**多源数据可信融合计算平台-任务书**

|  |  |
| --- | --- |
| **申请者姓名** | 余国先 |
| **所属机构** | 山东大学 |
| **提交日期** | 2024/04/01 |

**目录**

**1.项目概述**

1.1研究背景

1.2研究现状

1.3需求分析

1.4研究价值

**2.研究内容** 2.1隐私计算核心引擎  
 2.2管理工具  
 2.3应用组件  
 2.4应用验证

**3.研发计划**

**4.预期成果**  
**5.人力投入**

**1.项目概述**

**1.1研究背景**

自2019年党的第十九届四中全会首次将数据列为生产要素以来，我国数字经济蓬勃发展，已成为推动经济增长的核心引擎之一。数字经济在各个领域迅速展开，从电子商务到智能制造，从大数据分析到人工智能应用，无不受益于数据的赋能和数字技术的迅速发展。自从《数据二十条》政策发布以来，各行各业在数据要素交易方面进行了积极探索，公共数据授权运营也在各地陆续开展起来，应用场景已经逐步从单一数据源的开放共享、流转、增值服务，扩展到多源数据的融合计算，即分析、挖掘融合后的数据价值，例如通过融合银行、医院、药店、保险公司医保局等多方数据以支持贷款风控评估、疾病预测、个性化治疗、医疗资源优化、药品经济学分析等智能数据服务。然而，这一迅速发展伴随着众多数据隐私安全的潜在危险，数据安全事件频发引起了全球范围内对数据安全和个人信息保护的重视。隐私泄露、大数据杀熟、暴力催收等种种乱象也号召业界建立起安全合理有效的数据可信计算机制，其既要保证模型的隐私，也要保证数据的隐私，同时还要保证性能。

多源数据融合可以涌现更多的数据价值，更好地满足社会经济发展的需求；浪潮、山东区块链研究院、长安链、趣链、阿里、微众银行、上交所、贵交所等公司正在积极打造与推进基于区块链与隐私计算的多源数据融合的可信流通平台与生态。目前，山大地纬股份有限公司在数据要素领域主要聚焦于单条明细数据精准授权，缺少对于多源数据可信融合场景的支持，也是公司的短板。此外，北方大健康、建设银行等客户对于数据安全融合分析、挖掘的需求越来越强烈，业界也在开始可信数据空间相关的研发与推广；因此，建设与推广的数据要素交易与交付平台需要强化与补充批量数据计算与多源数据融合计算能力。

**1.2研究现状**

在大数据时代，仅凭单一数据源的数据进行分析和挖掘往往难以满足现实需求。多源数据融合可以挖掘更多的价值，更好地满足社会经济发展的需求。利用零知识证明、多方安全计算、同态加密、差分隐私、可信执行环境、联邦学习等核心隐私计算技术，实现多源数据可信融合计算相关技术，能够使隐私保护从以往单纯加解密转变为明密文可信计算的全新领域，同时也带动了相关领域的快速发展，可以更好地满足社会经济发展的需求。

为了综合集成上述隐私计算技术，目前工业界和学术界已经涌现出许多隐私计算框架，如FATE，TensorFlow Federated，FedML，Pysyft，Fedlearner，SecretFlow-SPU、CrypTen、Delta和Rosetta等，以满足不同领域和应用场景的需求。如表1所示，这些框架各自具有一定的优势和不足之处。

表1. 现有隐私计算框架

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序 号 | 框架 | 机构名称 | 深度学习框架 | 框架特性 | | | | | | | | | | | |
| 适用场景 | 数据挖掘能力 | 框架应用支撑 | | | | 场景支持能力 | | | 产品易用性 | | |
| 联合建模 | 联合查询 | 联合统计 | 联合预测 | 多方安全计算 | 联邦学习 | TEE | 文档易用性 | 配置易用性 | 开发易用性 |
| 1 | FATE | 微众银行 | Pytorch | 金融 | 一般 | √ | 不全 | √ | 不全 | √ | √ | 不支持 | √ | 较复杂 | 不易扩展 |
| 2 | TensorFlow Federated | 谷歌 | TensorFlow | 科研 | 一般 | √ | 不支持 | 不支持 | 不全 | √ | 仅横向联邦 | 不支持 | √ | √ | 未落地 |
| 3 | FedML | 南加州大学 | TensorFlow | 科研 | 一般 | √ | 不支持 | 不支持 | 不全 | 不支持 | √ | 不支持 | 较少 | √ | 未落地 |
| 4 | Pysyft | Open Mined | Pytorch | 物联网 | 不足 | √ | 不支持 | 不支持 | 不全 | √ | 仅横向联邦 | 不支持 | 较少 | √ | 未落地 |
| 5 | Fedlearner | 字节跳动 | PaddlePaddle | 电商领域 | 不足 | √ | 不支持 | √ | 不全 | √ | √ | 不支持 | 较少 | √ | 编译和运行复杂 |
| 6 | SecretFlow-SPU | 阿里巴巴 | Pytorch、TensorFlow、JAX | 通用 | 一般 | √ | PSI  PIR | √ | 不全 | √ | √ | 支持 | √ | 较复杂 | 编译和运行复杂 |
| 7 | CrypTen | Meta | Pytorch | 科研 | 不足 | √ | 不支持 | 不支持 | 不全 | √ | √ | 不支持 | 较少 | 较复杂 | 未落地 |
| 8 | Delta | / | Pytorch | 科研 | 不足 | √ | 不支持 | √ | 不全 | √ | 仅横向联邦 | 不支持 | √ | √ | 未落地 |
| 9 | Rosetta | 矩阵元 | Pytorch | 金融 | 不足 | √ | PSI | 不支持 | 不全 | √ | 仅横向联邦 | 不支持 | √ | √ | 较复杂 |

除了这些隐私计算框架，业界越来越多的研究院和公司，如浪潮、山东区块链研究院、长安链、趣链、阿里、微众银行、上交所、贵交所、洞见和华控清交等，正在积极打造与推进基于区块链与隐私计算的**多源数据融合可信流通平台与生态产品**（如表2所示），将隐私计算技术应用到实际生产中。以区块链技术为主体的山东区块链研究中心、长安链等致力于融合区块链与隐私计算能力，在保护隐私的前提下实现数据使用过程可信任、可追溯、公开透明，已落地转化为医疗健康全生态可信数据互联的“小通医链”（长安链）等实际产出。以构建数智平台为目的的洞见科技公司、华控清交致力于提供可信数据挖掘的平台应用，洞见科技公司的洞见数智联邦平台，华控清交与光大银行合作承建的多方数据安全计算平台，实现了多场景多数据下的联合分析决策。构建可信开源框架的微众银行、谷歌、蚂蚁集团等推出FATE、TensorFlow Federated、SecretFlow等框架，为后续隐私计算产品提供了大量借鉴指导，推动了隐私计算产业落地孵化。各大数交所，也开发相应软件平台并制定产业规则，如e正通app（上交所），数据交易规则体系（贵数所），为数据资产保护、数据交易等切实应用提供了有益经验。这些在多源数据融合计算中的探索与研究都在积极推进高效、安全的数据跨域可信流转，为数字经济主体与数据赋能的实施与发展添砖加瓦。

表2. 业界已有的数据融合计算应用实践

|  |  |  |
| --- | --- | --- |
| 企业单位 | 代表产品 | 技术实践与突出贡献 |
| 山东区块链研究院 | 医疗领域平台 | 利用多方安全计算、区块链技术保障数据安全，实现医疗数据的可信流转 |
| 长安链 | 小通医链 | 利用加密技术，在保障隐私前提下通过AI、区块链技术应用支撑疾病诊断与新药研发，造福于民 |
| 洞见科技公司 | 洞见数智联邦平台 | 首次将隐私计算与区块链技术相融合，实现多场景多数据下计算可信可链接 |
| 浪潮 | 浪潮云 | 已合作超240个政府部门，赋能千行百业助力数字化转型 |
| 华控清交 | 光大银行多方数据安全计算平台 | 已适用于联合营销、联合风控、统一授信和业务合规等诸多场景 |
| 微众银行 | FATE | 全球首个工业级联邦学习开源框架，功能全面 |
| 蚂蚁集团 | SecretFlow | 提供了隐私保护数据分析和机器学习统一框架 |
| 上交所 | e正通app | 多项隐私安全技术促进数据交易的安全合理可行 |
| 贵数所 | 数据交易规则体系 | 发布了全国首套数据交易规则体系，为数据交易的合法合规保驾护航 |

如表1和表2所示，现有隐私计算框架和隐私计算平台主要存在以下不足：

1）**无法满足对多样化需求和场景的灵活支持与高效应用**。当前平台大都侧重于以联合建模为主的应用场景，对其他业务场景尤其是联合预测场景支持不足。

2）**对模型的隐私安全保护不足**。当前平台以联合建模和联合查询为主，虽然在推动联邦学习领域（联合建模）的发展方面做出了显著贡献，其主要关注如何在多个数据拥有方之间共享模型的更新，而不直接共享数据本身，以此来保护数据隐私和安全，**但忽略了模型的隐私安全保护需求**。因此它们在模型和数据不出域情况（模型和数据均需要进行加密）下的联合计算场景中进行应用时具备较大的局限性。这种场景要求在确保数据和模型双方隐私保护的同时完成计算任务，其不仅需要保护数据所有方的隐私，避免数据在传输或处理过程中被泄露，同时也要确保模型所有方的知识产权得到保护，防止模型在预测过程中被复制或反向工程。

3）**无法实现模型的自动导入和动态装载。**当前平台普遍将模型硬编码到平台中，这样的编码方式一方面无法支持使用者将自己本地训练好的模型自动导入到平台中进行隐私保护，另一方面也无法支持使用者进行模型自定义开发，模型无法实现灵活可配置、动态可插拔。这既阻碍了平台的扩展性，也会导致模型的隐私存在一定程度的泄露风险。

4）**普遍缺少隐私计算脚本的个性化编写功能。**当前平台无法帮助使用者通过简单易用的描述语言编写完整的、适应个性化业务场景的任务需求，因此降低了平台的易用性。此外，大部分平台在实现业务需求时，会将业务模型分发到所有节点进行执行，导致业务逻辑存在泄露的风险。

5）**缺乏异构数据的接入方式。**当前平台不能有效地实现不同类型的多源异构数据的接入，难以适应项目的实际需求。

为了解决上述痛点，项目拟研发一套支持多种数据和模型隐私保护策略以及多样化场景下的数据分析与挖掘的数据可信融合**计算核心引擎**，一套多源数据接入、部署运维和系统状态监测的**管理工具**，一套支持多机构进行联合预测、联合统计、联合查询和联合建模的**平台应用组件库**，从而实现多源数据可信融合计算具体功能。

**1.3 需求分析**

目前，山大地纬股份有限公司在数据要素领域主要聚焦于单一数据源的开放(即单条明细数据精准授权)，缺少对于多源数据可信融合场景的支持，从而无法满足多源数据融合计算场景中经常涉及到的联合预测、联合统计、联合查询和联合建模的计算需求(如表3)。

表3. 多源数据可信融合的常用计算需求

|  |  |  |  |
| --- | --- | --- | --- |
|  | 简介 | 支撑能力 | 应用场景 |
| 联合预测 | 只占有模型部分的多个参与方联合进行预测；数据拥有方和模型拥有方联合进行预测 | 能够在保证多方数据和模型安全的基础上完成分析预测任务 | 多个金融机构可以联合进行欺诈检测预测；银行和客户进行风控系数预估；药店和用户进行电子处方询价 |
| 联合统计 | 对不同数据集共同统计，以解决单个机构因样本不足、分布不均而难以可信融合计算问题 | 能够在可信融合计算中承担前期的样本统计分析与特征统计分析任务 | 联合多家保险机构的客户数据，统计分析客户需求、行为和喜好，实现个性化保险产品的制定；广告平台和广告商联合统计分析广告活动的点击率、转化率和受众行为，改进广告投放策略 |
| 联合查询 | 多方数据隐私求交和融合，支持广泛的数据集内容和数据集规模 | 能够支持用户在保证检索条件和返回结果的隐私性基础上完成隐私数据的检索功能 | 银行、投资公司和金融监管机构可以通过联合查询数据以检测金融犯罪，例如欺诈、洗钱和市场操纵，同时确保客户的隐私不受侵犯 |
| 联合建模 | 联合多源数据机构扩展样本数量及丰富特征程度以训练更好的模型 | 能够在不泄露原始数据等敏感信息的情况下完成数据和模型的计算与更新 | 联合多家医院的就医数据进行DRGs模型训练，实现医保精准控费；联合多家银行的交易数据进行欺诈交易识别模型训练，有效规避欺诈风险 |

更进一步而言，北方大健康、建设银行等客户对于多源数据融合分析与挖掘的需求越来越强烈，包括多种场景下的多源数据可信融合计算需求，例如**基于区块链和普惠金融的银行贷款风控场景**，**基于DRGs的医保精准控费场景，药品经济学分析场景，保险产品制定场景和电子处方询价场景**。

在基于区块链和普惠金融的银行贷款风控场景中，平台需求包括用户隐私**数据**和银行风控**模型不可见**下的风控系数和贷款金额预测，即在**同时保护数据和模型隐私**的条件下完成**联合预测**任务，并通过**区块链**保证数据结果正确性。因此，平台需要支持针对资产数据和风控模型的数据加密解密及密态计算算法，并提供接入区块链解决方案，以支撑该场景的计算和隐私保护需求。

在药品经济学分析场景中，平台需求包括在保障多源异质的医疗机构病患数据隐私前提下，帮助医药企业获得药品市场需求，以指导新药的研发。因此平台需要适配多重异构场景，提供**多源数据接入功能**，并基于隐私计算技术，实现多样化的**联合查询**功能，以确保病患的敏感信息得到充分保护。

在保险产品制定场景中，平台需求包括协助保险机构联合政府的人社医保的数据统计信息来指导保险产品的制定，同时确保保险机构用户数据信息的隐私安全。因此，平台将提供差分隐私的**联合统计算法**和**数据匿名化处理技术**，确保政府的人社医保数据和保险机构的客户敏感信息得到高度隐私保护。

在电子处方询价场景中，平台需求包括在保护用户和药店数据安全和处方询价模型不可见情况下，即在**保证数据和模型信息安全**的情况下完成**联合计算**任务，并提供**较高并发的服务能力**。因此，平台提供对模型和数据的加密解密及密态计算算法，并将密态处方询价模型部署在多个分布式节点，使得平台在提供较高并发联合预测服务的同时保证了信息和模型的安全。

在基于DRGs的医保精准控费场景中，医院需要面对多样化的需求场景，因此需要便捷的需求转化方法，即**易用的隐私计算脚本**，以简化业务人员的使用和开发流程；与此同时，平台接入来自不同医院的多种数据来源，并调度数据完成可信融合计算任务，需要对于不同数据类型**的多源数据接入能力**和**任务调度能力**支撑。在具体的业务流程中，平台通过**数据可信融合计算引擎**的支持，达到包括数据隐私保护，不同医院业务差异的处理，以及模型精准度的平衡的业务需求。确保患者的隐私得到有效保护，同时在不同医院的业务差异中实现**联合建模**模型的灵活性，平衡精准度以保证医疗水平和医保经费的有效管理。

为满足上述多样化场景的需求，本项目旨在建设一个多源数据可信融合计算平台，其建设内容主要包含:一套支持易用隐私计算脚本、任务调度和数据密态计算的多源数据可信融合**计算核心引擎**，一套支持多源数据接入、部署运维和系统状态监测的**管理工具**和一套支持多机构进行联合预测、联合统计、联合查询和联合建模的**平台应用组件库**。平台根据信通院的功能、安全、性能等标准进行开发，具备能够通过检测的能力。

**1.4研究价值**

目前，业界已开始可信数据空间相关的研发与推广，多源数据可信融合计算是建设可信数据空间的重要一环，并且公司建设与推广的数据要素交易与交付平台需要强化与补充批量数据计算与多源数据融合计算能力。因此，本项目拟申请立项“多源数据可信融合计算平台”，支持融合社保、医保、公积金、医院、药店等数据源，并提供联合预测、联合统计、联合查询和联合建模等能力，支撑模型和数据不出域场景下的联合计算，依次推动更多的企业、机构等数据提供方，数据使用方和模型拥有方入场。建设的平台内置多种隐私计算与隐私保护算法组件与策略，支持开发更多融合增值数据产品，释放多元数据的融合倍增价值，并在银行风控、住房服务、医疗健康、金融科技、商业保险等场景进行应用验证与推广，提升山大地纬在公共数据授权运营和数据要素市场领域的核心竞争力。 **2.研究内容**  
 本项目期望构建一个综合性的多源数据可信融合计算平台，重点针对医保精准控费场景，药品经济学分析场景和保险产品制定场景等隐私计算场景，建设一套包括隐私计算脚本、任务调度和数据密态计算功能在内的**隐私计算核心引擎**与一套包括部署管理、多源数据接入和平台运维在内的**平台管理工具**以支撑包括联合预测、联合统计、联合查询和联合建模等多源数据分析和挖掘需求的**平台应用组件库**。该平台能够支撑包括政府、医疗、金融和保险等多类机构进行不同场景下的数据可信融合和可信计算（如图1）。

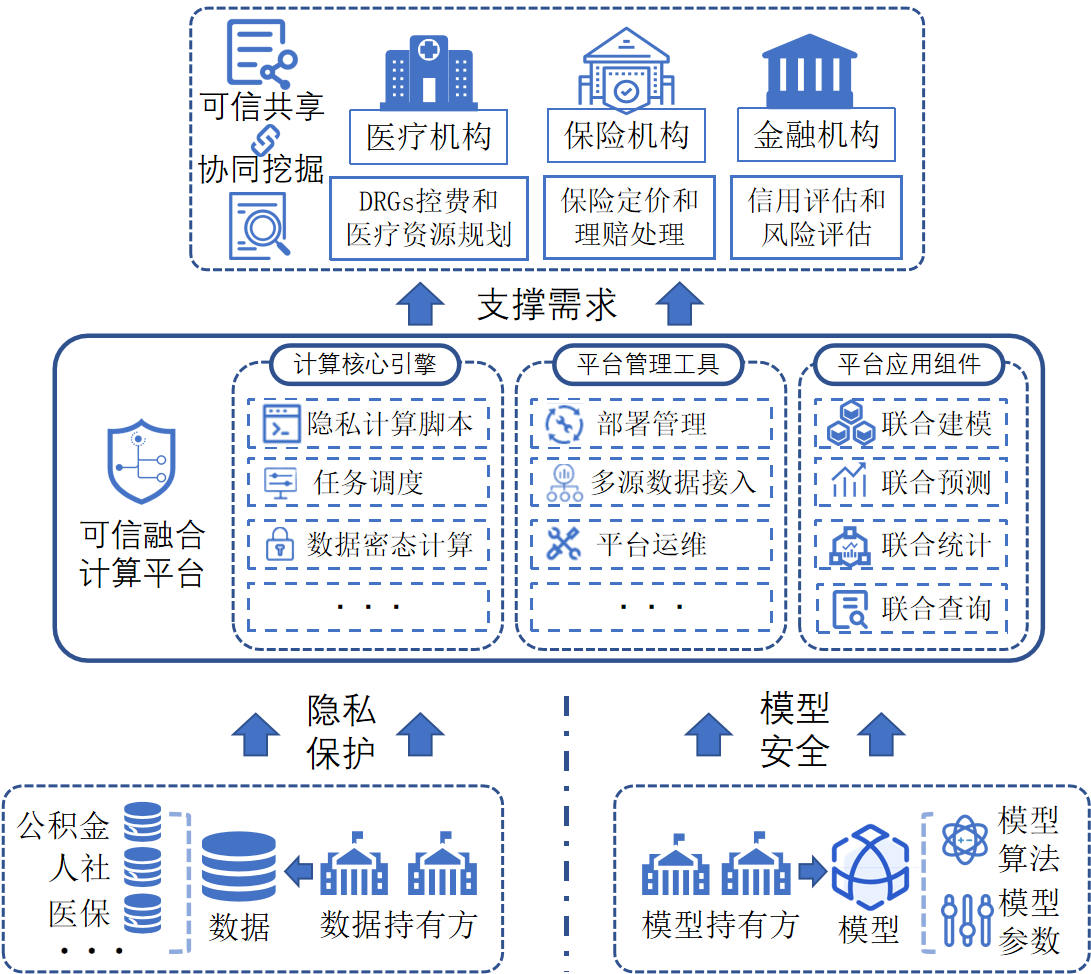


图1. 多源数据可信融合计算平台

**2.1 隐私计算核心引擎**

多源数据可信融合计算平台的隐私计算核心引擎由隐私计算脚本、任务调度和密态计算三个模块共同组成，包括计算代码的编译、执行，计算任务的调度、通信，计算能力的算子、算法和模型设计，这三个模块的共同协作支撑了平台的计算需求。下面我们将详细介绍这三个模块。

2.1.1 隐私计算脚本

隐私计算脚本用于将任务发布者的需求转换为平台可以理解和执行的指令，然后通过全局调度器，调度各节点的密态计算模块协同完成隐私保护的联合计算任务，提升平台易用性。

如图2所示，隐私计算脚本将具备如下能力：

首先，支持用户通过类SQL语言和类高级编程语言（兼容Python和JAVA）混合编写隐私计算脚本，用户可以通过混合使用类SQL语言和类高级编程语言编写多行脚本代码，以实现完整的、复杂的任务需求描述。例如，用户可以通过类SQL语言实现多参与方进行联合查询的需求描述，然后通过类高级编程语言编写自定义计算逻辑实现使用联合查询结果进行后续任务的需求描述。

然后，隐私计算脚本可以被平台解析、编译成平台可以理解、执行的工作流，工作流由多个任务组成，代表一个完整的任务需求集合。工作流包含每个任务的执行节点、执行顺序以及执行优先级，可由全局调度器进行调度执行。

为实现隐私计算脚本的定义、解析、编译功能，我们将预定义一系列映射规则，映射规则描述了类SQL和类高级编程语言与平台可理解代码的对应关系，然后通过设计解析器将平台可理解代码编译成可被调度的工作流，最后，由全局调度器根据工作流的执行信息将具体任务分发到相应执行节点进行任务调度执行。此外，平台还将为代码或者模型提供一定的缓存能力，在频繁的任务调度中，优化代码分发和执行速度，以充分发挥系统性能。

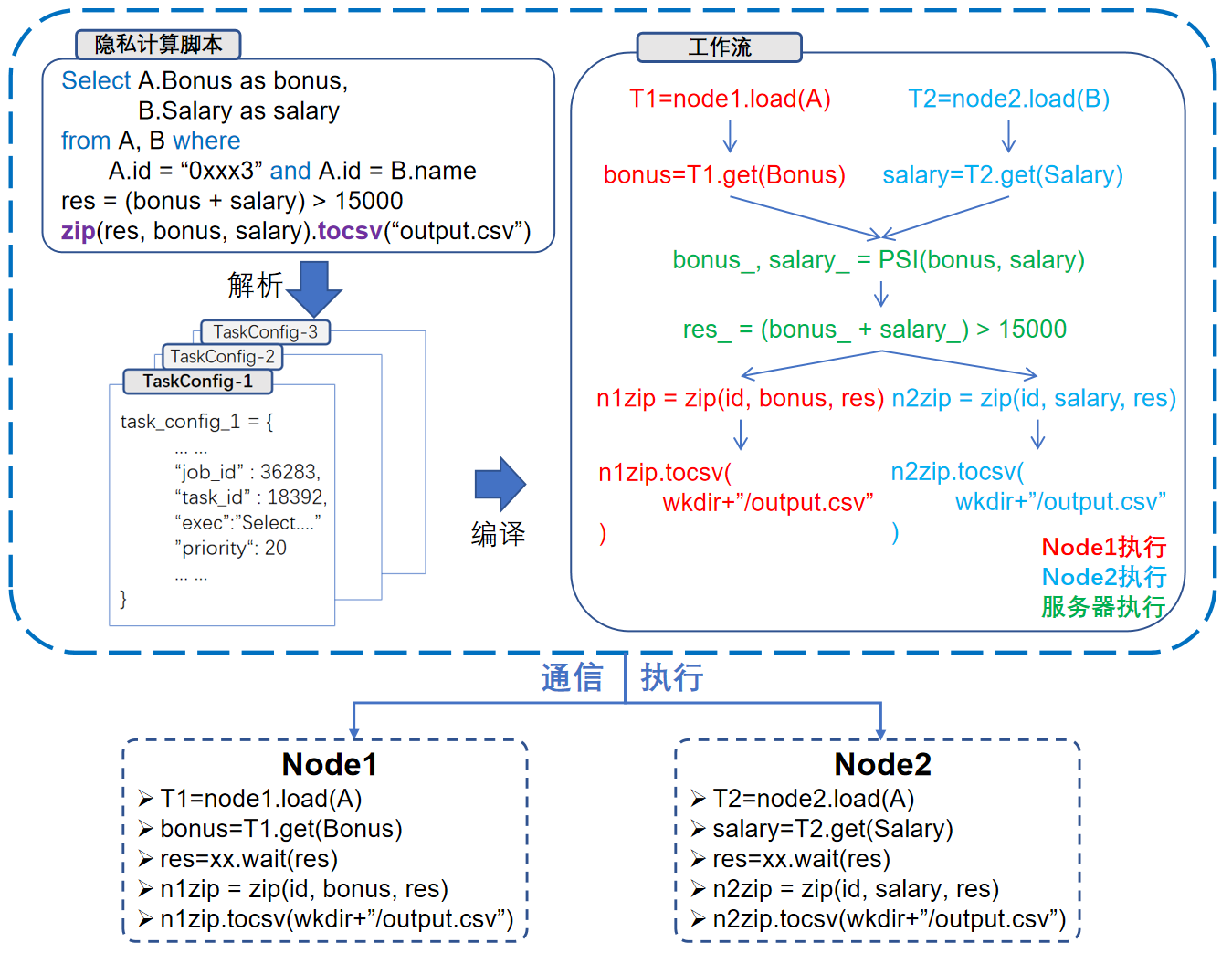


图2. 隐私计算脚本功能示意图

2.1.2 任务调度

如图3所示，任务调度是指平台能够根据隐私计算脚本编译后形成的工作流，调度多方参与者联合完成隐私计算任务，由调度器实现，包括全局和本地调度两种功能，从而提高平台执行效率和执行作业吞吐量。

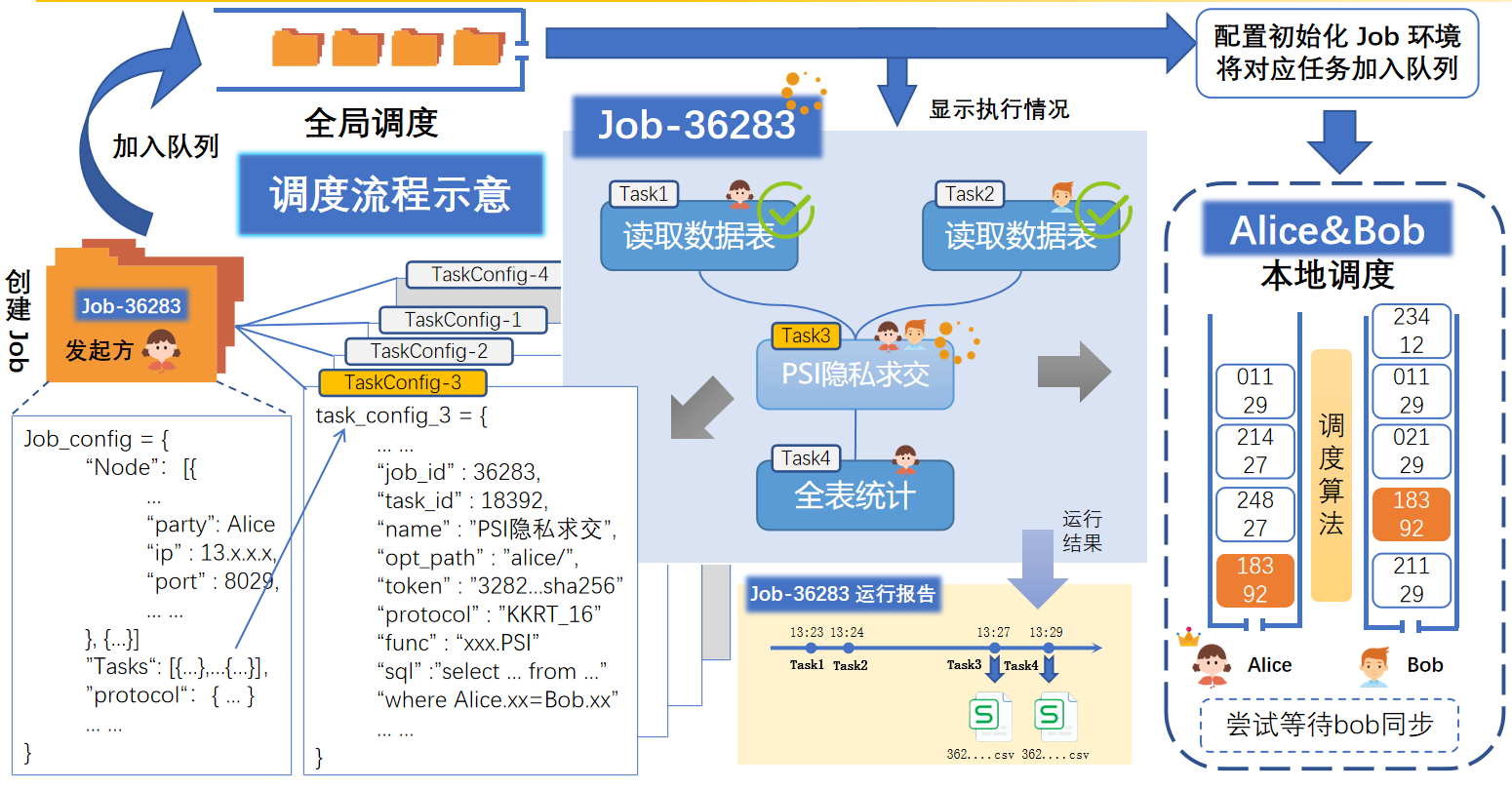


图3. 任务调度功能示意图

**全局调度：**全局调度能够将工作流分解成多项子任务并对应到具体参与方，协调各参与方有序地完成隐私计算任务的协作执行。在平台中，一次完整的隐私计算活动可以被解析为一个工作流（Job），可以由有向无环图（DAG）表示，其中节点代表工作流中不可分割的最小计算单元（称为**任务**，即Task），有向边代表调度的拓扑先后顺序。如图4所示，Job包含了一次隐私计算活动的所有基本信息和链接索引，详细包含**参与数据节点配置**、**任务执行顺序**、**采取的数据加密协议**、**通信的协议规范**、**项目优先级**等具体内容；Task包含了每一计算的具体逻辑和参数，可以表示联合预测、联合统计、联合查询和联合建模等多项细分功能。我们将基于标准的通信框架进行全局调度逻辑的设计实现，并支持任务的启停和状态同步。在中心化部署模式中，全局调度器位于中心服务器（如山大地纬公司），在去中心化部署模式中，每个任务参与方的调度器都具有全局调度功能。

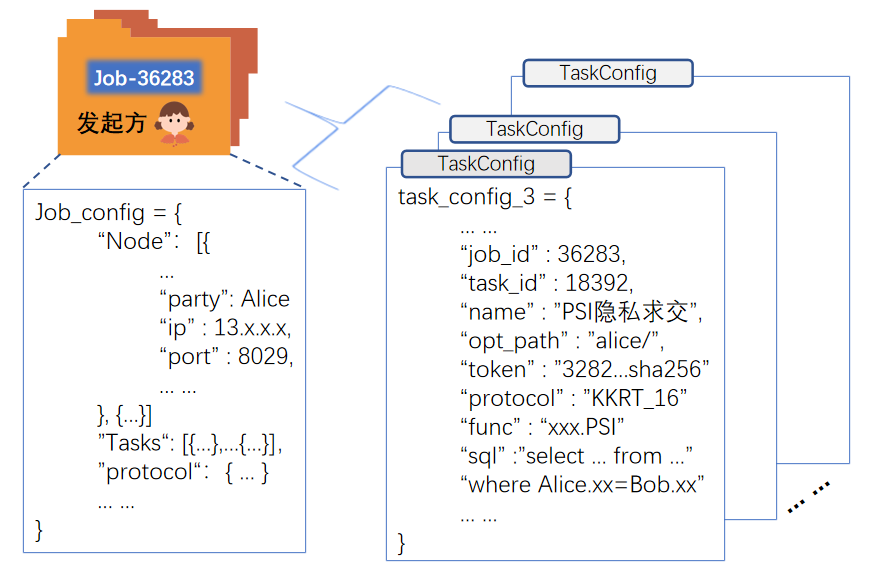


图4. 一次隐私计算活动的工作流和子任务示意图

**本地调度：**本地调度功能能够调度参与方本地的计算资源，并支持多实例集群化部署，以提高平台性能、可用性和可扩展性。具体来说，我们将通过Kubernetes实现对资源和实例的调度，基于Kubernetes，本地调度能够按需为计算任务分配CPU和内存等计算资源，并实现多实例集群化部署，从而支持高并发请求。此外，本地调度还能够通过通信接口接收全局调度器发来的任务执行信息，并及时向全局调度器同步本地的任务执行状态。

**全局和本地调度功能将遵循标准规范进行实现，并预留好统一的标准接口，方便后续的开发与升级。**

2.1.3 密态计算

数据密态计算的目的是支撑可信融合计算功能需求，包括联合预测、联合统计、联合查询和联合建模等具体功能。现有开源隐私计算框架如FATE和SecretFlow等能够支持多方安全计算、同态加密、差分隐私等多项隐私计算技术，并且能够支持跨源数据节点之间的隐私通信，但在自定义算法设计、模型自动导入、动态装载和模型隐私保护方面仍有所欠缺，且在联合预测等应用场景存在局限性。因此，我们借鉴了开源框架的设计理念，复用开源框架的隐私计算协议（如MPC和同态加密等协议），将上层模型代码编译为可执行的隐私计算代码逻辑，进而构建安全可信的数据隐私计算引擎。如图5所示，该引擎包含基础算法层、算子层、算法层和模型层，以构建数据隐私计算应用服务：

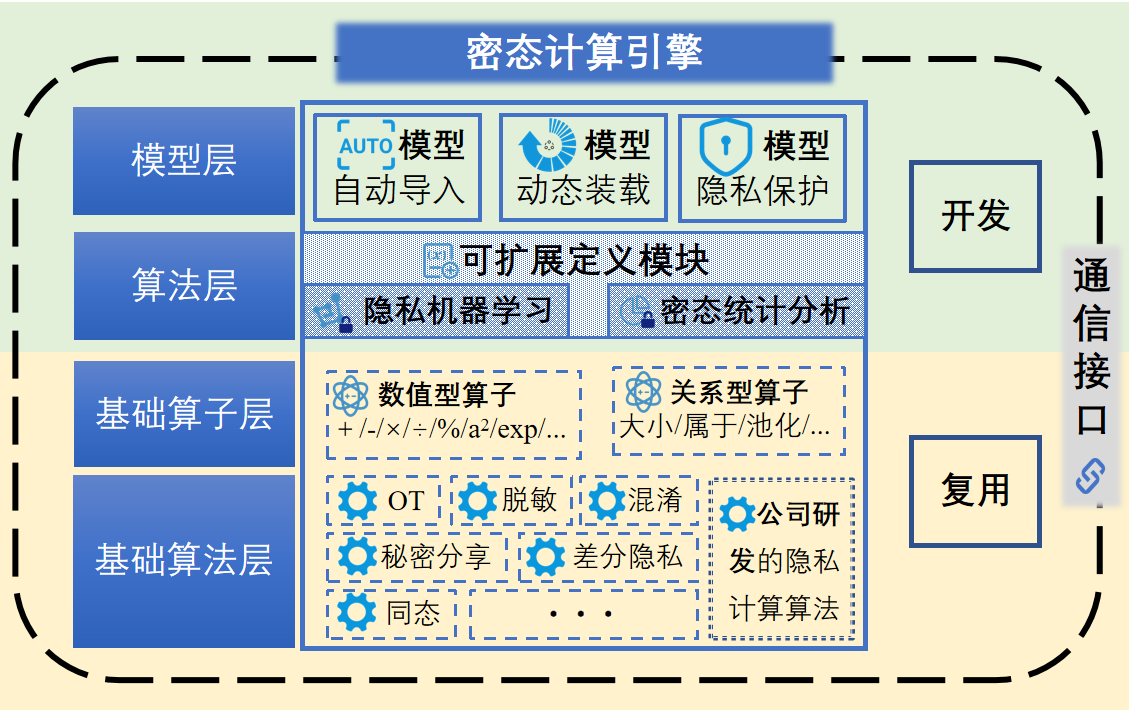


图5. 密态计算引擎示意图

**基础算法层（复用）**：隐私计算的基础是密码学的众多算法，根据算法类别又分为同态加密、秘密分享、不经意传输、差分隐私、数据混淆与数据脱敏等诸多类别。这些基础算法基于国标实现。此外，基础算法层设计了统一的接口和调用模式，可与地纬公司已有的基础算法进行融合，并方便未来密码学算法的更新、替换与使用。

**基础算子层（复用）**：基础算子层由基础算法层构建而来，实现隐私计算的基本运算功能，这些基础算子可分为数字型算子与关系型算子。数字型算子包括加、减、乘、除、开方、指数、幂等运算，而关系型算子包括大小比较、从属关系判断、池化等关系运算。为实现基础算子层，我们将参考主流的开源框架，复用开源框架提供的MPC协议（如基于三方的ABY3、Semi2k，基于两方的Cheetah）、同态加密协议（如Okamoto-Uchiyama，Paillier，Elgamal）、差分隐私协议（Local DP）等主流隐私计算协议来实现基础算子，在复用这些协议的时候，我们将确保这些协议以模块化的方式封装在底层，为上层的算法模型提供隐私计算支持，在需要更新升级时，可以方便地被**拆解**和**替换**。

**算法层（开发）:**为了实现隐私计算的应用需求，平台提供了包括**隐私机器学习**和**密态统计分析**在内的通用算法，如表4所示。具体而言，我们将基于基础算子层提供的多种隐私计算协议，实现通用的隐私机器学习和密态统计分析算法，为此，我们设计了统一规范的数据和参数格式便于算法的**级联**和**复用。**这些算法将部署在所有参与节点上，以支持不同业务模型的实现，从而满足各种应用场景下的数据分析和挖掘需求。

除此之外，我们还提供了**可扩展定义模块**，通过设计实现算法的基础API，为算法开发者提供插件化的开发方式。任务发布方可以基于这些API开发满足特定需求的个性化隐私计算算法。通过算法层算法的组合搭配，隐私计算引擎能够支持不同业务模型的构建，满足如银行贷款风控、药品经济学分析、保险产品制定、电子处方询价和医保精准控费等诸多现实场景的应用需求。

表4. 平台集成的通用基础算法

|  |  |
| --- | --- |
| **隐私机器学习** | **密态统计分析** |
| 决策树 | 分箱统计 |
| 逻辑回归 | 时序分析 |
| 主成分分析 | 全表统计 |
| 聚类 | 数据降维 |
| 神经网络 | 回归分析、方差分析 |
| 支撑向量机 | 隐私求交、匿名信息检索 |
| ... | ... |

**模型层（开发）：**在模型层，我们将设计实现模型的**自动导入**、**动态装载**和**隐私保护**三种功能。具体来说，模型的自动导入功能支持使用者将本地训练好的模型转换为密态形式导入到密态计算引擎中，引擎可以为使用者的本地模型提供隐私保护功能，确保模型在与外部参与方进行联合计算时信息不被泄露；模型的动态装载功能为使用者提供模型自定义模块和模型载入接口，支持使用者利用密态计算引擎提供的通用算法和可扩展自定义算法来构建自定义的模型，构建好的模型可以动态地装入本地平台中，而无需更新其他参与节点的平台代码，从而实现了模型的灵活可配置、动态可插拔。此外，因为其他节点无需具有模型完整代码，模型隐私也因此得到了保护。最后，我们通过将模型解耦为多个算法的组合，确保除模型的拥有者外，模型的算法和参数隐私不会泄露给其他参与节点，进一步保护了模型隐私。

**通信接口设计**：我们将为密态计算引擎之间的加密数据通信设计通信接口。接口将基于符合信通院标准的通信协议进行设计，可以为不同形态的密态计算引擎间互相通信提供支持。对于节点与节点间的通信服务，我们将采用国密通信算法实现对链路的加密（如DH密钥交换算法），并支持链路两端的发起方和接收方互相进行身份认证。此外，通信接口中还将预留密态计算引擎与**大纬链**结合的接口，基于该接口，隐私计算节点可以将计算过程的关键信息摘要哈希上链，包含数据模型的元信息（如明密属性、隶属关系等）、关键参数、计算结果等内容，以确保数据、结果、中间交付的存证与授权。通信接口的功能如图6所示。

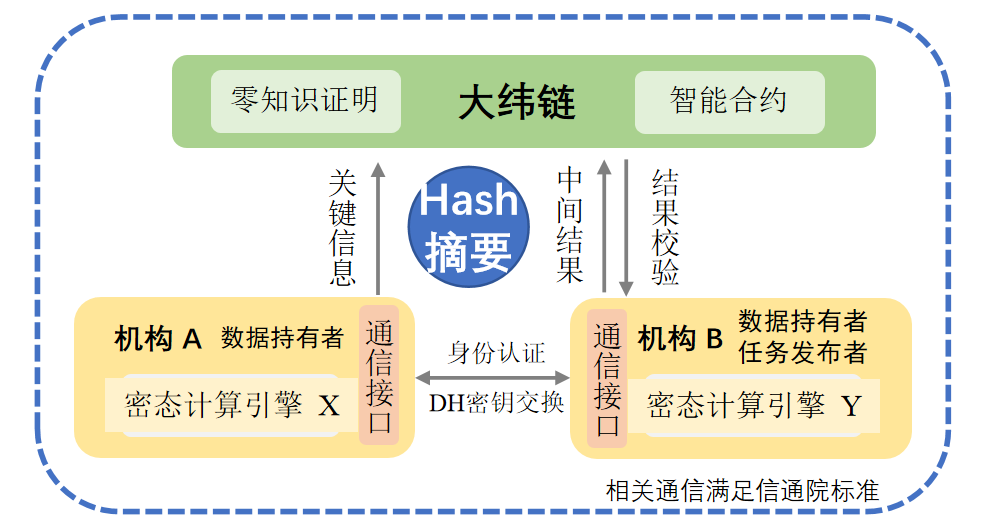
****

图6. 通信接口功能示意图

**2.2管理工具**

2.2.1运维工具

平台提供基于终端的运维操作工具，通过对于容器的编排和管理等能力，实现对于节点和作业的运维管理以及对于硬件等状态的监控。运维工具通过提供便捷的运维控制指令，为运维人员提供了易用的使用方式。

运维操作工具提供易用的终端系统状态监控组件，能够实现对于不同节点的资源状态和节点使用情况的监控。系统监控工具能够将系统的运行情况和节点的设备状态、资源状态及时地反映出来，业务人员和运维人员可以通过系统监测工具实时监控多源数据可信融合计算平台的运行情况，从而实时对平台运行进行调整。

运维工具能够实现对于全局调度和本地调度的控制。在全局维度而言，实现的功能包括如下：

1）实现节点的注册、停用，注销等能力。能够把业务机构注册为对应的多源数据融合计算节点，从而便捷的使业务机构承担任务发布者或者任务参与者的身份，并提供对应的管理功能。

2）实现任务的启停、任务状态的查看、同步等能力。能够控制任务整体的运行过程，可以通过提高部分任务的优先级，使某些任务更先执行，也可以对任务的执行状态进行管理。

3）对调度策略的控制和管理能力。能够选择任务的全局分发和执行策略，从而更好的调度系统执行任务。

在本地维度而言，实现的功能如下：

1）实现对数据元信息的管理。通过设定数据元信息，控制了节点对外暴露的信息标签和信息量，从而能够在计算节点达成一致的情况下，更好的开展计算任务。

2）实现对于本地计算资源的管理，能够控制当前节点的计算资源，实现更好的资源-效率均衡。

3）实现节点本地调度策略管理，调控任务在单节点上的运行状态和运行优先逻辑。

2.2.2部署管理

1）部署架构

在部署过程中，平台为各个参与方提供统一的接入接口，各个参与方被视为平台的隐私计算节点，可以担任不同的角色包括任务发布者和任务参与者，一般而言，任务发布者为数据需求方，任务参与者为数据提供方，值得注意的是，数据需求方也可以作为任务参与者提供数据参与隐私计算。

如图7和图8所示，平台提供**中心化**和**去中心化**两种部署方式，并采用**异步消息触发**的方式进行任务执行。

在中心化部署模式下，中心服务器作为多源可信融合计算服务的中心节点，部署在平台服务提供方（如山大地纬公司）内部，便于对总体服务进行监控和调整。每个多源数据融合计算节点可以担任任务发布者或者任务参与者的角色，部署在参与计算的业务机构内，实现联合计算功能。任务发布者通过编写平台支持的隐私计算脚本将自己的任务需求转换为平台可执行的指令逻辑，经由部署在中心服务器上的全局调度器调度参与者执行任务，并最终从平台获得可信计算结果。中心服务器提供全局任务分发、调度与管理等功能，通过为各任务参与节点分派任务、确定执行顺序、同步任务状态等操作实现任务的高效执行。

在去中心化部署模式下，平台中没有中心服务器，隐私计算节点均部署在各参与机构本地，且均具有需求转换、全局和本地任务调度功能，任一参与机构都可以作为任务发布者通过隐私计算脚本编写自己的任务需求并转换为平台可执行的指令逻辑，然后全局调度其他参与者进行任务执行。

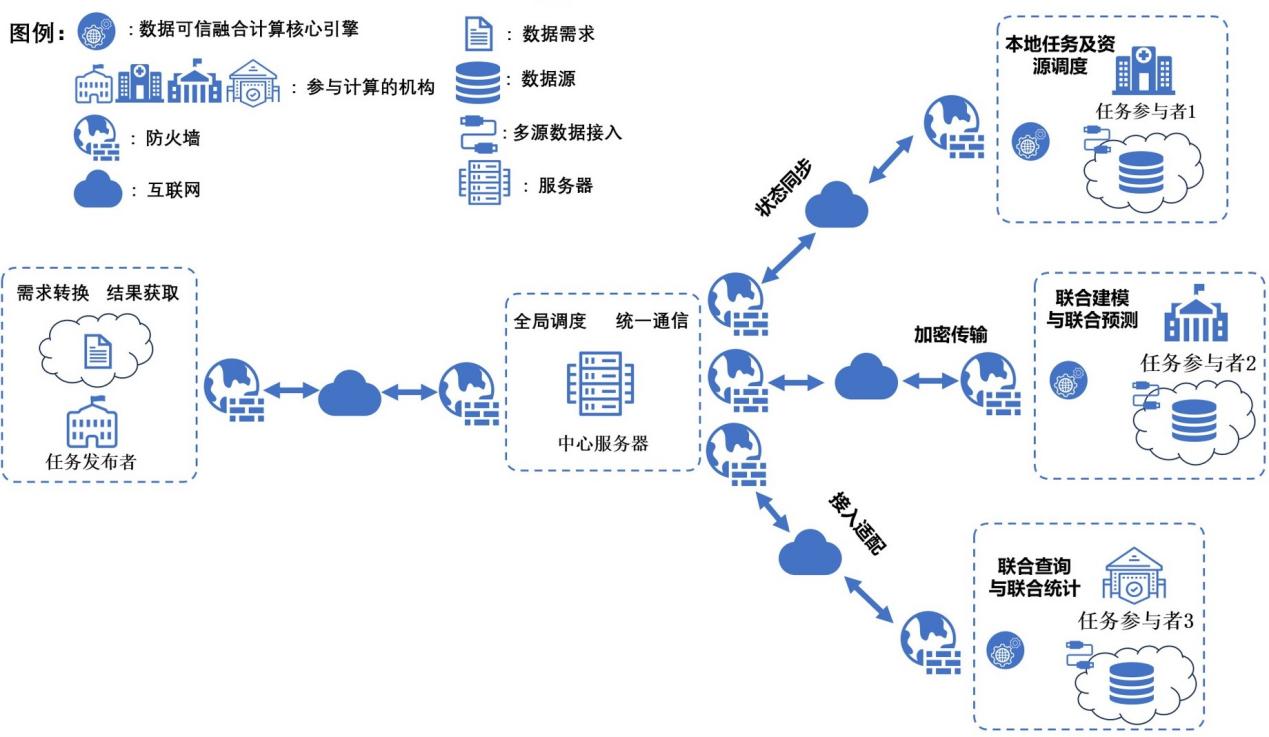


图7. 中心化部署架构图

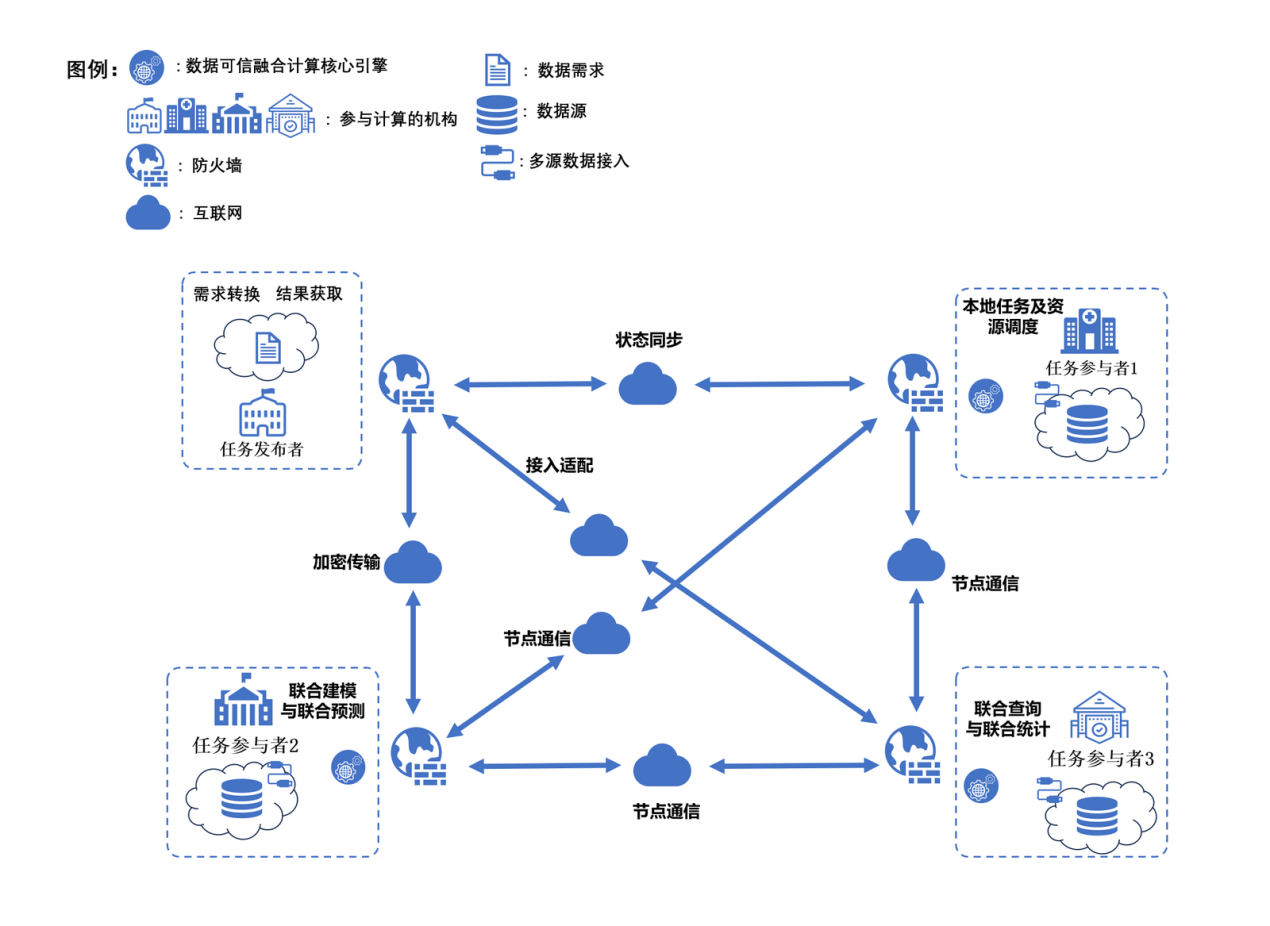


图8. 去中心化部署架构图

2）部署工具

项目将开发一套完整的部署管理工具管理隐私计算节点和集群，能够以简单的流程完成上述部署架构和部署流程中的隐私计算节点的部署。从而实现任务参与者或任务发布者角色的注册，高效完成多源数据可信融合计算任务。

具体的部署过程如下：

中心化部署：平台通过组建中心组网的方式实现中心化部署任务，中心节点作为组网中心，需要被首先部署。具体而言，使用部署工具执行给定的部署脚本程序，并启动中心节点，从而在给定的端口上提供节点接入服务，并生成相应的公钥私钥和证书。然后是部署本地节点，本地节点的部署采用基于token认证的方式注册到中心节点，以加入到组网中。此外，本地节点还需要与其他参与任务的隐私计算节点互相授权，以确保任务参与方的真实可信。

去中心化部署：平台通过组建点对点组网的方式实现去中心化部署任务。在该组网中，每个节点是平等的，拥有独立的需求转换、全局和本地任务调度功能。在执行部署脚本后，每个节点都会生成各自的公钥私钥和证书，在任意两个节点之间建立通信前，需要先互相颁发证书并配置授权，以确保互相的真实可信。然后，互相认证后的节点间可以进行任务的协作执行。

2.2.3多源数据接入管理

平台提供一套支持分布式多样化数据格式的多源数据接入工具，旨在将来自不同分布式数据源（如医院、公司、政府等）的具有不同数据类型（包括数据库、CSV/TXT、Restful API和自定义数据格式）的数据接入到平台中执行隐私计算任务。

为此，该多源数据接入工具将提供数据加载、数据管理和数据转换三个主要功能，功能示意图如图9所示，我们接下来将详细介绍三个功能。

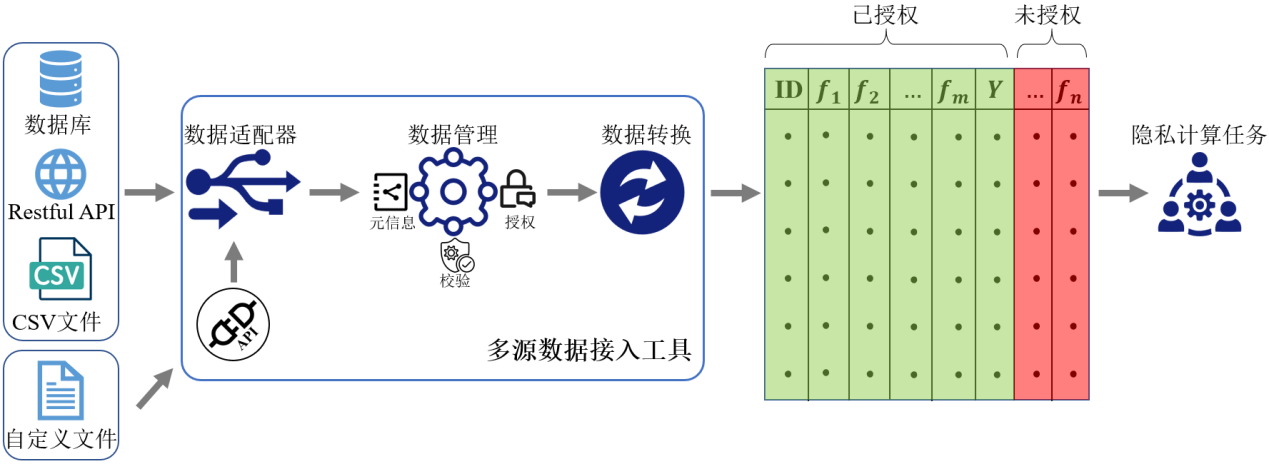


图9. 多源数据接入功能示意图

**数据加载：**我们将开发**数据适配器**接入不同类型的数据源。具体来说，我们主要为数据库、Restful API、CSV文件三类主流数据源提供数据库连接器、API接口、文件导入工具。数据库连接器支持用户通过配置数据库连接信息（包括主机名、端口、用户名、密码等）进行数据库连接并选择数据表加载到平台中；API接口支持用户提供API的终点URL、认证信息以及参数信息来将数据接入到平台中；文件导入工具支持用户选择本地文件进行上传。此外，我们还将提供一套应用编程接口（API），开发者可以基于该套接口以编程的方式与平台交互，从而构建定制的数据适配器，以满足自己特定的数据接入需求。通过这种方式，我们扩展了平台支持的数据源范围。

**数据管理：**工具将提供**元信息读取、数据授权**和**格式校验**三个主要功能实现数据管理。元信息读取指工具能够在连接到数据源后自动分析源数据的元数据，包括字段名称、数据类型、长度等。数据授权指用户可以通过该功能指定接入平台中的数据在参与隐私计算任务时的权限，包括是否可以共享给其他用户以及哪些字段可以参与隐私计算任务。格式校验指工具可以校验用户指定参与隐私计算任务的数据的字段和格式是否符合任务要求。

**数据转换：**工具将提供格式转换和字段映射两个主要功能实现数据转换。格式转换是指用户可以将自己数据字段的格式进行兼容性转换（如int转float）以满足隐私计算任务需求。字段映射是指用户可以通过手动选择或自动匹配的方式将源数据的字段映射到隐私计算任务需要的字段上。

**2.3应用组件**

平台高层提供平台的应用组件，包括联合预测、联合统计、联合查询和联合建模功能。平台用户可以基于这些组件构建或参与特定的隐私计算任务。这些组件的具体功能如下：

1）**联合预测：**联合预测通常涉及多个参与方合作进行预测和推断任务，其应用场景通常分为两种，分别为各参与方只掌握部分模型的场景和一方拥有完整模型，另一方拥有数据样本的场景。联合预测功能将基于计算核心引擎实现模型预测和推断任务。

2）**联合统计**：联合统计为多机构研究的前期可行性分析、回顾性分析以及深入研究中的数据分析与挖掘提供了技术手段，也是联邦学习前期特征工程的重要工具。联合统计包括样本统计分析（如联合统计样本均值、方差、峰度等）和特征统计分析（如皮尔逊系数计算、特征分箱、特征求交等）。联合统计功能基于数据密态计算中封装的密态统计分析算法进行

3）**联合查询**：联合查询在数据隐私保护和多方合作中扮演着关键角色，是实现联合统计、联合建模以及联合预测功能的基础，通常包括隐私集合求交、求并、求补、求差和隐私信息检索等功能。联合查询功能基于计算核心引擎中封装的安全协议（如迪菲-赫尔曼密钥交换和不经意传输等）实现。

4）**联合建模**：联合建模通过联合多个数据拥有方来扩充样本数量或特征维度，以训练出效果更好的模型。联合建模功能包括横向和纵向的联邦LR, GBDT， DNN，迁移学习, 无监督学习，纵向半监督学习等。联合建模功能基于数据密态计算中封装的隐私机器学习算法进行实现。

平台为联合预测、联合统计、联合查询和联合建模组件提供了功能接口，接口内部封装了具体实现这些功能的算法和协议。通过这样的设计，我们的平台提供了丰富且高效的数据分析与挖掘应用支持。

**2.4应用验证**

我们将在**基于区块链和普惠金融的银行贷款风控场景**、**药品经济学分析场景**、**保险产品制定场景、电子处方询价场景**和**基于疾病诊断的医保精准控费场景**对多源数据可信融合计算平台的适用性、可用性和可靠性等多个方面进行验证。

2.4.1 基于区块链和普惠金融的银行贷款风控场景

在传统的银行贷款风控场景中：1）大数据局等数据所有方通过统计个人公积金等信息，将数据资产化后以数据明文的形式完成数据区块链上链。2）区块链提供数据安全保险服务，将公积金等数据资产在大数据局和银行等机构间安全流转。3）当客户请求贷款时，银行从区块链中获得下链的公积金等数据资产明文。4）银行将明文数据资产输入风控系统，经过未加密的风控模型计算，获得风控系数和预期贷款金额。

然而，信息的过度披露导致数据隐私泄露的风险，目前该场景存在以下几个方面的困难和挑战：1）明文的公积金缴费基数、公积金余额、单位名称等信息直接暴露给了银行；而数据提供方缺乏相关的手段，无法监管数据的具体用途，存在信息泄露、信息贩卖的风险。2）银行风控系统中的风控模型，通过判定公积金缴费基数、公积金余额、单位名称等信息是否在一定范围内，或者是否满足某些规则，来输出风控系数和贷款金额。根据输入的明文数据和数据，相应判别项目和判别规则可能被恶意模拟和推测，导致银行风控模型出现泄露风险。

为解决上述问题，本项目开发针对资产数据和风控模型的数据加密解密及密态计算算法，并提供对应算法的数据加工服务，以支撑该场景的计算和隐私保护需求：1）系统为银行和数据所有方提供数据加工服务，数据所有方将数据通过加工服务加密后进行区块链上链。2）当用户发起贷款请求后，区块链将数据密文传递到银行侧的数据加工服务中。3）银行将自己的模型加载到数据加工服务软件中，完成模型的加密。4）银行侧的数据加工服务软件，通过算法的密态计算能力，计算出风控系数后，由风控系统计算出最终贷款金额，提供给用户。系统保证了密态数据在密态模型中运算，即使得明文数据不出数据提供方本地、明文模型在银行方进行加密后使用，保证了银行贷款风控场景中的用户数据和风控模型的安全。

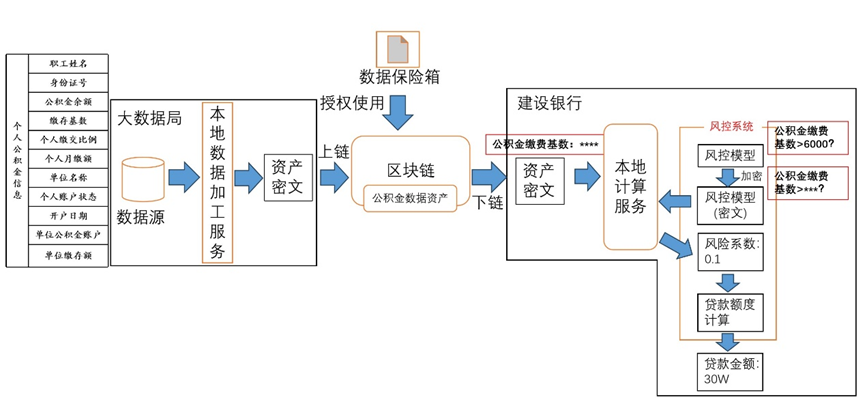


图10. 基于区块链和普惠金融的银行贷款风控场景

2.4.2 药品经济学分析场景



图11. 药品经济学分析场景

在药品经济学分析场景中：1）医药企业根据实际需求编写漏斗式筛选条件。2）根据查询需求，基于隐私计算获取各个参与方的相关数据。医药企业据此优化供给侧的输出结构，以适应需求侧实际的发展。然而，目前该场景下存在以下问题与挑战：

1）挖掘内容涉及各方隐私数据，因此如何做好敏感信息加密、保障挖掘过程隐私安全是亟需解决的问题。

2）各个参与方系统存在多重异构现象，数据名称、类型，表单组织关系等并不一致，并且查询要求形式亦呈现多样性。因此，如何指导医药企业描述需求、基于平台帮助实现隐私查询，也是需要解决的关键问题。

为解决上述问题，平台搭载了隐私安全相关模块以解决隐私安全问题，并根据平台搭载的诸多统计分析与联邦学习算法屏蔽多重异构场景下的查询差异，平台还为医药企业提供了基于漏斗式筛选条件的需求描述规范，通过构建统一编译体系，将漏斗式筛选条件转化为可被平台调度执行的隐私计算代码，从而实现药品经济学分析场景下跨源数据的可信融合计算。

2.4.3 保险产品制定场景

在保险产品制定场景中：1）保险机构首先需要对收集到的客户数据信息进行初步分析和挖掘。2）利用政府机构的的人社数据和医保数据来进一步帮助指导产品的制定。然而，目前该场景存在以下几个方面的困难和挑战：

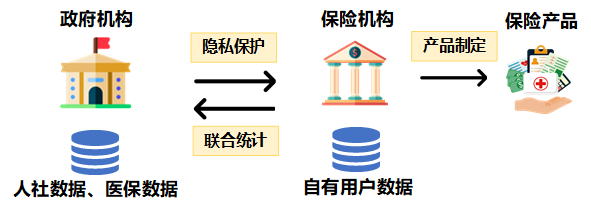


图12. 保险产品制定场景

1）保险机构需要处理敏感的个人信息，例如个人金融信息等，因此数据分析与挖掘过程中，必须采取严格的数据隐私保护措施以确保客户的隐私得到保护。

2）保险机构需要利用政府机构的人社数据和医保数据，但由于隐私安全条例限制，这些数据不能出域，因此需要实现数据可用不可见的条件下综合利用政府机构的人社数据和医保数据。

为解决上述问题，本项目将基于研发平台的可扩展算法定义模块集成基于匿名化处理的敏感信息混淆算法和基于差分隐私的联合统计算法，以支撑该场景的计算需求。其中，基于匿名化处理的敏感信息混淆算法，通过对敏感数据进行信息混淆或批量删除，以确保用户数据的安全性和保密性。基于差分隐私的联合统计算法，通过基于拉普拉斯机制的差分隐私对数据持有者的隐私数据进行扰动，确保数据持有者的个体数据在分析过程中不被泄露。保险机构可以基于本项目的研发平台通过平台集成的数据挖掘算法和工具来直接挖掘分析自有数据和间接利用政府机构的数据，最终制定具有竞争力的产品。

通过基于区块链和普惠金融的银行贷款风控场景、基于疾病诊断分组的医保精准控费、药品经济学分析场景和保险产品制定场景，我们旨在验证所研发平台在数据安全流转、隐私保护、模型传输和业务应用方面的实际可用性。这些验证将为推动医疗和保险领域的数字化转型提供有力支持，同时也为未来类似领域的隐私保护和数据可信流转问题提供了有益借鉴。

2.4.4 电子处方询价场景

在电子处方询价场景中，医保定点零售药店可以凭借定点医疗机构开具的电子外配处方销售药品：1）用户通过处方询价平台选择电子处方，并根据排序选项，如“距离”、“费用”等进行排序和选择，发起处方的询价请求。2）处方询价平台将处方中的药品名称、天数以及满足一定条件的药店药品信息输入算法模型，为处方匹配合适的药店。3）处方询价平台依据输入的排序选项要求，向用户展示对应的药店信息列表，供用户选择。

然而，电子处方的成功实施需要解决一系列隐私和数据安全等问题：1）药店的药品信息、供销存信息等原始数据必须得到保护，而个人患病信息属于敏感信息，必须确保其不会被滥用或泄露。2）处方询价平台的处方询价模型根据输入的处方信息寻找合适的药店，存在恶意模拟用户不同处方输入，模型被推测和泄露的风险。3）处方询价场景中同时刻用户请求量大，对于处方询价平台的并发性能要求较高，部署在单节点上的处方询价模型可能无法达到对应的并发性能要求。

为了解决上述问题，本项目开发针对处方询价模型和对应的处方、药店信息的数据加工服务，提供对模型和数据的加密解密及密态计算算法：1）系统为药店和用户提供数据加密服务，数据所有方能够将数据加密后上传。2）系统将原有的处方询价模型进行加密，采用分布式系统，将密态处方询价模型部署在多个分布式节点上，以提供高并发的服务。3）用户发起处方询价请求后，请求 经处方询价平台转发后，将被匹配到空闲的分布式计算节点。密态处方数据及药店数据将输入到节点对应的密态模型中进行计算，计算出对应的密态药店信息列表后返回处方询价平台，解密后向用户展示。根据以上的算法服务流程，系统保证了输入数据和模型的安全性，并能提供较高并发的服务。

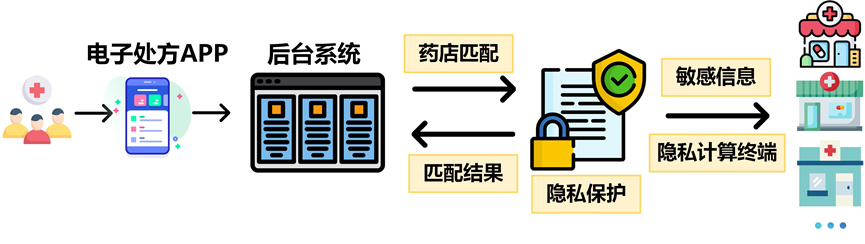


图13. 电子处方询价场景

2.4.5 基于疾病诊断分组的医保精准控费场景

在基于疾病诊断分组的医保精准控费场景中，以济南为例：1）济南医保局部署DRGs模型（局端模型），该模型由医保局专门采购，并且医保局仅公布分组目录和编码。2）各医院独立采购DRGs产品（院端模型），院端模型的承建厂商不能与局端模型的承建厂商相同。3）当参保人住院时，医院向院端模型录入参保人的信息来计算参保人此次住院的报销比例和金额。医院据此调整诊疗方案，旨在保证病人治疗效果和康复效果的情况下减少医院资金垫付，实现经费控制与精细化诊疗。然而，目前该场景存在以下几个方面的困难和挑战：

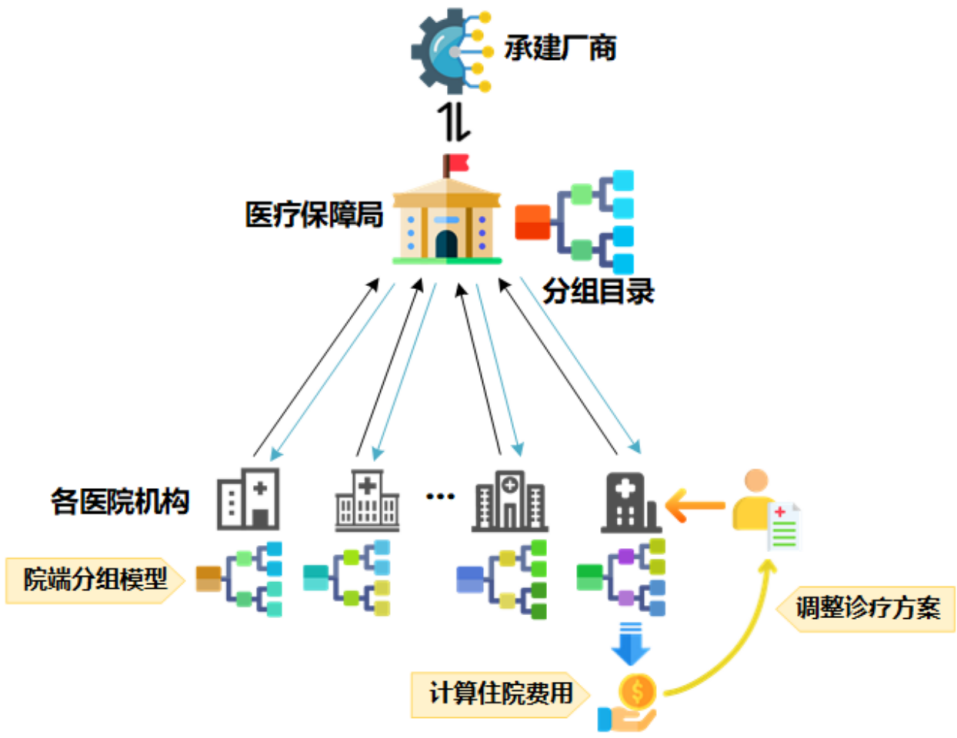


图14. 基于疾病诊断分组的医保精准控费场景

1）医保局端DRGs模型不公布具体分组规则、报销比例，且各医院的患者病例数据均属于隐私数据，因此，如何在实现数据隐私保护和数据可用不可见的条件下综合利用各家医院的疾病诊断数据，使得医院端DRGs模型接近局端模型的分组规则与报销比例是一个需要解决的关键问题。

2）各医院各具特色、业务差异大，这些业务差异导致数据集之间存在明显的差异，因此需要综合考虑各个医院的业务差异对各自院端模型的影响，避免结果不均衡，导致有些医院收益过低或亏损。

3）院端模型不能过于精准，以免导致医保经费被过早耗尽或者导致医疗水平急剧下降，因此如何平衡院端与局端模型是一个亟需解决的关键问题。

为解决上述问题，本项目将基于研发平台的可扩展算法定义模块集成基于个性化联邦学习协同计算和基于动态博弈的智能决策隐私保护算法，以支撑该场景的计算需求。其中，基于个性化联邦学习协同计算算法具备横向联邦学习和纵向联邦学习的能力，以实现多医院间的数据可用但不可见条件下的信息安全共享和个性化模型训练。基于动态博弈的智能决策算法，通过求解博弈模型的纳什均衡解，帮助参与协作的各方制定最优策略，以最大化自身利益。各个医院可以基于本项目的研发平台来间接利用其它医院的数据，通过平台集成的数据挖掘算法和工具，进行数据的联合建模，最终建立起高效的院端模型。

**3.研发计划**

**3.1项目期限**：以实际合同签字生效日期为准，合同期1年。

**3.2进度安排**：

|  |  |  |  |
| --- | --- | --- | --- |
| **阶段** | **研究内容** | **时间** | **提交结果** |
| 1 | 隐私计算框架分析、多源数据可信融合计算平台设计 | T~T+3个月 | 项目报告书 |
| 2 | 多源数据可信融合计算平台开发、扩展算法研发 | T+3~T+6个月 | 源代码 |
| 3 | 多源数据可信融合计算平台场景验证、测试 | T+6~T+9个月 | 项目报告书 |
| 4 | 扩展算法论文撰写、软著专利等申请 | T+9~T+12个月 | 论文、专利 |

**4.预期成果**

**论文**：合作投稿或发表CCF-A类或者领域内顶级会议、一区期刊论文2篇。

**专利**：以山大地纬公司为申请人，提交国内发明专利申请3项。

**平台**：本项目期望实现一个功能全面的多源数据可信融合计算平台，其建设内容主要包含:一套支持易用隐私计算脚本、任务调度和数据密态计算的多源数据可信融合计算核心引擎，一套支持多源数据接入、部署运维和系统状态监测的管理工具和一套支持多机构进行联合预测、联合统计、联合查询和联合建模的平台应用组件库。最终交付的产品根据信通院的功能、安全、性能等标准进行开发，具备能够通过检测的能力。

通过以上平台开发，本项目能够支持基于区块链和普惠金融的银行贷款风控、药品经济学分析场景、保险产品制定场景、电子处方询价场景和基于疾病诊断的医保精准控费场景等业务需求，这将有助于医疗和金融领域的数据安全流转、模型协同训练和智能决策的实现。

**5.人力投入**

|  |  |  |  |
| --- | --- | --- | --- |
| **人员姓名** | **职务** | **参与项目时间(折合全时人月数)** | **主要承担职责** |
| 余国先 | 教授 | 12 | 项目整体统筹与进度管理 |
| 王峻 | 教授 | 12 | 项目整体统筹与进度管理 |
| 吕洪涛 | 博士后 | 12 | 扩展算法研发、场景应用验证 |
| 赵云峰 | 博士生 | 12 | 扩展算法研发、场景应用验证 |
| 苏聪 | 博士生 | 12 | 运维、部署及数据管理工具研发 |
| 杨德智 | 博士生 | 12 | 运维、部署及数据管理工具研发 |
| 康祥平 | 硕士生 | 12 | 隐私计算脚本、任务调度功能研发 |
| 桂孝强 | 硕士生 | 12 | 隐私计算脚本、任务调度功能研发 |
| 陈博文 | 硕士生 | 12 | 密态计算框架、加密通信功能研发 |
| 李新昀 | 硕士生 | 12 | 密态计算框架、加密通信功能研发 |
| 朱江跃 | 硕士生 | 12 | 系统功能测试 |
| 苟丛林 | 硕士生 | 12 | 系统功能测试 |