话信息等，可覆盖个人信息的多个维度。因此，在各种隐私计算应用场景中扮演着重要的数据提供者的角色。再者，政务数据不仅价值高、规模大，而且种类多。近年来，我国各地政府积极推进政务数据的开放共享。隐私计算可以帮助实现跨机构间的个人身份确认、企业经营监管等。

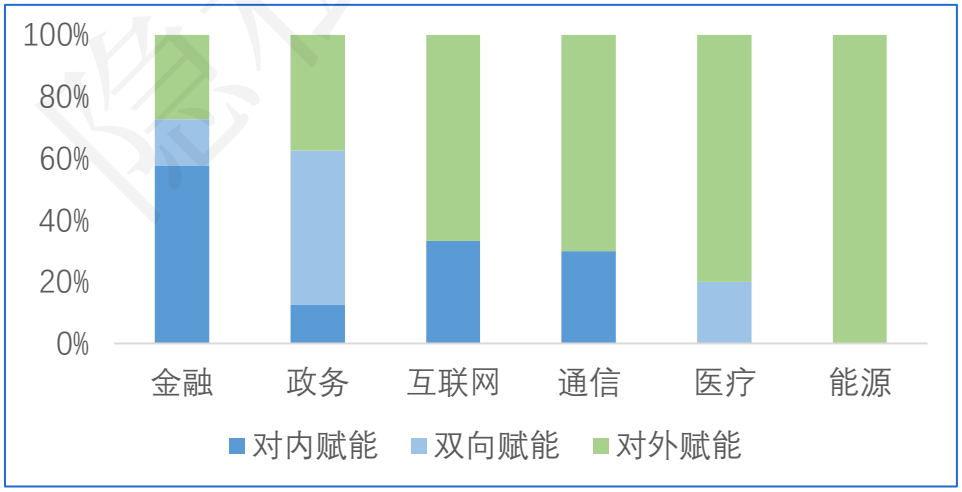


图 1-3　隐私计算行业招标目的比例图

三是从技术需求与产品提供来看，隐私计算技术的综合运用以解

决面向场景的问题是隐私计算技术的主流需求，产品提供方结合需求提高了产品在场景支持的全面性。如图 1-4 所示，招标中不限定技术方向的需求占 55%，三大主流方向均有涉及，其中联邦学习为单一技术中最高，占比 29%，两种及以上隐私计算技术综合应用的技术需求占 8%，这也说明隐私计算的市场培育逐渐显现出成效，隐私计算需求方开始将技术应用于业务场景，隐私计算技术与场景将进一步深度融合。

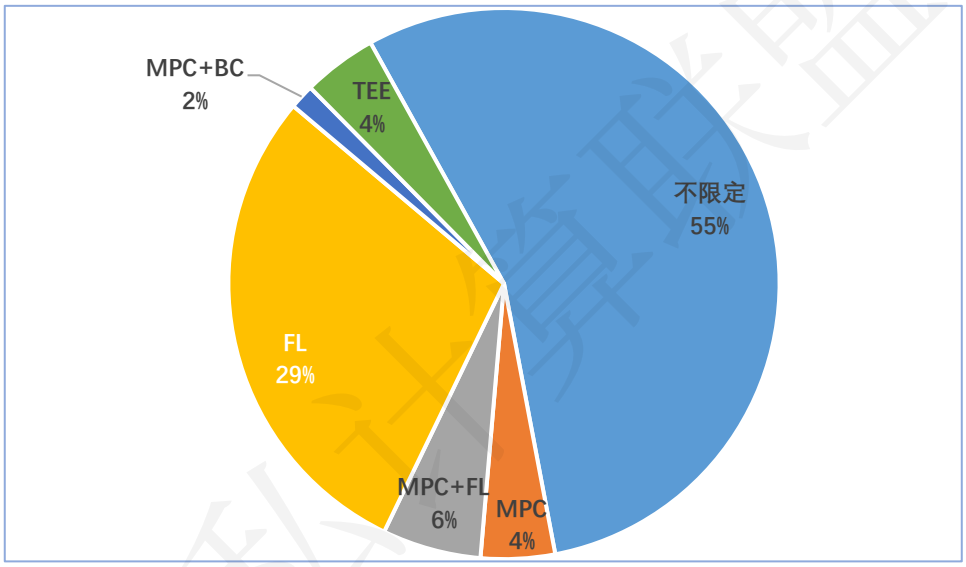


图 1-4 不同行业招标技术方向要求占比

产品提供方在产品研发时往往结合数据流通需求方的实际需求进行相关适配，因此通过对调研产品应用行业及技术路线（见图 1-5、图 1-6、附录三）进行分析，得到以下结论：一是目前产品对金融、政务、医疗行业支持最为广泛，并已有产品能够支持新兴场景如能源、税务等。二是联邦学习、多方安全计算技术应用最为广泛，并随着监管存证需求日益加强，支持区块链辅助的隐私计算产品占比约占 42%。三是为满足更广泛场景、综合提高产品可用性，28%的产品同时支持

2 种及以上技术方向，15%的产品同时支持 3 种技术方向。

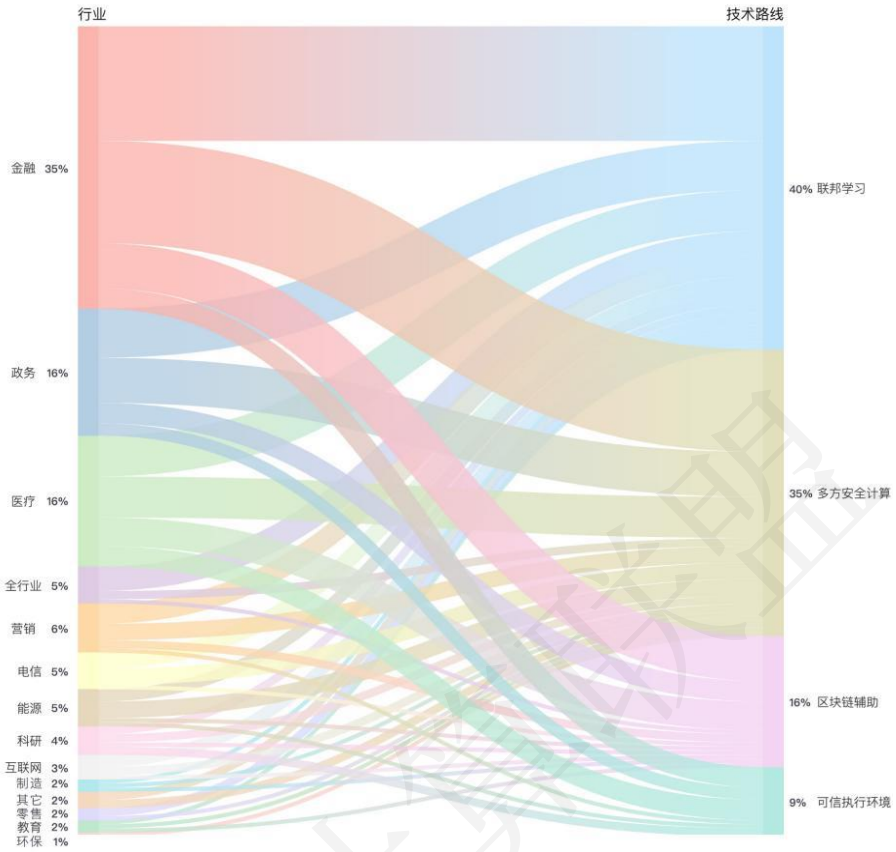


图 1-5 产品支持行业及技术方向

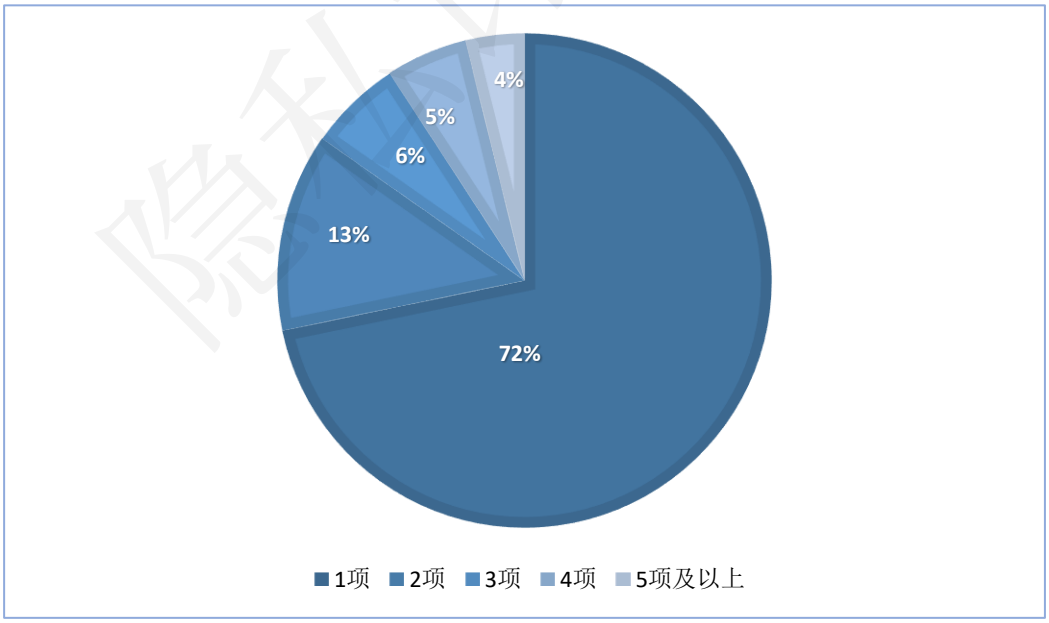


图 1-6 产品融合技术路线数量

第二章

隐私计算应用现状

随着政策与需求的双重推动，隐私计算技术和产品成熟度迅速提升，从 2018 年起逐渐由研发阶段转化到实施阶段。根据统计（见图 2-1），进入实施阶段的产品比例逐年提升。截至 2022 年 6 月，进入实施阶段的产品比例由 2021 年的 48%上升至 55%，市场从落地初期验证阶段进入到加速实施阶段。

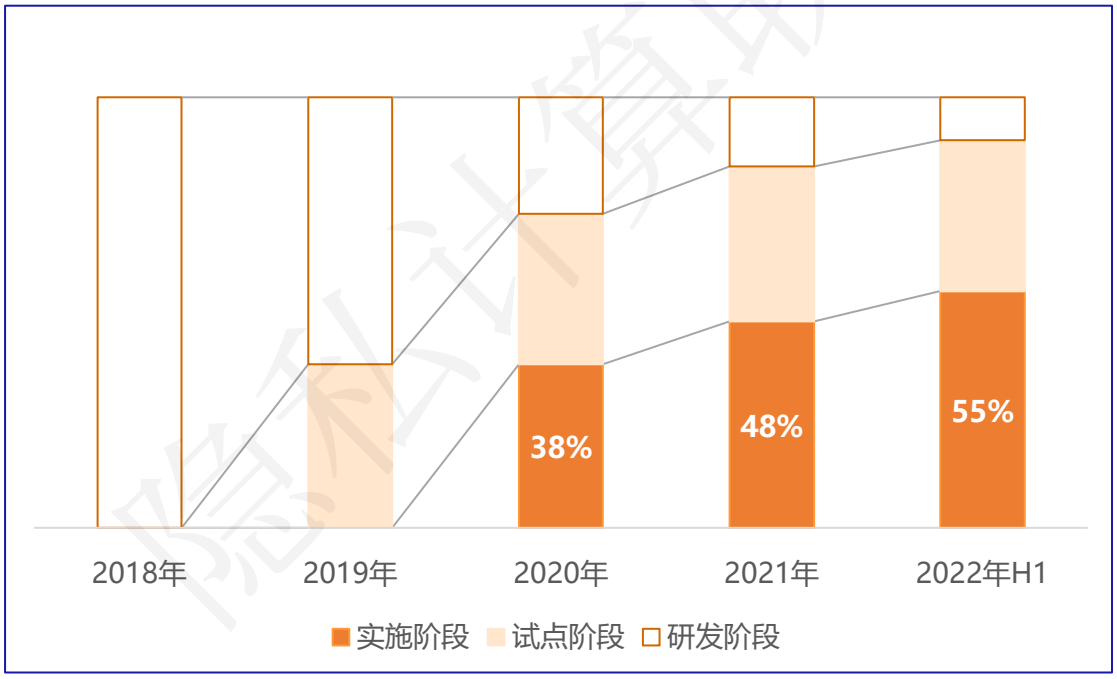


图 2-1 2018 年-2022 上半年产品落地阶段分布

隐私计算应用场景进一步丰富，基于金融、政务、医疗、互联网等数据密集型行业开展落地实践，覆盖金融风控、精准营销、政务服务、保险定价、医疗健康等场景，探索数据资源开放共享，进一步释

放数据价值。本报告首次系统、全面地梳理金融、政务、医疗、互联网等**典型行业隐私计算应用全景图**，并完成细分场景经典解决方案的梳理，凝聚了业内专家的共识。

（一） 金融场景现状

1. 行业传统痛点分析

随着隐私数据保护要求的提高和相关法律法规的逐步出台，金融数据在营销、风控、监管的使用上需保证隐私数据不外泄。

在**营销方面**，各金融机构投入大量人力物力财力来构建客户画像，从而提升营销收益最大化。金融机构通过建立营销模型在潜在客户及存量客户中更好地筛选营销目标客户，在保证营销效果不受明显影响的前提下节约营销资源、减少对低兴趣客户的干扰。而金融机构本地的用户数据或者其特征是有限的，营销建模效果往往不及联合多方数据源。因此，如何在保护金融数据隐私前提下，利用多家金融机构数据提升营销建模的效果,成为现阶段金融领域亟待解决的问题。

在**风控方面**，有效风险控制一直是金融领域的重要工作。当客户申请相关金融服务的时候，金融机构需对该用户进行资格审查、风险控制，以尽可能避免信用卡循环套现、洗钱、骗贷、电信诈骗等不良甚至违法行为发生，同时也降低银行因为不合格用户而造成的损失。联合多方数据在风控领域可以帮助金融机构更好地进行客户检测,降低坏账率等风险指标。单家金融机构数据资源是有限的，无法非常精准地评价某个客户的资质、还款能力等。如何在保护金融数据安全的前提下，寻求更多的可能性来提升风控模型的能力成为一个热门问题。

在**监管方面**，通过隐私计算聚合数据分析，提升监控合规效率。目前金融行业在防洗钱、黑名单等监管合规方面主要依赖内部的金融属性数据，存在数据源单一、数据信息整合分析困难、可疑交易检测模型更新滞后、单一可疑交易检测精准度差等问题。而相关数据分散在不同领域和行业的系统中，且相互隔离，数据共享缺乏安全保护，难以确保获取数据的合规性与使用数据的合法性。金融行业可通过隐私计算技术融合其他领域，整合外部收集到的各种维度数据，提升监管合规效率。

2. 隐私计算应用逻辑

在金融场景中，金融机构一般作为数据需求方，通过隐私计算技术引入外部数据提高普惠金融、风控管理、精准营销等效果。数据提供方主要是金融机构、互联网平台、运营商、政府部门等。由于金融场景广泛、复杂，本节以联合风控、联合营销、监督场景三个大场景举例，根据细分场景的业务逻辑及目标结果，可通过不同的隐私计算算法完成，如表 2-1 所示。

表 2-1 隐私计算金融典型场景及其常用算法

场景 \ 算法		联合统计	联合查询		联合建模及预测	
		联合统计	安全求交	隐匿查询	监督模型	无监督模型
联合风控	贷前风控		√	√	√	
	贷后风控				√	
	信用评级				√	
	反欺诈识别		√	√		
	黑名单查询		√	√		
	合格投资者认证	√				
	供应链金融			√	√	

场景 / 算法		联合统计	联合查询		联合建模及预测	
		联合统计	安全求交	隐匿查询	监督模型	无监督模型
联合营销	纳新拓客			√	√	√
	存量客户营销				√	
	客户画像				√	
	信用评级				√	
	个性化广告				√	
	名单共享		√	√		
监管场景	监管方查询企业	√	√	√		
	资金监管	√				
	金融企业内部监管	√				
	金控企业内部监管	√				

在**联合风控**方面，一方面可通过融合多个金融机构数据，解决单个金融机构样本量有限的问题，形成在相关场景中的全局认知，提升模型精准度；另一方面，可以综合利用金融机构同其他行业数据，在各方原始特征不出域的前提下建立风控模型，形成对业务的多维度认识，提升风控质量。在信息核验时，可通过隐私计算实现多方黑名单数据共享，对电诈、洗钱、骗贷等行为的黑名单用户进行匿踪识别，数据方不能获知查询的具体内容，提升客户背景调查的安全可信程度。

在**联合营销**方面，一方面是银行、保险等金融机构利用运营商、政务、征信等外部数据更精准的对用户客群进行分类，识别高价值用户，制定更精准的金融营销策略。例如，保险公司结合电商、航旅等其他合作方的消费、出行、行为偏好等数据与自身用户基本信息、购买保险、出险赔付等数据,更精准识别目标客户，提升保险销售转化率；另一方面，金融机构利用隐私计算在不输出原始数据的基础上与外部机构共享各自的用户数据，进一步丰富用户画像，提升交叉营销效果。例如，金融机构和电信运营商合作进行联合营销，同时提高金融产品、运营商通信产品的建模精度。

在**监管场景**方面，典型场景为监管方查询企业、资金监管、金融企业内部监管、金控企业内部风控监管，实现方式通常为联合统计及联合查询。监管方查询企业、资金监管往往涉及到外部监管，且周期较长，多为季度、半年度、年度监管，因此安全性要求较高而性能要求较低；而金融企业内部监管、金控企业内部监管只涉及集团或企业内部自行监管，且周期较短，多为月度监管，因此相对来说信任度更高，可以采用安全性相对较低但性能较高的方法。

金融场景采用的合作方式中联合统计、联合查询、联合建模及预测均比较广泛。由于联合建模及预测中也需要联合统计、联合查询为前置步骤进行标签对齐，并且需要进行联合建模的细分场景中一部分也可以通过联合统计、联合查询方式获取结果，甚至在监督场景中很少使用联合建模。因此可以说金融场景中联合统计、联合查询应用最为广泛。这一现象的原因为金融场景信息化起步早、水平高，积累了丰富的数据分析经验，这些经验以专家模型的形式保留下来，将复杂的分类问题转化为较为简单的统计、比较问题。因此在隐私计算场景中，通过联合统计、联合查询即可得到相应场景下专家模型的输入数据，并快速得到计算结果。除以上介绍的场景外，金融行业已拓展出很多创新场景，比如绿色金融等。

3. 典型案例

案例一、苏州多方安全数据分析平台与金融反诈应用

在反欺诈场景中，客户数据流通风险高，协同分析不够，导致数安全合规性存在隐患，反诈识别和预警精准度不高。通过建设数据综

合应用平台，为用户提供黑灰名单匿名查询、潜在风险识别预警、风险排查处置管理、反洗钱调查等功能，有效防范打击电信网络违法犯罪，维护金融秩序，保护人民群众财产安全。运用区块链、多方安全计算和联邦学习等隐私计算技术构建了多方安全数据分析基础服务系统与上层多项应用，在各方数据不出库前提下，完成多方数据安全计算和协同分析，双向保护数据安全，提升模型精度和预测效果。

苏州市多方安全数据分析联合实验室及反诈应用项目，该系统具体功能模块分为隐私计算平台、区块链平台和账号反诈业务系统三部分: 隐私计算平台以可用不可见的方式实现了数据隐私安全的联合计算，具体包含隐私查询、可信数据分析和联合建模功能，隐私查询在不泄露查询条件的情况下获取查询结果; 可信数据分析提供了四则运算、逻辑运算等基础算子及其组合计算; 联合建模提供了聚类、回归模型、树模型、神经网络等丰富的算法类型，并具备从用户管理、数据资源管理、任务调度、流处理、结果定制化输出、大屏监控告警等全流程的操作管理机制。区块链平台的定位是实现对联合计算产生的任务数据请求、授权、使用、计算等环节进行存证，利用区块链的不可篡改的特性保证隐私计算任务全流程可追溯、可验证，确保数据使用的合法合规。账户反诈业务系统通过建设数据综合应用平台，为用户提供黑灰名单匿名查询、潜在风险识别预警、风险排查处置管理、反洗钱调查等功能，有效防范打击电信网络违法犯罪，维护金融秩序，保护人民群众财产安全。

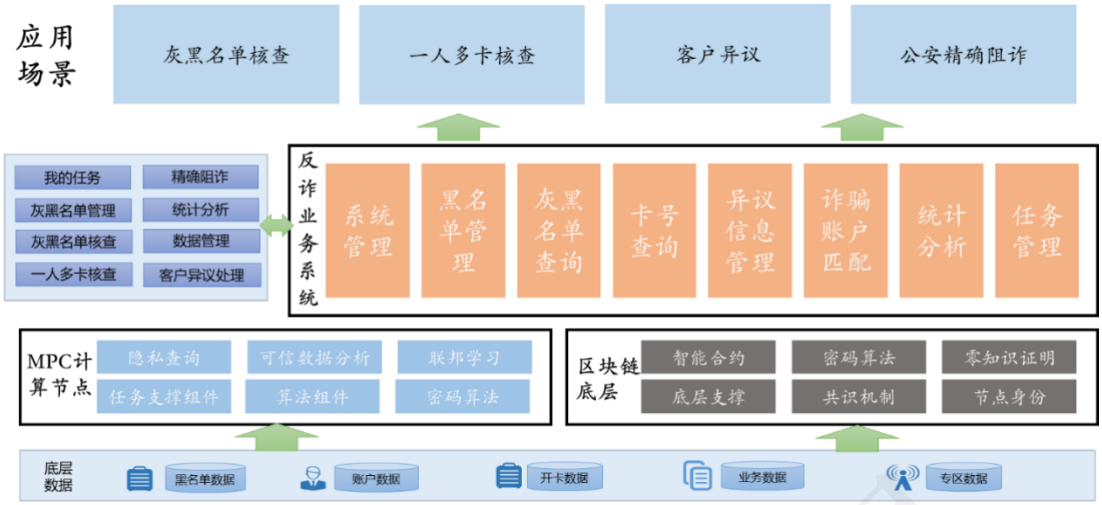


图 2-2 平台系统架构

本项目融合区块链与隐私计算技术搭建了安全可信、隐私强化的数据流通基础设施，有效支撑了多商业银行间的多方数据联合统计需求，通过金融、公安、运营商数据的进一步融合与模型构建，实现更加精准的模型反诈反洗钱与更加高效的实时业务监管与审查能力。截止到目前，已累计完成区域内新开个人账户命中线索数 1 万条以上，存量个人账户命中黑灰名单线索数 5 万条以上，同一客户周期内多行开卡线索数 1 万条以上，并向反诈中心推送涉案线索与潜在受害人近 1 万条。

案例二、基于隐私计算的保险数据智能产品

近年来，随着大数据与人工智能技术在各行各业的广泛应用，数据作为新型生产要素的重要性急剧上升，数据的频繁跨境、跨系统、跨生态圈交互已成为常态。然而，反复出现的数据安全与隐私泄露问题也愈发被关注，数据使用与隐私保护之间的矛盾日益突出。隐私数据的收集与使用曾一度处于灰色地带，但随着《网络安全法》《数据

安全法》《个人信息保护法》等相关政策法规的出台实施，使以往的粗放式数据收集、使用与交易模式受到严格限制。

在上述行业背景下，中国人寿财产保险股份有限公司联合洞见科技共同搭建隐私计算平台，来满足与外部机构联合计算、联合建模的需求，以安全合规的方式释放数据智能在保险业务中的价值。平台整体技术架构设计主要包括 5 大板块：计算资源管理、计算引擎管理、计算服务管理、运维管理及可信网关服务。

图 2-3 隐私计算平台技术架构图

计算资源管理支持对平台接入的原始数据进行数据预处理、数据加工和特征工程，完成数据计算前的数据治理工作，在数据接入类型上支持多种异构数据库、数据文件和标准接口形式的输入，以及为客户提供多种调度策略、配置组合的数据路由机制，保证为计算引擎提供稳定、高可用的数据来源。

计算引擎管理提供了安全多方计算和联邦学习相结合的隐私计算核心能力，支持秘密分享、混淆电路、不经意传输、同态加密等密码学基础算法库，以及封装出的基础运算、集合运算、多项式运算和复杂运算等多种计算算法，支持逻辑回归、决策树、聚类、神经网络

等联邦学习人工智能算法库，提供典型联邦学习、快速联邦学习和无可信第三方联邦学习等多种技术方案，根据业务应用场景和参与方角色定位自动适配最优协议方案。计算引擎同时支持第三方异构算法接入，提供统一的互联互通协议连接来自不同厂商的算法框架。

计算服务管理基于计算引擎封装的隐私计算算法，构建不同领域的落地应用，为多种应用场景提供可视化的、可交互服务能力，如：多方数据智能的联合建模和联合计算，全局在线模型服务和匿踪私密查询，对传统金融风控工具进行匿名化和隐私安全的改造，在多方数据融合应用场景中实现数据的隐私保护和外部数据的安全合规应用。

运维管理功能提供了对隐私计算技术能力平台的节点管理、用户管理、权限管理、计费管理、审计管理、报表管理和运行监控，整体管理和监控隐私计算任务的多方联合运行。

可信网关提供了与隐私计算技术能力平台联盟区块链和其他区块链架构的对接，为了增强多方参与隐私计算的可信性，基于智能合约完成计算存证、过程证明、价值计算和资源确权。

中国人寿财险公司与洞见科技联合搭建的隐私计算平台有两方面意义：一是对内能将隐私计算能力输出到中国人寿集团上下，提供给集团及成员单位使用，融合各级公司、各部门、各险种间的数据能力，充分发挥内部数据价值；二是对外能够通过数据交互建立健全完备的保险数据生态，即通过隐私计算技术，消除各方对于数据安全及合规使用的担忧，从而与外部数据源展开充分合作，引入各类具有价值的外部数据，建设可持续发展的保险数据生态。

（二）政务场景现状

1. 行业传统痛点分析

目前数据的使用已经贯穿于政府管理各个领域、各个环节和各个过程之中，依数据决策、依数据管理、依数据监督已成为常态，政府管理和决策已离不开数据的支撑。政务数据的应用场景主要有三种，分别是数据共享、数据开放及数据运营，然而基于当下的管理机制及技术情况，在不同的应用场景中会存在不同的应用瓶颈。

在**政务数据共享**中，依据管理要求，对于一些重要或敏感的数据不能出域进行应用，然而这部分数据对于开展政府治理或社会服务工作均有着重要的支撑作用，导致了部分政务应用场景难以开展，因此如何解决重要或敏感的数据在部门间的共享问题是当下政府数据共享的一个迫切需要解决的痛点；

在**政务数据开放**中，目前数据开放主要是政府基于公开信息条例的基础上，结合自身管理要求，向社会进行单项开放，但由于难以监管数据应用的合规性，且存在数据泄露的安全风险，目前对外开放数据的维度、颗粒度及价值远远不足，各地方政府亦在探索如何既安全又合规的方式开展数据开放的工作；

在**政务数据运营**中，政府一般掌握城市的大部分的数据资源，在培育数据要素市场工作的要求下，政府需要起到主导及监管的作用，一方面需要建设支撑数据要素市场运作的各类基础设施，保障数据流通的安全性与合规性；另一方面亦需要面向社会去开放政府的数据资源，既推动政府数据资源的价值化，同时亦能促进社会力量去挖掘数

据的价值，从而全面推动数据要素市场的建设。然而数据有别于其他生产要素，其具有易被复制、难以确权的特性，导致在数据流通过程中难以实现数据所有权和使用权分离的效果，且难以保障政府数据在对社会进行赋能时的安全性及合规性，因此如何通过有效的手段去支撑数据要素市场的建立亦是政府工作的一大挑战。

2. 隐私计算应用逻辑

隐私计算技术为政务数据的开放提供了有效解决方案。在企业自有数据、第三方数据或政府共享数据都需要保护且不能离开本地节点的场景下，基于隐私计算进行数据安全利用。

表 2-2 隐私计算政务典型场景及其常用算法

场景 / 算法		联合统计	联合查询		联合建模及预测	
		联合统计	安全求交	隐匿查询	监督模型	无监督模型
政务数据内部共享	精准防疫			√		
	智慧养老		√	√	√	
	精准扶贫		√		√	
	医保控费		√		√	
政务数据对外开放	惠民保险		√		√	
	社会基层治理	√		√		
	普惠金融	√			√	
	数据招商		√		√	
数据运营	数据公共服务			√	√	

在**政务数据共享**上，政务公共数据分布在各部门，通过隐私计算技术搭建政务公共数据密文开放共享交换平台，打通跨域数据的应用价值链，使得数据基于业务应用需要在各业务条线之间，安全地共享和流通，实现数据安全共享融合而不泄密。此时数据提供方及使用方往往都是政务部门。

在**政务数据开放**上，政府机构建设保护各方隐私安全的公共数据

开放平台，使用隐私计算技术融合政府数据和社会、企业数据进行安全计算，联合统计，联合建模，实现数据融合价值。此时数据提供方往往都是政务部门，数据使用方是金融机构、医疗机构等。通过政务数据为社会赋能，可以广泛应用在信用评估、服务选址、健康医疗、家政服务、旅游投资、营销设计等众多领域，让政府部门掌握的数据在安全保护前提下，最大限度造福社会。

在**数据运营**上，随着“数字政府”积极推进，各地政府数据开放共享的制度体系逐步完善、落地实施进展加快，通过加强政府数据开放平台、大数据中心、数据交易所等基础设施建设，推动政府、智库、企业之间数据信息资源的汇聚、整合和协同共享。通过数据运营，政务、各行业数据可以有效流通、发挥价值。

3. 典型案例

案例一、基于隐私计算的政府数据价值流通应用实践

中山市政务服务数据管理局（下述简称“中山市政数局”）为探索与实践如何以数据赋能中山市社会与经济的发展，先后搭建起“云网数安”的基础能力，通过共享体系已归集沉淀超 70 亿条数据，并有效以数据支撑了政务服务、社会信用、征信金融、税务管理、宏观经济、行政监管等领域的工作开展，为加快培育中山的数据要素市场，进一步以数据支撑及赋能社会发展，打造具有中山特色的数据流通体系，由市政数局主导继续探索与实践数据流通应用的可行路径，以创新性的技术来保障数据流通及应用过程中的安全及合规应用。

为搭建起政府数据价值流通的应用渠道，由市政数局主导，联合

京信数据科技有限公司共同建设中山市数据安全可信计算平台，平台定位于政府数据面向社会进行安全共享与应用的统一渠道，核心解决政务数据如何安全向社会机构进行共享应用的问题。平台核心由三个部分构成，分别是统一运营服务端、数据资产运营服务门户及安全计算节点。在技术上主要基于隐私计算主流技术体系包括联邦学习、多方安全计算、可信执行环境为核心，并已以本地化计算节点+协同平台调度的模式，提供一体化的隐私计算服务支撑，其中各参与方均需在本地部署计算节点，通过数据安全可信计算引擎配置的各类隐私算法，实现对本地原始数据的隐私处理，确保计算过程中原始数据安全，协同平台可以创建可执行环境 TEE、多方安全计算 MPC、联邦学习 FL 项目，基于不同计算逻辑和协助模式，协同平台可按需调度本地计算节点中的不同的隐私计算算子，灵活应对多方协助要求(如下图)。

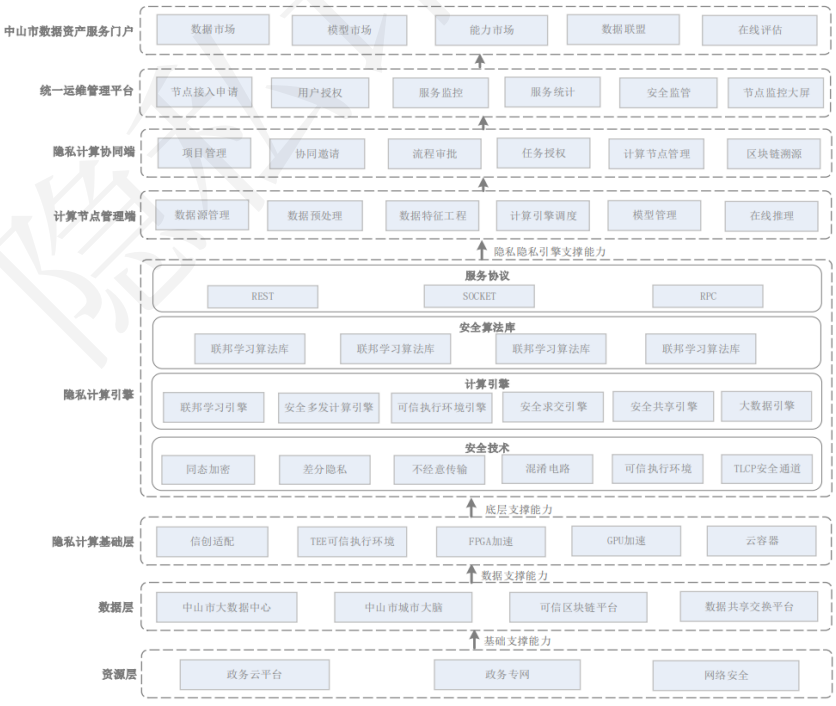


图 2-4 隐私计算平台技术架构图

本项目以企业投融资、普惠金融等重点领域为试点，推进公共数据和社会数据深度融合应用，通过将政务数据及金融征信数据进行融合打造政企联合风控监测体系，破解小微企业贷款风控数据不足难题，市政数局联合本地农商银行、建设银行和农业银行开展政务数据授信试点应用，通过使用中山市数据安全可信计算平台，按需搭建形成贷款全周期政银数据联合运算分析体系。在贷前授信上，为市农商银行计算出 9.6 万家企业 504 亿元可授权金额，大幅提高银行授信效率。在贷中风控上，为市农业银行提供近 90 万户个人用户联合风控分析并提供评分分值，降低信息不对称性与不透明性，缩短信贷审核成本，提升信贷风控能力。在贷后风控上，为市建设银行提供 14140 家企业贷后风控分析，挖掘出潜在高风险企业 1728 家，提升银行贷后监测能力。

案例二、基于隐私计算的省级政务数据开放平台

近年来，国家先后出台政策文件和法律法规，一方面要求政府数据开放、扩大信息公开，另一方面，严控隐私泄露乱象、督促数据流通合规。因此，各级政府面临着数据开放和隐私保护之间难以两全的局面。

根据《山东省数字政府建设实施方案（2019-2022 年）》要求，要实现省一体化大数据平台统一数据汇聚、数据治理和数据应用服务，充分释放数据价值，进一步提升省一体化大数据平台支撑能力。在洞察政务数据开放痛点以及明确山东省公共数据开放平台要求后，洞见科技凭借领先的隐私计算技术优势，联合智慧齐鲁公司为山东省大数

据局提供了“基于隐私计算技术的省级一体化公共数据开放平台建设”解决方案。

平台整体基于洞见数智联邦平台（InsightOne）的成熟框架开发，支持多方安全计算和联邦学习融合应用模式，并通过联邦区块链保证过程的不可篡改性与可溯源性，达到原始数据不出私域即能完成数据共享应用，实现“数据可用不可见、计算可信可链接”，帮助政府解决数据开放和隐私保护的“两难”问题。

图 2-5 基于隐私计算技术的省级一体化公共数据开放平台

在技术方面，具有四大创新突破。首先，平台基于多方安全计算和可信联邦学习双引擎设计，保证了数据安全性的同时又保证了模型精确度；其次，支持跨平台间互联互通，支持多厂商隐私计算平台的无缝对接；第三，应用无可信第三方联邦学习技术，较大程度上提升了算法的性能；最后，算法容器框架设计，使算法可以在计算框架内自定义设计、实现和执行。在应用方面，该平台上线后以“数据可用不可见、计算可信可链接、用途可控可计量”为原则，促进政府数据的开放共享，加强数据资源整合和安全保护，释放公共数据资源价值。

政务数据隐私计算平台的建设提升了公共数据存储、计算、应用、通用支撑和服务管理能力，能够服务于匿踪安全查询、安全联合统计

分析、多方联合建模、银政企合作（地方金融服务平台）等众多场景。通过该平台，不仅将政府数据进行聚合开放，辅助政府决策，增强工作透明度，提升政府公信力，而且通过数据开放释放数据红利，激发企业利用政务数据，开发新应用，带动新兴产业发展，发挥数据资源经济价值和社会效益。

作为省级政务数据隐私计算平台，该平台具有行业标杆意义突出、示范性和可复制性强等特质，为公共数据的开放、应用奠定扎实的基础。在该案例的合作基础上，洞见科技与山东省大数据中心、智慧齐鲁公司三方联合成立了国内首个省级政务数据隐私计算实验室，树立隐私计算“政产学研金服用”创新创业共同体典范。

案例三、蚂蚁链数据隐私协作平台

2021 年 6 月新发布的《数据安全法》提出， 建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。区块链+隐私计算框架，结合了隐私计算和区块链的优势，能在数据共享过程中有效保护个人信息，并为数据真实性、数据确权等问题提供可行解决方案，实现全流程可记录、可验证、可追溯、可审计的安全、可信数据共享网络，实现“数据不动模型动”，并为进一步建设高效率、高安全和高流动性的数据要素交易市场打下基础。

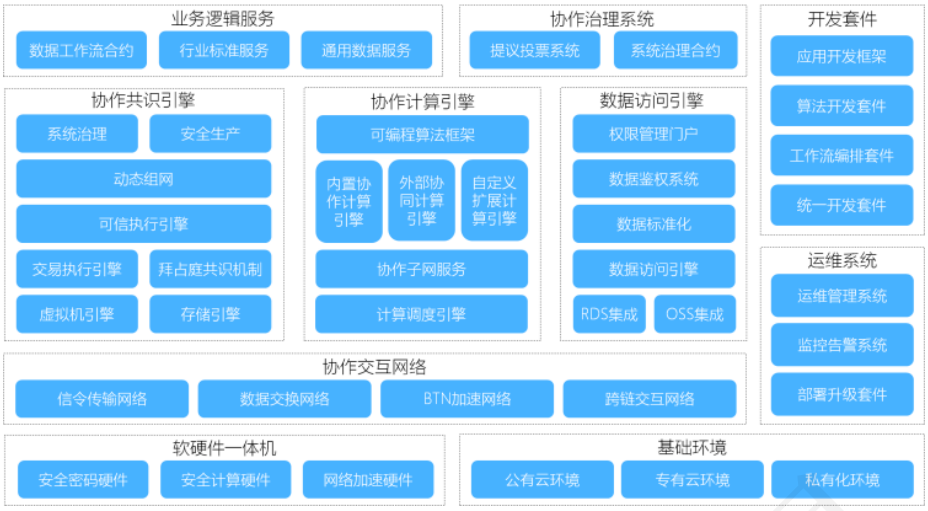


图 2-6 隐私计算平台架构

以区块链+隐私计算技术为依托，针对传统数据中台及大数据平台明文数据流转、裸数据流出等数据安全问题，进一步将不同安全等级的重要数据分级分类管控，采用加密入库的方式在隐私数据库（数据隔离区）中独立存储、重点保护。并针对不同安全等级的数据，制定相应的数据流转规则、共享开放规则，采用密文流转、加密计算、模型计算等方式，避免明文数据流转引发的安全问题，真正做到重要数据全生命周期安全管控，高敏感数据可用而不可见。

具体建设内容包括“1”个区块链+隐私计算基础平台+“1”个数据隔离区+“1”个安全管控中台+“N”个数据应用的方式，通过区块链+隐私计算基础平台夯实基础，通过隐私数据中台和安全管控中台做深数据通用能力及业务通用能力，通过数据应用层做强生态。

蚂蚁链数据隐私协作平台实现了对数据全生命周期的安全管理，具体包括数据全生命周期链上行为存证、数据智能分级分类、

数据行为安全智能评分、数据行为安全预警、数据行为与审批智能关联、数据使用鉴权等。

“区块链+隐私计算”技术融合，结合了多类隐私计算和区块链的优势，能在数据共享过程中有效保护个人信息，并为数据真实性、数据确权等问题提供可行解决方案，实现全流程可记录、可验证、可追溯、可审计的安全、可信数据共享网络，实现“数据不动模型动动”，并为进一步建设高效、高安全和高流动性的数据要素交易市场打下基础。

通过数据协作工作流的定义与执行改进技术路线，实现了联盟网络多方数据可信安全协作与数据可信开放的能力，与原有技术路线相比的优势是有效实现了数据全生命周期的可视化定义与管理，可按需灵活定义与扩展数据隐私计算协作网络，有效保证了数据安全的前提下最大化释放数据价值。

（三）医疗场景现状

1. 行业传统痛点分析

在建立全国统一的电子健康档案实现信息共享的大形势下，医疗数据价值的挖掘需求日益强烈。但是医疗数据本身涉及个人隐私，相关法律规定不明确，数据共享开放存在隐私泄露风险，尤其是在医疗数据内部共享和对外开放场景使用上，要做到隐私不泄露。

在**临床辅助决策**方面，各家医院患者的数据样本和特征维度相互补充，从而助力疾病诊疗。人工智能模型在医学影像分析、电子病历信息抽取、疾病判断等临床辅助决策场景中的应用，可以借助模型

的预测结果，提供检验检查、用药的推荐，提高诊疗的效率，帮助医生减轻工作量；也可以辅助基层医院的医生完成高质量的病历书写，提升基层医生的诊疗水平和患者在社区医院首诊的意愿度。在这种场景下，如何更好地在保护患者数据隐私前提下，利用多家医院分散的数据扩充样本量，提高人工智能模型的预测精度成为当前医疗领域迫切关注的问题。

在**医学研究**方面，在各家医疗机构数据安全的情况下，丰富数据量和数据维度，通过联合统计和联合建模，创建更加精准的模型，助力药物有效化合物的开发、基于基因序列的疾病筛查等场景。但是医疗机构间对数据价值的归属难认定，如发生过很多知识产权的纠纷案例，所以很多医疗机构，特别是处于科研从属或弱势地位的医院都不愿意将自己的数据共享，或者数据共享后得到的回报难以度量，因此数据流通困难。

在**风险控制**方面，降低医保基金损失风险、保单的理赔损失等都是医疗相关领域的难题。当根据患者疾病诊断确定医保支付标准、确定保险核保理赔的时候，相关机构会严格对医疗诊断进行审查，进行风险控制，以避免骗保等违法行为的发生，也降低机构的损失风险。人工智能模型在风控领域的应用，可以有效提高疾病诊断等的预测精准度，从而降低损失的可能性。然而，单家医疗机构的数据资源有限，无法精准的评估，因此，如何利用多家机构的数据来提高风控模型的能力时亟需解决的问题。

在**营销**方面，与政企、运营商数据等行业数据相互融合应用，丰

富数据特征维度，提高医疗服务精准推荐等场景业务能力。通过人工智能模型，提高问诊、体检等场景的精准推荐能力，具有重要的场景价值。但是如何在保护医疗数据安全的前提下，寻求更多的特征维度来支撑精准推荐是有待解决的问题。

2. 隐私计算应用逻辑

在医疗场景中，医疗机构一般作为数据提供方，一是医疗机构间数据融合，相互补充患者样本数量，常用于临床辅助决策系统、医学研究场景。二是通过隐私计算技术将数据在不出域的前提下，提供给外部机构，从而提高风控管理、精准营销等效果。本文以上述四大场景为举例，根据细分场景的业务逻辑和目标，可通过不同隐私计算算法完成，如表 2-3 所示。

表 2-3 隐私计算医疗典型场景及其常用算法

场景 \ 算法		联合统计	联合查询		联合建模及预测	
		联合统计	安全求交	隐匿查询	监督模型	无监督模型
临床辅助决策	医学影像分析				√	
	电子病历信息抽取				√	
	疾病诊断				√	
医学研究	药物研发	√			√	
	基因组分析	√			√	
联合风控	医保控费（DRGs 付费预测）				√	
	人寿保险核保				√	
联合营销	医疗精准推荐				√	

在临床辅助决策方面，通过融合医联体、专科联盟等多家医院的患者诊疗数据，解决了单个机构样本量有限的问题，形成了更加丰富的认知，提高联合建模模型的精准度和鲁棒性。从而，在医学影像识别处理、电子病历信息抽取、医学知识图谱构建等需要大量数据支持

的场景有效消除了数据壁垒。另外，通过隐私计算对智能临床辅助决策支持系统的模型准确性和鲁棒性的提高，也帮助基层医院提供检验检查、疾病诊断、用药等推荐，提升基层医生的诊疗水平以及市民在社区基层医院首诊的意愿度。

在医学方面，通过融合医院、医学科研院所、生物企业、疾控中心等医疗机构的数据，在药物研发和基因组分析等场景中，通过联合统计、联合建模等方式进行多维度融合，在不泄露患者疾病诊断或基因分型数据的前提下，实现了数据的安全共享，丰富了医疗数据资源，为科研创新提供了强有力的支撑。

联合风控方面，一是医疗机构间数据流通，通过联合多家医院数据，增大样本量扩充患者数据规模，基于联合建模构建更为准确的 DRG 分类模型，在保障医疗机构数据利益的同时充分释放了数据价值。二是，外部机构数据共享，例如人寿保险公司，通过隐私计算联合建模提高医疗类产品的核保风控能力，有效减少理赔损失。保险公司内部数据以保单、流程数据为主、数据维度不足、质量不够，而且分散隔离。可以通过隐私计算与其他行业数据，如互联网数据进行融合，扩充数据丰富性，提高风控模型效果，助力完善健康产品的核保风控体系。

联合营销方面，主要是利用隐私计算在帮助医疗机构不输出原始数据的前提下，共享数据特征信息进行联合建模，准确预测医疗服务分类，提高模型预测精度，实现双赢的目的。例如，其他行业数据源包含海量高价值数据，可以解决传统健康导航平台或互联网运营医院

用户数据量受限的困境，基于联合建模有效解决了推荐营销效果欠佳的问题。

医疗场景采用的合作方式有联合统计、联合建模及预测，其中联合建模及预测中也需要联合统计、联合查询为前置步骤进行标签对齐。可以看出，联合建模及预测是医疗场景中最为广泛使用的算法，因为医疗数据种类多且复杂，除患者基本信息、检验、用药医嘱等结构化数据外，还包括影像（CT、核磁、扫描等）、文本（现病史、诊疗记录、病程记录等）、基因组序列等非结构化数据，许多场景的自动化高度依赖于人工智能算法，从而联合建模及预测也得到相应快速的应用。除以上介绍的场景外，政务数据和运营商数据融合可以用于疫情防控工作，其是公共卫生医疗场景的前置步骤。

3. 典型案例

案例一、基于“隐语”框架的医保 DRGs 建模应用

伴着医疗行业数字化转型进程的加速度，隐私计算在这一领域逐渐受到更多关注：运用隐私计算技术可以加强医疗数据整合与保护，且满足医疗数据类型通常更多更复杂、对安全性和计算性能要求也更高的需求，是解决医疗领域数据流通和提升数据价值的技术关键。

为破解数据孤岛，实现多方机构间信息聚合和资源价值，自 2016 年以来，蚂蚁集团自主研发了可信隐私计算框架“隐语”，率先突破了基于隐私保护的数据开放计算技术研发，并在医疗、金融、保险、营销等众多领域进行实践检验。以“隐语”在医保 DRGs 建模中的应用为例，通过与阿里云数字医疗团队合作，“隐语”成功联合多家医疗机构

数据建模训练，在保护患者隐私前提下，使得医疗机构实现了原始数据不出本地、数据隐私保护有所保障，又能同时扩大模型训练数据规模，提升本地 DRG 模型准确度，帮助医疗机构进行 DRG 预测。

基于蚂蚁隐私计算平台“隐语”提供的多方安全计算及联邦学习技术方案，通过阿里云医疗大数据管理平台，可通过初始化、医疗数据准备、样本对齐、模型训练、模型发布、服务集成、服务监控七个环节，成功实现多家医疗机构数据进行联合训练，使得医疗机构实现了原始数据不出本地、数据隐私保护有所保障，又能同时扩大模型训练数据规模，提升本地 DRG 模型准确度，帮助医疗机构进行 DRG 预测。

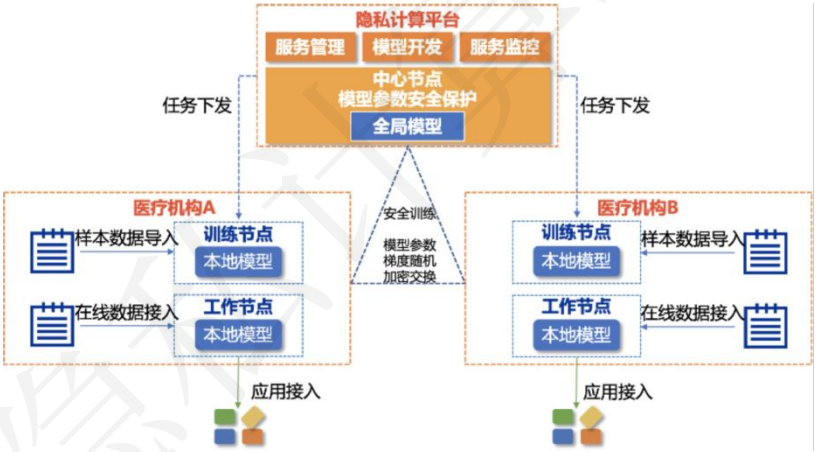


图 2-7 蚂蚁“隐语”平台在医保 DRGs 建模中应用总体框架

在本实践案例中，基于“隐语”平台，各医疗机构的患者数据不出本地节点即可进行汇总训练，通过模型梯度/参数共享来实现数据价值的流通，在确保各方医疗数据安全的前提下，充分挖掘数据价值，为医疗机构提供科学的参考、为人民群众就医提供便利和保障。

本案例中，原小规模医院使用两家医院数据后，其模型预测准确率显著提升；具体到某分组预测准确率，采用方案后，显著提升的为出现频次较低的 DRGs，如某 DRGs 在医院 A 较少，在医院 B 常见，两者结合后 A 医院该 DRGs 准确率显著提升。以建德市第一人民医院为例，通过医疗大数据管理平台 HData，选定 DRGs 模型训练样本主题数据集，基于“隐语”隐私计算服务，作为隐私保护计算节点之一，联合训练后的 DRGs 分组模型的分组预测准确率显著提升。

案例二、基于国产化可信执行环境的健康数据流通平台建设

随着数据成为生产要素，数据隐私保护相关法规的逐渐严格，如何在满足政策法规的前提下，让政务数据安全流通，在不泄漏的前提下为企业提供数据价值能力的输出，成为政府部门关注的问题，长江云通联合冲量在线为政府打造健康数据流通平台，采用国产化可信执行环境技术，打造健康数据流通平台在保证多方数据可用而不可见的前提下，实现数据价值的输出。

长江云通集团有限公司联合冲量在线基于冲量数据互联平台打造——基于国产化可信执行环境技术的健康数据流通平台，联合国产芯片提供商飞腾，保证数据在自主安全的国产芯片的可信执行环中进行数据协作，利用可信执行环境执行任务过程不可见的特性，保证计算过程的绝对安全和隐私，该平台还具备区块链、人工智能和云原生多种技术栈，通过可信数据查询、可信数据互联、联邦机器学习等多种功能，实现跨组织的数据进行安全、可信、公平、高效的多方共享与协作，助力政府打造健康数据共享平台，最终为智慧政务、智慧产

业、智慧医疗和智慧民生提供强大的数据协作能力和丰富的数据协作生态。

整个系统架构图如下所示：

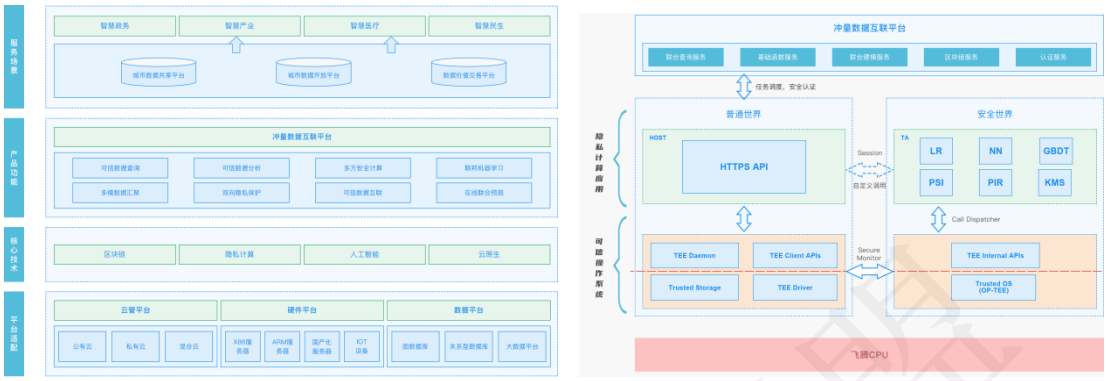


图 2-8 冲量在线数据互联平台技术架构图

基于飞腾 TEE 的隐私计算核心流程如下图所示：

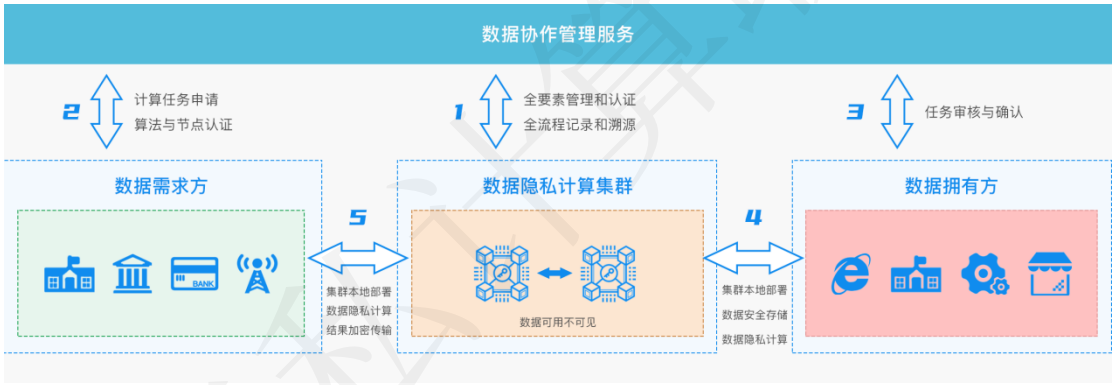


图 2-9 冲量在线隐私计算业务流程图

第一步，数据协作各方加入联盟链，在完成数据结构对齐和算法的协商后，将原始数据的指纹和算法的哈希上链存证；各协作方部署飞腾 TEE 可信执行环境（下文简称“TEE”），节点互认证之后构建隐私计算网络；

第二步，数据需求方发起多方数据协作计算的任务请求，各数据提供方验证算法哈希与链上存证信息一致后，开始参与任务；所有数

据将在 TEE 网络内加密传输，在每个 TEE 计算节点的可信空间中被解密运算。计算结果将会以加密的方式汇聚到调度节点中，然后由调度节点进行结果汇总并再次以加密形式返回给可信数据网关;

第三步，所有原始数据将在 TEE 中被销毁，仅结果数据输出给任务发起方。所有数据提供方可以通过 TEE 可信度量值验证数据计算和原始数据在 TEE 中被销毁的过程。

该方案保证了企业和其数据提供方的数据安全。基于企业和其数据提供方的数据，在可信执行环境 TEE 中进行计算，获得有效而准确的业务模型，便于企业更好的进行精细化数据运营。硬件层面基于飞腾芯片，软件层面使用由冲量独立开发的数据互联平台，满足了企业对 IT 设施和软件严格的自主安全的要求。

整个业务流程的所有环节都和区块链模块打通，执行任务的多方数据流通平台与区块链网络共用一套身份体系，保证隐私计算的过程审计数据带有身份信息，并能对等关联到区块链机构、角色身份。保证所有的数据调用和数据使用记录链上可查，保证了数据调用的透明和安全。

案例三、YIDUMANDA 重庆医联体临床科研大数据平台

医渡云和重庆医科大学在大数据、人工智能、医学研究等领域展开了深入合作，包括：数据结构化处理、映射及归一化、深度搜索及高级筛选、在线分析挖掘、信息抽取、医学知识图谱构建、图像识别理解等数据处理的核心技术研究；心脑血管、肿瘤等病种的个性化精准治疗，临床效果比较、临床决策专家系统、DRGS 等临床应用研究；

消除数据壁垒、数据资源开放共享的机制研究；数据安全防护、隐私保护等审查机制研究等。

依托重庆医科大学各附属医院的数据资源，已合作建成了跨多家医疗机构的联合研究网络及平台。已接入重庆 8 家大型医院的临床数据，包括门诊病历、门诊处方、病案首页、检查报告、检验报告、入院记录等临床医学数据。

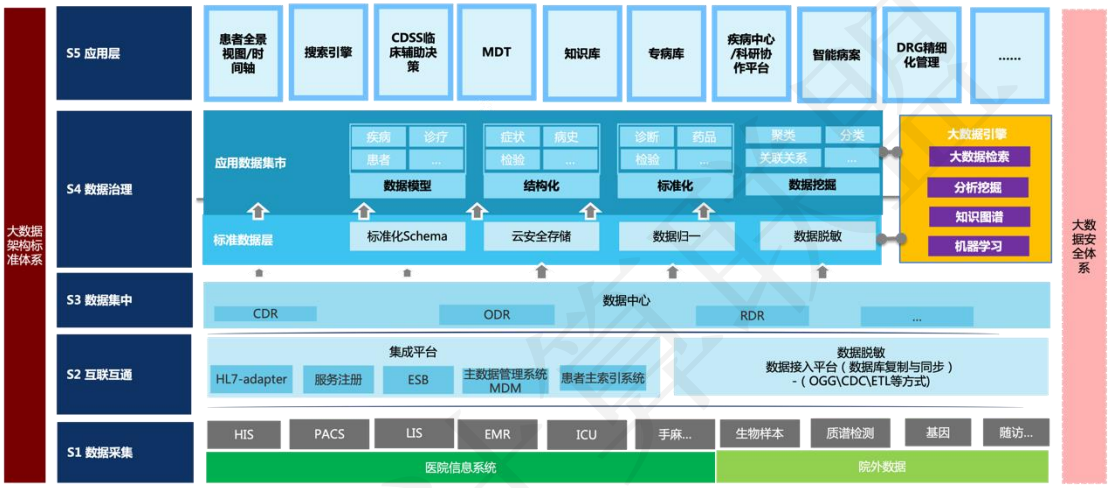


图 2-10 平台技术架构图

通过多中心联合研究网络，在重庆医科大学附属医院、附属大学城医院开展了心血管疾病的医疗大数据应用示范，建立了高血压、糖尿病的疾病知识库与智能健康管理模型，建立的以时间轴为主线的患者全局视图可以展示患者的全治疗周期，记录患者在每一个时间节点的诊断、用药、体征数据、检查、检验、治疗、手术等数据，通过大量患者时间轴的堆叠，得出医院常规的诊疗路径，以及特定患者的个性化方案，为医疗决策提供了技术及数据支撑。

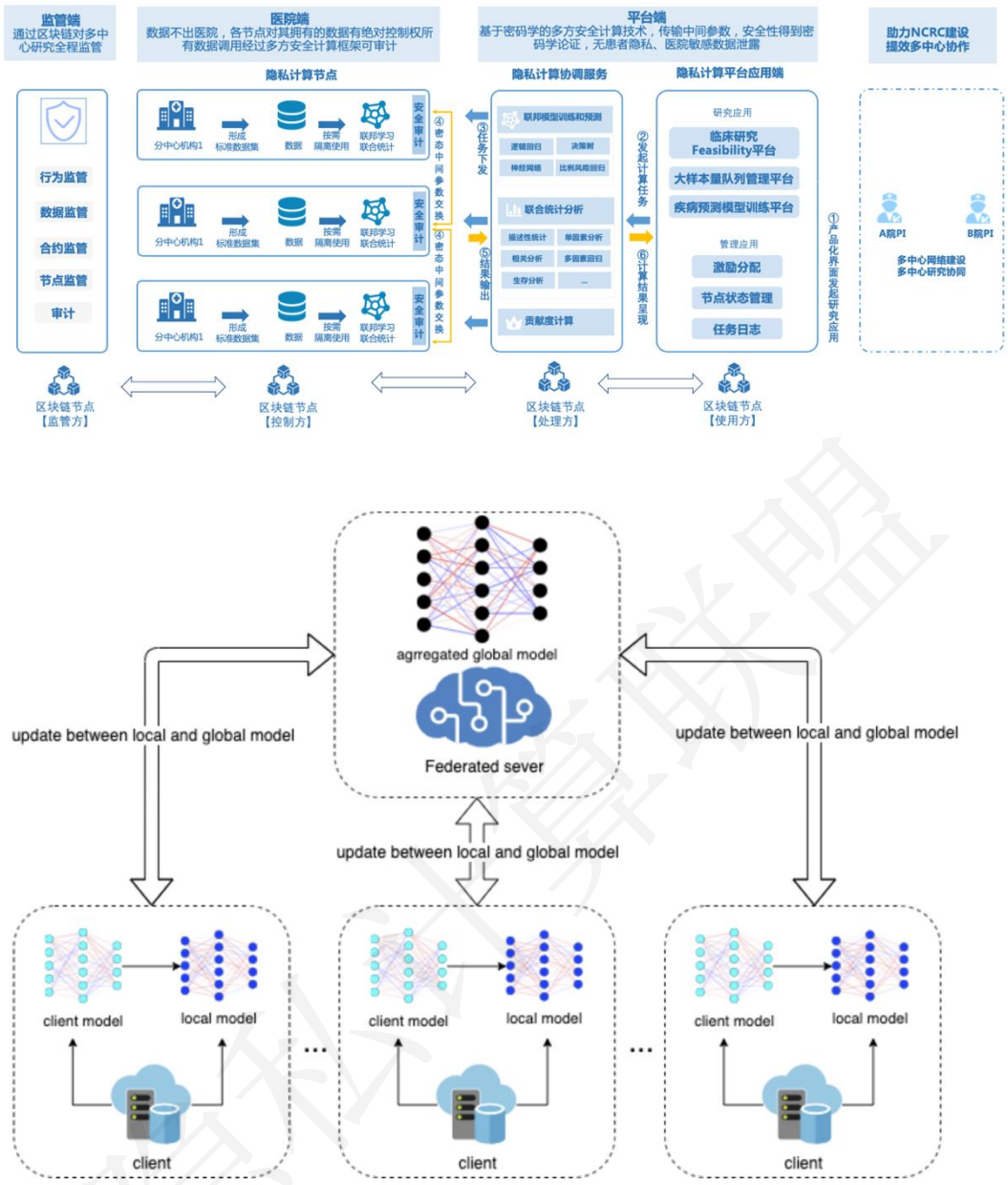


图 2-11 解决方案流程图

同时，医渡云为缓解联邦学习在非独立同分布数据上的性能退化，提出了一种新方法 FedGFO，对多重庆家医院的真实世界数据进行联邦学习实验，研究结果表明，与其他方法相比，新算法使研究人员能够同时获得更高精度的全局模型和更强的泛化能力。

（四）互联网场景现状

1. 行业传统痛点分析

互联网场景中，隐私计算主要用于精准营销、客户拓展等领域。近几年结合大数据、人工智能等技术描绘用户画像的营销推荐方式已在互联网行业内广泛应用，整合多机构间多维度的数据，构建更立体的用户画像，是达到资源优势互补、开拓市场广度和挖掘服务深度等营销目标的有效手段之一。

在**精准营销**方面，由于互联网机构间的用户画像数据相互割裂，且这些数据涉及用户隐私，具有一定敏感性，也是互联网机构的核心资产之一，具有较高商业价值，难以以明文形式共享使用，需要以密态方式共享和交换。另外，在互联网机构之间开展联合营销、个性化广告等业务需要进行数据交互时，由于原有技术手段仅能通过哈希加密算法、脱敏算法或去标识算法隐藏用户的真实标识，增加了数据被碰撞攻击，业务留存和反向查询的风险，难以达到高安全级别的数据安全和隐私保护。互联网公司利用自身拥有的大量用户行为信息和基础画像数据，与广告数据方拥有的深度转化链路数据（如付费信息）进行安全求交，并通过多方安全计算或联邦学习技术联合训练、建模、优化广告模型效果。在游戏、金融、教育、电商行业的广告应用案例中都能提升广告投放效果和用户体验。

在**客户拓展**方面，由于《数据安全法》、《个人信息保护法》和互联网机构自身数据安全政策的限制，用户挖掘依赖基于业务经验的实时策略调整，互联网流量平台和互联网营销平台都很难单纯依赖

自身数据构建高质量的机器学习模型，无法充分发掘各自数据的价值。互联网营销平台如何通过与互联网流量平台之间的密态数据的交换与共享，来实现用户挖掘，完成拓客纳新的目标，成为互联网领域的难点。

2. 隐私计算应用逻辑

在互联网领域，隐私计算技术主要用于实现目标客户的精准推荐和新客户的拓展。在保护用户隐私及实现数据方用户信息可用不可见的前提下，隐私计算技术用于拓宽数据样本量及数据维度，帮助互联网机构实现存量客户高效触达，支持客户输出画像标签的精准预测，极大地提高了用户转化率。同时，也可以用于基于模型训练来拓展新用户，实现用户纳新。

本文以精准推荐、客户拓展两大场景举例，根据细分场景的业务逻辑及目标结果，可通过不同的隐私计算算法完成，如表 2-4 所示：

表 2-4 隐私计算互联网典型场景及其常用算法

场景 \ 算法		联合查询		联合建模及预测	
		安全求交	隐匿查询	监督模型	无监督模型
精准营销	存量客户营销	√		√	
	内容推荐	√		√	
	个性化广告	√		√	
	客户画像		√	√	
	名单共享	√	√		
客户拓展	纳新拓客		√	√	√
	客户挖掘		√		√

在**精准营销**方面，利用隐私计算可以帮助互联网机构之间共享和交换密文数据，构建用户画像和推荐模型，实现对已有客户的精准推荐，包括个性化广告、内容推荐等。在模型训练阶段，互联网机构

之间可以利用隐私求交算法(PSI)找到双方用户交集，明确双方训练数据特征维度。在模型预测阶段，由互联网机构根据自有数据筛取出内部潜在营销客户的名单，利用模型预测，将客户分至各个业务领域的高价值客户。

在**客户拓展**方面，互联网营销推荐机构基于隐私计算技术，与互联网流量机构进行数据协作，利用互联网平台的流量，进行获客引流。依托隐私计算技术，互联网流量机构可以结合营销推荐机构的服务需求进行个性化定制，丰富完善目标客户的画像，为潜在客户的挖掘提供有力支撑。双方之间通过密态数据的交换与共享，充分挖掘数据价值，形成潜在客户名单，通过线上线下营销，将不同客户推荐至其对应高价值领域，“千人千面”，形成定向营销。

3. 典型案例

案例一、多方联邦技术助力广告营销

在大数据及人工智能飞速发展的今天，法律法规和信任问题严重阻碍了企业之间的数据流通，数据孤岛问题像一只无形的手挡在了企业之间，限制了诸多有价值的数据合作，无论是金融风控还是营销都或多或少地遇到了效果瓶颈，企业对更多方高质量的数据合作诉求日益强。

腾讯云安全隐私计算平台基于腾讯 Angel PowerFL 隐私计算框架，保证原始数据不出本地即可快速完成隐私计算任务，保障数据安全的同时又能发挥数据最大价值。

在多方联邦助力广告营销的应用案例中，其技术架构如下图所示:

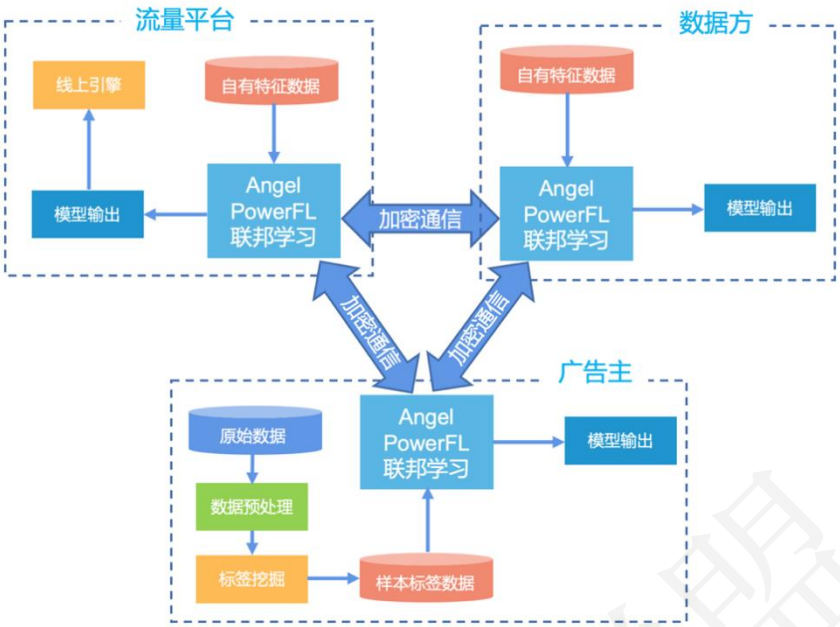


图 2-12 平台技术架构图

在本次信息流广告投放案例中，客户在过往营销转化的高质量样本，基于各合作方数千纬度的特征，多方联合建模最终调试出超预期的效果。完成模型训练后借助平台的隐匿查询功能完成了批量设备号联邦预测打分。整个过程各合作方的原始数据始终不出本地，平台通过交换加密中间参数即完成了联合建模。

本应用案例成功实现了多方联邦在广告营销的新突破。在此之前联邦学习在广告营销领域的应用只停留在双方联邦学习上，此次突破了双方联邦的限制，成功实现了三方联邦的落地。从线上实际投放结果来看，运用有限的 CRM 数据进行联邦学习训练的精准模型，在较短的广告营销活动周期中，也获得了比对照组高两倍的高质量曝光。

案例二、纵向联邦深度学习助力跨域视频推荐

某视频 APP 希望通过平台方的基础用户兴趣特征数据帮助解决新用户视频推荐冷启动问题，从而进一步提高新用户观看时长、APP

使用时长、次留率等指标。但是受限于数据安全政策与用户隐私保护法律法规，平台方的用户兴趣特征数据不能直接共享给该视频 APP 方。

腾讯 Angel PowerFL 隐私计算框架基于纵向联邦神经网络的跨域视频推荐方案，不需要直接共享数据，在保护隐私数据的前提下，平台方和视频 APP 方进行联合建模，可以利用平台方的用户兴趣特征数据来辅助视频 APP 方更精准的向新用户推荐视频，以便提升新用户的视频 APP 使用时长等指标。

针对数据不能共享导致的数据孤岛问题，腾讯 Angel PowerFL 团队制定了基于纵向联邦神经网络的跨域视频推荐解决方案。在合作双方数据都不出域的情况下，平台方与视频 APP 方进行联合建模和联合模型推理，以便提升视频推荐模型效果。

平台方与视频 APP 方进行联合建模的总体建模流程如下图所示：

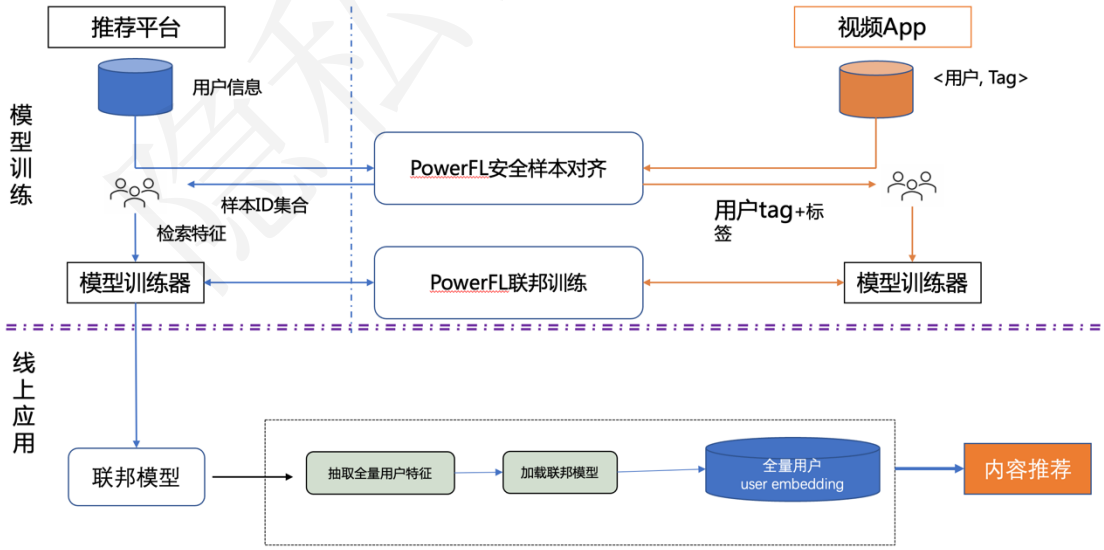


图 2-13 联合建模流程图

跨域联合视频推荐流程主要包括数据准备、安全样本对齐、联合

模型训练，以及线上模型服务等步骤。纵向联邦神经网络的两个参与方首先要进行训练样本对齐，找出公共的样本 ID 集合，之后再联合进行神经网络模型训练。联邦训练的模型为推荐系统中召回阶段常用的双塔模型，平台方训练的是用户兴趣嵌入塔，视频 APP 侧训练的是视频特征嵌入塔。最后是基于训练模型，进行线上应用。

在这个跨域联合视频推荐的案例中，每次生成的训练数据集规模约为 10 亿条训练样本，突破了计算量大、通信消息交互量大的技术挑战。

纵向联邦神经网络建模有效解决了新用户视频推荐冷启动问题，在数据不出域的前提下实现了数据协同应用，助力提升基于联邦深度学习的推荐模型效果，提升推荐模型业务应用价值。视频 APP 新用户次留率提升 20%以上，人均视频播放时长和人均 APP 使用时长均增长 15％以上，正向效果显著。

（五）新兴场景现状

1. 行业传统痛点分析

随着隐私计算应用不断探索，新兴场景进一步涌现，如能源、供应链金融、税务、车联网等。新兴场景涉及行业较广，但共同点都在于受到政策以及强烈的数据流通需求推动，并且具有丰富的数据资源，但数据共享交换存在较多问题和困难。

例如，在税务领域，2022 年 1 月 13 日中共中央办公厅、国务院办公厅印发了《关于进一步深化税收征管改革的意见》，提出“充分运用大数据、云计算、人工智能、移动互联网等现代信息技术，着力

推进内外部涉税数据汇聚联通、线上线下有机贯通”，但目前数据共享交换存在较多问题和困难，部分涉税数据联合分析流程没有打通，基于传统明细数据的共享交换，同时包括结果共享、区间共享方式，在数据安全保密日趋严格的形势下，已不满足日常工作要求。

在车联网领域，在“碳达峰、碳中和”的背景下，大力发展纯电驱动的新能源汽车是我国交通强国战略的重大需求，也是实现“30·60”双碳目标的重要举措。随着计算机和通信技术的飞速发展，车端、充电桩端已成为充换电信息化网络的关键环节，支撑着大规模人、车、运营商和电网的深度互动和数据共享。但是，目前“车-桩-网-云”数据流通中存在充换电网络信息流、数据流与价值流的运转不畅导致的整体运行低效、伪造充电账户盗用他人账户等问题。同时，新能源汽车的相关数据大多具备较高的隐私性，其信息与车主的日常生活轨迹、个人隐私息息相关，如果敏感信息在使用中产生泄漏，则会直接关系到车主的个人隐私，后果非常严重。

2. 隐私计算应用逻辑

在新兴场景中，数据需求方往往由新兴行业企业组成，如能源企业、车企、供应链企业等，数据提供方往往为金融、通信、政务等典型行业，通过隐私计算技术引入外部数据提高风控管理、精准营销、反欺诈等效果。新兴场景合作方式往往为联合建模及预测，背后原因可能为数据需求方与数据提供方在新兴场景上的合作往往处于启动或初期，缺乏成熟、简单易用的专家模型或已有模型，因此需要通过建模探索两个数据集样本间的相关性及对因变量的影响程度。

3. 典型案例

案例一、基于隐私计算的“通信+电力”大数据服务平台

在今年通过的国家第十四个五年规划中提出要“加快数字化发展，建设数字中国”，并要求加强公共数据开放共享“统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范”。电力和通信作为现代社会的重要基础，在生产过程中均产生大量数据，已具备先行先试的条件。

图 2-14 背景分析

运营商、电力分别私有化部署隐私计算平台节点，通过专线实现节点间的互联互通。双方数据各自保存在自有私有化平台上，通过 MPC 服务引擎、控制台服务、API 服务、中间件服务实现多方安全计算、安全求交、联邦学习、匿踪查询四大核心隐私计算技术服务，通过网关服务进行分片、加密等数据交互，实现双方数据在不出域的情况下完成融合和计算，保障数据安全性。整体平台架构如下图:

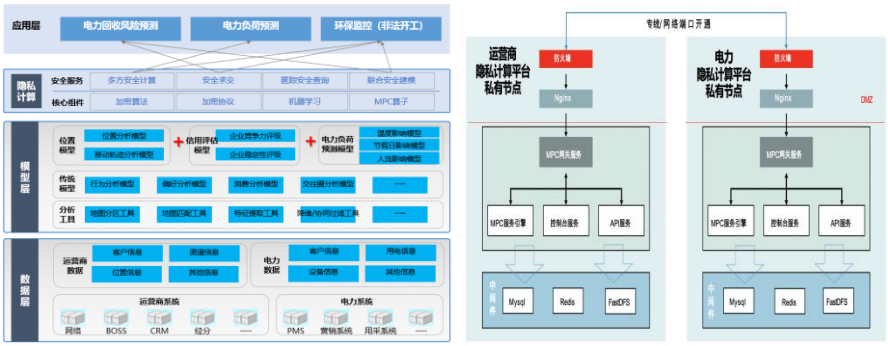
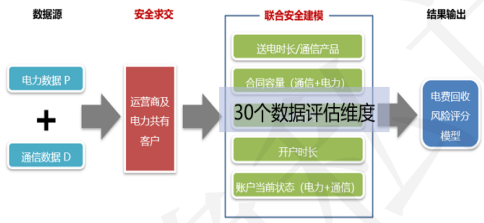


图 2-15 平台功能及部署架构

主要应用于电费回收预测以及电力负荷评估两个场景:

场景一： 电费回收风险预测是电力运营过程中的一个重要业务点。在该场景中，将运营商和电力数据进行融合将有效提升风险预测模型效果，但因其涉及企业用电行为及企业通信行为等敏感信息，需要利用安全求交技术和联邦学习技术进行数据安全保护。其整体实现流程如下图:



模型	拖欠费用户预测查准率/%	拖欠费用户预测查全率/%
利用单一电力数据的电费回收风险预测模型	63.55	5.32
电力+通信数据的电费回收风险预测模型	92.41	13.37

利用电力+通信数据不出本地的纵向学习明显提升了模型查准率和查全率

图 2-16 场景一实现流程图

效果：利用电力+通信数据不出本地的纵向联合方式将电费回收风险预测的查准率和查全率分别提升到 92%左右和 13%左右，这将有效帮助电力企业减少坏账率，目前已在绵阳电力落地运用，通过对高风险企业的加强催款及降低授信，预计每年将为绵阳电力减少损失约 2000 万元

场景二： 四川电力单一依靠自身的电力数据对电力负荷进行评

估拥有较大的局限性，结合四川移动的人口统计数据，再通过隐私计算平台多方安全计算技术实现数据融合和模型计算，也有较大的应用价值。

图 2-17 场景二实现流程图

效果：基于传统预测方式（仅基于温度及节假日）以及结合通信数据的预测方式进行了误差率对比，传统方式预测平均误差率在3.23%，而通信+电力数据平均误差率约为 0.87%，基于通信人口数据的预测可有效提升预测准确率。

案例二、智邦平台在产业链金融中的应用实践

某产业集团正在实施集团内的数字化转型战略，充分利用其集团内的数据资源，发挥数据资产价值，集团的金融子公司承担了该阶段的重要角色。但是在战略实施过程中发现，集团内部因不同子公司法人主体不同，无法使用原始数据进行共享，进而导致客户的维度不齐，实际业务的拓展和创新存在障碍；同时，集团计划也在加快推进以工程机械物联网数据为中心的数据生态构造，整合供应链上下游，推动产业数字金融的发展；需要在保护用户隐私数据安全的前提下，完成数字化转型及业务拓展，因而联合同盾科技采用隐私计算的方式进行。

本项目总体上是采用基于联邦学习的分布式机器学习架构，并综合应用同态加密、不经意传输、秘密共享等加密技术；同时结合区块

链技术，实现可监管、可审计、可追溯的监管目标；在考虑到集团层面的战略和业务要求的基础上，采用同盾科技“弱中心化”架构的方式进行部署实施。整体的业务逻辑架构如下图所示：

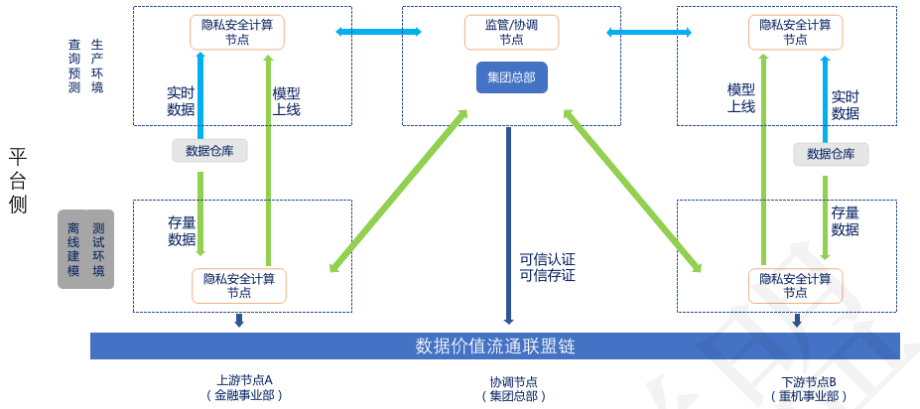


图 2-18 业务逻辑架构图

本应用实践分为三个阶段进行：

阶段一：集团内的金融机构联合同盾科技，在汽车金融场景基于联邦学习实现贷前风控，进而推动集团的去担保化目标；

阶段二：集团内的金融机构、汽车租赁机构联合集团内的数据源子公司，通过联邦学习实现贷中监控，将内部的可用数据源以联邦的方式进行串联，并引入联盟链技术，实现隐私保护条件下的数据资产要素挖掘的同时，实现数据要素使用的可审计等合规性要求；

阶段三：通过集团的业务服务综合管理平台，联合多家银行，基于多方的数据采用联邦学习的方式进行风控全流程的联合建模服务，并结合联盟链技术，实现综合管理平台对数据使用的智能合约等功能要求，构建产业数据赋能生态，串联起供应链上下游数字价值。

本案例通过联邦学习和联盟链的方式，在三个不同的业务场景进行实践与探索，完成集团数字化转型目标，其创新点及对产品价值：

一方面，应用联邦学习技术充分激活内部数据价值，解决数据孤岛问题；并实现具体业务的创新，有助于扩大信用赋能比例，是实现集团内数字化转型的关键一步；

另一方面，在集团的业务服务综合管理方面，实现上下游供应链的打通，有助于实现产业数字价值循环；

最后，在满足监管要求层面，联合联盟链技术，实现全业务流程可审计、可监管的要求，符合科技向善的总体要求，并为社会创造价值。

案例三、基于隐私计算的税电联合分析系统

某省作为重工业大省，历年来环保治理问题一直是政府和百姓关心的热点问题。据生态环境部下发的《中国生态环境公报》显示，2019年、2020年该省在城市空气质量、地表水环境质量排名较为落后，且每万元GDP耗电量较大。根据国家税务总局税收大数据和风险管理局与国家电网联合开展数据共享的报告精神，按照总局《税电共享合作试点工作方案》的安排，该省税务局作为承接单位，积极推进税务与电力数据融合应用，进行税电联合分析。

某省的税电联合分析隐私计算解决方案深入挖掘电力数据价值，与国网电力公司在“双高”企业税收指数分析、钢铁行业税收风险分析、煤焦化行业税收风险分析、电费回收风险模型、税电综合信用模型等业务场景，联合开展指数分析、风险模型分析。基于隐私计算的税电联合分析系统采用“同态加密技术+分布式计算技术”，保障各部门之间不泄露数据，安全合规的前提下，进行数据合作。

隐私计算执行过程分为复杂模型训练过程和规则模型计算过程。国税局和国家电网是项目中的数据交互参与方，在国家电网侧部署中央服务器。针对目标企业，国家电网和国税局将样本数据，按照规则进行样本对齐，上传中央服务器，依据模型复杂程度选择不同训练计算方式，针对机器学习、神经网络等预测类模型的复杂过程，通过训练参数传递的方式进行模型训练。规则类模型的联合分析过程，通过同态加密和授权审核机制来保证数据的安全性和联合分析的效率，在国网和税局双方部署安全环境，负责模型应用的计算调度，不存储任何一方原始明细数据。

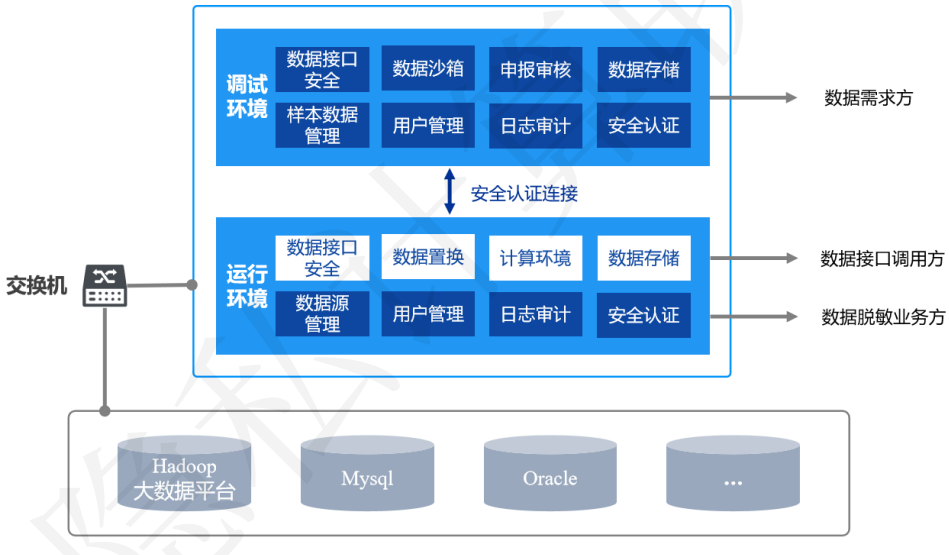


图 2-19 技术架构图

基于隐私计算技术的税电联合分析系统打通了多方涉税数据共享与联合分析中隐私安全的屏障，实现信息数据在无可信第三方场景下跨部门、跨行业、跨区域的交换共享，解决了现行外部涉税数据交互不足、数据孤岛、数据传递渠道受阻、单类数据价值低等问题。基于隐私计算的税电联合分析系统是隐私计算技术首次应用于税务领

域的成功范例，是国家税务总局某省税务局一次创新尝试。

案例四、车联网“车-桩-网-云”数据协同服务平台

在当前传统经济向数字经济转型的过程中，依据数据安全相关法律法规，车联网信息化系统需要充分融合隐私计算技术，建设车联网隐私计算服务平台，能够合规合理使用新能源车相关的敏感信息解决相关数据融合问题，在平台中需要实现车联网数据、电网数据、桩端数据、保险数据等多个数据源和应用场景的数据安全融合共享，引领我国车联网领域的数字经济健康发展。

2022 年，北理新源与航天信息联合建设的车联网隐私计算平台在确保多方原始数据、业务模型参数不出用户平台前提下，满足两方和多方的基本运算、联合统计、联合建模、模型预测等功能需求。平台应提供一套完整的跨域交互信息管理机制，有效帮助机构和企业满足用户隐私保护、保障数据安全、高效多方数据融合。

在总体架构上，平台采取分布式节点参与计算、隐私计算服务平台中心节点负责管理的架构模式，总体业务架构如下图所示。隐私计算服务平台分为中心服务节点和分布式节点两类。中心服务节点：不拥有任何业务数据以及不接受、转发、留存任何业务原始数据，可以帮助分布式计算节点转发隐私计算相关的加密数据和业务控制数据，具有任务分发、节点调度、监管存证等管理功能；分布式计算节点分为车端、桩端、电网端等，拥有多个数据管理节点和一个分布式计算节点，该参与方的多个数据管理节点可能对接一个或多个数据源。

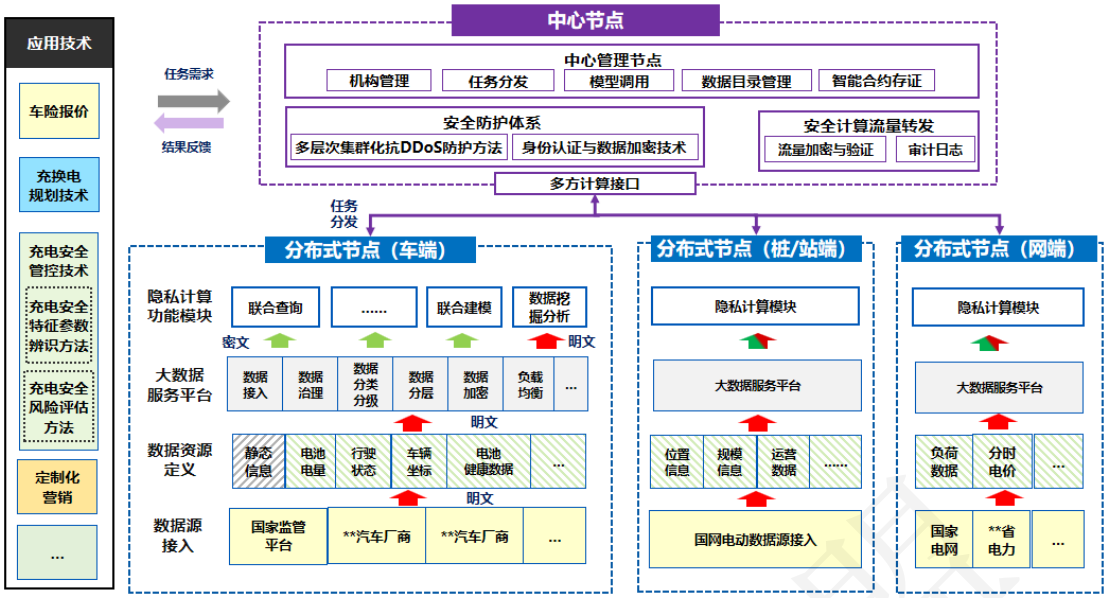


图 2-20 技术总体架构图

北理新源车联网协同隐私计算平台为充电用户提供准确的车载动力电池健康检测报告及用车建议，增加与用户互动，提高充电粘性。智能选址业务构建“人-车-桩-网”协同互动的数据体系，为充电设施布局优化提供数据支持。无感有序充电达成降低用户充电成本同时提高了电网低谷时间利用率的双赢局面。协同车险业务提供案件的欺诈性分数和车辆出险风险概率判定，优化保险公司的车险报价业务模型。

隐私计算联盟

第三章

隐私计算项目应用部署难点及解决方案

目前，隐私计算技术正处于快速迭代的发展阶段，可一定程度解决企业和机构面临的数据合规流通难题，为数据安全制度落地提供有力的技术支撑。随着众多数据流通项目需求方及产品提供方开拓创新，先行先试，隐私计算以满足实际产业需求、解决实际产业问题为牵引，逐步完成从理念到落地应用。按照“边试点、边总结、边推广”的思路，本章将从项目管理角度出发，以隐私计算项目建设部署前、中、后三个阶段进行划分，全面梳理项目常见难点并总结优秀解决实践，为探索隐私计算项目可复制、可推广的实施路径和模式提供参考。

（一）建设部署前

1. 产品安全性

隐私计算并非单一的技术，而是包含多种隐私保护技术，涉及密码学、安全硬件、信息论、分布式计算、人工智能、区块链等多个学科。隐私计算基于其实现隐私保护的原理可分为密码学、可信执行环境、信息混淆脱敏等。在基于数学、密码学和硬件技术等综合形成的保障机制内的交互与计算呈现多样性和复杂性的特点，基于安全仿真用例的 POC 测试有难以完全检验产品安全性问题。

目前对产品安全性验证的主要方式是中国信通院云大所可信隐私计算产品的安全评测等三方评测，通过原理核验、代码核验、网络抓包、日志核验等方式佐证通信内容的符合安全要求。

2. 产品合规性

行业用户对隐私计算技术不理解和隐私计算相关法律法规要求程序不够明确，对基于隐私计算的数据流通是否合规存在顾虑。

目前解决方案是通过可视化、参数分析、抓包等方式展示复杂的内部模型结构，或通过对比实验解释模型的运行原理，从而降低用户的顾虑、帮助用户理解现有技术方案的合规优势。

3. 产品功能

行业用户对隐私计算的应用场景不明确，导致行业用户要求的功能测试项覆盖面大而全，基本覆盖隐私计算的技术场景；行业用户现有传统模型的迁移问题。

目前主要参考产品在中国信通院云大所、隐私计算联盟等机构的相关标准测试报告中的各项指标表现，考察隐私计算产品支持的技术路线以及技术方案能力实现情况，参考产品在业务场景的落地实施情况，进而展开产品与技术选型，并根据实际业务需求进行定制化实施。

对于迁移传统模型的主要解决方案是在深入理解客户业务场景的前提下，深度剖析客户已有的传统模型，将其进行算子模块化拆解。利用隐私计算平台已实现的安全计算算子和模型，构建出与传统模型相同功能的隐私计算新模型。

4. 产品性能

隐私计算产品的性能相比明文计算慢很多，影响隐私计算产品的性能的因素主要有以下三个方面：

加密算法对性能的影响。加密算法在计算过程中存在较多的加密、

解密步骤，让计算量以几何级增长，相比明文计算，密文计算需要更大的存储、计算资源和通信负载，导致性能损失;

资源因素的影响。在加密算法的计算和通信过程中，网络通信环境、数据预处理情况、算力、运行环境等因素也会对隐私计算的性能产生相应的影响;

多方协同的“木桶效应”。多方计算模式下，需要多个参与方同步计算、实时通信，在性能上的体现出了“木桶效应”，即：性能最弱的参与方或者计算节点将成为整个网络的计算瓶颈。

目前对产品性能提升主要有硬件加速方案和软件加速方案，硬件加速方案有基于 GPU、FPGA 或将算力加速能力固化至 ASIC 的硬件加速方案和结合 TEE 的加速方案；软件加速方案有强化并行计算能力、算法优化、通信优化等。

（二）建设部署中

1. 机构内部网络

金融、通信等行业机构的网络环境对安全有着极高要求，同时机构内基础环境复杂，比如会存在异构云之类的情况，厂商往往对行内的部署环境缺乏了解，在对技术方案的设计和具体实施部署过程中往往遇到非常规的问题，增加部署成本。

为实现高易用性，提倡系统采用容器化部署的方式，对功能模块进行强解耦，从而在面对不同的基础环境和网络架构时，便于部署与迁移，实现降本增效。

2. 软硬件资源的多样性

因不同客户所要求的软件、中间件等版本不同，需在隐私计算平台部署过程中对不同软件、中间件版本进行适配，以提高平台部署效率。同时，因隐私计算平台在多方进行部署，需注意不同版本之间的兼容性。

隐私计算联盟

专栏 1：趣链网络隔离个节点网络不易联通解决方案

杭州趣链科技有限公司在“风险信息协同共享平台”项目中，通过“自研网络代理节点”方式解决“项目建设部署中，平台采用分布式架构，因存在网络隔离各节点网络不易联通”问题，达到了“以应对网闸、光闸、防火墙、内外网等复杂网络隔离问题”效果。

项目部署过程中，因涉及到隐私数据，各方均不允许明文数据出库，因此计算节点应部署在机构数据的网络环境中，通常会存在网闸、光闸、防火墙、局域网等不同形式的网络隔离情况，造成内部节点不能安全的与其他节点或区块链进行交互。

为了完成 BitXMesh 跨网闸数据传输，拟采用添加跨网闸 Agent 的方式进行中继数据传输，节点网络传输部分使用 Lightp2p 库，基于 Lightp2p 库开发 Agent 节点，开发跨网闸 Agent 应用层协议及在 Lightp2p 中添加跨网闸通信协议。

跨双网闸场景中，本地数据传输和远程文件下载速度基本只与网络隔离设备的参数设置有关，不受文件大小、节点数量等限制。GB 级文件下载速度稳定在 5MG/s（网闸限制的最大数据传输量为 5MB/s）

专栏2：联易融适应多方用户复杂的网络结构的隐私计算解决方案

联易融数科在某集团基于隐私计算的数据要素流通项目中，通过隐私计算适配可扩展的双中心集中式网络架构的方式，解决了隐私计算在面对多方用户在内外网复杂网络结构部署的问题，达到了隐私计算算法在内部星状网络与外网多个节点顺利执行，各节点数据安全自由流通的效果。

某集团要求能与内外部合作机构通过隐私计算节点进行数据要素流通，多个蕴藏数据的隐私计算节点组成了一个安全的数据流通网络。为了实现此目标，首先应解决两个问题：一是多个机构之间的网络比不是理想中的同一个分布式网络，而是有层级，且又会分布在内外网。二是为了提高数据提供方参与的积极性，降低其接入成本，客户对隐私计算产品的可推广性提出较高要求，隐私计算节点应该能够即插即用，而不是要和另外所有的节点都保持通信。

为了能够解决以上两点问题，联易融基于核心隐私计算底层技术，将节点分为了两层，转发节点和计算节点。其中，中心化的转发节点提供服务注册功能，接收来自计算节点的注册，使得转发器可以通过服务注册中心动态获取计算节点的地址信息来实现转发规则的动态维护。通过改变传统的多方安全计算分布式的网络架构，联易融提出可扩展的双中心集中式网络架构，满足隐私计算在局域网和公网等混合网路灵活部署的要求，方便客户的多个合作机构随时接入，从而解决了隐私计算节点轻量灵活部署 “最后一公里”的问题。

（三）建设部署后

1. 隐私计算应用部署后的监管审计

隐私计算应用中的数据的真实性、数据来源、数据确权及流转过程是否安全合规，是隐私计算应用日常使用中需要面临的问题。如何在隐私计算应用中建立多方互信和多方有序协作，为隐私计算应用做好后督工作，是隐私计算应用部署后需要解决的一大难题。

目前的解决方案是结合区块链的数据可溯源、难以篡改、公开透明、分布式架构、智能合约自动执行等技术特点，对隐私计算应用全流程的关键信息和任务信息进行区块链上链存证，形成原生的可穿透式的可信存证与协同，便于对隐私计算应用全流程的监管维护和事后的审计检验，确保隐私计算应用可信、高效、有序执行。

2. 隐私计算产品跨平台互联互通

在应用实践中，数据使用方通常需要和不同的数据源合作，而不同的数据源也往往部署着不同的隐私计算平台。因为多数隐私计算厂商平台主要采取闭源形式，加之技术路线多样化、各平台间系统架构不同、功能实现方式差异等问题，导致不同平台之间无法实现数据可信流通，出现了“计算孤岛”问题。

目前解决方案是基于独立的闭源算法实现，厂商推动互联互通标准化协议落地。

3. 隐私计算产品部署后的运维和更新

隐私计算技术体系庞大且复杂，行业用户运维力量无法保障，产品运维、版本更新部署等方面普遍存在问题。

目前的解决方案是软件层面基于云容器技术提供强大的统一运维管理平台，运维工作事项可视化、直观性操作；另一方面是提供隐私计算一体机，为用户提供开箱即用能力。

对产品更新的解决方案是兼容新旧版本的互通，保障继续正常使用。

4. 算法可解释性

隐私计算拥有多元且复杂的算法以及多样化的计算与交互逻辑，增加了技术的可解释性难度。这将让隐私计算的实践过程的多方参与者难以一致评估、理解算法模型，难以确定相关算法出现问题时就在何种程序上实现成功检测。

受隐私保护要求，建模方无法获知原始数据，缺少对建模过程数据的感知。针对此问题，可采用数据审计，建模全流程关键信息留存、建模效果多维度评估等技术，提高建模方对建模过程数据感知能力，提高对模型结果的多维度有效性验证。另一方面提供全体完整模型报告，方便用户了解整个建模过程的理论依据和对已有样本数据进行准确率验证。

专栏 3：浦发银行算应用部署后的监管审计解决方案

浦发银行在“数据多方安全计算应用系统”项目中，通过结合区块链技术对隐私计算任务全流程关键信息进行上链存证，解决了隐私计算应用部署后的监管审计问题，确保隐私计算应用可信、高效、有序执行。

在隐私计算应用中如何建立多方互信和多方有序协作,并为隐私计算应用做好后督工作,是隐私计算应用部署后需解决的一大难题。浦发银行的“数据多方安全计算应用系统”，结合区块链技术的可溯源、难篡改、公开透明、分布式架构、智能合约自动执行等特点，以区块链作为各个节点任务的驱动，对任务流程和关键信息进行上链存证，形成原生的穿透式监管服务模式。上链信息仅经过加密处理，保持了数据的原生性，在后续监管审计时可直接将链上信息与本地存储信息进行比对校验。在穿透式的监管模式下，系统中数据流转过程可通过区块链智能合约进行全流程的规范化约束，流转流程的关键信息从数据持有者的注册登记到数据确权以及数据流通的各个方面，都会进行上链存证以便后续的溯源校验。可穿透式的监管模式还可满足面临不同的监管要求时需提供的单一信息到系列循环报送方式。

在数据多方安全计算应用系统中结合区块链技术形成原生的穿透式监管存证服务模式，确保系统运营中，实现在隐私计算技术保护下对数据流通全流程的监管与维护，确保隐私计算应用可信、高效、有序执行，有助于结合隐私计算技术的业务场景应用的合规落地与推广，也便于后续配合想相关的监管审计工作。

专栏 4：数牍科技针对自定义算子解决方案

北京数牍科技有限公司（简称：数牍科技）在粤港澳大湾区大数据中心数据要素化支撑平台项目（简称：粤港澳项目）中，通过可视化创建/修改算子方式解决部署后用户使用算子的高学习成本问题，达到低门槛灵活配置算子效果。

项目中，数牍部署多方安全计算平台后，一直致力于解决如何可以低成本地使用联邦学习等算子。对每个具体的任务算子，数牍可视化子系统以方框图的方式展示在 DAG 画布上，对算子直接的输入输出关系，可视化子系统以箭头的方式展示在 DAG 画布上，如下图所示。同时对算子的具体参数(包含参与方，数据源，模型超参数等)以编辑列表方式展示。

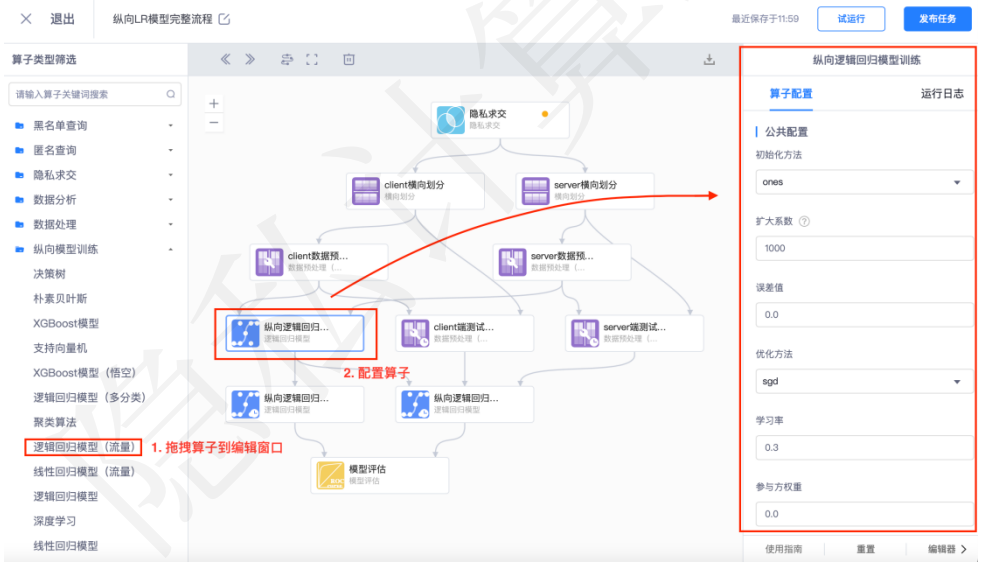


图 3-1 可视化子系统算子输入输出关系图

通过可视化创建/修改算子的方式，在已有算法的基础上，便捷定义所需的算子，减少了重新定制化开发的时间成本（10～30 人天/个）。

第四章

隐私计算应用展望

（一）技术提升

目前整个隐私计算行业的产品化能力仍处于初期，市场上隐私计算产品众多，水平参差不齐，可用性是个值得思考的角度。在隐私计算场景中，会涉及到大量的密文运算及节点间通信，所以计算和通信的代价会非常高昂，而且很容易使其性能远远劣于传统的本地算法，性能的巨大差异可能导致实际落地场景无法忍受。面对大规模场景，数十亿数量级数据运算时，分布式计算节点的故障、网络波动等引发的稳定性问题，隐私计算平台该如何来保证其可用性；不同的行业、不同的场景下，隐私计算的安全性和性能该如何保障；这些都是产品可用性遇到的问题。

在未来的发展中，隐私计算平台需应对数据量的不断增长，那么算力和通信问题的解决必然是一个趋势，技术厂商们也将会通过软硬件结合的方式在兼顾性能和安全性。在 3 月初结束的全国两会上，“建设数字信息基础设施”“提升关键软硬件技术创新和供给能力”被政府确定为 2022 年重点工作内容。软硬件协同隐私计算方案可有效降低应用落地的部署门槛，同时加强软硬件的全栈能力。软硬件协同产品从底层芯片的选择、硬件电路的涉及、国产密码算法的研发，到上层的隐私计算平台，一键式实现完全的国产自主可控。通过软硬协同方

案，可将隐私计算核心算法、算子等进行功能抽取，将其能力下沉并部分托管至硬件环境中，通过调用芯片的加速能力提升平台算力；在“存储”和“传输”方面，可引入物理隔离的通信通道，实现算法及算子的单独运行、数据的单独传输，从逻辑上封装算法/算子的安全加速单元，完成数据“算、存、传”的安全隔离处理。通过结合硬件可插拔的特性，让企业服务器一插即用，即可将之变为隐私计算专用服务器，这无疑提升了产品的可用性，推动隐私计算基础设施的快速落地进程。

在软硬件结合的探索中，隐私计算一体机方案被广泛采用。隐私计算一体机为需求方提供开箱即用的一套隐私计算解决方案，与此同时通过软硬结合的方式实现性能和安全性的增强，更好得提升隐私计算技术在实际应用场景的可用性，推动隐私计算大规模商业化落地。

（二） 规模丰富

随着隐私计算技术提升及可用性增强，隐私计算应用规模将持续增强。其市场空间将来自于两个方面：一是传统数据流通模式（数据包传输、API 调用等）将被隐私计算的可信数据流通方案所重构；另一方面，传统模式下难以共享的数据（如政务数据等）将在隐私计算的加持下实现安全合规开放。

根据 Gartner《2021 年隐私成熟度曲线》报告中预测：2023 年之前全球 80%以上的企业将面临至少一项以隐私为重点的数据安全保护规定；到 2024 年以数据隐私驱动的合规投入将突破 150 亿美元。到 2025 年 60%的大型企业组织将在分析、商业智能或云计算中使用一种或多种隐私增强计算技术。根据艾瑞咨询报告《中国隐私计算行

业研究报告：云程发轫，精耕致远》，2021 年中国隐私计算市场规模为 4.9 亿元，预计 2025 年将达到 145.1 亿元，数据运营占比持续升高。Gartner 发布的 2022 年十二大重要战略技术趋势中指出，预计到 2025 年，60%的大型企业机构将使用一种或多种隐私计算技术（其称为隐私增强计算技术）。

（三）行业拓展

2019 年，Gartner 首次将隐私计算列为处于启动期的关键技术。2020 年，Gartner 又将隐私计算列为 2021 年企业机构九大重要战略科技之一。近两年来，伴随着技术的不断成熟，国内外隐私计算产业化的步伐明显加快。可以预见，未来几年将是技术产品加速迭代，应用场景快速升级，产业生态逐步成熟的重要阶段。

隐私计算的主要应用领域在金融、通信、政务、医疗、能源等方面。目前的拓展方向一是新的行业领域，二是原有行业的细分领域。

1) 证券基金行业拓展

隐私计算在金融行业主要应用在银行风控和营销领域，目前在向保险、证券及基金行业拓展。

对于证券基金行业，证券基金公司总部及其子公司的客户隐私数据无法在内部整合，在满足法律合规要求前提下，通过隐私保护计算技术可以进行一体化风险度量和管理，可以降低证券公司内部金融风险的隐蔽性和复杂性。探索合格投资者判断、穿透式风控、联合反洗钱及黑名单共享等应用场景，能够帮助证券公司全面提升综合风控能力。在联合营销场景中，可以探索通过联邦学习技术丰富业务数据和

模型，能够更精准有效地定位业务目标，挖掘数据最大价值。

2) 能源电力行业拓展

能源电力领域数据具有数据质量参差不齐、成熟度不高、复杂度较高、协同性较差等特点。目前业内部分领先厂商已经开始探索能源电力领域的技术应用。

在虚拟电厂运营、充配电网协同、电力市场交易等与能源区块链关联的业务场景中，可采用区块链实现数据流通与融合的可信、可溯、可审计。在此基础上，借助隐私计算进一步提升业务系统对黑客解密、篡改数据的难度，确保数据流通融合的隐匿、安全、合规，实现源网荷储一体化数据协同。

在与工业互联网关联的业务场景中，可通过区块链和隐私计算实现数据流通的可信、可塑、可审计、隐匿、安全、合规，建立工业互联网设备画像，并实现设备、数据及网络层面的互联互通。

3）车联网行业拓展

在泛车联网行业，可通过建立省级的平台部署，提供覆盖全省的业务服务，面向全国示范应用。推动车联网数据安全共享生态的建立，推进车联网数据可信体系建立，研究多企业数据联合应用的合作模式，促进车联网行业数据安全共享应用。

在车联网隐私计算平台的应用示范、逐省推广和业务拓展的基础上，可进一步推广至智能交通领域，进行积极拓展商业化项目推广，建立领先、高安全、高性能、高可靠的隐私计算产品和应用示范，树立跨平台车联网数据安全应用的示范标杆；研发跨行业、跨领域的数

据融合应用技术，建立合作机制，通过技术服务为智能交通领域企业赋能；支持隐私计算技术在智能交通领域的商业化、规模化应用，引领智能交通全行业的隐私计算技术发展。

隐私计算联盟

参考文献

[1] “Gartner Report: Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation”,Gartner,2021

[2] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[3] Yao A C. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982: 160-164.

[4] 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.

[5] Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: what it is, and what it is not[C]//2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015, 1: 57-64.

[6] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers[C]//Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2010: 465-482.

[7] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. PMLR, 2017: 1273-1282.

[8] 闫树，袁博，吕艾临等.《隐私计算——推进数据”可用不可见”的关键技术》[M]. 电子工业出版社,2022-03-01

[9] 隐私计算联盟、中国信通院云大所《隐私计算白皮书（2021 年）》

[10] Yang Y, Wei L, Wu J, et al. Block-smpc: A blockchain-based secure multi-party computation for privacy-protected data sharing[C]//Proceedings of the 2020 The 2nd International Conference on Blockchain Technology. 2020: 46-51.

[11] Ding Z, Wang Y, Wang G, et al. Detecting violations of differential privacy[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 475-489.

[12] Chen Y, Machanavajjhala A, Hay M, et al. Pegasus: Data-adaptive differentially private stream processing[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017:

1375-1388.
[13] Avent B, Korolova A, Zeber D, et al. {BLENDER}: Enabling local search with a hybrid differential privacy model[C]//26th USENIX Security Symposium (USENIX Security 17). 2017: 747-764.
[14] Geyer R C, Klein T, Nabi M. Differentially private federated learning: A client level perspective[J]. arXiv preprint arXiv:1712.07557, 2017.
[15] Canonne C L, Kamath G, Steinke T. The discrete gaussian for differential privacy[J]. Advances in Neural Information Processing Systems, 2020, 33: 15676-15688.
[16] Bagdasaryan E, Poursaeed O, Shmatikov V. Differential privacy has disparate impact on model accuracy[J]. Advances in Neural Information Processing Systems, 2019, 32.
[17] Luo Z, Wu D J, Adeli E, et al. Scalable differential privacy with sparse network finetuning[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2021: 5059-5068.
[18] Liu J, Jin W, He Z, et al. HUT: Enabling High-UTility, Batched Queries under Differential Privacy Protection for Internet-of-Vehicles[J]. arXiv preprint arXiv:2202.06495, 2022.
[19] Zhu J, Hou R, Wang X F, et al. Enabling rack-scale confidential computing using heterogeneous trusted execution environment[C]//2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020: 1450-1465.
[20] Valero J M J, Sánchez P M S, Lekidis A, et al. Trusted Execution Environment-enabled platform for 5G security and privacy enhancement[M]//Security and Privacy Preserving for IoT and 5G Networks. Springer, Cham, 2022: 203-223.
[21] Janjua H, Ammar M, Crispo B, et al. Towards a standards-compliant pure-software trusted execution environment for resource-constrained embedded devices[C]//Proceedings of the 4th Workshop on System Software for Trusted Execution. 2019: 1-6.
[22] 闫树, 吕艾临. 隐私计算发展综述[J]. 信息通信技术与政策, 2021, 47(6): 1.
[23] 王付群.全同态加密的发展与应用[J].信息安全与通信保密,2018(11):81-91.
[24] Ducas L, Stehlé D. Sanitization of FHE ciphertexts[C]//Annual

International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2016: 294-310.
[25] 贾轩, 白玉真, 马智华. 隐私计算应用场景综述[J]. 信息通信技术与政策, 2022,48(5):45-52.
[26] Fiore D, Mitrokotsa A, Nizzardo L, et al. Multi-key homomorphic authenticators[C]//International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2016: 499-530.
[27] Wang X, Han Y, Wang C, et al. In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning[J]. IEEE Network, 2019, 33(5): 156-165.
[28] Konečný J, McMahan H B, Yu F X, et al. Federated learning: Strategies for improving communication efficiency[J]. arXiv preprint arXiv:1610.05492, 2016.
[29] Reisizadeh A, Mokhtari A, Hassani H, et al. Fedpaq: A communication-efficient federated learning method with periodic averaging and quantization[C]//International Conference on Artificial Intelligence and Statistics. PMLR, 2020: 2021-2031.
[30] Kang J, Xiong Z, Niyato D, et al. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal, 2019, 6(6): 10700-10714.
[31] Truex S, Liu L, Chow K H, et al. LDP-Fed: Federated learning with local differential privacy[C]//Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking. 2020: 61-66.
[32] Kanagavelu R, Li Z, Samsudin J, et al. Two-phase multi-party computation enabled privacy-preserving federated learning[C]//2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID). IEEE, 2020: 410-419.
[33] Zhang C, Li S, Xia J, et al. {BatchCrypt}: Efficient Homomorphic Encryption for {Cross-Silo} Federated Learning[C]//2020 USENIX Annual Technical Conference (USENIX ATC 20). 2020: 493-506.
[34] Yang X, Li W. A zero-knowledge-proof-based digital identity management scheme in blockchain[J]. Computers & Security, 2020, 99:

102050.
[35] Xu S, Cai X, Zhao Y, et al. zkrpChain: Towards multi-party privacy-preserving data auditing for consortium blockchains based on zero-knowledge range proofs[J]. Future Generation Computer Systems, 2022, 128: 490-504.
[36] 赵双阁, 李亚洁. 区块链技术下数字版权保护管理模式创新研究[J]. Journal of Southwest University of Political Science & Law, 2022, 24(1).
[37] Yue D, Chengqi Y, Qianqian H, et al. Constructing a Common Data Circulation Infrastructure Platform for the National Unified Data Factor Market——Technical Path and Policy Thinking of Constructing the National "Data Networking" Root Service System[J]. Data Analysis and Knowledge Discovery, 2022, 6(1): 2-12.
[38] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
[39] 王腾,霍峥,黄亚鑫,范艺琳.联邦学习中的隐私保护技术研究综述[J/OL]. 计算机应用:1-15[2022-05-25]
[40] Chongchitmate W, Ostrovsky R. Circuit-private multi-key FHE[C]//IACR International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2017: 241-270.
[41] 谈玉胜, 殷丹丽. 基于智能合约的可信物联网 SLA 协议模型[J]. Computer Science and Application, 2022, 12: 923.
[42] Li P, Li J, Huang Z, et al. Multi-key privacy-preserving deep learning in cloud computing[J]. Future Generation Computer Systems, 2017, 74: 76-85.
[43] 梁秀波, 吴俊涵, 赵昱, 等. 区块链数据安全管理和隐私保护技术研究综述[J]. 浙江大学学报 (工学版), 2022, 56(1): 1-15.

附录 A

国内隐私计算相关政策

表 A.1　国内隐私计算相关政策列表

时间	发布机构	名称	重点内容
2019	国家网信办	《数据安全管理办法》（征求意见稿）	对网络运营者在数据采集、处理使用、安全监管等方面提出了要求
2019	国家网信办	《个人信息出境安全评估办法》（征求意见稿）	就维护国家安全、社会公共利益，保障个人信息安全和重要数据安全给出了评估办法。
2020	工业和信息化部办公厅	《工业数据分级分类指南（试行）》	提出工业数据的基本概念，明确适用范围和原则；明确企业为数据分类分级主体，承担开展数据分类分级、加强数据管理等主体责任；按照每类工业数据遭篡改、破坏、泄露或非法利用后可能带来的潜在影响，将数据划分为 3 个级别。
2021	国家医疗保障局	《关于加强网络安全和数据保护工作的指导意见》	提出加强医疗数据安全保护的相关要求，包括：实施数据全生命周期安全管理、实施分级分类管理、加强重要数据和敏感字段保护、强化数据安全审批管理、落实数据安全权限、推动数据安全共享和使用、建立健全数据安全风险评估机制。
2021	国家网信办	《汽车数据安全管理若干规定（征求意见稿）》	明确汽车行业中重要数据的范围；对于汽车数据收集进行车内车外双场景区分；提出数据全生命周期的处理要求；明确汽车行业数据本地化存储的原则要求和跨境数据传输具体要求。
2021	国务院办公厅	《要素市场化配置综合改革试点总体方案》	提出建立健全数据流通交易规则：探索“原始数据不出域、数据可用不可见”的交易范式；探索建立数据用途和用量控制制度，实现数据使用“可控可计量”。
2022	上海市人大	《上海市数据条例》	聚焦数据权益保障、数据流通利用、数据安全管理三大环节，涵盖了数据分级分类保护、重要数据目录管理、数据安全管理等配套措施，落实重要数据备案和数据安全评估制度。
2022	深圳市人大	《深圳经济特区数据条例》	作为国内数据领域首部地方综合性立法开始实施，要求数据处理者应当对其数据处理全流程进行记录，保障数据来源合法以及处理全流程清晰、可追溯。
2022	国务院	《“十四五”数字经济发展规划》	推动提升重要设施设备的安全可靠水平，增强重点行业数据安全保障能力。进一步强化个人信息保护，规范身份信息、隐私信息、生

时间	发布机构	名称	重点内容
			物特征信息的采集、传输和使用，加强对收集使用个人信息的安全监管能力。
2022	中央网信办、农业农村部、国家发展改革委、工信部、科技部、住房和城乡建设部、商务部、市场监管总局、广电总局、国家乡村振兴局	《数字乡村发展行动计划（2022-2025年）》	加强安全保障加强农业农村数据安全保护，落实涉农关键信息基础设施安全保护制度和网络安全等级保护制度，开展网络安全监督检查专项行动。组织开展面向农村居民的网络安全教育培训，提升个人信息保护意识。
2022	国家网信办	《互联网信息服务深度合成管理规定（征求意见稿）》	深度合成服务提供者应当加强训练数据管理，确保数据处理合法、正当，采取必要措施保障数据安全。训练数据包含涉及个人信息数据的，还应当遵守个人信息保护有关规定，不得非法处理个人信息。
2022	国务院	《关于加快推进政务服务标准化规范化便利化的指导意见》	以全国一体化政务服务平台为数据共享总枢纽，在确保数据安全的基础上，充分发挥政务数据共享协调机制作用，建立政务数据共享供需对接机制，推进国务院部门垂直管理业务信息系统与地方政务服务平台深度对接和数据双向共享，强化部门之间、部门与地方之间、地方之间政务数据共享，提高数据质量和可用性、时效性，满足各类普遍性数据需求。
2022	国家网信办、发展改革委、工业和信息化部等	《网络安全审查办法》	《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围，要求掌握超过100万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查。《办法》规定为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。
2022	中央网信办、教育部、工业和信息化部、人力资源社会保障部	《2022 年提升全民数字素养与技能工作要点》	筑牢数字安全保护屏障。增强网络安全、数据安全防护意识和能力，加强个人信息和隐私保护
2022	国务院办公厅	《要素市场化配置综合改革试点总体方案》	建立健全数据流通交易规则。探索“原始数据不出域、数据可用不可见”的交易范式，在保护个人隐私和确保数据安全的前提下，分级分类、分步有序推动部分领域数据流通应用。

附录 B

隐私计算标准、论文、专利、软著现状

表 B.1　国内外标准列表

时间状态	标准名称	组织
2016 年发布	Information technology - Security techniques - Secret sharing（信息技术-安全技术-秘密分享）	ISO
2019 年发布	Information technology - Security techniques - Encryption algorithms - Part 6: Homomorphic encryption（信息技术-安全技术-加密算法-第 6 部分：同态加密）	ISO
2020 年立项	Information security - Secure multiparty computation - Part 1: General（信息安全-多方安全计算-第 1 部分：　通用）	ISO
2020 年立项	Information security - Secure multiparty computation - Part 2: Mechanisms based on secret sharing（信息安全 - 安全多方计算 第 2 部分：基于秘密共享的机制）	ISO
2021 年发布	Technical Framework for Shared Machine Learning System（隐私保护机器学习技术框架）	ITU-T
2019 年立项	Technical Framework for Secure Multi-Party Computation（多方安全计算技术框架）	ITU-T
2019 年立项	Recommend Practice for Secure Multi-Party Computation（多方安全计算参考框架）	IEEE
2019 年立项	Standard for Technical Framework and Requirements of Shared Machine Learning（共享学习系统计算框架及要求）	IEEE
2020 年立项	Standard for Secure Computing Based on Trusted Execution Environment（基于可信执行环境的安全计算）	IEEE
2021 年发布	Guide for Architectural Framework and Application of Federated Machine Learning（联邦学习架构框架与应用指南）	IEEE
2020 年立项	Standard for Secure Computing Based on Trusted Execution Environment（基于可信执行环境的安全计算）	IEEE
2021 年发布	Guide for Architectural Framework and Application of Federated Machine Learning（联邦学习架构框架与应用指南）	IEEE
2022 年立项	Standard for Requirements of Privacy-preserving Computation Integrated Platforms(隐私计算一体机要求)	IEEE
2020 年发布	多方安全计算金融应用技术规范	全国金融标准化技术委员会
2021 年立项	联邦学习技术金融应用规范	全国金融标准化技术委员会

时间状态	标准名称	组织
2021 年立项	隐私计算技术应用指南	全国信息安全标准化技术委员会
2021 年立项	隐私保护的数据互联互通协议规范	全国信息安全标准化技术委员会
2019 年发布	基于多方安全计算的数据流通产品 技术要求与测试方法	中国通信标准化协会
2020 年发布	基于联邦学习的数据流通产品 技术要求与测试方法	中国通信标准化协会
2020 年发布	基于可信执行环境的数据计算平台 技术要求与测试方法	中国通信标准化协会
2020 年发布	区块链辅助的隐私计算技术工具 技术要求与测试方法	中国通信标准化协会
2021 年发布	隐私计算 多方安全计算产品性能要求和测试方法	中国通信标准化协会
2021 年发布	隐私计算 联邦学习产品性能要求和测试方法	中国通信标准化协会
2021 年发布	隐私计算 多方安全计算产品安全要求与测试方法	中国通信标准化协会
2021 年发布	隐私计算 联邦学习产品安全要求与测试方法	中国通信标准化协会
2021 年发布	隐私计算 跨平台互联互通 第 1 部分: 总体框架	中国通信标准化协会
2022 年立项	隐私计算 金融场景应用规范及测试方法	中国通信标准化协会
2022 年立项	隐私计算 可信执行环境产品性能要求和测试方法	中国通信标准化协会
2022 年立项	隐私计算 可信执行环境产品安全要求与测试方法	中国通信标准化协会

下文数据统计方法为：在知网专利数据库中检索专利，在企查查中检索软著，在 WOS 核心数据库中检索论文，并在检索结果中去除重复项后进行统计。其中使用的中文检索词分别为“多方安全计算”、“差分隐私”、“可信执行环境”、“同态加密、“联邦学习”、“零知识证明”、“区块链”，并使用中英文扩展检索海外专利，使用对应英文名

称检索论文。从专利、软著、论文三个维度对近五年的检索结果进行可视化展示，对应结果分别见图 B.1 至图 B.3[1]。

通过对检索结果的分析，有以下三个结论。首先，所有隐私计算技术的受关注程度在逐年上升。无论是专利、软著，还是 SCI 论文的数量，每年均呈现上升趋势，这与国内外各国政府重视数据隐私安全的调控政策一致。其次，不同隐私计算技术在专利、软著、论文三个维度上的分布存在显著差异。在专利方面，联邦学习、区块链、可信执行环境公开和授权的数量最多；在软著方面，联邦学习、多方安全计算、区块链的转换成果最多；在论文方面，联邦学习、差分隐私、可信执行环境的发表和引用数量最多。最后，从三个维度综合来看，多方安全计算和区块链的技术基本成熟，联邦学习、差分隐私、可信执行环境的研究处于技术爬升期，其中联邦学习在专利、软著、论文各维度的数量最大并且增长速度最快。

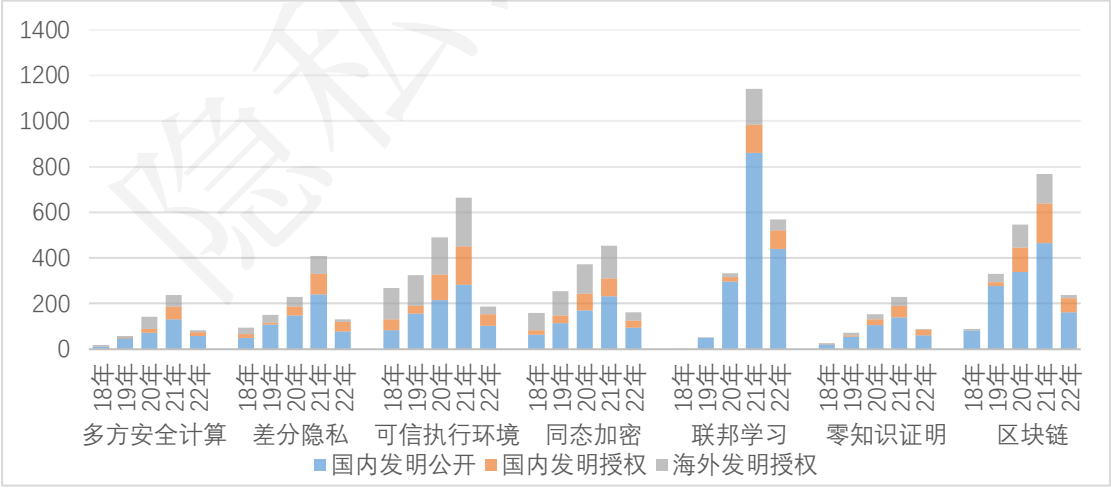


图 B.1 隐私计算近五年专利公开和授权数量

[1] 专利、软著、论文的检索截止时间为 2022 年 5 月 6 日，并非 2022 年全年。

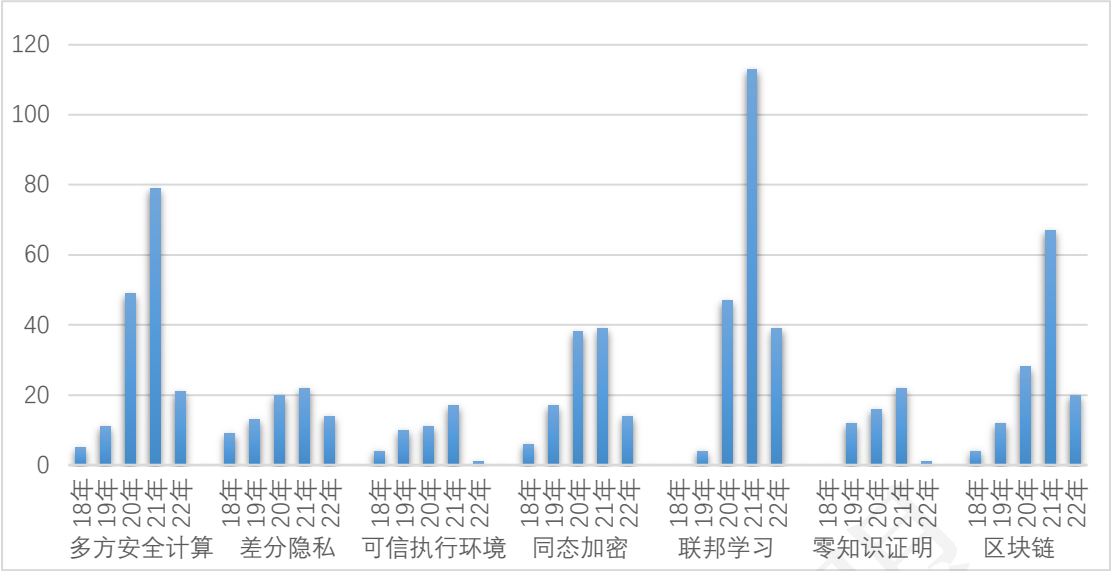


图 B.2 隐私计算近五年软著数量

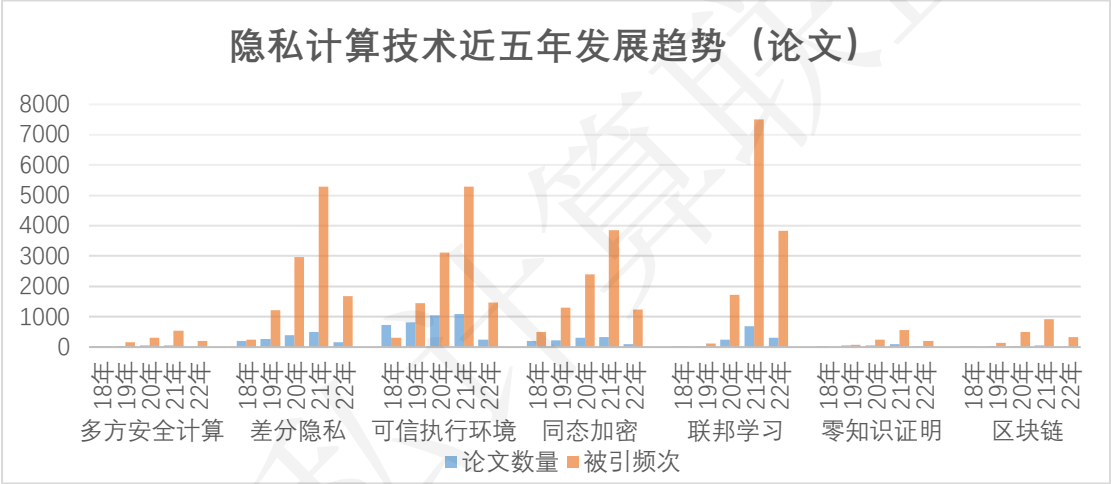


图 B.3 隐私计算近五年论文发表和被引数量

附录 C

国内主要隐私计算平台

以下为截至 2022 年 6 月依据中国通信标准化协会、隐私计算联盟的相关标准，通过中国信通院云大所“可信隐私计算评测”的技术产品，以通过测试时间为序。

表 C.1 国内主要隐私计算平台列表

序号	企业名称	产品名称	通过的测试	通过时间
1	蚂蚁区块链科技(上海)有限公司	蚂蚁链摩斯安全计算平台（MORSE）	多方安全计算 基础能力专项评测	2019.12
			多方安全计算 基础能力专项评测	2020.12
		蚂蚁链数据隐私服务	可信执行环境 基础能力专项评测	2020.12
		蚂蚁链摩斯安全计算平台	多方安全计算 基础能力专项评测	2022.6
			联邦学习 基础能力专项评测	2022.6
			多方安全计算 性能大规模专项评测	2022.6
			联邦学习 性能大规模专项评测	2022.6
2	腾讯云计算(北京）有限责任公司	腾讯神盾沙箱	多方安全计算 基础能力专项评测	2019.12
		腾讯云联邦学习应用平台软件	联邦学习 基础能力专项评测	2020.12
		腾讯神盾 Angel PowerFL 联邦计算平台	多方安全计算 基础能力专项评测	2020.12
			联邦学习 基础能力专项评测	2020.12
			多方安全计算 性能专项评测	2021.6
			联邦学习 性能专项评测	2021.6
3	华控清交信息科技（北京）有限公司	华控清交多方安全计算平台	多方安全计算 基础能力专项评测	2019.12
		清交 PrivPy 多方计算平台	联邦学习 基础能力专项评测	2020.12
			多方安全计算 性能专项评测	2021.6
			联邦学习 性能专项评测	2021.6
4	北京百度网讯科技有限公司	百度点石	多方安全计算 基础能力专项评测	2019.12
		联邦计算平台	多方安全计算 基础能力专项评测	2020.6
		百度智能云度信金融安全计算平台	多方安全计算 基础能力专项评测	2020.6

序号	企业名称	产品名称	通过的测试	通过时间
		点石安全计算平台（MesaTEE）	可信执行环境 基础能力专项评测	2021.6
		点石联邦学习平台	联邦学习 基础能力专项评测	2021.12
		百度点石联邦学习平台	联邦学习 性能大规模专项评测	2022.6
			多方安全计算 安全专项评测	2022.6
			联邦学习 安全专项评测	2022.6
			隐私计算 金融场景专项评测	2022.6
5	上海富数科技有限公司	富数安全计算平台	多方安全计算 基础能力专项评测	2019.12
		阿凡达安全计算平台	多方安全计算 基础能力专项评测	2020.12
			联邦学习 基础能力专项评测	2020.12
			多方安全计算 性能专项评测	2021.6
			联邦学习 性能专项评测	2021.6
			联邦学习 安全专项评测	2021.12
6	杭州趣链科技有限公司	趣链联邦计算软件	多方安全计算 基础能力专项评测	2020.6
			区块链辅助隐私计算 基础能力专项评测	2021.6
			多方安全计算 性能专项评测	2021.6
			联邦学习 基础能力专项评测	2022.6
7	北京数牍科技有限公司	Tusita 多方安全隐私计算平台	多方安全计算 基础能力专项评测	2020.6
		Tusita 隐私计算平台	多方安全计算 基础能力专项评测	2022.6
			联邦学习 基础能力专项评测	2022.6
			多方安全计算 性能大规模专项评测	2022.6
			联邦学习 性能大规模专项评测	2022.6
8	同盾科技有限公司	同盾智邦学习平台	多方安全计算 基础能力专项评测	2020.6
		同盾智邦知识联邦平台	联邦学习 基础能力专项评测	2020.12
9	厦门渊亭信息科技有限公司	DataExa-Insight 人工智能中台系统	多方安全计算 基础能力专项评测	2020.6
			联邦学习 基础能力专项评测	2020.12
10	深圳市洞见智慧科技有限公司	洞见安全多方数据智能平台	多方安全计算 基础能力专项评测	2020.6
		洞见数智联邦平台（INSIGHTONE）	联邦学习 基础能力专项评测	2020.12
			多方安全计算 基础能力专项评测	2021.6
			区块链辅助隐私计算 基础能力专项评测	2021.6

序号	企业名称	产品名称	通过的测试	通过时间
			多方安全计算 性能专项评测	2021.6
			联邦学习 性能专项评测	2021.6
			多方安全计算 安全专项评测	2021.12
			联邦学习 安全专项评测	2021.12
			隐私计算 金融场景专项评测	2022.6
11	蚂蚁智信（杭州）信息技术有限公司	共享智能平台	多方安全计算 基础能力专项评测	2020.6
			可信执行环境 基础能力专项评测	2020.12
12	天翼电子商务有限公司	密流安全计算平台	多方安全计算 基础能力专项评测	2020.6
		CTFL 天翼联邦学习平台	联邦学习 基础能力专项评测	2020.12
		PrivTorrent 密流安全计算平台	可信执行环境 基础能力专项评测	2021.6
		大禹-天翼数据融通平台	区块链辅助隐私计算 基础能力专项评测	2021.6
13	北京融数联智科技有限公司	UPAI 安全计算平台	多方安全计算 基础能力专项评测	2020.6
		善数隐私计算平台	联邦学习 基础能力专项评测	2022.6
			区块链辅助隐私计算 基础能力专项评测	2022.6
14	蓝象智联（杭州）科技有限公司	GAIA·Edge	多方安全计算 基础能力专项评测	2020.12
		GAIA 隐私计算平台	联邦学习 安全专项评测	2021.12
15	深圳前海微众银行股份有限公司	联邦学习云服务平台	多方安全计算 基础能力专项评测	2020.12
			联邦学习 基础能力专项评测	2020.12
		多方大数据隐私计算平台 WeDPR-PPC	区块链辅助隐私计算 基础能力专项评测	2021.6
16	矩阵元技术(深圳)有限公司	矩阵元隐私计算服务系统	多方安全计算 基础能力专项评测	2020.12
		JUGO 隐私计算平台	多方安全计算 安全专项评测	2021.12
17	翼健（上海）信息科技有限公司	翼数坊 XDP 隐私安全计算平台	联邦学习 基础能力专项评测	2020.12
			可信执行环境 基础能力专项评测	2020.12
			多方安全计算 基础能力专项评测	2021.12
			多方安全计算 性能专项评测	2022.6
			联邦学习 性能专项评测	2022.6
18	京东云计算有限公司	京东智联云联邦学习平台	联邦学习 基础能力专项评测	2020.12
19		联邦模盒	联邦学习 基础能力专项评测	2020.12

序号	企业名称	产品名称	通过的测试	通过时间
	京东数科海益信息科技有限公司	万象+隐私计算平台	区块链辅助隐私计算 基础能力专项评测	2021.6
20	杭州锘崴信息科技有限公司	锘崴信联邦学习平台	联邦学习 基础能力专项评测	2020.12
			联邦学习 性能专项评测	2022.6
			联邦学习 安全专项评测	2022.6
		锘崴信隐私计算平台	可信执行环境 基础能力专项评测	2020.12
21	深圳前海新心数字科技有限公司	新心数述联邦学习平台	联邦学习 基础能力专项评测	2020.12
22	中国电信股份有限公司云计算分公司	天翼云诸葛 AI-联邦学习平台	联邦学习 基础能力专项评测	2020.12
23	光之树（北京）科技有限公司	云间联邦学习平台	联邦学习 基础能力专项评测	2020.12
24	神谱科技（上海）有限公司	神谱科技 Seceum 联邦学习系统	联邦学习 基础能力专项评测	2020.12
25	星环信息科技（上海）有限公司	星环联邦学习软件	联邦学习 基础能力专项评测	2020.12
26	北京冲量在线科技有限公司	冲量数据互联平台	可信执行环境 基础能力专项评测	2020.12
			区块链辅助隐私计算 基础能力专项评测	2021.6
			联邦学习 基础能力专项评测	2021.12
			隐私计算 金融场景专项评测	2022.6
27	上海隔镜信息科技有限公司	天禄多方安全计算平台	可信执行环境 基础能力专项评测	2020.12
28	华为云计算技术有限公司	可信智能计算服务 TICS	可信执行环境 基础能力专项评测	2020.12
			联邦学习 基础能力专项评测	2021.6
29	浙江天猫技术有限公司	DataTrust 阿里云隐私增强计算软件	多方安全计算 基础能力专项评测	2021.6
			联邦学习 基础能力专项评测	2021.6
			可信执行环境 基础能力专项评测	2021.6
			联邦学习 性能专项评测	2021.6
			多方安全计算 性能专项评测	2021.12
30	上海凯馨信息科技有限公司	凯馨多方安全计算平台	多方安全计算 基础能力专项评测	2021.6
31	深圳市云计算科技有限公司	ELF 隐私计算服务平台	多方安全计算 基础能力专项评测	2021.6
32	杭州金智塔科技有限公司	金智塔隐私计算平台	多方安全计算 基础能力专项评测	2021.6
			多方安全计算 性能专项评测	2021.12

序号	企业名称	产品名称	通过的测试	通过时间
			多方安全计算 安全专项评测	2022.6
33	南京三眼精灵信息技术有限公司	智力共享平台·数链	多方安全计算 基础能力专项评测	2021.6
		智力共享平台·知脑	联邦学习 基础能力专项评测	2021.12
34	北京瑞莱智慧科技有限公司	隐私保护机器学习平台 RealSecure	多方安全计算 基础能力专项评测	2021.6
			联邦学习 基础能力专项评测	2021.6
		RealSecure 隐私保护机器学习平台【简称 RSC】	多方安全计算 安全专项评测	2022.6
			联邦学习 安全专项评测	2022.6
35	联易融数字科技集团有限公司	蜂密隐私计算平台	多方安全计算 基础能力专项评测	2021.6
			区块链辅助隐私计算 基础能力专项评测	2021.6
		蜂隐联邦学习平台	联邦学习 基础能力专项评测	2021.6
36	医渡云（北京）技术有限公司	多方安全计算平台（YIDUMANDA）	多方安全计算 基础能力专项评测	2021.6
			联邦学习 基础能力专项评测	2021.6
37	苏州同济区块链研究院有限公司	梧桐隐私计算平台 WPC	多方安全计算 基础能力专项评测	2021.6
38	北京火山引擎科技有限公司	火山引擎隐私计算平台	联邦学习 基础能力专项评测	2021.6
		火山引擎 Jeddak 联邦学习平台	联邦学习 安全专项评测	2021.12
39	深圳致星科技有限公司(星云 Clustar)	星云隐私计算平台	联邦学习 基础能力专项评测	2021.6
			联邦学习 性能专项评测	2022.6
40	云从科技集团股份有限公司	云从隐私计算平台	联邦学习 基础能力专项评测	2021.6
41	北京九章云极科技有限公司	DataCanvas FL 联邦学习平台	联邦学习 基础能力专项评测	2021.6
42	天冕信息技术（深圳）有限公司	天冕联邦学习平台	联邦学习 基础能力专项评测	2021.6
43	度小满科技(北京)有限公司	貔貅隐私计算平台	联邦学习 基础能力专项评测	2021.6
44	北京神州泰岳智能数据技术有限公司	数联盈	联邦学习 基础能力专项评测	2021.6
45	中移系统集成有限公司(雄安产业研究院)	中移联邦计算服务平台	联邦学习 基础能力专项评测	2021.6
46	阿里云计算有限公司	阿里云机器学习 PAI	联邦学习 基础能力专项评测	2021.6

序号	企业名称	产品名称	通过的测试	通过时间
47	零幺宇宙（上海）科技有限公司	光笺可信执行环境	可信执行环境 基础能力专项评测	2021.6
48	西安纸贵互联网科技有限公司	纸数魔方-基于区块链的可信执行环境数据计算平台	可信执行环境 基础能力专项评测	2021.6
		纸数魔方-区块链辅助的隐私计算平台	区块链辅助隐私计算 基础能力专项评测	2021.12
49	光之树（杭州）科技有限公司	天机可信计算平台	可信执行环境 基础能力专项评测	2021.6
50	杭州安恒信息技术股份有限公司	安全岛数据共享访问控制系统 DAS-SMPC	区块链辅助隐私计算 基础能力专项评测	2021.6
		安全岛数据共享访问控制系统	可信执行环境 基础能力专项评测	2022.6
51	第四范式（北京）技术有限公司	云知隐私计算平台	多方安全计算 基础能力专项评测	2021.12
			可信执行环境 基础能力专项评测	2021.12
			联邦学习 基础能力专项评测	2021.12
52	上海光之树科技有限公司	隐私计算平台	多方安全计算 基础能力专项评测	2021.12
			区块链辅助隐私计算 基础能力专项评测	2021.12
			联邦学习 性能专项评测	2021.12
53	中移（苏州）软件技术有限公司	多方安全计算平台	多方安全计算 基础能力专项评测	2021.12
54	三未信安科技股份有限公司	多方安全计算数据安全平台	多方安全计算 基础能力专项评测	2021.12
55	中投国信（北京）科技发展有限公司	多方安全计算平台	多方安全计算 基础能力专项评测	2021.12
56	海智讯通（上海）智能科技有限公司	爱前台电商多方安全计算系统	多方安全计算 基础能力专项评测	2021.12
57	招商银行股份有限公司	慧点隐私计算平台	多方安全计算 基础能力专项评测	2021.12
			联邦学习 基础能力专项评测	2021.12
58	京东科技控股股份有限公司	京东万象+隐私计算开放平台	多方安全计算 基础能力专项评测	2021.12
			联邦学习 性能专项评测	2021.12
			可信执行环境 基础能力专项评测	2022.6
59	优刻得科技股份有限公司	安全屋安全多方计算产品	多方安全计算 基础能力专项评测	2021.12
60	北京熠智科技有限公司	典枢数据合作平台	可信执行环境 基础能力专项评测	2021.12
61	中国电子系统技术有限公司	CECloud 数据安全沙箱系统	可信执行环境 基础能力专项评测	2021.12

序号	企业名称	产品名称	通过的测试	通过时间
62	百融云创科技股份有限公司	百融 INDRA-隐私计算平台	联邦学习 基础能力专项评测	2021.12
63	亚信科技（中国）有限公司	亚信科技联邦学习平台 AISWare AI² FL	联邦学习 基础能力专项评测	2021.12
		亚信科技联邦学习平台 AISWare MPC	多方安全计算 基础能力专项评测	2022.6
64	北京三快在线科技有限公司	美团联邦学习平台	联邦学习 基础能力专项评测	2021.12
		美团隐私计算平台	多方安全计算 基础能力专项评测	2022.6
			联邦学习 安全专项评测	2022.6
65	联通（广东）产业互联网有限公司	密算魔方	联邦学习 基础能力专项评测	2021.12
66	福州数据技术研究院有限公司	SOLAR 数据共享平台	联邦学习 基础能力专项评测	2021.12
67	上海光简信息技术有限公司	信也联邦学习平台	联邦学习 基础能力专项评测	2021.12
68	中国电子科技网络信息安全有限公司	区块链联邦计算系统	联邦学习 基础能力专项评测	2021.12
69	华为技术有限公司	iMaster NAIE 联邦学习部署服务	联邦学习 基础能力专项评测	2021.12
70	上海游昆信息技术有限公司	Mob 联邦学习平台	联邦学习 基础能力专项评测	2021.12
71	杭州卷积云科技有限公司	卷积云联邦学习平台	联邦学习 基础能力专项评测	2021.12
72	上海零数科技有限公司	零数联邦学习平台	联邦学习 基础能力专项评测	2021.12
73	科大讯飞股份有限公司	图聆·抱朴联邦学习平台	联邦学习 基础能力专项评测	2021.12
74	中国人寿财产保险股份有限公司	天元数创平台	联邦学习 基础能力专项评测	2021.12
			多方安全计算 基础能力专项评测	2022.6
			多方安全计算 性能专项评测	2022.6
			联邦学习 性能专项评测	2022.6
75	杭州比智科技有限公司	奇点云联邦学习系统	联邦学习 基础能力专项评测	2021.12
76	上海浦东发展银行股份有限公司	波塞冬联邦学习产品	联邦学习 基础能力专项评测	2021.12
			联邦学习 性能专项评测	2022.6
			联邦学习 安全专项评测	2022.6
77	续科天下（北京）科技有限公司	与日数据隐私数据连接平台 yConnect	联邦学习 基础能力专项评测	2021.12

序号	企业名称	产品名称	通过的测试	通过时间
78	建信金融科技有限责任公司	数据安全计算平台	联邦学习 基础能力专项评测	2021.12
79	京信数据科技有限公司	京信数据安全可信计算平台	区块链辅助隐私计算 基础能力专项评测	2021.12
80	杭州医康慧联科技股份有限公司	Arya 隐私计算平台	区块链辅助隐私计算 基础能力专项评测	2021.12
81	奇安信科技集团股份有限公司	奇安信网神数据交易沙箱系统	区块链辅助隐私计算 基础能力专项评测	2021.12
82	深圳壹账通智能科技有限公司	加马区块链隐私计算协作平台	区块链辅助隐私计算 基础能力专项评测	2021.12
83	京东城市（北京）数字科技有限公司	联邦数字网关系统	联邦学习 性能专项评测	2021.12
84	蚂蚁金服（杭州）网络技术有限公司	蚂蚁隐私计算隐语平台	多方安全计算 安全专项评测	2021.12
			联邦学习 安全专项评测	2021.12
85	北京蚂蚁云金融信息服务有限公司	蚂蚁隐私计算隐语平台	多方安全计算 安全专项评测	2021.12
			联邦学习 安全专项评测	2021.12
86	腾讯云计算(北京)有限责任公司	腾讯云联邦学习应用平台（Angel PowerFL）	联邦学习 安全专项评测	2021.12
87	神州融安数字科技(北京)有限公司	融安隐私计算平台	多方安全计算 基础能力专项评测	2022.6
			联邦学习 基础能力专项评测	2022.6
			联邦学习 性能专项评测	2022.6
			多方安全计算 性能大规模专项评测	2022.6
			多方安全计算 安全专项评测	2022.6
			联邦学习 安全专项评测	2022.6
88	神州融安科技(北京)有限公司	融安隐私计算平台	多方安全计算 基础能力专项评测	2022.6
			联邦学习 基础能力专项评测	2022.6
89	杭州煜辰数智科技有限公司	“星际”安全多方联合计算平台	多方安全计算 基础能力专项评测	2022.6
90	联通数字科技有限公司	联通链隐私计算平台	多方安全计算 基础能力专项评测	2022.6
91	杭州萝卜智能技术有限公司	数密院隐私计算平台 [简称：Data phi]	多方安全计算 基础能力专项评测	2022.6
92	国广清科（北京）科技有限公司	青稞隐私计算平台	多方安全计算 基础能力专项评测	2022.6
			联邦学习 基础能力专项评测	2022.6
93	重庆大司空信息科技有限公司	建筑大数据平台	联邦学习 基础能力专项评测	2022.6

序号	企业名称	产品名称	通过的测试	通过时间
94	随行付支付有限公司	结行联邦学习平台	联邦学习 基础能力专项评测	2022.6
95	杭州半云科技有限公司	半云隐私计算平台	联邦学习 基础能力专项评测	2022.6
96	北京八分量信息科技有限公司	八分量隐私计算平台	联邦学习 基础能力专项评测	2022.6
97	国网智能电网研究院有限公司	“智数”电力隐私计算平台	联邦学习 基础能力专项评测	2022.6
			联邦学习 性能专项评测	2022.6
			联邦学习 安全专项评测	2022.6
98	北京众尖同屏数字科技有限公司	吉利数科联邦学习平台	联邦学习 基础能力专项评测	2022.6
99	银联商务股份有限公司	银联商务隐私计算平台	联邦学习 基础能力专项评测	2022.6
100	中国电信股份有限公司北京分公司	AI 智算平台	可信执行环境 基础能力专项评测	2022.6
101	武汉天喻信息产业股份有限公司	BluePPC-T	可信执行环境 基础能力专项评测	2022.6
102	北京国双科技有限公司	国双联邦计算系统	区块链辅助隐私计算 基础能力专项评测	2022.6

隐私计算联盟

隐私计算联盟

联系方式：

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

邮箱：jiaxuan@caict.ac.cn

网址：www.caict.ac.cn