联邦学习平台

亚信科技联邦学习平台 V2.3 白皮书

亚信科技联邦学习平台（AISWare AI^2 FL），面向行业客户的跨域建模和数据要素价值共享需求，提供低门槛、可视化、安全可信的企业级联邦学习模型服务的开发和运行能力，基于隐私计算基础设施提供跨机构的可信数据运营能力。通过多种密码学手段保护交换的模型参数、梯度信息安全性，从技术上实现安全合规的 AI 协作。

声明

任何情况下，与本软件产品及其衍生产品、以及与之相关的全部文件（包括本文件及其任何附件中的全部信息）相关的全部知识产权（包括但不限于著作权、商标和专利）以及技术秘密皆属于亚信科技（中国）有限公司（“亚信科技”）。

本文件中的信息是保密的，且仅供用户指定的接收人内部使用。未经亚信科技事先书面同意本文件的任何用户不得对本软件产品和本文件中的信息向任何第三方（包括但不限于用户指定接收人以外的管理人员、员工和关联公司）进行开发、升级、编译、反向编译、集成、销售、披露、出借、许可、转让、出售分发、传播或进行与本软件产品和本文件相关的任何其他处置，也不得使该等第三方以任何形式使用本软件产品和本文件中的信息。

未经亚信科技事先书面允许，不得为任何目的、以任何形式或任何方式对本文件进行复制、修改或分发。本文件的任何用户不得更改、移除或损害本文件所使用的任何商标。

本文件按“原样”提供，就本文件的正确性、准确性、可靠性或其他方面，亚信科技并不保证本文件的使用或使用后果。本文件中的全部信息皆可能在没有任何通知的情形下被进一步修改，亚信科技对本文件中可能出现的任何错误或不准确之处不承担任何责任。

在任何情况下，亚信科技均不对任何因使用本软件产品和本文件中的信息而引起的任何直接损失、间接损失、附带损失、特别损失或惩罚性损害赔偿（包括但不限于获得替代商品或服务、丧失使用权、数据或利润、业务中断），责任或侵权（包括过失或其他侵权）承担任何责任，即使亚信科技事先获知上述损失可能发生。

亚信科技产品可能加载第三方软件。详情请见第三方软件文件中的版权声明。

亚信科技控股有限公司（股票代码：01675.HK）

亚信科技是中国领先的软件产品及服务提供商，拥有丰富的软件产品开发和大型软件工程实施经验。公司深耕市场 30 年，在 5G、云计算、大数据、人工智能、物联网、数智运营、业务及网络支撑系统等领域具有先进的技术能力和众多成功案例，客户遍及通信、广电、能源、政务、交通、金融、邮政等行业。

2022 年，亚信科技完成收购商业决策服务领域的领先企业艾瑞市场咨询股份有限公司（「艾瑞咨询」），并整合形成新的“艾瑞数智”品牌。通过此次收购，亚信科技的核心能力从产品研发、交付服务、数据运营、系统集成延伸至咨询规划、智能决策，成为领先的数智化全栈能力提供商。

亚信科技始终致力于将 5G、AI、大数据等数智技术赋能至百行千业，与客户共创数智价值。公司以“产品与服务双领先”为目标，产品研发围绕数智、云网、IT 及中台产品体系持续聚焦，实现行业引领，其中云网产品保持国际引领，数智产品实现国内领先，部分国际先进，IT 领域产品处于国内第一阵营。

面向未来，亚信科技将努力成为最可信赖的数智价值创造者，并依托数智化全栈能力，创新客户价值，助推数字中国。

部分企业资质

能力成熟度模型集成 CMMI5 级认证

信息系统建设和服务能力评估（CS4 级）

云管理服务能力评估证书卓越级

数字化可信服务－研运数字化治理能力认证

1S09001 质量管理体系认证证书

150200001T 服务管理体系认证证书

1S027001 信息安全管理体系认证证书

企业信用等级（AAA 级）证书

信息系统安全集成服务资质（二级）

信息系统安全开发服务资质（二级）

部分企业荣誉

连续多年入选中国软件业务收入百强榜单

连续多年入选中国软件和信息服务竞争力百强企业

中国软件行业最具影响力企业

中国软件和信息服务业最有价值品牌

中国软件和信息服务业最具影响力的行业品牌

中国数字与软件服务最具创新精神企业奖

中国电子信息行业社会贡献 50 强

中国人工智能领航企业

新型智慧城市领军企业

IDC 未来运营领军者

目录

1 摘要

数据是人工智能的基础，AI 发展到现在的阶段，能否获得量大质高的数据已成为制约其进一步发展的重要因素。在这样背景之下，数据共享、融合的需求越来越强烈，但是在数据共享的过程中，遇到以下问题：

数据孤岛问题严重，由于安全问题、竞争关系和审批流程等因素，数据在行业、甚至是在公司内部以“孤岛”的形式存在。而数据共享越来越重要，但在数据共享中因为缺乏有效的保障手段，进而导致数据安全问题频发。

重视数据隐私和安全已经成为世界性的趋势，在国外，2018 年 5 月，欧盟的《通用数据保护条例》（General Data Protection Regulation, GDPR）正式开始生效，该条例对于数据保护做出了严格规定。同时在国内，对于数据保护的力度越来越严格，国家先后发布《网络安全法》、《信息安全技术——个人信息安全规范》和《互联网个人信息安全保护指南》等法律法规，同时公安部也在严厉打击数据安全犯罪行为。在这样的背景之下，即便行业有意共享数据，也面临政策、法律合规的严峻问题。

另一方面，传统的机器学习方法，需要把训练数据集中于某一台机器或是单个数据中心里，为了满足逐渐增加的数据量级，只能进行垂直拓展、横向拓展或者建设基础设施；而在数据集中的过程中，会存在数据泄露的风险。同时，目前的 AI 市场模式是科技巨头在主导，他们提供基于云的 AI 解决方案以及 API，这种模式使用户无法控制 AI 产品的使用以及个人隐私数据，而通过数据集中，科技巨头公司却可以垄断数据。一定要注意这一点，从企业发展角度而言，必须重视这一点，因为，未来世界的竞争是基于数据的竞争，而数据的垄断必将带来市场的垄断；而传统的集中模式很可能在未来限制初创企业乃至大型企业的创新。

以上提到的问题导致传统的数据共享技术难以满足需求。新的技术应运而生——联邦学习（Federated Learning, FL），在融合安全多方计算以及其他加密技术的基础之上发展越来越成熟。该技术实际上是一种加密的分布式机器学习技术，各个参与方可在不泄露底层数据并在底层数据加密（混淆）形态的前提下共建模型。

本白皮书将从产品架构、优势特性、产品价值及应用案例等多个方面介绍亚信科技联邦学习平台。

2 缩略语与术语解释

亚信科技联邦学习平台常见术语如表 2-1 所示。

表**2-1** 术语解释

缩略语或术语	英文全称	解释
FL	Federated Learning	联邦学习，是一个机器学习框架，能有效帮助多个机构在满足用户隐私保护、数据安全和政府法规的要求下，进行数据使用和机器学习建模。
数据提供方	Host	联邦学习中负责提供无标签数据的一方，增加训练中的数据特征，进行数据变现。
任务发起方	Guest	联邦学习中提供数据标签，发起联邦训练任务，使用外部数据提升模型性能。
协调方	Arbitor	联邦学习中负责收集、处理以及分发训练参数信息。
同态加密	Homomorphic Encryption	同态加密是基于数学难题的计算复杂性理论的密码学技术。对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。
RSA	RSA algorithm	公开密钥密码体制，是一种使用不同的加密密钥与解密密钥；加密密钥（即公开密钥）PK 是公开信息，而解密密钥（即秘密密钥）SK 是需要保密的。加密算法 E 和解密算法 D 也都是公开的。虽然解密密钥 SK 是由公开密钥 PK 决定的，但却不能根据 PK 计算出 SK。

缩略语或术语	英文全称	解释
OT 协议	Oblivious Transfer	OT（不经意传输）是一种密码学协议，由 Rabin 在 1981 年提出，是一种基础的多方安全计算协议。协议由发送方、接收方两方参与，发送方拥有一个“消息-索引”对（M1, 1），（M2, 2），…，（MN, N）。每次传输的时候接收方选择一个索引 I，i∈[1, N]，并接收 Mi。接收方不能得知发送方的任何其他信息，发送方也不能了解接收方选择了哪个消息。
区块链	Blockchain	区块链是把加密数据（区块）按照时间顺序进行叠加（链）生成的永久、不可逆向修改的记录。相比于传统的网络，区块链具有两大核心特点：一是数据难以篡改、二是去中心化。
数字签名	Digital Signature	数字签名（又称公钥数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

3 产品概述

亚信科技联邦学习平台（AISWare AI^2 FL），面向行业客户的跨域建模和数据要素价值共享需求，提供低门槛、可视化、安全可信的企业级联邦学习模型服务的开发和运行能力，基于隐私计算基础设施提供跨机构的可信数据运营能力。通过多种密码学手段保护交换的模型参数、梯度信息安全性，从技术上实现安全合规的 AI 协作。

3.1 趋势与挑战

当前，数据共享和数据保护似难以同时保障，如要共享数据，数据安全就容易受到威胁；而如果要严密地保护数据，那么信息孤岛就难以打破。隐私法制约现有的数据变现模式，数据隐私相关法规禁止交易个人用户数据，原有的数据售卖变现方式无法满足要求。

2020 年，数据增列为生产要素，数据要素市场化改革上升至国家战略高度。2021 年，数据安全法、个人信息保护法等关键法律相继实施。2022 年 12 月，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》，又称“数据二十条”。

同时，企业之间数据无法互通，少数巨头公司垄断大量数据，小公司很难获得数据，形成大大小小的“数据孤岛”。而在企业内部，部门不会把数据与其他部门做简单的聚合。导致即使在同一个公司内，数据也往往以孤岛形式出现。

联邦学习技术可以通过“数据不动，模型动”的方式，能够有效解决各方数据价值无法协同利用的问题。参与方在具备完备的数据安全保护能力，整个联合建模过程中，数据不出库，全程无数据传输，仅交换模型参数；参数的交互采用先进同态加密技术对建模参数进行全程严格加密，并叠加 RSA 等密码技术进行多层加固。

3.2 产品定义

亚信科技联邦学习平台，是由各参与方和协调方共同组成的一套跨网络的开发平台，让各参与方能够基于平台完成联邦学习模型的训练以及部署推理；为各个联邦参与方的模型开发和运维人员，提供低门槛、可视化的企业级联邦学习模型服务的开发和运行能力，支撑联邦学习模型在企业之间快速落地。

平台首创“运营商+”一站式联邦学习服务开发与应用平台，采用联邦学习、多方安全计算、区块链等技术，提供低门槛、可视化的企业级联邦学习服务开发和运行能力，创新性打造“运营商+”跨域协作新模式，充分挖掘海量数据价值，助力通信大数据赋能千行百业。

3.3 产品定位

亚信科技联邦学习平台，面向联邦学习场景化应用，提供低门槛、可视化、安全可信的企业级联邦学习模型服务的开发和运行能力，实现联邦学习模型和应用快速落地；聚焦客户在保障数据隐私安全前提下的分布式 AI 建模和使用业务需求，提供从联邦数据处理、联邦建模、再到联邦推理的平台能力支撑，打造数据要素流通时代的 AI 安全协作平台。

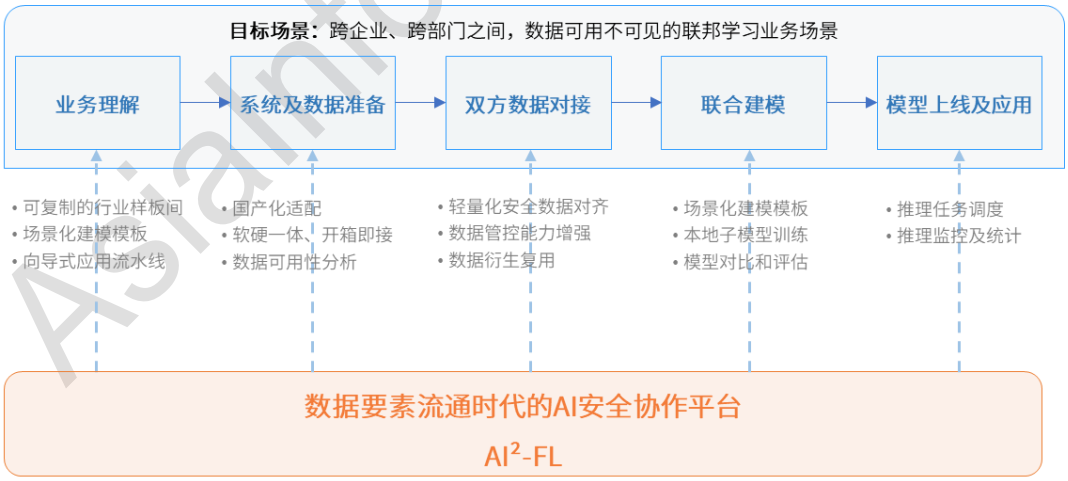

图**3-1** 客户业务洞察与产品定位

4 产品功能架构

AISWare AI^2 FL 产品为各个联邦参与方的模型开发人员、运维人员、业务人员，提供低门槛、可视化的企业级联邦学习模型服务的开发和运行能力，支撑联邦学习模型在企业之间快速落地。

- 支持横向和纵向联邦学习，联邦在线/离线推理能力，能够灵活的满足绝大多数的联邦学习应用场景。
- 容器化部署，可在线扩展联邦参与方组织，单个组织的算法、算力以及数据存储能力都可以方便的横向扩展。
- 提供从数据接入到部署模型一站式的联邦学习开发能力，简化联邦学习模型的开发、上线工作，降低使用的门槛。
- 面向重点行业客户的跨域建模需求，提供可复制的场景化建模模板和行业样板间。通过数据预处理和单边建模增强数据可用性；流程解耦，灵活编排。
- 联邦学习引擎组件支持国产化适配，支持 BC-Linux、麒麟、欧拉等国产操作系统，支持国产 GPU 加速卡。
- 引擎层多框架支持，基于 RAY 的分布式计算；一键自动化部署。

图**4-1** 产品功能架构

5 产品基础功能

产品提供从接入数据到发布联邦推理服务一站式的开发能力，可完成从数据准备到联合推理的服务开发与运行闭环。

- 联邦环境准备：可视化配置联邦学习的各方组织信息，包括组织管理及组织节点认证、用户管理、审批待办管理、API 用户管理、服务权限管理等系统维护所需相关功能。
- 数据管理：参与联邦学习的各个组织自行准备事先协商确定的、可用于建模的数据集，接入的数据集可直接用于创建联邦学习模型，并对数据进行授权和审计。
- 联邦训练：可编排训练任务并发起训练，开始训练后可以实时监控训练任务进行状态，训练成功后可以发布模型。合作方可以查看发起方发起的训练任务。支持 3 方以上建模；通过拖拽需要的组件，连接组件输入输出，编排训练任务，可片段式执行任务；支持 JSON 配置。
- 隐私求交：各参与方可分别接入数据集后以加密对齐的方式进行数据安全对齐，以获得共有数据的交集。求交完成后，可下载结果。并支持对求交任务和执行记录进行管理。支持按周期执行求交任务。
- 匿踪查询：基于 OT 协议进行安全隐匿查询，支持 ID 查询和批量查询，支持上传批量 ID 列表后查询；可导出查询结果。
- 模型库：可对发布的模型进行管理，可以对模型及其版本进行查看、删除、部署在线推理、部署为离线任务。用户在发布模型时，可同时为模型开启防篡改保护；可对已发布的存量模型开启防篡改保护，开启后，使用模型时系统自动记录防篡改保护日志。
- 联邦推理：提供在线推理服务功能，供业务系统进行实时调用；可创建离线推理任务，推理完成后可导出结果。
- 软硬一体化适配：提供轻量化的联合建模、隐私求交、匿踪查询等功能，简化配置步骤，支持更便捷的一体化部署和交付。支持一站式运维，提供安装引导、服务配置、节点维护、软件升级、运行监控、安全审计等功能。

6 产品特色功能

亚信科技联邦学习平台，支持从数据接入到服务发布全流程可视化管理，降低开发门槛和落地成本；全链路安全防护体系，提供多维度的安全防护能力。

6.1 行业样板间

面向垂直行业的开箱即用、可定制场景化应用模板，助力联邦学习技术在垂直行业快速落地；广泛应用于精准营销、联合风控、数据交叉分析等跨行业场景。

- 精准营销：整合跨行业数据优势，联合建模提升营销精准度，降低营销成本，适用于保客营销、纳新拓客等营销场景。
- 联合风控：适用于隐匿三要素验证服务、金融联合信贷风控服务、金融监管场景服务。
- 数据交叉分析：多维数据结合联邦学习数据隐私保护技术，补足传统企业数据维度痛点，构建更丰富的特征标签。

6.2 一站式联邦学习开发与应用

提供从数据准备、联邦建立、联合训练到模型部署、联合推理的全流程拉通能力，通过低门槛、开放普惠的联邦学习开发、应用、服务能力，助力联合建模能力在垂直行业低门槛落地。

- 可视化的联邦模型编排：提供拖拽式的联邦模型开发功能，开发者无需再编辑复杂的配置文件，通过简单的界面操作和配置完成联邦训练任务开发。
- 开放普惠：企业可平滑接入生产环境自有数据，大幅降低数据对接成本：多种存储类型、多种规模数据合规接入。

6.3 全栈安全协作体系

构建全栈安全联邦协作体系，促进数据价值在垂直行业安全合规共享。

- 安全原生：通过授权、认证与鉴权防止非授权访问，提高保证机密性；基于可信存证防止重要数据被非法篡改，保证完整性；通过动态切换、持久化等提高系统可用性。
- 全维度安全加固：通过身份认证、通信加密、安全算法、可信存证、安全信息检索等手段，进行应用、网络、系统层面的安全加固。

6.4 可信数据服务及数据运营

基于 TDaaS（可信数据即服务）为行业客户提供安全、合规的数据调用及数据智能服务，与数据及服务提供商、数据应用方共同构建数据安全可信流通的能力新范式。

- 高质量可信数据源：预置运营商数据集，充分发挥运营商大数据维度丰富、质量高、时效性强的优点，助力通信大数据变现。
- 联邦生态构建：结合数据源链接、开源引擎等，增强跨平台联邦合作能力。
- 可信数据运营能力：通过对数据的可用性开发、基于场景的建模（单边/跨域）和利用，打通数据运营业务流。

6.5 数据可用性分析增强

通过联邦学习各方的数据进行数据预分析、轻量化数据安全对齐、衍生数据集管理功能，强化从数据准备到联邦训练和推理的一站式开发能力，真正做到“数据可用”，更好地满足业务需求，提高开发效率并保障数据的安全与隐私。

- 数据预分析：提供丰富的数据预处理、特征工程、数据探索、可视化组件，提高数据质量，降低人工干预成本。
- 轻量化数据对齐：通过更高性能的求交算法和通信协议，实现快速高效的隐私求交，提高工程实战能力。

- 衍生数据集：无需每次都对原始数据进行预分析和安全对齐，直接复用衍生数据集，加速项目启动。

6.6 软硬协同，智能加速

通过算法和计算引擎的深度优化，实现与不同计算资源的无缝对接，从而充分利用硬件加速带来的性能提升。针对不同任务进行针对性的性能优化，确保在各种场景下都能获得最佳的性能表现。

- 软硬件协同加速：通过优化算法和计算引擎，使其与底层硬件紧密结合，从而充分发挥硬件的计算潜力。确保任务在硬件上高效执行，减少数据传输和通信开销，提高整体计算效率。
- 智能调度：利用智能调度策略，根据任务的特性和需求，选择合适的硬件设备和计算引擎进行任务处理。
- 任务执行监控：实时展示任务执行状况及性能指标，实时异常检测。

6.7 全面信创融合

提供从芯片、操作系统、数据库、算法、计算引擎的全面国产化适配，打造国产信创全面融合的联邦学习产品，降低系统的外部依赖、提高兼容性、强化自主可控能力。

- 全面国产化适配：提供从芯片、操作系统、数据库、算法、计算引擎的全面国产化适配。
- 信创可信数据交付：全面信创融合，为 DSSN 提供网络化、模块化联邦建模交付服务。
- 信创可信数据流通：通过集团虚拟专网进行联邦计算能力传送，实现全网统一、跨地域、跨资源池的联邦计算节点管理和调度。

6.8 即启即用，可视管理

通过可视化界面和自动化技术，将复杂的运维工作简化为直观、易操作的过程，使用户可以聚焦于平台的使用和业务需求，更轻松地进行平台管理和维护。

- 自动化部署：根据预设的配置参数自动安装和配置平台所需的各个组件，屏蔽底层组件类型和依赖的复杂性。
- 运维白屏化：通过可视化界面配置系统所需参数，提高平台运维的直观性和易操作性，简化配置管理工作，降低用户的运维负担，提高工作效率。

7 产品差异化优势

AISWare AI^2 FL 具备软硬协同、安全自主可控和可信数据流通三大优势。

通过智能加速和调度、自动化部署以及场景化建模，实现开箱即用，大幅提升运维效率。同时，产品全面国产化适配，构建全栈安全体系，确保数据安全合规共享。此外，还提供可信数据运营，支持数联网节点和跨计算引擎的互联互通，降低整合成本，推动生态系统发展，为用户带来高效、安全、易于管理的数据处理和运营体验。

7.1 软硬协同，开箱即用

自动化、可视化、极简运维、行业样板间，用户可聚焦于平台的使用和业务需求，实现开箱即用。

- 智能加速和调度：算法和计算引擎深度优化，无缝对接多种计算资源，充分利用硬件加速带来的性能提升。针对不同任务进行针对性优化，多场景极致性能。
- 自动化部署：支持多种部署方式，容器化形式可支持一键部署。降低部署门槛，提高配置和使用的灵活性。
- 白屏化运维：提供部署页面以简化配置方式，按需配置，通过将复杂的配置过程可视化并实时监控系统的运行状态，提高整体运维的效率和准确性。
- 场景化建模：通过训练模板和应用模板，将行业知识和经验转化为可复用的知识，帮助用户快速上手联邦学习技术，降低技术使用门槛，提高开发效率。

7.2 安全自主可控

提供国产化适配和全栈安全体系，增强跨域数据自主可控能力，使数据能够安全合规共享；通过可信数据交付服务，提升数据要素流通的效率和创新合作。

- 全面信创融合：提供从芯片、操作系统、数据库、算法、计算引擎的全面国产化适配。降低系统的外部依赖、提高兼容性、强化自主可控能力。
- 可信数据交付：为数据要素流通基础设施提供网络化、模块化联邦建模交付服务。为可信数据共享网络（DSSN）提供专门支持，提高交付效率、促进合作与创新。
- 全栈安全体系：数据、通信、算法、流程、接口全流程安全保障，全链路数据隐私保护。安全原生能力加固、安全运营服务增强，促进数据价值安全合规共享。

7.3 可信数据流通

数据可用性开发及数据价值运营，支持多种互联互通方式，强化互操作性、降低整合成本、促进生态系统发展。

- 可信数据运营：预置高质量电信行业数据源，垂直行业客户可快速接入并获取数据价值；结合数据预分析、轻量化数据安全对齐、衍生数据集管理等功能，强化从数据准备到联邦训练和推理的一站式开发和运营能力。
- 数联网节点互联互通：遵循移动集团 1+X 纳管集成规范，数据使用方/提供方可通过双方均部署隐私计算底座或单侧部署底座的模式进行项目和数据授权，之后双方通过计算引擎节点进行联邦建模及推理。
- 跨计算引擎互联互通：双方部署不同厂家的联邦学习计算引擎（如：FATE & 隐语），其中一方同时部署异构引擎节点镜像，双方实现跨引擎的联邦训练作业提交。

8 场景解决方案

平台基于新型分布式机器学习范式，能够有效解决数据孤岛问题，让多个参与方在不共享数据的基础上联合建模，并通过多方安全计算等密码学的最新技术手段确保交换的模型参数、梯度信息安全性，从技术上实现安全合规的 AI 协作。

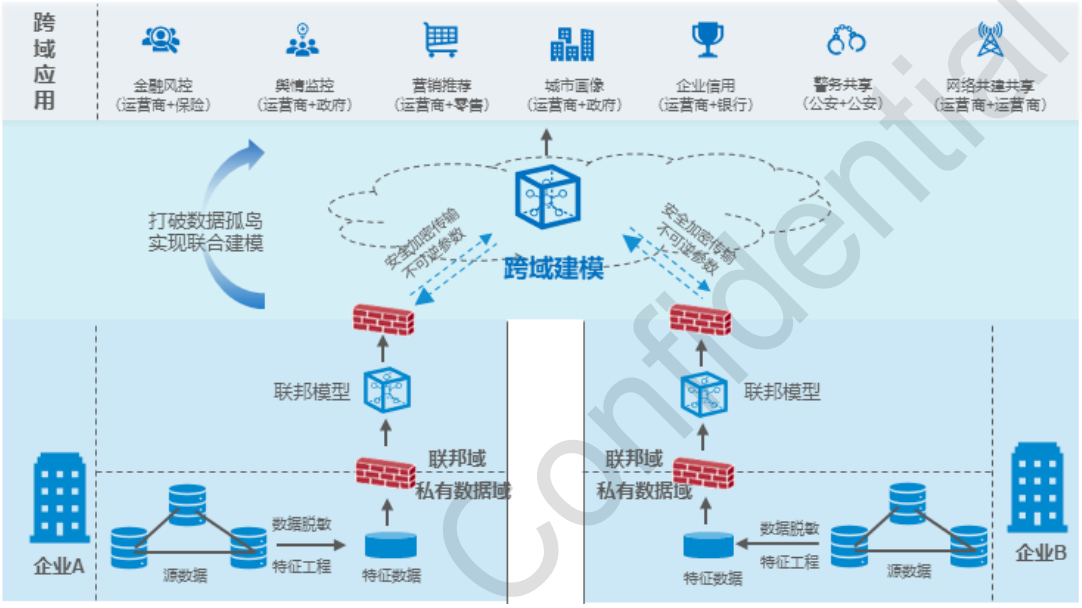

图**8-1** 应用场景综述

8.2 汽车行业云边协同联合营销

为汽车行业提供安全可信的创新营销路径。整合运营商与车企双方的行业数据优势，持续实时对购车用户、购车意向进行模型推理及预测。

业务痛点

传统的增换购推荐模型基于车企自有数据进行建设，由于数据维度不足导致增换购模型效果一直未达预期，亟需寻找外部数据进行大数据合作赋能，深度挖掘保客价值。

解决方案

在车企中心化平台部署的基础上挖掘边端数据源价值，以云边协同的形式，边缘侧数据源通过一体机参与可信联邦建模，在保证本地数据安全的基础上补全中心数据特征维度。基于车企自有数据及运营商大数据，根据数据标准及要求，双方各自选取客户相关特征，输出重点标签并建立单边子模型，通过联邦学习平台联合建模，构建意向度模型及意向车型模型，赋能精准挖掘。

该方案能够发挥通信行业数据规模及维度优势，补足汽车行业数据特征；为车企有效节省营销成本，提高营销推荐活动中的有效线索占比，实现营销活动的闭环评估。

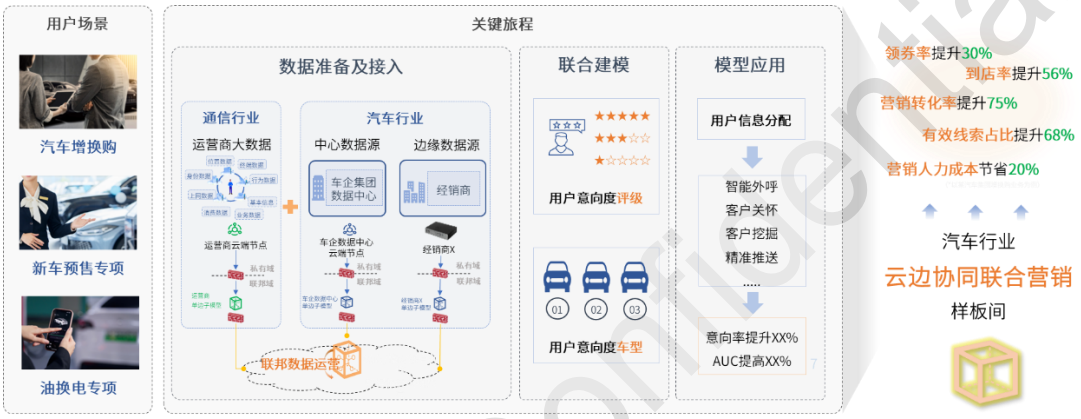

图**8-2** 汽车行业云边协同联合营销解决方案

方案亮点

- 开箱即接：汽车经销商可通过开箱即用的一体机快速接入数据，保障本地数据安全。
- 云边协同：将联邦计算节点拓展至边缘端，补全车企特征维度。
- 软硬一体：充分利用硬件加速带来的性能提升，提高整体训练效率。
- 业务赋能：内外用户数据安全联合分析，赋能增换购通用场景和专项场景。

8.3 金融行业全面信创联合建模

在满足数据隐私安全的前提下，通过对潜在贷款用户模型的纵向联合建模，联邦学习模型的效果查全率和营销准确率都得有效提升。

业务痛点

数据隐私法规日趋严格，机构间无法互通数据。尽管运营商有大量用户的属性和行为数据，如：上月消费、XX 银行通话次数、通话联系人数量、上网日志，历史搜索，APP 使用记录等，银行却难以获得，形成数据割裂现象。

解决方案

全面国产化适配，包括芯片、操作系统、数据库、算法和计算引擎等；满足金融行业信创要求，确保解决方案在自主可控的环境中运行。

金融机构和运营商分别接入数据集后，通过安全数据对齐和纵向联邦学习完成建模，满足数据隐私安全的前提下，通过对潜在贷款用户模型的纵向联合建模有效提升银行贷款营销推荐模型的查全率和营销准确率。

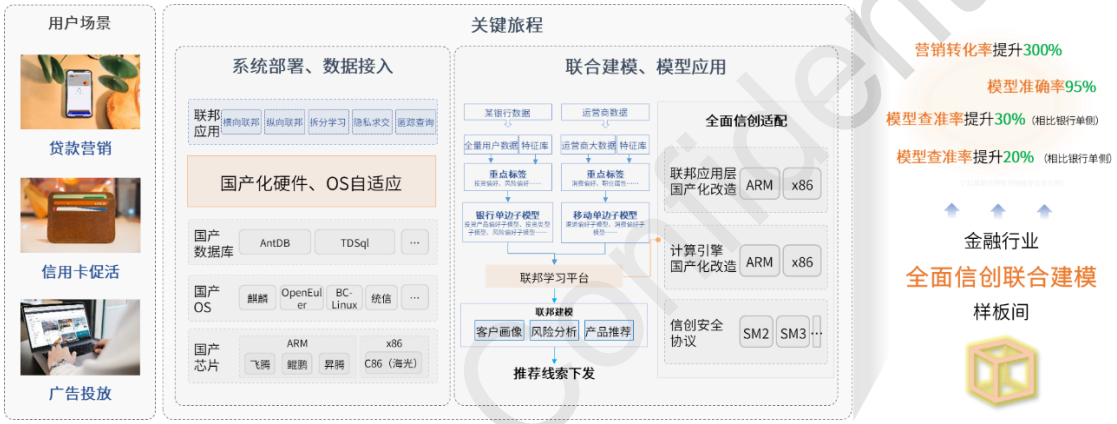

图**8-3** 金融行业全面信创联合建模解决方案

方案亮点

- 全程自主可控：通过全面信创融合，从系统部署到联邦建模及模型应用的全过程均在信创环境中进行，有助于推动金融行业的自主可控发展，提高金融行业的安全性和稳定性。
- 可信数据流通：在满足用户隐私保护、数据安全和政府法规的要求下，基于电信业务使用数据和金融机构的标签数据实现联合建模，通过运营商数据要素的安全合规流通及价值释放，为金融机构实现业务创新赋能。

8.4 基于区块链的可信联邦学习

通过区块链的加密和去中心化特性，强化数据安全和隐私保护，同时提高系统对故障的抵抗力。通过智能合约促进节点间的互信与合作，而透明的激励机制鼓励了积极参与和数据共享。

业务痛点

联邦学习过程中，由于数据在多个参与方之间流通和协作，存在中间参数安全、系统鲁棒性、多方信任建立、激励机制设计、数据确权以及合规性等关键业务痛点。

解决方案

将联邦学习技术与区块链技术结合，提供一种在数据本身不用交换的情况下实现数据价值共享的解决方案，在数据共享过程中实现价值挖掘与隐私保护之间的平衡。结合区块链优势解决联邦学习的安全问题， 打破数据壁垒，实现多方安全计算的新机制，打造联邦学习的模型共享训练引擎，实现更精准的建模。

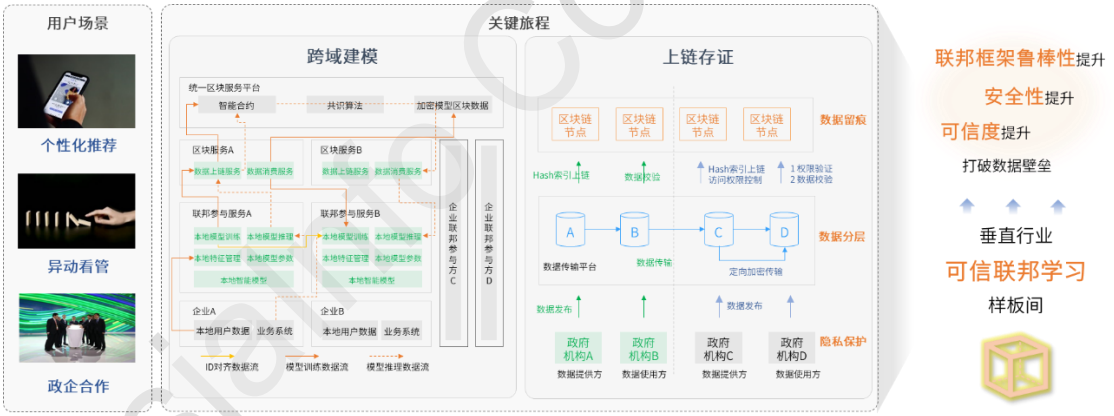

图**8-4** 基于区块链的可信联邦学习解决方案

方案亮点

- 去中心化可信联邦：区块链替代联邦中心服务器，提供相应的激励机制，增强数据流动效率，增强审计可信度。整合多方数据，模型参数上链，保障本地模型及数据的安全性与可靠性。
- 参与方识别与贡献度判定：通过智能合约及共识算法对各参与方请求进行规则判定，屏蔽非法上链请求，规避风险，控制流量，保障优质合作方。

基于各参与方的数据上链区块，对全部参与方的模型贡献度进行量化判断，为数据融通合作提供谈判依据。

9 产品客户成功故事

本节主要介绍亚信科技联邦学习平台的客户成功故事（应用案例）。

9.1 AISWare AI² FL 助力某车企增换购业精准营销

本节主要介绍“运营商+汽车”在联合营销场景的应用案例。

9.1.1 客户需求

精准营销是汽车产业市场竞争中非常重要的一环，以往传统的汽车营销推荐基于车企自有数据进行建设，存在客户信息实时性和准确性难以保证、数据维度不够全面、数据样本体量不足等局限，导致模型精度不足、跟进营销效率低下，造成营销人力浪费并错失商机。在车企数字化转型加速、数据应用安全要求加强的多重因素推动下，传统车企迫切需要安全可信的创新营销路径。

9.1.2 建设方案与成效

基于以上背景，某车企通过寻找外部数据进行跨域合作赋能，在保障各方数据隐私安全的前提下，帮助该企业识别增换购高意向需求客户，联动其营销业务板块满足增换购业务需求。

本案例整合运营商与车企双方的行业数据优势，持续实时对购车用户、购车意向进行模型推理及预测。非平衡条件下联合分析，运营商侧涉及 13 亿数据及 1000 余个模型标签的分析及建模。基于真实样本的推理结果，模型表现出较好的预测能力，支撑某车企进行应用触达等。

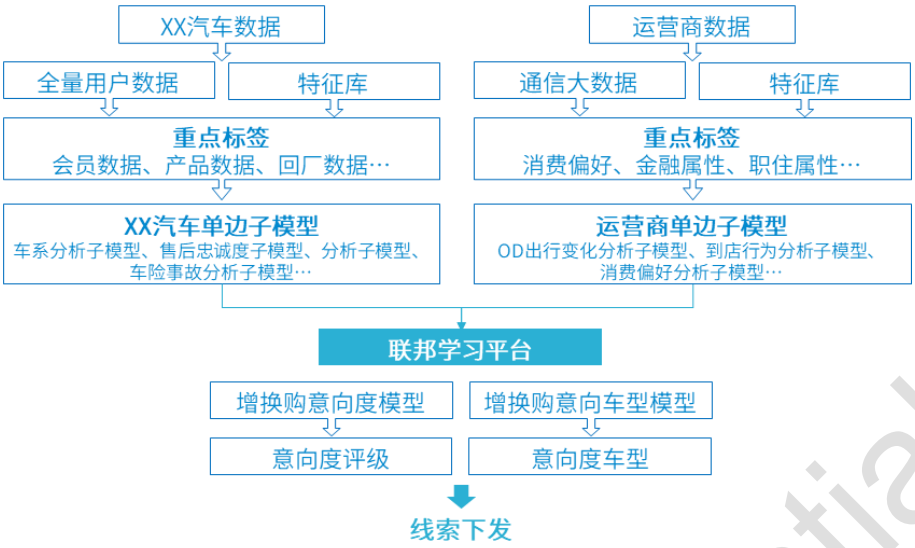

图**9-1** 建模过程示例

通过该案例的实施，某车企保客增换购营销的到店率、领券率、有效线索占比均得到明显提升，实现了营销活动的闭环评估。应用效果体现在：

- 增换购客户意向率提升 60%，AUC 提升 20%。
- 客户领券率提升 30%，到店率提升 56%。
- 有效推荐线索占比提升 68%，营销成本节省超 20%。

图**9-2** 案例应用效果

通过本案例的实施，为客户提供了以下业务价值：

- 基于跨行业数据融合分析，打造汽车行业首个跨域联合营销创新路径。
- 实现了某车企的营销活动的闭环评估，最终促进增换购业务的精准营销。
- 基于运营商+汽车跨域合作的知识沉淀，将联邦协作知识提炼为可通用、可迁移的模板，并转化为可观测、可量化的业务价值，实现应用场景的快速复制。

9.2 AISWare AI² FL 赋能医疗行业智能推荐

本节主要介绍“运营商+医疗”在智能推荐场景的应用案例。

9.2.1 客户需求

某省移动公司作为全集团的标杆企业、省内规模最大的电信运营商，在数据价值挖掘及模型提升方面，面临以下痛点：

- 数据变现受到制约，有大量数据资产，但受隐私法规的制约无法变现。
- 由于数据维度、数据量不够，模型准确性提升遇到瓶颈。
- 无法实现海量训练、海量连接，物联网、5G 等数据量特别大，并且不易于汇聚起来训练。

该客户需要购置一套联邦学习平台，满足某移动与合作医疗机构在保证数据隐私与安全合规的前提下，进行多方数据联合建模、数据协同利用，赋能智能推荐场景。主要需求包括：

- 能够进行在保证数据隐私安全前提下的跨域建模。
- 要求平台提供可扩展的多方协作建模、联合学习的能力。
- 需具备系统管理功能，包括但不限于项目管理、组织管理、用户管理、角色管理等相关功能。

9.2.2 建设方案与成效

通过新型分布式的机器学习范式，打造基于纵向联邦学习的“运营商+医疗”智能推荐模型；基于联邦学习框架打造联邦学习模型架构，实现某移动与合作医疗机构的本地化部署联调。基于某移动与合作医疗机构的数据特点构建专家咨询/极速问诊联邦推荐模型，并应用于该机构预约挂号 APP 的推荐场景。

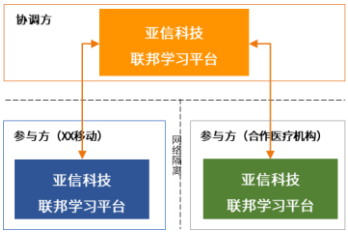

图**9-3** 部署方案示意图

通过基于纵向联邦学习的智能推荐模型，达到了以下应用效果：

- 在数据不出库的前提下，建立联邦学习模型架构，实现了某移动与合作医疗机构的数据虚拟打通。
- 打造专家咨询/极速问诊联邦推荐模型，实现精准营销，解决所有用户推荐同样内容的问题，点击率提升 10%，转化率提升 50%，累计查准率提升 10%。
- 后续逐渐扩充体检推荐、挂号医院推荐、医生推荐等，最终联邦移动数据实现不同用户登录 APP“千人千面”的目标。

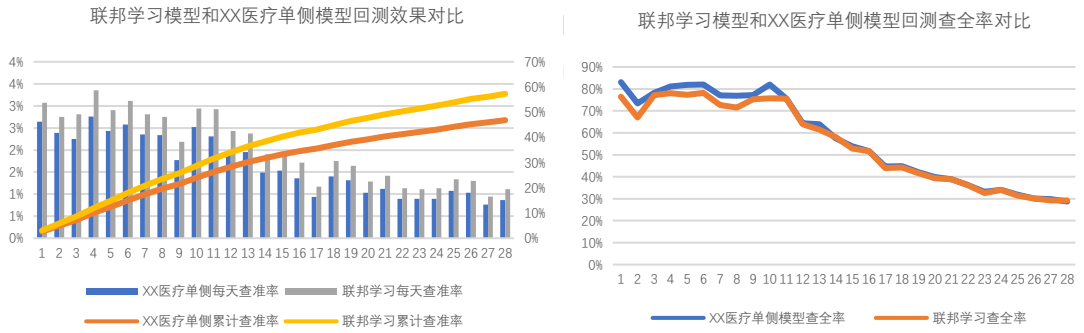

图**9-4** 联邦学习智能推荐模型效果

通过本案例的实施，为客户提供了以下业务价值：

- 基于联邦学习模型架构，打造某运营商与合作医疗机构在保证数据隐私安全前提下的跨域建模能力，赋能医疗智能推荐场景，实现对不同用户推荐专家咨询、极速问诊、体检等。
- 发挥周边数据（除基础通信数据之外的数据），特别是高质量数据（如客户征信信息、行为习惯等）的跨行业共享。
- 保证用户隐私和数据安全的前提下，将周边数据赋能给千行百业。

10 资质与荣誉

本节主要展示产品获得的资质及荣誉相关资料。

10.1 资质认证

- 国产生态兼容性认证

平台已获得海光 CPU/DCU 生态兼容性互认证。

图**10-1** 海光 **CPU/DCU** 生态兼容性互认证证书

- 通过中国信通院可信隐私计算评测

AISWare AI^2 FL 平台资源调度管理能力、数据处理能力、算法实现、应用效果和效能、平台安全性等方面全面达到标准和要求。

图**10-2** 国信通院可信隐私计算评测证书

- 隐私计算联盟组织成员单位

图**10-3** 隐私计算联盟组织成员证书

- 入选中国通信标准化协会首批隐私计算产业图谱

平台作为“电信级”一站式联邦学习服务开发与运行平台；采用联邦学习、多方安全计算、区块链等技术，提供低门槛、可视化的企业级联邦学习服务开发和运行能力；创新性地打造“运营商+”跨域协作新模式，助力各行业充分挖掘数据价值，赋能转型发展；于 2022 年入选信通院首批《隐私技术产业图谱 1.0》

图**10-4** 入选信通院首批隐私计算产业图谱

10.2 开源社区贡献

- **FATE** 社区首批成员单位

图**10-5 FATE** 社区首批成员单位

- 在 **FATE** 社区牵头成立多平台支持特别兴趣小组

联合微众银行、VMware、中国联通、中国移动、广电信安、艾瑞数智等机构，积极推动 FATE 社区成立多平台支持特别兴趣小组（SIG on Multiplatform），致力于推动 FATE 开源框架在多平台环境下的适配与优化，以确保其能在各种环境中稳定运行并发挥最佳性能。

成员	所属单位
袁志勇（Chair）	亚信科技
范涛（Co-Chair）	微众银行
姚云飞	亚信科技
高峰	联通数科
叶慧杰	联通数科
毕剑锋	中移信息
谢毅星	广电信安
苏志凌	艾瑞数智

图**10-6 SIG on Multiplatform** 成员名单

10.3 报告入选

平台在汽车行业的应用案例于 2023 年入选 Forrester《亚太地区隐私保护技术现状》报告。


TRENDS REPORT

The State Of Privacy-Preserving Technologies In Asia Pacific

Learn The Value Of Privacy-Preserving Technologies From Early Adopters

April 10, 2023

By Charlie Dai, Danny Mu with Enza Iannopollo, Tianchen Feng, Bill Nagel

FORRESTER

Summary

Privacy-preserving technologies (PPTs) help organizations reduce risk by giving them more granular control over the use of personal data. PPTs are quickly becoming popular for high-risk, high-value use cases that process strictly regulated personal data. Forrester believes that today's simple PPTs offer immediate benefits, but the ability to handle advanced use cases is at least two years away. This report helps technology leaders at firms in Asia Pacific (APAC) understand the current state of PPT adoption in the region and key considerations for implementation.

Vertical	Customer	Scenario	Tech partner	Description
	Tsingtao big data bureau	Secure public data exchange	BaseBit.ai	Use PPT, blockchain, and data sandbox to develop a public data exchange platform for government, financial institutions, and companies; raw data remains in the platform and data can be used but is invisible to all parties.
Retail	Chinese eCommerce firm	Marketing effect enhancement	Alibaba Cloud	In collaboration with an external media platform, use private set intersection to improve ad promotion ROI by 30%.
	Chinese eCommerce firm	Marketing effect enhancement	Volcano Engine	Use vertical federated learning to train data from marketers and the eCommerce platform to enhance deal conversion rates.
	Yum China	Marketing effect enhancement	4Paradigm	In collaboration with internet platforms, use vertical federated learning and an enhanced prediction model to improve new customer acquisition ratios and lower advertising costs.
Martech	Umeng	Multiparty data analytics	Ant Group	Realize joint and secure data joining and modeling with Ele.me and Didi to attain analytics data volumes on the order of billions of records.
Telco	China Mobile Group	Data interoperability enhancement	AsiaInfo	Combine secure multiparty computing and federated learning to create a secure, reliable data privacy circulation platform to support seamless integration of heterogeneous algorithms.
Automotive	Chinese automotive firm	Customer acquisition	Alibaba Cloud	Use federated learning to enhance seed ratings and improve store entering and deal ratios by 10%.
	Chang An Automobile	Marketing effect enhancement	AsiaInfo	Collaborating with telcos, use federated learning to improve the customer intent prediction model and increase intent rate by 60% and the area under the curve by 10%.

图**10-7** 入选 **Forrester**《亚太地区隐私保护技术现状》报告

10.4 标准贡献

AISWare AI^2 FL 产品参与了多个行业级标准贡献，以下列举部分：

序号	标准组织	标准名称
1	3GPP	5G 核心网元 NWDAF 的新型联邦学习技术标准
2	IEEE	P3117™ - 隐私保护计算互通框架标准草案
3	IEEE	P3127 区块链联邦学习
4	IEEE	P2986 隐私保护与反击

5	CCSA	TC1WG1-H-202104141929 联邦学习算法跨框架互操作的总体技术要求

10.5 专利贡献

AISWare AI^2 FL 产品参与了多项的国内外专利，下面为部分成果：

序号	专利名称
1	Federated learning in telecom communication system
2	一种支持异构可信协调方互联互通的纵向联邦学习方法
3	一种适配异构引擎的联邦学习训练流程编排的方法
4	PCT 区块链联邦学习
5	PCT 算力网络联邦学习
6	一种基于高维矩阵运算与同态加密算法融合的隐匿查询方法
7	算力内生网络的资源编排与调度方法及联邦学习应用

11 联系我们

亚信科技（中国）有限公司

地址：北京市海淀区中关村软件园二期西北旺东路 10 号院东区亚信大厦

邮编：100193

传真：010-82166699

电话：010-82166688

Email：5G@asiainfo.com

网址：www.asiainfo.com

Thank you

依托数智化全栈能力，创新客户价值，助推数字中国。