北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

联邦学习技术金融应用
白皮书

北京金融科技产业联盟
2022 年 3 月

版权声明

本报告版权属于北京金融科技产业联盟，并受法律保护。转载、编摘或利用其他方式使用本报告文字或观点的，应注明来源。违反上述声明者，将被追究相关法律责任。

编制委员会

主　编：

潘润红

编委会成员：

何　军　　刘承岩　　聂丽琴

编写组成员：

强　锋　　魏博言　　薛雨杉　　李宏宇　　黄翠婷　　昌文婷

陈天健　　李克鹏　　姚　明　　何　浩　　王湾湾　　李晶晶

李　博　　卞　阳　　方　竞　　袁鹏程　　赵　原　　王　磊

王云河　　陈　琨　　靳　晨　　范　涛　　刘筠璨　　吴博峰

赵　伟　　郝　洁　　彭宇翔　　孟　丹　　张明明　　毛仁歆

郭　超　　王　超　　金银玉　　单进勇　　蔡超超　　王　雪

李武璐　　霍昱光　　王健宗　　黄章成　　卢春曦　　陈嘉俊

张敬之　　曹旭涛　　窦永金　　许海洋　　陈　浩　　孙赞美

刘站奇　　张　雄　　薛瑞东　　陈　剑　　傅跃兵　　傅　杰

葛明嵩　　焦惠芸　　倪裕芳　　王铀之　　王煜惠　　王光中

杨　波　　邱晓慧　　胡师阳　　张育涵　　张　垚　　牛博强

何东杰　　周雍恺　　王　琪　　张晓武　　胡祎波　　陈浩栋

宋雨筱　　张亚申　　陈　鑫　　蒋嘉琦　　贾雪丽　　樊昕晔

朱德立　　唐剑飞　　夏正勋　　杨一帆　　陈　凯　　张骏雪

张健哲　　曹　伟　　郭　铸　　王润元　　徐安滢　　陈　俊

郭　林　　车春雷　　赵亚敏　　谢晨浩　　郑晓娟　　谢宗晓

黄雅琼　　张子怡　　张姗姗　　高志民　　王锐源　　孙中伟

袁　晨　　夏家骏　　段　兵　　林　凡　　解浚源

主　审：　黄本涛　　刘宝龙

统　稿：　郭　栋　　魏博言

参编单位：

北京金融科技产业联盟秘书处

中国工商银行股份有限公司

成方金融信息技术服务有限公司

同盾科技有限公司

深圳市洞见智慧科技有限公司

上海富数科技有限公司

蚂蚁科技集团股份有限公司

深圳前海微众银行股份有限公司

蓝象智联（杭州）科技有限公司

北京数牍科技有限公司

建信金融科技有限责任公司

深圳壹账通智能科技有限公司

浙商银行股份有限公司

北京国家金融科技认证中心有限公司

北京百度网讯科技有限公司

腾讯云计算（北京）有限责任公司

华控清交信息科技（北京）有限公司

北京融数联智科技有限公司

招商银行股份有限公司

北京瑞莱智慧科技有限公司

交通银行股份有限公司

北京银联金卡科技有限公司
中国民生银行股份有限公司
中国银联股份有限公司
云从科技集团股份有限公司
北京冲量在线科技有限公司
度小满科技（北京）有限公司
光大科技有限公司
星环信息科技（上海）股份有限公司
深圳致星科技有限公司
中国银行股份有限公司
中国农业银行股份有限公司
中国建设银行股份有限公司
京东科技信息技术公司
中金金融认证中心有限公司
华为技术有限公司
网联清算有限公司
上海光之树科技有限公司
北京火山引擎科技有限公司

目 录

名词术语

1. 特征(feature):数据提供者提供用于训练或计算的指标。
2. 标签(label):模型使用者提供的用于训练模型的目标数据。
3. 联邦算法(federated algorithm):联邦参与方使用的机器学习算法，一般由非联邦的机器学习算法演化而来。
4. 联邦模型(federated model):联邦参与方通过与其它联邦参与方共同训练生成的模型。
5. 联邦参与方(federated learning participant):提供联邦学习数据或作为建模发起者的组织或机构。联邦参与方角色有时候亦可分为Guest和Host。

   Guest: 一般是任务的发起方，在纵向联邦的场景中，一般为带有标签Y的一方，除了提供数据样本和标签外，还会负责任务的发起和主要调度等。

   Host: 也是数据提供方之一，纵向联邦场景中，一般是没有标签的一方，仅提供数据和协同训练推理
6. 联邦协调方(federated learning coordinator):为联邦参与方的活动提供协调、辅助等支撑功能的组织或机构，主要完成联邦过程中的辅助计算，不存储数据，有时候也成为Arbiter。

一、研究背景

近年来，数字经济蓬勃发展，已经成为带动中国经济增长的核心动力。2020 年 4 月，中共中央国务院发布了《关于构建更加完善的要素市场化配置体制机制的意见》，首次将数据与土地、劳动力、资本、技术等传统要素并列为生产要素。2021 年 12 月，中国人民银行发布《金融科技发展规划（2022—2025 年）》明确提出从强化数据能力建设、推动数据有序共享、深化数据综合应用、做好数据安全保护方面充分释放数据要素潜能。数字经济时代，数据成为新的关键生产要素，成为了社会基础性战略资源，蕴藏着巨大潜力和能量，必将成为提升金融行业赋能实体经济的有力抓手。

随着大数据技术的快速发展，人们每天的活动产生了大量的数据，这些数据被众多的企业收集和使用，数据在空间和时间里面流动产生了价值。在价值产生的过程中，需要对数据进行保护。但是数据往往分布在不同的企业、机构，形成了一个个数据“孤岛”。例如，在机构间，尤其政府部门，很多数据没有充分共享。又比如银行和税务，希望通过“银税合作”来获取客户的风险评估信息。在企业内部也是如此，集团化的企业公司越来越大，子公司、分公司，就连部门内部的系统都可能是自己分别开发的，数据之间完全孤立。为了挖掘数据中蕴藏的巨大价值，消除行业数据孤岛现象，让数据相互之间协作起来，必然是未来发展趋势。

数据在为人们的生活带来了种种便利的同时，也使得大家对于个人的数据隐私和安全产生了担忧，这俨然已经成为世界性的问题。各国针对这个情况，纷纷立法进行规范，例如：欧盟提出了《通用数据保护条例》(General Data Protection Regulation, GDPR)，该法案已于2018年起正式生效；我国也在近几年陆续颁布了《中华人民共和国数据安全法》和《中华人民共和国个人信息保护)》等法令法规，用以加强数据监管和隐私保护。可见，对用户数据隐私和安全管理的日渐收紧已经成为了必然的趋势。这就对企业利用数据开展业务提出了一个挑战。如何才能在遵循法规的要求下，既充分发挥数据的价值，同时又不会影响到用户的数据隐私和安全，尤其是对于依赖外部数据的企业，如何能够利用合作伙伴的数据价值，又不会见到原始数据，造成数据泄露的问题。

（一）概述

针对这一情况，近年来，学术界和工业界都已经开始在数据安全和隐私保护方向进行探索，尤其是在大数据、人工智能和密码学等领域。如何在满足数据隐私、安全和监管的前提下，设计一个机器学习框架，让人工智能能够更高效、更准确的共同使用各方数据成为了研究的核心。联邦学习(federated learning)、多方安全计算(secure multi-party computation，也叫安全多方计算)、知识联邦(knowledge federation)等领域成为学术界

和工业界关注的重点，其主要目的是利用多个参与方数据进行安全计算或训练。

1. 联邦学习的内涵

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，能够有效的解决数据孤岛、数据合规性以及两者的冲突，进而达到“数据可用不可见”的目标。

联邦学习从名字上看，有两个明晰的主题：学习和联邦。什么是学习？这个概念源自于我们谈论的数据和信息。数据一般被认为是原始素材，客观描述事物的数量、属性、位置等关系。信息则是经过加工处理之后、具有逻辑关系的数据，通常会是对决策有价值。学习的内容是知识，知识则更多是在信息上再进一步归纳演绎之后，沉淀下来的有价值的信息。通常情况下，学习到的知识被认为是与决策有关的。

从学习到联邦，其最终目的是希望通过一种安全的方式解决数据孤岛现象，达到“数据可用不可见”的目标。在联邦学习里，联邦本质上是一种安全协议下的数据交换共享，目的是有效利用各参与方的数据来进行知识的共创、共享和推理。

2. 联邦学习的外延

联邦学习与很多技术有一定关系，比如可信执行环境、密码学、隐私计算。例如，可信执行环境是一种芯片级的硬件安全计算技术，联邦学习可以依靠这种方式来实现更高的硬件层面的安全性能。如表 1 所示，列举了在联邦学习中涉及到的密码学相关技术和算法。

表 1. 联邦学习中涉及的密码学相关技术

相关技术	方法
同态加密算法	联邦学习常使用的加法同态加密算法是 Paillier 算法[1]、EC-ElGamal 算法。
密钥交换协议	联邦学习常使用 Diffile-Hellman 进行密钥交换[2]。
安全伪随机数生成算法	NIST.SP.800-90 标准中规定了四种安全伪随机数生成算法 Hash_DRBG，HMAC_DRBG，CTR_DRBG 和 Dual_EC_DRBG。联邦学习常使用 HMAC_DRBG 算法[3]。
一次一密算法	联邦学习使用一次一密算法时，先将待加密的数值转换为整数，然后与密钥相加或相减，解密时需要再将整数转换为浮点数。由于密钥需要参与方在线生成，所以一次一密通常要调用密钥交换协议和安全伪随机生成算法。
格式保留加密算法	联邦学习常使用 NIST.SP.800-38G 标准中的 AES-FF1 算法[4]。
OT 协议（不经意传输）	联邦学习常采用的 1-n 的 OT 协议方法参考文献[5]。

3. 数据可用不可见

数据可用不可见，即充分利用各方的数据，让数据保持对外开放，同时能够让数据不直接共享，不离开机构或个人。

为了实现“数据可用不可见”这个目标，传统的中心化计算模式，也就是大数据经常会做的中心化聚集，把数据存储聚集再做训练，已经不能满足合规性的要求。中心化不可行，那就让数据分散在各个机构中，采用分布式或者去中心化方式计算或学习。

原始数据直接共享不可行，我们可以采用两种方式，第一种方式是对数据进行加密，加密后也不破坏原始数据的统计特征。第二种方式，参与计算的原始数据均不出域，只在自己的节点内部进行计算，模型训练交互的只是中间的计算结果。从而达到数据不出门，保护用户隐私数据，同时能够完成联合建模，打破数据壁垒，实现数据的可用不可见。

需要注意的是，“数据可用不可见”并不等同于个人信息告知同意，也就是说当我们在使用联邦学习进行学习任务时。当触及到敏感个人隐私数据的时候，依然要确保获得个人信息主体对其信息进行特定处理的授权同意或明示同意。

（二）标准情况

国际上，现有联邦学习标准有:

IEEE 发布的 IEEE/P3652.1-2020：IEEE Guide for Architectural Framework and Application of Federated Machine Learning，联邦学习基础架构与应用指南

国内，现有联邦学习标准主要为团体标准。由中国信息通信研究院发布的《基于联邦学习的数据流通产品技术要求与测试方法》（BDC 41-2020）；由中国人工智能开源软件发展联盟发布的《信息技术服务 联邦学习 参考架构》（AIOSS-03-2019）；由中关村金融科技产业发展联盟发布的《联邦学习金融行业应用指南》（T/ZFIDA0004-2020）。

近期，北京金融科技产业联盟推动制定联邦学习金融应用技术规范，将从联邦学习的系统技术框架、功能要求、非功能要求、安全要求方面对联邦学习在金融场景的应用进行技术层面的规范。由于联邦学习不是一个单方应用的技术，而是多方协同运行使用数据的技术。亟需制定行业内的联邦学习技术的应用规范或标准，规范化联邦学习应用流程和数据交换协议。

二、联邦类型

（一）数据视角

根据参与各方数据源分布的情况不同，联邦学习可以分为横向联邦学习、纵向联邦学习、联邦迁移学习 3 类。

1. 横向联邦学习

在两个数据集的用户特征重叠较多而用户重叠较少的情况下，可将数据集按照横向(即用户维度)切分，并取出双方用户特征相同而用户不完全相同的那部分数据进行训练。这种方法称为横向联邦学习，或跨样本联邦学习，如图 2.1 所示。

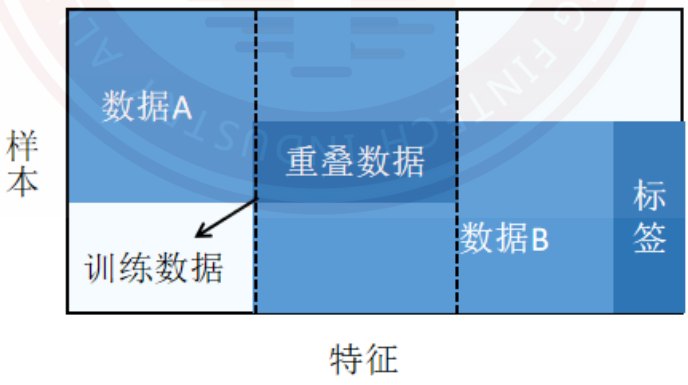

图 2.1 横向联邦示意图

在实际场景中，对业务相同但是分布在不同地区的两家企业而言，用户群体分别来自各自所在的地区，相互的交集很小但业

务相似，记录的用户特征项相似度较大。此时，就可以使用横向联邦学习来构建联合模型。

2. 纵向联邦学习

在两个数据集的用户重叠较多而用户特征重叠较少的情况下，可将数据集按照纵向（即特征维度）切分，并取出双方用户相同而用户特征不完全相同的那部分数据进行训练。这种方法称为纵向联邦学习，或跨特征联邦学习，如图 2.2 所示。

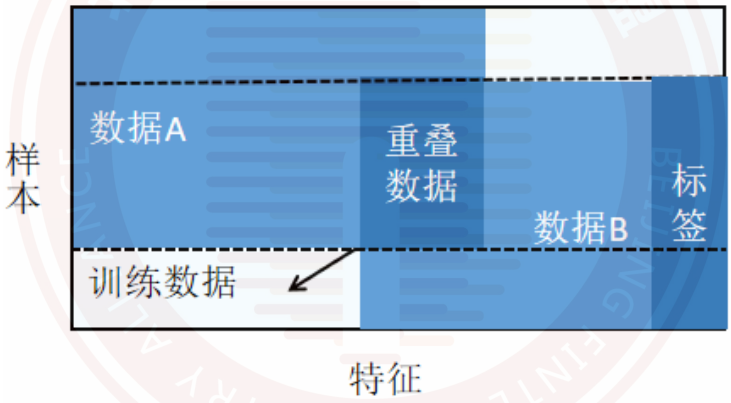

图 2.2 纵向联邦示意图

目前金融机构中的联邦学习，纵向联邦学习较为普遍。例如，在银行与某运营商之间的用户群体交集较大，但是，由于银行记录的都是用户的收支行为与信用评级，而运营商则具有用户的通信行为和网络行为，因此两者的用户特征交集较小。纵向联邦学习就是将这些不同特征在加密的状态下加以聚合，以增强模型能力的联邦学习。

3. 联邦迁移学习

在两个数据集的用户与用户特征重叠都较少的情况下，不对数据进行切分，而利用迁移学习技术来克服数据或标签不足的情况。这种方法称为联邦迁移学习，或复合型联邦学习，如图 2.3。

图 2.3 联邦迁移学习示意图

在机构间合作中，纵向联邦会更常见，因为各家机构间特征互补可对业务形成更全面的试图。尤其是有些发起方在业务实践中积累了一些标签和少量特征，需要更多外部特征才能得到理想模型。此时不仅仅要保证特征数据的安全，还要防止标签数据的泄漏。而且由于模型需要用多方数据才能训练，模型推理时也同样需要多方数据才能完成，这也就意味着纵向联邦在生产环境还需要联邦推理。

而横向联邦往往发生在同业或个体之间。尽管由于行业竞争的原因，很多大型机构不愿与同业进行联邦，但是很多中小型机构迫于生存压力期待加入联邦来提升行业竞争力。跨样本联邦中，由于用户特征数据和标签都是在同一个参与方内，可以直接在内部计算或训练，因此安全问题主要集中在模型汇集和更新中。此外，横向联邦的模型推理过程无需多方参与，因此不存在类似于纵向联邦推理的安全问题。

（二）参与方视角

在实际应用中至少有两个参与方才能组成联邦，联邦中是否需要有协调方取决于联邦架构设计模式。在联邦学习中，主要由以下角色协作完成联邦学习任务。

（1）数据方

数据方需通过 CA 认证方进行认证，以保证数据的真实性与正确性。通过认证的数据方可对外发布数据资源。其他跨平台参与节点经授权后，可发现这些由获得可信认证的数据方发布的数据，并通过授权申请参与到跨平台的联邦学习任务。

（2）算法方

算法方提供的算法以算法组件和算法描述的形式输出。算法组件是满足互联互通标准定义下可执行代码，包括计算逻辑和算法参数，算法描述，包括算法的版本号以及兼容性说明，描述可以运行的计算环境、依赖的底层算子、适用的场景和兼容的版本

信息等。算法组件在兼容性上要满足算法组件的热插拔和算法组件的管理能力，根据算法交换协议，可以在不同联邦学习系统中迁移和部署算法组件。

算法方提供的算法应获得安全性认证，通过认证后的算法可通过热插拔组件的方式在跨联邦学习平台部署。部署在不同联邦学习平台的相同算法组件，可通过互联互通管控协议和互联互通计算协议，共同完成跨平台的联邦学习任务。

（3）调度方

调度方通过调度数据方、计算方、算法方等多个参与角色完成联邦学习任务，在跨联邦学习平台互联互通中，调度方应获得可信第三方的认证，确保调度方的可信性、安全性与正确性。

（4）计算方

计算方在联邦学习互联互通要求下，应保证可扩展性和兼容性，可执行来自不同平台满足互联互通协议要求的算法组件。计算方应在获取安全认证的基础上执行与其他跨平台参与方的协同计算，确保任务执行过程不会造成隐私数据泄露。

（5）结果方

结果方获取结果时应通过安全认证确保结果获取的合规性。在进行联邦学习之前，根据互联互通协议约定结果方，整个计算过程应按照约定的要求，只有结果方才能获取计算的最终结果，其它非结果方不能获得结果，也不能通过中间计算过程，计算或推断出最终结果。

（6）任务发起方

任务发起方应获得可信认证，才可触发跨联邦学习平台的任务。

（7）CA 认证方

CA 认证方为联邦学习参与方、节点、算法、平台等提供认证的角色。

各方之间进行通信时，需要建立双向的身份认证机制，保证各节点间通信安全的前提下，建立互联关系和访问授权。

CA 认证方，需要按照《金融业务 证书管理》（GB/T 27928-2011）和《金融电子认证规范》（JR/T 0118-2015）中的相关要求，使用自建或由第三方权威机构提供的证书认证中心服务，CA 认证方的功能活动包括：

（a）支持对证书的有效期、授权对象、秘钥管理、证书签发、证书撤销等操作；

（b）对联邦学习中的各个参与方，算法方、数据方、调度方、计算方、结果方、任务发起方等区分不同的角色，并对不同的角色颁发能够区分角色的数字证书，数字证书应与结算标识相关联，并且具备唯一性；

（c）对于联邦学习中的各种资源，应分别对不同资源进行授权，比如模型资源、算法资源、数据资源等，数字证书需要标识其资源版本和相关的描述信息。

（8）可信存证方

在互联互通的联邦学习系统中，作为可信存证方，应获取可信认证。联邦成员中的参与方不仅是联邦需求的提出者，往往也是数据提供者，因此，参与方的数量和质量决定是联邦生态是否能顺利建设和良性发展的关键因素之一。当参与机构（数据提供者）足够多，联邦规模足够大，数据多样性就有保障，也就会吸引更多机构（数据使用者）愿意来使用联邦服务，也会有更多科技型机构(模型和应用开发者)来提供丰富的算法、模型和应用。

联邦学习系统的每个实体参与节点可以承担一个或多个角色。联邦学习的任务发起方可以是数据方之一，也可以同时是计算方、协调方、算法方或者结果方。数据方和计算方通常具有多个，分别处于不同的管理域。数据方提供联邦学习参与计算的数据；计算方执行联邦学习过程的计算任务，包括数据接入、结果存储、计算任务管理、计算任务执行、错误处理、运行监控等。算法方提供联邦学习的算法逻辑，可以由独立的算法方提供，也可以由参与计算的各方共同提供。协调方承担联邦学习任务的协调、调度等功能，在某些架构中，甚至包含密钥分发与解密等功能。结果方获取联邦学习的训练结果，通常是任务发起方，同时经协商，也可以是其他的参与方。可信存证方为联邦学习过程的任务、参与计算的数据、计算流程及计算结果等提供存证功能。CA 认证方为联邦学习的参与方和平台的算法等提供安全认证。CA 认证方和可信存证方，可由联邦学习系统的内部节点提供，也可以在联邦学习系统以外，以外部角色参与的联邦学习任务中。

（三）架构视角

由于联邦学习通常是解决多数据方之间寻求计算结果的问题，在具体架构中，会根据需要引入可信第三方来作为协调方，承担辅助计算模块，包括提供公私钥分发、加解密等服务，或提供计算能力等，辅助完成既定的学习目标。可信第三方可以承担算法方、调度方、计算方、CA 认证方、可信存证方等参与方中的一种或多种。

从具体架构视角，按是否引入可信第三方进行区分，可将联邦学习架构分为无可信第三方模式和有可信第三方模式两种模式，见图 2.4 所示。

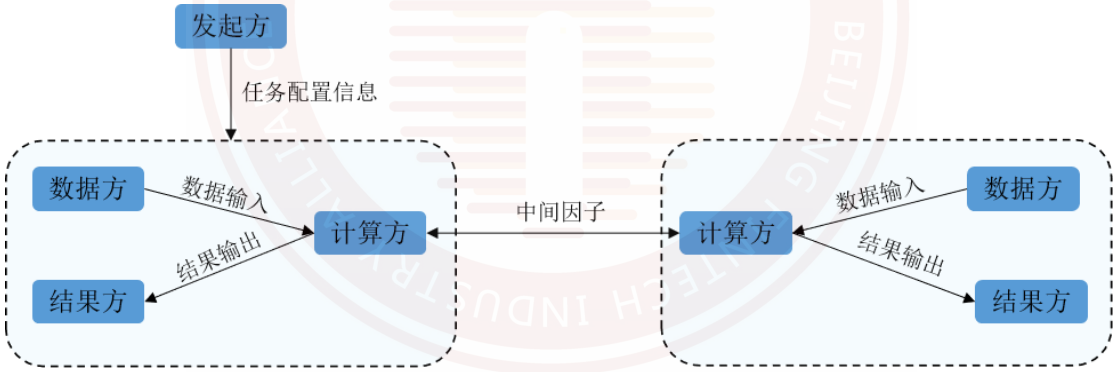

图 2.4 无可信第三方的架构

无可信第三方模式目前有两种技术实现路径：一种基于多方安全计算（MPC）协议，在 MPC 基础算子和函数算子之上实现协同机器学习，达成联邦学习效果；另一种仍保留原有联邦学习算法架构，本地明文计算与基于同态加密或 MPC 协议汇聚计算相结合的模式训练联邦学习模型。

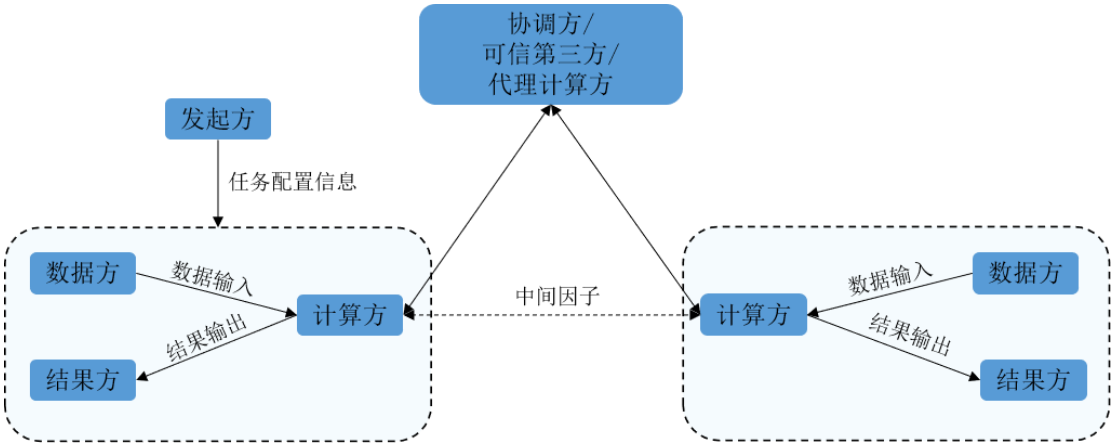

图 2.5 有可信第三方的架构

如图 2.5 所示，在有可信第三方架构模式中，联邦学习依赖第三方参与，一方面通过可信第三方（通常是协调方）执行约定的规则，并辅助参与方之间进行信息传输交换，中间结果汇算等；另一方面，可信第三方还可以进行联邦任务管理，统计各方调用量，制定贡献度模型和激励机制，推动建立共赢的联邦学习生态系统。可信第三方一般并不汇集和存储原始数据。

考虑到机构间进行联邦时，在业务合作上很难找到一个独立可信的第三方机构作为协调方的角色，无可信第三方的架构从技术层面保证了数据安全性从而达到商业信任，但可能需要更多的计算操作来对消息内容进行加密和解密，同时可能会带来大量或额外的基础设施建设成本，在一定程度上限制了联邦学习的市场拓展和产品化进程。因此，在金融或政务领域，有时会更关注可监管性，可使用一个各方都认可的带监管性质的协调方服务器参与联邦。

（四）建模视角

与传统的联合建模或机器学习流程类似，联邦建模的过程也大致可划分为如图 2.6 所示的三个阶段，包括联邦数据探查、联邦模型训练和联邦模型推理。

图 2.6 联邦建模流程

1. 联邦数据探查

联邦数据探查，包括联邦数据预处理、联邦隐私求交、联邦特征相关性、联邦分箱、联邦特征选择等技术，作为联邦学习建模的辅助基础功能。

其中联邦特征预处理包括数据的缺失值处理、异常值处理、特征转换、格式转换等多种特征预处理功能。

联邦探索性分析，是一种分析数据集以概括其主要特征的方法，通常可使用可视化方法，包括对特征的分布情况、最大值、最小值、缺失值情况、异常值情况、均值、方差等提供分析视图。通过这些分析指标，可以让建模人员了解数据集，和对数据集进行验证来确定所获得数据集可以用于接下来的联邦机器学习中使用。

联邦特征相关性分析是对参与联邦学习任务的特征进行特征与目标变量之间、特征与特征之间的相关性分析，主要的分析指标为 IV 值、WOE 值、VIF 值、Pearson 相关系数等。这些特征的相关性分析有可为后续的联邦特征筛选提供参照指标。同时在相关性分析的过程，可完成对特征的分箱操作。

2. 联邦模型训练

联邦模型训练是基于联邦化的机器学习算法对样本集进行模型训练的过程。包括了联邦模型调参、联邦模型训练、联邦模型评估的功能。其中联邦模型调参，通常具有与传统机器学习算法同样的参数进行配置。而联邦模型训练过程，通常可分为自治和联合两部分。自治的部分：首先，两个或两个以上的参与方们在各自终端计算初始化的模型，由于参与方们拥有不同的数据，各方所训练的模型也拥有不同的模型参数，并且不具有全局收敛性。联合的部分：各参与方加密联合计算梯度值、损失函数，并使用最新一轮中间值开始下一次的本地迭代。以上的程序会一直重复，直到整个训练过程的收敛。而联邦模型训练通常可以支持回归算法、树类算法、聚类算法、神经网络算法等。此外，联邦模型训练结束后，需要模型评估功能为训练得到的联邦模型进行评估，例如提供 KS 值、AUC、准确率、召回率、F-Score 等模型评估指标。

3. 联邦模型推理

联邦学习任务结束后的得到的联邦模型，要应用到实际金融场景中，需要通过联邦推理功能。联邦模型训练是通过从已有的数据中学习到某种能力，而联邦推理则是基于已有的联邦模型，和数据的特征值得到推理的结果。联邦模型推理通常包括基于单个样本 ID 的实时模型推理，以及基于多个 ID 的批量模型推理能力。其中实时模型推理能力通常要求高时效来满足实时业务场景的需求。

三、联邦学习建模流程

（一）联邦数据探查

1. 联邦数据预处理

联邦数据预处理可以分为线下数据预处理和线上数据预处理两个部分。其中线下数据预处理指联邦训练的参与方需要在数据加载之前将己方数据格式规范化，各方需要事先约定好输入数据的表头格式及内容，ID 格式，对应特征格式。

线上数据预处理包括联邦隐私求交，特征相关性计算，特征分箱，特征选择与过滤，特征缺失值处理，特征编码，特征降维，联邦特征稳定性计算等。

（1） 联邦学习数据中的缺失值，一般可以通过删除缺失行或利用联邦插值的方法进行填补。

（2） 联邦特征稳定性（Population Stability Index）是金融场景中衡量建模特征有效性的重要指标，体现了某一特征随着时间推移的波动程度。一般来说，联邦特征稳定性需要在建模之前对特征进行考量，当训练数据收集时间跨度较大，或推理数据与训练数据收集时间相差较大时，需要首先对每列特征的稳定性进行考核筛选。

在纵向联邦学习场景中，某一特征的数据由一方完全持有，可以直接采用本地计算的方式进行考核。而在横向联邦学习场景中，各数据源持有一部分特征，各数据源可先将本地特征按照取值大小等频分段，利用同态加密，多方安全计算等方法进行联邦特征稳定性计算。

2. 联邦隐私求交

在纵向联邦学习应用中，必须确保各个参与方对相同的样本群进行建模。在数据准备过程中，联邦应用需求方通过样本 ID 寻找与其他参与方之间的样本 ID 交集，即共同拥有的样本 ID 的集合。同时保护交集以外部分的样本 ID。

3. 联邦特征相关性

皮尔森相关系数也称皮尔森积矩相关系数(Pearson product-moment correlation coefficient)，是一种线性相关系数，是最常用的一种相关系数。皮尔森相关系数用来反映两个变量 X 和 Y 的线性相关程度，r 值介于-1 到 1 之间，绝对值越大表明相关性越强。

$$\rho_{x,y}=\frac{\mathrm{cov}(X,Y)}{\sigma_x\sigma_y}=\frac{E\left((X-\mu_X)(Y-\mu_Y)\right)}{\sigma_X\sigma_Y}=\frac{E(XY)-E(X)E(Y)}{\sqrt{E(X^2)-E^2(X)}\sqrt{E(Y^2)-E^2(Y)}}$$

两个连续变量(X,Y)的皮尔森相关系数等于它们之间的协方差 cov(X,Y)除以它们各自标准差的乘积(σ_x, σ_y)。系数的取值总是在-1 到 1 之间，接近 0 的变量被称为无相关性，接近 1 或者-1 被称为具有强相关性。

联邦特征相关性主要指应用于纵向联邦学习的特征相关性计算。

4. 联邦分箱

应用于在金融应用场景建模之前的数据预处理过程，将连续特征离散化，离散化后的特征可以提高模型的鲁棒性。如果联邦分箱需要利用标签信息指导分箱过程，那么它就是一种有监督的联邦分箱。这种有监督的联邦分箱在纵向联邦中应用较多。

5. 联邦特征选择

应用于模型训练前，通过算法筛选掉冗余或建模效果差的特征，从而提高建模效果以及加快训练速度。

6. 联邦特征编码

特征编码可将字符型特征或者分类类型特征进行特征编码，有利于提升模型效果。在不泄漏参与方的特征数据及标签数据情况下，完成联邦的特征编码。

（二）联邦模型训练

联邦模型训练的目的是要从多个参与方数据中学习一个模型，如果是有监督学习，则至少有一方提供标签数据(Y)。

联邦模型训练是利用参与方提供的数据计算模型参数，使模型函数结果逼近标签 Y。对于线性回归、逻辑回归等算法，横向联邦的模型训练过程相对比较简单，而纵向联邦会比较复杂。尽管联邦训练中数据交换过程会因采用的模型不同而变化，但是联邦训练对数据安全的要求基本是一致的，保证在数据交换的过程中不泄漏参与方的训练数据、不泄漏参与方的模型参数，同时也不泄露标签数据。常用的模型有线性回归、逻辑回归、树模型、神经网络模型，而每种模型根据联邦类型还分横向联邦和纵向联邦。

（三）联邦模型推理

联邦模型推理的目的是基于联邦模型训练得到的模型，得到待推理样本集合的推理结果。

联邦模型推理分为两种情况，横向联邦推理和纵向联邦推理。其中在横向联邦场景下，各参与方拥有完整联邦模型以及完整特征向量，因此可以在本地完成联邦推理。尽管联邦模型推理涉及的数据交换具有多种表现形式，但联邦模型推理对数据安全的要求基本是一致的，保证在数据交换的过程中不泄漏参与方的待推

理数据，也不会泄漏参与方的模型参数。常用的模型有线性回归、逻辑回归、树模型、神经网络模型，而每种模型根据联邦类型还分横向联邦和纵向联邦。

四、安全与审计

（一）安全性分析

1. 联邦学习计算安全

（1） 联邦学习的安全特性

基于各类联邦学习的特点，提炼联邦学习的安全性包含隐私性、正确性、可用性三个方面。

（a） 隐私性

隐私性是指需要保护输入数据的机密性、输出结果的机密性。这里的输入数据机密性跟传统安全领域的机密性略有区别，机密性可以是指不泄露输入数据任何信息的完全机密性，也可以是泄露部分信息的非完全机密性。某些应用并不要求完全的机密性，允许暴露输入数据的部分信息。输出结果的机密性是指只有指定结果方才可得到指定的结果。一个联邦学习应用中，可能输出多个结果数据，可能有多个结果方，每个结果方应得到的结果数据可以不同也可以相同，一个结果方应得到的结果数据可以是所有结果数据也可以是部分结果数据。

（b） 正确性

正确性是指联邦学习结果的正确性。这里的正确性跟传统安全领域的完整性略有区别：某些应用并不要求完全的正确性，而是允许一定精度的误差，引入一定精度的误差也是差分隐私这一联邦学习技术的要求和某些应用实现隐私保护的必然要求。

（c） 可用性

可用性是指联邦学习的结果方能得到联邦学习的输出。

（2） 联邦学习的安全攻击

（a） 合谋攻击

参与方（包括平台方）其中两个或者多个合谋，去推导出其他方的明文数据。

（b） 选择函数攻击

攻击方通过计算一个不安全的函数，从而推导出对方的明文数据信息。

（c） 差分攻击

攻击方通过不同的数据跟合作方进行某种多次联邦学习，拿到结果后，推导出想要的差异数据部分的明文数据。

（d） 侧信道攻击

通过联邦学习过程的各种运行时信息推测密文信息。

（e） 伪造数据攻击

由于联邦学习数据不可见特性，参与方可能会提供假数据参与计算，造成非预期的计算结果。

（f） 彩虹表/穷举攻击

安全参数或者算法本身的密文空间过小导致现实时间可破解。

（g） 额外信息泄露攻击

由于算法缺陷/弱点，计算的一些中间结果，从中间结果可以推测出原始数据的一些敏感信息。或者由于算法缺陷/弱点，原始数据的部分信息暴露。

（h） 计算结果泄露攻击

由于算法设计缺陷/弱点，计算结果输出给了非结果方。

（i） 恶意构造输入攻击

攻击者通过特殊构造的输入，使得可以从计算结果中获得对方的数据。

（j） 偏离协议攻击

攻击者不按约定的协议执行，从而破坏计算结果，且可能从计算结果中获取对方数据；攻击者也可通过不按约定协议执行使得协议执行失败，让全部或部分结果方无法得到计算结果。

（3） 联邦学习的计算安全分级

计算安全要保护的是两部分内容：个人隐私和数据的商业价值。原始数据的泄露肯定会导致个人隐私和数据商业价值的泄露，这也是联邦学习要解决的问题。

计算安全是针对计算过程的安全控制手段，与传统安全面对的问题不同，计算安全针对的是参与者的攻击，是联邦学习技术与传统机器学习技术最重要的差别点，为了规范联邦学习的安全性，适应不同场景的安全水位要求，在此对计算安全进行了分级。

联邦学习的攻击后果是指参与方通过中间信息反推、或者不遵守协议能够获得数据的隐私信息或者拿到数据的商业价值。

从防御强度方面，将联邦学习的安全性分为五级：

第一级安全要求：计算所需的原始数据未进行传输交换；不针对参与方发起的基于中间信息的反演攻击布置安全防御机制。

第二级安全要求：旨在概率性的保护有参与方进行半诚实攻击时的信息安全。在半诚实安全模型假设下，应可以计算出参与方不能从中间信息反推原始数据的概率。

第三级安全要求：旨在保护有参与方进行半诚实攻击时的信息安全。在半诚实安全模型假设下可证安全，参与方无法获得敏感数据。

第四级安全要求：旨在保护有参与方进行恶意攻击时的信息安全。在恶意安全模型假设下可证安全，攻击方获得敏感数据的概率极小。

第五级安全要求：旨在保护有参与方进行恶意攻击并且多个攻击方合谋时的信息安全。在恶意安全模型假设下可证安全，多个攻击方发起合谋攻击获得敏感数据的概率极小。

其中，非敏感数据是指不泄露用户隐私和商业价值的数据统称为非敏感数据，非敏感数据需要通过枚举进行定义。不属于非敏感数据的统称敏感数据。

2. 联邦学习业务安全

（1） 从业务场景来划分

（a） 高安全等级业务

智能风控

基于联邦学习，可以实现数据融合、联合建模以及模型发布一体化方案，实现大数据风控能力，提升风控效果。

在小微企业信贷这一特定场景中，联邦学习能够发挥较大的作用。在面对小微企业信贷需求时，经常出现因为缺乏企业经营状况等有效数据，而导致小微企业融资难、融资贵、融资慢的问题；针对小微企业企业信贷评审数据稀缺、因为不全面、历史信息沉淀不足等问题，通过联邦学习机制融合多源数据，丰富特征体系，银行可有效地节约信贷审核成本，提升信贷风控能力。

反欺诈

依托联邦学习技术等前沿技术，可打通银行间、银企间存在的数据孤岛，基于金融特征、交易特征、行为特征和干系人特征等信息构建联合反欺诈体系，共同提升银行业和其他企业反欺诈

能力。针对银行业当前面临的主要欺诈风险和联邦学习技术特点，可重点建设金融同业反欺诈业务场景。

大型银行已具备成熟的反欺诈能力和金融数据样本，反欺诈服务平台保证在数据资产、模型资产不外流的情况下，将大型银行积累的欺诈黑样本特征如欺诈交易、欺诈账户、恶意设备等信息通过共建模型的方法向中小银行输出，一方面弥补了中小银行欺诈样本少和反欺诈能力不足的缺陷；另一方面通过对同业欺诈数据的整合，将更多样的欺诈数据特征纳入共建反欺诈模型，提升了银行业整体反欺诈能力。

反洗钱

随着国际反洗钱监管环境日趋严苛，国际联邦反洗钱的各参与方希望在不泄露各自样本的前提下，充分利用跨国多家合作方的反洗钱样本，在可疑活动监测、客户尽职调查与监察名单筛选等模型中利用联邦学习框架，建立较单方样本训练效果更好、更稳健的联邦反洗钱模型，以降低罚款和声誉受损等业务风险。

（b） 低安全等级业务

智能营销

联邦学习可以提供精准权益策略，高风险识别率的安全合规共享环境。通过数据分析，能够对用户进行细分，实现对用户的精准画像和风险分析，实现“千人千面”的精准营销策略。如，银行/保险/互联网消费金融业务精准营销转化。

智能化运营

通过联邦学习、多方安全计算、隐私信息检索等隐私计算手段，安全合规利用第三方的数据，实现对存客的全维度用户画像，实现客户分群、客户特征描述、产品需求偏好分析等，充分发掘客户与金融机构间的关联行为以及需求状况，实现特定群体 客户向特定业务的引流，或促活效率的提升等。

（2） 从业务数据授权角度划分

根据金融行业实际应用场景来看，不同数据方对用户授权管理水位不同，这对业务安全性会有一定的影响。一般来说，联邦模型推理过程基本均需要用户授权，联邦模型训练过程不同场景差异较大，现根据模型训练过程各方数据所需授权强弱进行分类：

（a） 模型训练过程中无需用户授权，将 ID 信息隐去，便可以将多方本地数据直接进行训练模型。

（b） 模型训练过程中无需用户授权，将 ID 信息隐去同，还需将原始数据做一定脱敏操作才可用于模型训练。

（c） 模型训练过程数据需要用户授权。

上述业务场景数据安全性逐级增高。

3. 联邦学习平台数据安全

（1） 安全存储

联邦学习平台通常提供文件、数据库两种数据存储方式。为最大程度的保障数据安全，平台方需在数据上传环节提供数据加密及数据脱敏选项，以确保元数据、明细数据不会泄露任何个人用户隐私信息。

关于数据加密，平台方应提供秘钥生成服务，服务方授权平台对数据进行加、解密操作，服务方上传数据时对数据加密，解密后的数据即刻使用不做存储。

关于数据脱敏，服务方上传数据时，可以根据数据敏感情况对不同的字段执行不同类型的脱敏操作。协调方应提供的脱敏方式包括:

（a） 数据抽样、数据聚合等统计技术;

（b） 屏蔽、局部抑制、记录抑制等抑制技术;

（c） 噪声添加等随机化技术。

（2） 数据授权

数据授权是指在使用联邦学习平台过程中数据使用方(即数据需求方或结果获取方）使用数据前，需获取数据提供方授权，方可进行相关授权操作。数据提供方授权的内容包括但不限于授

权使用内容，授权使用领域和范围，授权使用时间，知识产权归属等。

数据使用方发起数据使用申请后，只有得到了数据提供方的审批同意，相关任务才可以启动执行。在实际业务中依据数据授权对数据安全的影响，以及所有任务申请及任务审批的存证方式有如下划分：

（a） 低安全等级：在系统后台做数据留存；

（b） 中安全等级：在第三方中立机构存证；

（c） 高安全等级：在区块链存证，确保数据授权信息未篡改、可追溯、可信任。

（二）审计功能

1. 功能概述

联邦学习系统通过存证记录或实时抽取参与方本地或交互数据的原始值或信息摘要，实现审计功能。其形式主要包括：利用存证等方式对任务进行记录，可在任务结束后针对某一参与方的权限、数据、行为等情况进行事后审计；对运行任务中的数据信息进行抽取，进行实时审计等。审计功能所应用的阶段包括联邦学习训练和推理环节。其目的为实现联邦学习任务的可核查性、可复现性、不可抵赖性，从而监督各参与方诚实、可靠地参与联邦学习任务。

2. 审计内容分类

（1）联邦学习参与方权限审计

在联邦学习任务执行过程中，应按照参与方的角色对其所拥有的权限进行划分。审计功能应以最小授权原则为基准，保证各方无法获取非本方应获取范围外的信息、无法进行本方权限外的操作，从而降低隐私泄露风险。对于联邦学习中的数据需求方、数据提供方、结果获取方、调度方等角色，应按照对其承担职责的定义，确认各自拥有的权限。

（2）联邦学习代码审计

对于联邦学习中各方所使用的代码或功能模块应支持审计功能，从而确保各方使用安全可靠的联邦学习功能，未被恶意篡改。

（3）联邦学习数据审计

对于联邦学习任务中各方使用数据应提供审计功能，从而确保各参与方使用真实、可靠的数据。此外，对于数据的不同信息应分多级进行权限设置（如数据具体内容、数据样本量、特征情况等），即数据信息应可针对不同参与方的权限、角色进行暴露。

（4）联邦学习计算过程审计

对于联邦学习任务各参与方接收和发送的信息应提供存证审计功能，从而确保联邦学习建模过程中各参与方交互的中间信息真实可靠，包括但不限于：随机数、三元组、加解密秘钥、加密中间结果等。

（5）联邦学习模型审计

对于联邦学习训练任务各参与方所获得的模型，应可进行审计操作，从而确保在后续联邦学习推理任务中各方使用正确、未经修改过的子模型。

（6）参与方操作行为和任务状态审计

对于联邦学习任务执行过程中各参与方的操作及任务运行指标、状态等信息，应提供审计管理功能，从而对各参与方的操作行为及运行情况进行检查，避免恶意操作的发生。

3. 审计实现方式

为实现审计功能，首先要通过本地存储、区块链存证、数据抓包等方式对审计的内容进行获取，从而进行事后或实时审计操作。

审计功能应在最小化暴露信息的前提下对各参与方提供、访问、使用的数据内容或信息摘要进行记录。对于敏感信息，原始数据的存储可能会暴露各参与方隐私，应采用信息摘要作为审计的内容。

对于各方本地产生的数据或接收到的数据，在保证执行与待审计任务过程一致的情况下，获取相同的处理数据，则认为该审计操作与之前一致。对于密文等无法获取数据具体信息的情况，

可通过校验摘要信息（如哈希、md5 值等）的方式在不需解密的条件下判断是否一致。对于无法获取与原始结果一致的情况，认为该步骤的执行方存在作恶的嫌疑。

此外，审计功能应包含在线审计与离线审计两种方式。具体区别为：在线审计需要原始任务全体参与方重新共同执行任务，通过新生成的信息与所存证的信息比对进行审计判断；离线审计仅需嫌疑作恶方参与，利用其本地存储的联邦学习计算过程信息即可独立完成审计任务的执行。

4. 可信第三方机构参与作为审计方

对于联邦学习任务存在纠纷的情况，可利用审计功能检查各方有无作恶行为。当联邦学习任务参与方无法承担审计执行方时（如审计执行过程可能造成某一参与方隐私额外泄露等），可由监管机构等权威、公正第三方承担审计任务，并且第三方机构应保证对于审计过程所获取的信息不向非必要知情方透露。

五、金融应用要求及案例

（一）应用性能指标

1. 精度指标

联邦学习的精度指标，即模型本身常用的效果评价指标，主要有以下几种:

（1） **ROC:** 模型打分时将正例分数排在负例前面的概率。

（2） **AUC:** 是衡量学习器优劣的一种性能指标，AUC 可通过对 ROC 曲线下各部分的面积求和而得。

（3） **伪阳性率(FPR):** 判定为正例却不是真正例的概率，即真负例中判为正例的概率。

（4） **真阳性率（TPR）:** 判定为正例也是真正例的概率，即真正例中判为正例的概率（也即正例召回率）。

（5） **伪阴性率(FNR):** 判定为负例却不是真负例的概率，即真正例中判为负例的概率。

（6） **真阴性率（TNR）:** 判定为负例也是真负例的概率，即真负例中判为负例的概率。

（7） **KS:** 好坏样本之间累计分布的差值(最大值)，用于评估模型的风险区分能力。好坏样本的累计差异越大，模型的风险区分能力越强，KS 指标越大。

2. 效率指标

依据联邦学习的执行流程对效率指标进行设计，主要有以下几种：

（1） **PSI 效率：**隐私求交所需要耗费的时间，时间越短性能越高。

（2） **分箱效率：**做数据特征分箱时所需要耗费的时间，时间越短性能越高。

（3） **IV 性能：**对特征和推理结果筛选的能力。时间越短性能越高。

（4） **建模效率：**应用逻辑回归、XGB 等算法建立模型时需要耗费的时间。

3. 安全性指标

联邦学习系统的安全性由运行环境安全性、算法安全性及数据隐私安全性三个方面共同构成。

（1） 运行环境安全性指标

运行环境安全性是指联邦学习运行环境的安全，需要采用技术手段，保证系统不被恶意第三方侵入，数据隐私不会泄露到系统之外，并保证系统本身运行的鲁棒性。

身份认证安全性:是指在联邦学习的各必要环节对参与方的身份进行认证。比如说，在任务发起时对任务发起方的身份进行认证，在参与任务、获取最终结果时对请求方的身份进行认证，在进行通信时对通信对方的身份进行认证等;

通信信道的安全性:是指在参与联邦学习的各节点之间采用如 TLS 之类的加密协议进行通信，建立安全通道来进行数据传输。安全通道的建立，使得参与方从其他节点获得的数据均为加密后的数据，非参与方的恶意第三方即使截取到通信数据，也无法对数据进行解密;

高可用及故障恢复: 系统具有高可用特性，可以在任务意外失败的情况下，恢复任务的执行。

（2） 算法安全性指标

传统的机器学习等算法在联邦学习场景下并不能直接使用，需要进行针对性的改造，改造后的算法需满足以下条件:

采用的联邦学习算法能够得到规定精度内的正确模型或结果;

采用的联邦学习算法理论上能够保证满足特定计算的隐私需求，不会造成隐私泄露;

采用算法时，需要对选用算法可能造成的隐私风险进行提示。

针对秘密分享、差分隐私等基于概率论或统计不可区分性的联邦学习技术路线，有统计安全参数，用于限定算法数据与均匀随机数据间的统计距离或攻击成功概率。

针对同态加密、不经意传输等使用密码算法的联邦学习技术路线，有计算安全参数，用于限定在标准模型或随机预言机模型下，攻击成功的计算复杂度。

针对正在迅速发展的量子计算攻击威胁，针对抵御量子计算攻击的安全性要求，有联邦学习的抗量子安全参数，用于限定在量子随机预言机模型下，攻击成功的量子计算复杂度。

（3） 数据隐私安全性指标

数据隐私安全性，涉及到系统底层所采用的加密算法以及系统对于参与方数据的规范性保护。加密算法在一定程度上决定了系统的隐私保护所能达到的程度，联邦学习系统中一般使用差分隐私、同态加密、多方安全计算等技术来实现学习过程的隐私保护，但这些加密算法在不同的安全级别要求下有不同的实现难度；另一方面，系统应该对参与方的数据做出一定的规范性保护，使参与方了解自己所提供的数据的使用情况，并在使用过程中按照规范记录日志。数据隐私安全性指标具体设计如下：

系统底层所采用的加密方法所能达到的隐私保护程度；

参与方可以查看己方数据的使用范围、使用状态和用途；

参与方无法获得其他参与方的数据，且无法反推出计算结果和原始数据；

只有规定的参与方可以获取到模型结果或计算结果，其他参与方以及第三方无法获得模型结果或计算结果；

只有本次参与方能获取本方本次联邦学习的日志，且参与方无法通过日志反推出计算结果和中间数据。

（二）应用案例

本报告中案例涉及数据均已获得相关数据主体的授权，个人数据满足个人主体“知情同意原则”，满足《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等相关法律法规、管理办法要求。

1. 智慧风控

（1） 工商银行-工银瑞信债券违约预测案例

案例背景

工银瑞信通过已有数据和债券发行人向市场披露的信息，发行人向市场披露信息具有一定的滞后性，对债券和发债主体进行评估和债券投资效果有限。而工行总行沉淀着大量反映企业和企业法人的资金情况、偿债能力等数据，但是基于《中华人民共和

国数据安全法》和监管要求，以及工行总行和工银瑞信的数据保护要求，双方数据无法出库。

案例方案

基于工商银行自研的联邦学习平台，采用纵向联邦学习技术方案，利用行内沉淀企业法人资金情况、偿债能力等高时效数据+工银瑞信的债券的风险标签数据，完成工商银行与子公司工银瑞信数据“可用不可见”的联合建模，上线债券违约风险推理模型，并取得良好的落地成效。

案例价值

该业务场景的落地，突破了集团内不同法人主体之间的数据壁垒，有效解决工银瑞信由于自有数据的局限性和所用公开披露数据的低时效性导致的模型效果不佳痛点。投产后经业务验证，工银瑞信与工商银行的交集企业的比例占 95%以上，联邦模型 AUC 指标超过了 0.8。违约企业前 6%召回率提升 7%；前 11%召回率提升 13%；全量召回率分位数降低了 9%，联邦学习技术有效提升了工银瑞信对债券产品市场风险的预判能力。

（2） 招商银行-银联联合企业法人风控案例

案例背景

联邦学习在风控领域的应用一直是金融行业重点关注的领域。联邦学习技术使金融机构、信贷机构、互联网科技公司等主体间的数据孤岛得以相互连接，合法合规地最大化了自有数据价值，金融机构得以进一步靠近支付及消费场景，信贷机构核心竞争力获得增强。

案例方案

招商银行与中国银联合作，利用招商银行内风控建模数据和银联数据建模，优化招商银行风控模型。在行内已有风控模型入模特征基础上，增加银联 C 端和 B 端的数据进行补充构建离线联邦模型，主要沉淀企业主行外行为模型以及企业主消费能力模型，用于企业风控场景，和存量企业客户违约推理。

案例价值

该案例利用银联全国性数据，扩展银行风控模型入模特征，提升银行现有风控模型效果；在遵循数据信息保护的前提下，在对公风控中通过联邦学习的方式，与其他机构进行合法合规的数据合作探索。

（3） 浙商银行-运营商联合信贷风控案例

案例背景

银行在应对小微企业信贷需求时，往往缺少企业经营状况等有效数据，从而导致小微企业融资难、融资慢等问题。同样对于消费金融产品，银行也因缺少用户行为画像等有效数据，导致信贷审批困难、放款慢等问题。如果可以在保护用户数据隐私的前提下，合法合规的从多源数据中训练出更加准确的联合风控模型，则可以助力银行更加快速地做出信贷风控评估，让小微企业更好地共享惠普金融政策，让用户更好地体验消费金融服务。

案例方案

浙商银行拥有企业或个人用户的经济收入、逾期记录、信用评级、征信数据、工商信息等数据，运营商 A 则拥有企业或个人用户的上网行为、通话时长、话费余额、欠费次数、常驻地址等数据。虽然两个行业拥有用户数据的特征空间完全不同，但是它们之间彼此有着紧密的联系。浙商银行通过纵向的联邦学习，可将两方数据用于小微企业和消费金融业务的反欺诈、信用评分、贷后预警等模型建设。使用联邦学习的方式可以使原始数据不出本地，达到共享数据最小化，从而实现在保护用户数据隐私的前提下完成联邦风控模型的训练。

在信贷风控领域，基于用户社交数据、互联网应用行为数据、定位(LBS)数据等进行用户画像描绘，涵盖用户的消费能力、兴

趣偏好、线下场景等，对用户的风险水平、额度利率敏感等进行推理，能够有效节约信贷审核成本，大幅提升信贷风控能力。这些用户数据在现实中一般分散在各机构、各公司主体内。使用联邦学习技术能够使得不同主体间在用户数据不泄露的前提下实现风险控制对象的上下文信息的有效收集和转发，从而实现对风险控制对象的有效风险监测。在某公司的信贷风控场景，通过联邦学习的方式与其他公司进行合法合规的数据合作和探索，在信贷主要模型上已经取得 2%到 3%的效果提升。

案例价值

基于联邦学习的信贷风控模型可以更好的推理小微企业和个人用户的信贷能力，更好的支撑惠普金融和消费金融行业，并提升此类业务的银行风控能力。另一方面，由于数据样本的提升和丰富，信贷风控模型效果会有大幅提升，从而可以有效节省传统的信贷审核成本。

通过联邦学习，银行和电信运营商的数据孤岛问题得以解决，银行业可以合法合规的最大化利用数据的价值，助力银行在信贷审批过程中进行更加快速和准确的评估判断。

（4） 交通银行-运营商联合企业信贷风控案例

案例背景

智能风控是银行智能化转型的重要抓手之一。然而，由于信息不对称、数据割裂，银行无法对交易背景形成全面的了解，导

致资金不能完全准确的投入到需要的实体经济中。如何在数据安全合规、数据隐私保护的前提下，将多方数据有效融合，发挥数据多元价值，挖掘隐藏的欺诈行为，提升风控水平与效率，成为智能风控面临的难题。

案例方案

交通银行综合利用联邦学习、多方安全计算和大数据分析技术，通过数据融合应用，强化智慧风控成效，为客户鉴权、增信，切实服务实体经济。

一是运用在线金融工具实现信贷业务从申请、审批、签约、提款的全线上操作，将技术成果运用在中小微企业融资场景中。

二是利用联邦学习、多方安全计算技术，在确保各方原始数据不出域的基础上，将银行内部数据与移动、电信等运营商数据融合，打破现有数据壁垒，通过多方安全计算技术准确识别企业集群背后的复杂关系链条及欺诈风险，通过联邦学习技术构建更精准的中小微企业风控模型，有效识别高危用户，提升银行整体的风控水平。

案例价值

本案例通过提高融资服务精度，有效缓解了中小微企业融资难问题，进而助力中小微企业复工复产。

一是提升银行风控模型精准度。通过融合联邦学习、多方安全计算技术，对多源数据进行协同建模分析，在数据使用安全合规、保护用户隐私的前提下，缓解由于信息不对称而无法有效识

别的问题。在进行中小微企业融资风控建模时，通过联邦学习定制风控模型，实现了数据不出域前提下的联合建模，并有效提升了模型效果。此外，方案中将训练得到的模型一键式分布式部署，模型严格加密，有效降低模型信息泄露风险。

二是提升普惠金融服务质效。依托银行内外多维度数据，通过将客户电信网络信息与申贷信息进行交叉比对分析和联合建模，精准防范和打击伪冒申贷等扰乱金融秩序的行为，满足客户差异化融资需求，提升普惠金融服务质效。

2. 智慧营销

（1） 联邦学习获客营销案例

案例背景

在数字化时代，数据日益成为至关重要的生产要素，也是银行数字化经营和精准营销的关键。但数据产生于不同的场景，因隐私保护、数据安全等要求，各个场景之间数据很难实现互联互通，导致形成“数据孤岛”。政务场景是富含“数据金矿”的核心场景。为挖掘数据“金矿”，获得企业客户价值实现精准营销，利用纵向联邦学习技术，在招商银行与合作方（政务部门）部署联邦节点，利用行内和政务数据训练联邦模型之后，无需各数据方披露底层数据即可使用模型推理，模型结果用于各种实际业务

流程。同时部分项目根据实际情况利用区块链技术将各数据方行为数据上链，方便追溯验证监督以及出现问题之后追责。

案例方案

如图 5.1 所示，招商银行在联邦获客营销问题上主要采用两类解决方案：

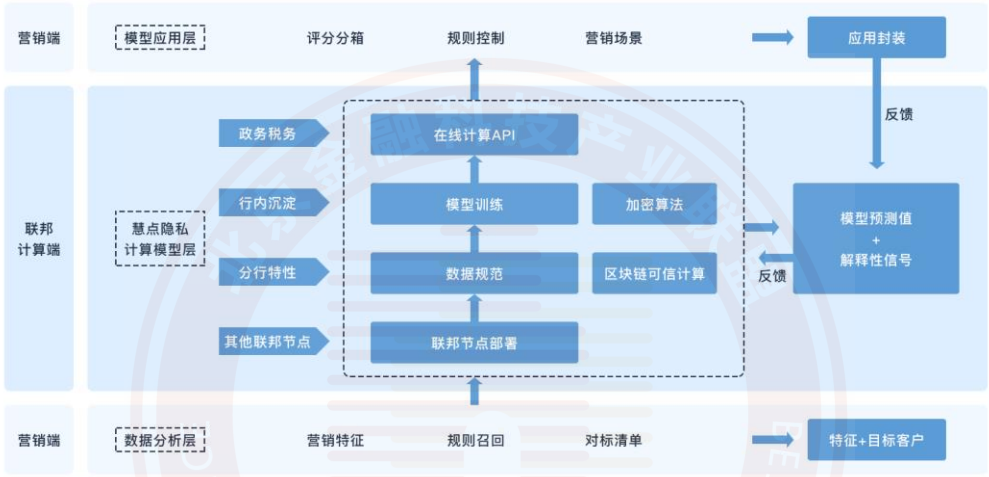

图 5.1 联邦学习获客营销案例

a) 批量筛客

模型训练完成之后，利用行内客户名单批量推理，识别不同领域优质客户，不同客户有针对营销贷款、存款等不同业务。

① 模型训练阶段（无需授权）：

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。

② 模型推理阶段：

该过程一般需要用户授权。一般的做法是先由招商银行根据自有数据筛取出行内开户客户，但还未办理各种业务的潜在营销客户名单，利用模型推理，将客户分至各个业务领域的高价值客户。

③ 批量拓客阶段:

名单筛选完毕进入线上线下营销阶段,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。

b) 流量拓客

模型训练过程与批量筛客相同，但模型推理过程不同。招商银行信贷产品利用合作方政务门户网站用于引流,单个企业点击申请授权，通过联邦实现线上拓客，让企业不再等“贷”，有效助力普惠金融场景，解决中小微企业融资难、融资贵问题。

案例价值

依托联邦学习技术，招商银行与多政务部门继续深化合作，共同挖掘数据价值。一是合作研发企业信用评分模型，结合银行客户营销服务需求进行个性化定制,进一步丰富完善我行企业用户画像，为精准营销提供有力支撑。二是合作信用数据校验，对于开户、授信环节需要人工审核校验的一些隐私数据，通过联邦学习技术进行校验，进而实现流程优化，提升客户体验。三是利用政务门户网站流量，为招商银行进行获客引流，同时也为政务部门监管提供助力。

交叉营销是指发现客户多种需求并有针对性的进行产品组合，促使客户在购买某种产品的同时可以继续购买其他关联产品。交叉营销是以客户为中心的跨产品整合或者相互关联的多种营销渠道配置。成功的交叉营销不仅需要一定的管理哲学和销售技巧，更离不开与其相匹配的数据基础作为 fintech 决策支撑。随着大数据挖掘与分布式处理技术的成熟应用，为交叉营销领域提供了有力技术支持。

（2） 联邦学习信用卡交叉营销案例

案例背景

信用卡业务作为银行最前端的金融服务，是客户接入银行服务的主要渠道，一直以来都是各家银行营销的重点领域。但是随着我国线上金融业务的不断发展，原有信用卡营销模式已经不能满足当前业务的发展需求。与此同时，各家银行也在积极布局线上生活消费服务类平台或者直接与现有互联网平台进行合作。针对已有的借记卡银行客户，结合具体消费场景的交叉营销与信用卡销售前移，已经成为银行信用卡获客新的营销重点。

案例方案

本案例就是基于银行信用卡和互联网生活消费类平台的交叉营销成功案例。如果采用传统单边营销模式，互联网生活平台缺乏潜在信用卡办卡客户的金融属性特征，银行信用卡方面则缺少银行客户在具体消费场景中的行为数据。消费平台无法准确筛

取银行想要营销的目标群体，银行则无法根据用户消费行为有针对性的进行交叉营销。为了解决以上问题，在充分保护用户个人隐私数据的同时打破“数据孤岛”，引入联邦学习技术，如图 5.2 所示。

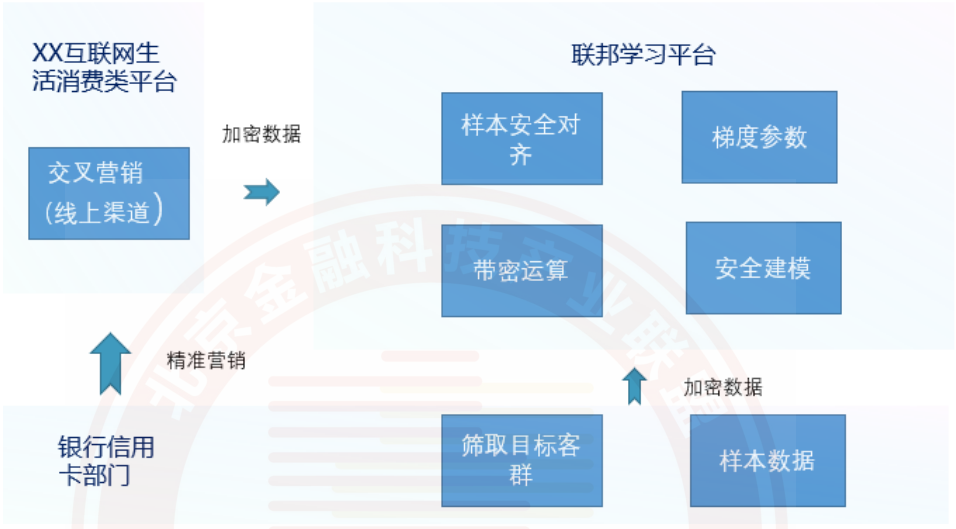

图 5.2 银行与互联网生活消费类平台协作过程

在该案例中，银行先根据自有数据筛取出已经是银行客户，但还未办理该行信用卡的潜在营销对象。再通过联邦学习体系与互联网生活消费平台进行数据对齐，各自进行模型训练并上传梯度参数，通过联邦学习联合建模，挖掘出潜在营销对象以及与其最为匹配的信用卡产品。整个过程主要分为“单方参与”和“双方参与”两个阶段，如图 5.3 所示：

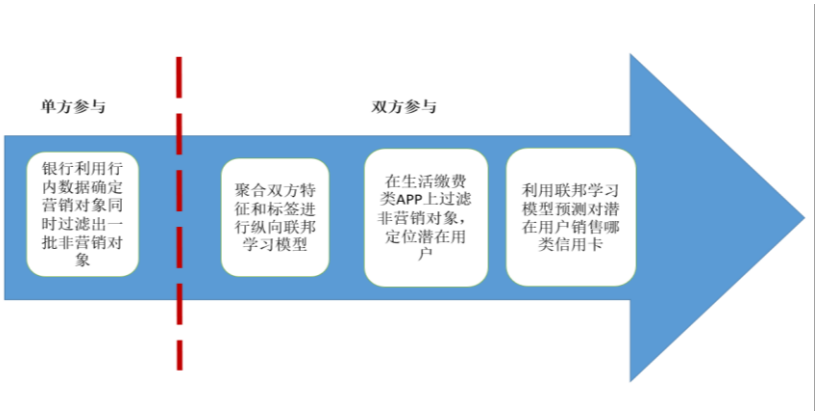

图 5.3 银行与互联网生活消费类平台协作过程

在“单方参与阶段”，银行会综合考察用户基本信息、金融资产状况、已办卡情况等信息，建立规则抽取模型，确定营销对象，即还未办理该行信用卡，且高概率会通过线上渠道办理信用卡的现有银行客户。基于规则确定营销对象可解释性强，易于落地。

在银行确定营销对象之后，继续利用联邦学习进行“双方参与阶段”的训练。为了充分利用互联网生活消费平台流量，银行信用卡部门希望结合用户购物喜好、消费习惯与不同信用卡产品进行交叉营销，即推理“某用户在使用生活平台某类服务的同时，会更倾向于办理某款类型的信用卡”。例如，对于成熟商务类客户，在其购买机票时，可推荐其办理某旅行联名信用卡，享贵宾厅权益。

在“双方参与阶段”，首先是基于保护双方隐私情况下的特征聚合。互联网生活消费平台拥有用户的消费能力和消费偏好等特征；而银行信用卡方拥有信用卡类型标签 Y，用户人口统计属

性，用户金融属性等特征如图 5.4。由于银行需要补充的是用户互联网消费特征标签，遂采用纵向联邦学习建模。

	消费能力			消费偏好		
ID	X1 月均消费次数	X2 消费金额	...	X3 消费类别	X4 消费时段	...
U1	3	100		通勤类	凌晨	
U2	1	200		购物类	上午	
U3	2	500	...	娱乐类	中午	...
U4	1	2000		旅游类	凌晨	
U5	2	100		购物类	下午	
U6	5	1000		通勤类	晚上	
U7	1	1000		其他类	中午	

	人口统计属性		金融属性			信用卡标签
ID	X5 年龄	...	X6 用户总资产	X7 用户风险评级	...	Y 信用卡类别
U1	24		100	低		一类
U2	50		250000	中		二类
U3	55	...	30000	低	...	一类
U4	43		450000	高		一类
U8	42		285000	中		二类
U9	33		55000	低		一类
U10	28		20000	中		一类

图 5.4 互联网生活类平台样本特征（上）和银行信用卡样本特征（下）示例

银行作为拥有 Y 标签的一方，由其发起建模流程，互联网生活消费平台作为数据提供方参与建模，双方选用客户手机号作为样本 ID。由于不能将样本 ID 的差集泄露给对方，在合作时需要将双方的 ID 进行加密匹配，找到用户的交集，这一步骤称为加密样本 ID 对齐（PSI）。在基于 FATE 的联邦学习平台上，PSI 基于 RSA 和 HASH 的机制实现。对齐样本之后，对于这部分交集用户，联邦学习平台可以完成特征工程和模型训练。在加密训练模

型的过程中，包括分发公钥，加密多方交互的中间计算结果和汇总梯度与损失，及联合训练的模型参数等多个步骤。

案例价值

通过联邦学习体系，不光解决了互联网生活消费平台消费表现和银行信用卡客户数据联合建模的隐私保护问题，使得不同机构间不同产品的交叉营销与信用卡销售前移得以实现。并且因为增加了更多的用户特征，较之银行单边营销训练模型，联合建模下的信用卡营销结果客户头部提升，也得到一定水平的提高.对于前 20%的客户，银行单边营销模型提升度为 1.85。加入消费行为特征后联合建模结果，在相同样本下的提升度为 2.45。

3. 反洗钱反欺诈

（1） 商业银行-运营商联合反洗钱案例

在银行反洗钱业务中，传统的做法主要是“模型筛查+名单监控+人工甄别”的可疑交易分析报告监测模式，这种模式存在数据源比较单一、数据处理时效性差、数据信息整合分析困难、可疑交易监测模型更新滞后、单一可疑交易监测标准精准度差等问题。将“联邦学习”应用到银行反洗钱业务中，探索商业银行与电信运营商等数据提供方共同利用“联邦学习”进行建模，弥补传统银行反洗钱业务中基于规则的模型存在的数据来源少、覆盖范围不足等问题。同时，利用现存的多种机器学习模型，能提

升反洗钱业务的智能化水平，减少人工判断和干预，自动识别风险因素，有效提升反洗钱系统的识别准确率，如图 5.5 所示。

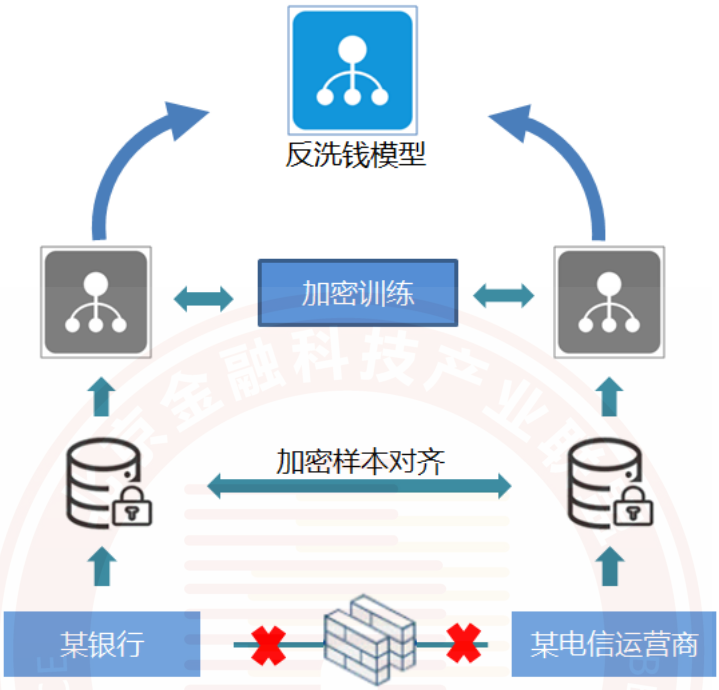

图 5.5 商业银行-运营商联合反洗钱案例

某银行运用隐私计算技术，为银行反洗钱场景引入运营商数据，例如：“手机号码是否为 170 号段”、“归属地是否为诈骗高发地区”、“个人名下号码个数”、“是否二次号”、“在网状态”、“入网时长”、“异地跨国通话次数”、“夜间跨境通话次数”等。基于联邦学习技术，该银行与当地电信运营商的数据特征实现安全融合，建立了基于纵向联邦学习的反洗钱模型，在双方原始数据不出库的前提下，为反洗钱场景模型

补充了更多有价值的数据。基于联邦学习技术，建立新的反洗钱模型后，该银行反洗钱模型召回率和准确率均有 3%以上的提升。

（2） 招商银行-平安集团联合反欺诈案例

案例背景

招商银行在推理行内交易、企业风险等级时，主要使用行内信息，行外尤其是同业银行交易信息及黑名单、风险等级标志信息对招商银行构建反欺诈模型有很高的的价值，但因数据隐私安全法律法规的相关规定，同业银行的此类信息招商银行无法获取，这为招商银行训练反欺诈交易模型设置了上限。

基于此，招商银行与平安集团合作，技术侧与科技公司合作，利用隐私求交技术使招商银行与平安集团安全共享名单数据，实现“数据可用不可见”，优化现有模型，模型结果用于实际业务流程。

案例方案

如图 5.6 所示，参与双方分别部署隐私求交的查询模块和数据加密模块。

参与双方利用匿踪查询的相关技术，通过混淆、去混淆、不经意传输（OT）、验证，在不共享底层数据前提下共享双方名单数据。保护双方交集外客户信息安全，查询发起方无法获取被查询方数据中除查询 ID 以外的信息。被查询方也不知道查询方有

没有匹配到的结果。另外，方案也保护查询意图，被查询方无法获取查询方具体查询的 ID 信息。

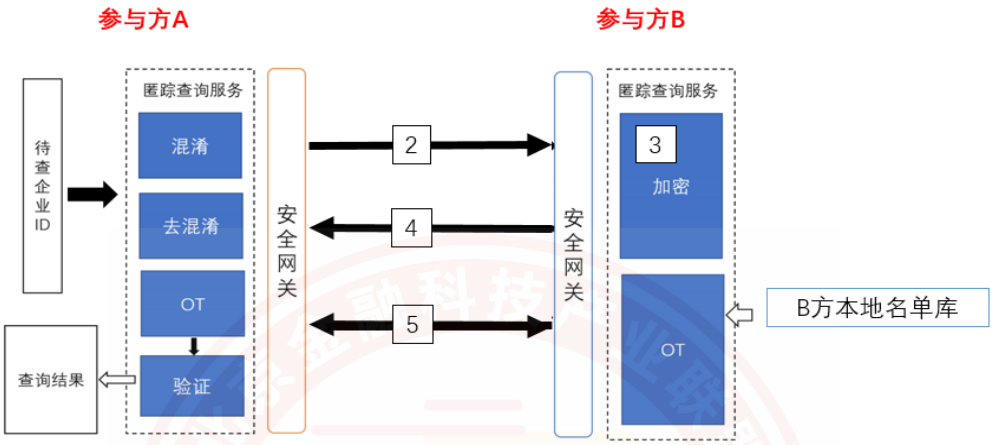

图 5.6 招商银行-平安集团联合反欺诈案例

案例价值

依托联邦学习隐私求交技术，可安全有效地使招商银行与同业银行共享名单，获得更真实完整的企业交易信息，提高模型上限。同时，该案例为同业银行形成了普适的技术解决方案，未来如有更多同业银行加入合作中来，可在反欺诈反洗钱、多头抵押多头贷款等更广阔领域实现业务价值。

六、展望与结论

（一）联邦生态激励机制展望

传统的数据合作往往是两方之间的合作，数据需求方通过评估数据的质量和应用效果给出相应的出价价格，数据提供方根据自己提供的数据数量和质量进行产品定价，双方进行磋商确定各自的利益分配。

由传统数据合作模式进化到联邦合作模式，参与方由原来的两方扩展到多方，每个参与方都需要贡献出自己的资源，或贡献自己的数据，或消耗自己的计算资源、通信资源、和能源（电力）等。虽然各参与方是平等的，但各方的贡献是完全不一样的。例如，银行与运营商、银联、小型互联网公司一起合作构建一个联邦学习模型，各机构参与方贡献的价值肯定存在差异，如何去激励这些在联邦学习生态中做出更多贡献的参与方，如何建立一个合理、有效的激励机制，是联邦学习具有重要意义的一个研究方向。

针对联邦生态的参与方所采用的激励措施可以分为正向激励和反向惩罚。正向激励是通过奖励的方式来激励各参与方，而反向的激励则是通过惩罚参与方来避免恶意行为。

在联邦学习激励机制设计中，有两个主要的挑战和难点。一是如何尽量公平的评估每个参与方的贡献量。二是如何吸引更多

的机构参与联邦学习贡献其数据与计算资源，并形成正向激励。三是如何对恶意的参与方进行识别和惩罚。

在设计联邦学习激励机制方案时，在规则设计层面，不少学者提出将数据、信誉、资源等因素纳入重要考虑范畴，例如基于参与方互相评分的激励体系、基于客户资源配置的激励机制等；在技术应用层面，也有将区块链技术应用在激励机制的安全审计环节中，保证激励机制的公平性、真实性，同时也可以对恶意方进行识别。但在联邦学习生态中，量化每个参与方的贡献价值、并对联邦学习系统的最终模型性能进行建模是十分困难的。虽然业内也有基于博弈论的联邦学习奖励机制方案的提出，但目前尚未成熟，在联邦学习主流厂商产品中还未广泛加入有效的激励机制。然而在实际的业务场景中，对收益分配又有着迫切的需求。为保证联邦学习在商业场景的大规模应用落地，合理有效的激励机制设计是至关重要的一个研究方向。

（二）联邦学习平台互联互通展望

随着越来越多的机构投身到联邦学习领域，研发了各自的隐私计算平台，或服务于自有生态，或服务于市场化机构，或服务于政府机构，将原本割裂的“数据孤岛”连接了起来，实现了“数据的可用而不可见”。但各机构的联邦学习平台一般都是基于自有知识产权的算法原理和系统设计实现的，平台之间原生无法完成信息的交互，因而又形成了新的“计算孤岛”。对于数据提供

机构和数据应用机构而言，面对着和不同的机构合作时需要部署不同机构的联邦学习平台，存在着严重的系统建设和运营成本浪费。因此“互联互通”成为联邦学习平台建设过程中必然面临的挑战。

联邦学习互联互通的目标在于使基于不同设计原理和功能实现的联邦学习平台之间协同完成某一项算法学习任务，具体指通过对不同联邦学习平台间规范的系统接口、算法协议、操作流程等的统一，实现数据资源与计算能力的交互与协同，解决使用不同联邦学习平台的联邦学习参与机构间的协作问题，实现资源与价值的跨平台互联互通。联邦学习平台互联互通的标准化工作，应对于通信协议、资源管理、任务调度、算法协同等互联互通的基础环节形成统一共识，提出标准化的技术规范；对于不同平台间的差异化设计（例如具体的算法和个性化服务功能等）可以支持自定义扩展，力求保留平台的个性化和可扩展性。

不同机构联邦学习平台之间的差异主要集中在支撑算法运行功能组件和核心算法组件的差异化上，实现平台之间的互联互通，需要努力实现这两个层面的互通。支撑算法运行功能组件主要包括通信模块、加密组件、资源管理、任务管理、模型管理、节点管理、授权管理等，可通过标准规范的方式进行逐步的统一。核心算法组件的互通可通过两种方式实现，一种是算法白盒化，基于公开透明的联邦学习算法设计流程，不同的平台方通过不同的技术栈进行算法实现，并完成对接和协同计算；另一种是算法

黑盒化，只定义好算法的基本信息、参数模板、输入、输出，通过同步黑盒化的算法组件来实现平台的互通。前者在算法上是公开可信的，但是在一定程度上限制了各家算法设计的自由度和创新性，存在算法开发实现的工作量重复，后者算法原理设计的知识产权受到了保护，但对互通参与方来说存在黑盒效应，遇到问题只能求助于算法原有提供方来解决，并需要权威评测机构来对黑盒化的算法插件进行安全审计和检测。

异构平台之间通过互联互通方式进行联邦学习，在安全性方面的挑战除了同构平台之间进行联邦学习面临的问题之外，还存在着由于对“算法插件”的信任问题导致的安全性风险：在黑盒方式算法协议互通时，算法插件可以由任一参与方撰写、在多方平台上运行，当非本方开发的算法插件运行在本方平台上时，会存在对算法插件安全性的质疑。目前这种风险可以常用“算法插件”开源化，或者由权威评测机构对“算法插件”进行检测认证两种方式来增加对于互联互通的算法插件的信任问题，从而降低这部分风险。

联邦学习平台的互通不论是从经济效益角度还是推进联邦数据生态角度来看都大有裨益，通过联邦学习平台的互通，才能使联邦连接更加广泛，才能将数据背后蕴含的真正价值更大程度地释放出来。

（三）总结

在国家法律法规以及金融行业标准规范对于数据管理尤其是个人隐私数据严格要求的情况下，联邦学习技术正成为行业以及产业内数据流动的关键基础，充分保障数据“可用不可见”，将推进数字社会、数字经济的发展，助力金融机构数字化转型。

国内金融机构已经在联邦学习技术、应用等方面开展了大量的工作，并在精准营销、风险防控等场景进行了小范围的试点应用，已经取得了良好的成绩和效果。

随着研究深入和应用推进，联邦学习技术在功能和性能等方面也正迎来快速发展的时期，相关技术标准尤其是金融场景的标准也正在建立。联邦学习技术也将与人工智能、物联网、区块链、云计算等相关技术深度融合，并在不同的场景中实现不同技术的商业应用。联邦学习将充分发挥数据要素的价值，也将成为金融机构必不可少的金融科技。

参考文献

[1] Shamir, Adi "How to share a secret,"Communications of the ACM*. **22** (11): 612–613, November 1979.

[2] Blakley, G.R. "Safeguarding Cryptographic Keys," Managing Requirements Knowledge, International Workshop on (AFIPS), 48: 313–317, 1979.

[3] A. C. Yao, "Protocols for secure computations," 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 1982, pp. 160-164, doi: 10.1109/SFCS.1982.38.

[4] A. C. Yao, "How to generate and exchange secrets," 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), Toronto, ON, Canada, 1986, pp. 162-167, doi: 10.1109/SFCS.1986.25.

[5] ARM. ARM Security Technology – Building a Secure System using TrustZone Technology. ARM Technical White Paper, 2009. http://infocenter.arm.com/help/topic/com. arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_ trustzone_security_whitepaper.pdf.

[6] Craig Gentry. "Fully homomorphic encryption using ideal lattices," In Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09). Association for Computing Machinery, New York, NY, 2009

[7] Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. “CryptDB: Protecting Confidentiality with Encrypted Query

Processing,” In Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP), Cascais, Portugal, October 2011.

[8] Ittai Anati, Shay Gueron, Simon P Johnson, and Vincent R Scarlata. "Innovative technology for cpu based attestation and sealing," In Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, HASP, volume 13, 2013.

[9] Brendan McMahan, Eider Moore Daniel Ramage, Blaise Agüera y Arcas. "Communication-Efficient Learning of Deep Networks from Decentralized Data," AISTATS 2017, 1273-1282

[10] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. "Federated Machine Learning: Concept and Applications,"" ACM Trans. Intell. Syst. Technol. 10, 2, Article 12 (February 2019), 19 pages.

[11] Qiang Yang; Yang Liu; Yong Cheng; Yan Kang; Tianjian Chen; Han Yu, Federated Learning , Morgan & Claypool, 2019

[12] Cheng, K., T. Fan, Yilun Jin, Yang Liu, Tianjian Chen and Qiang Yang. “SecureBoost: A Lossless Federated Learning Framework.” ArXiv abs/1901.08755 (2019)

[13] Y. Liu, Y. Kang, C. Xing, T. Chen and Q. Yang, "A Secure Federated Transfer Learning Framework," in IEEE Intelligent Systems, vol. 35, no. 4, pp. 70-82, 1 July-Aug. 2020

[14] Liu, Y., Yan Kang, Xin-wei Zhang, Liping Li, Yong Cheng, Tianjian Chen, M. Hong and Q. Yang. “A Communication Efficient Vertical Federated Learning Framework.” ArXiv abs/1912.11187 (2019)

[15] D. Gao, Y. Liu, A. Huang, C. Ju, H. Yu and Q. Yang, "Privacy-preserving Heterogeneous Federated Transfer Learning," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2552-2559

[16] Lyu, Lingjuan, Han Yu and Q. Yang. “Threats to Federated Learning: A Survey.” ArXiv abs/2003.02133 (2020)

[17] Han Yu, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang. 2020. A Fairness-aware Incentive Scheme for Federated Learning. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (AIES '20). Association for Computing Machinery, New York, NY, USA, 393–399

[18]S. Sharma, C. Xing, Y. Liu and Y. Kang, "Secure and Efficient Federated Transfer Learning," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 2569-2576

[19] Di Jiang, Yuanfeng Song, Yongxin Tong, Xueyang Wu, Weiwei Zhao, Qian Xu, and Qiang Yang. 2019. Federated Topic Modeling. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management (CIKM '19). Association for Computing Machinery, New York, NY, USA, 1071–1080

[20] Zhang, Chengliang and Li, Suyi and Junzhe, Xia and and Wang, Wei and Yan, Feng and Yang, Liu. "BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning", the 2020 USENIX Annual Technical Conference (ATC), 2020

[21] Liu, Y., Huang, A., Luo, Y., Huang, H., Liu, Y., Chen, Y., Feng, L., Chen, T., Yu, H., & Yang, Q. (2020). FedVision: An Online Visual Object Detection Platform Powered by Federated Learning. Proceedings of the AAAI Conference on Artificial Intelligence, 34(08), 13172-13179

[22] Luo, Jiahuan, X. Wu, Y. Luo, Anbu Huang, Y. Huang, Y. Liu and Qiang Yang. “Real-World Image Datasets for Federated Learning.” ArXiv abs/1910.11089 (2019)

[23] Li, S., Cheng, Y., Liu, Y., Wang, W., and Chen, T. “Abnormal Client Behavior Detection in Federated Learning”, arXiv,, 2019

[24] FATE： https://github.com/FederatedAI/FATE

[25] fedlearner : https://github.com/bytedance/fedlearner

[26] Flex: https://github.com/tongdun/iBond-flex

[27] 9NFL: https://github.com/jd-9n/9nfl

[28] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]. International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 1999: 223-238.

[29] Gillmor D. Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)[J]. IETF RFC 7919, 2016.

[30] NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators [OL]. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-90a.pdf. Last accessed on 10/21/2020.

[31] NIST Special Publication 800-38G. Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption[OL]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf. Last accessed on 10/21/2020.

[32] Chou T, Orlandi C. The simplest protocol for oblivious transfer[C]. International Conference on Cryptology and Information Security in Latin America. Springer, Cham, 2015: 40-58.

附录:

联邦学习算法应用实现

1. 联邦数据探查

1.1. 联邦隐私求交

1.1.1. 场景说明

金融机构通常为应用需求方，用参与方 Guest 表示。其他机构通常为数据服务提供方，用参与方 Host 表示。应用于使用纵向联邦学习应用的数据准备过程，联邦应用需求方通过用户 ID 寻找与其他参与方之间的用户 ID 交集，即共同拥有的用户 ID 的集合。

1.1.2. 扩展安全要求

参与方不能知道交集外的真实用户 ID。

交互过程中使用的 ID 为散列处理后结果，不使用原始 ID 进行交互。

可选地，参与方 Host 可不被告知具体的用户 ID 交集。

1.1.3. 两方数据交换流程

金融机构作为参与方与其他机构共同对齐用户 ID 集，找到共同拥有的用户 ID 集合。安全对齐的交换流程如图 1 所示，数据交换流程应满足如下要求:

——加密使用的秘钥和加密随机数分别由一方参与方生成;

——各参与方首先对己方 ID 做散列处理，Guest 使用公钥以及随机数加密 ID，Host 使用私钥进行加密，各参与方调用应用层通信协议发送各自加密 ID;

——Host 使用自有私钥加密 Guest 方 ID 并发送给 Guest;

——Guest 利用己方生成随机数加密 Host 的加密 ID,Guest 方计算各参与方 ID 密文集合的交集。

——如选择同步，Guest 把加密的交集 ID 集合返回给其他参与方 Host，各参与方根据加密交集 ID 还原原始 ID 交集集合，完成双方的样本对齐。

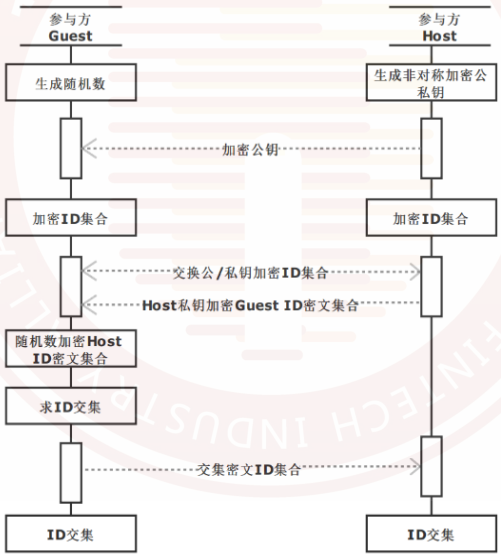

图 1 两方安全对齐的数据交换流程

1.1.4. 三方数据交换流程

可信第三方作为协调方，金融机构作为参与方与其他机构共同对齐用户 ID 集，找到共同拥有的用户 ID 集合。安全对齐的交换流程如图 2 所示，数据交换流程应满足如下要求：

——各参与方分别生成一个大质数用于加密；

——各参与方首先对己方 ID 做散列处理，然后分别使用大质数对 ID 进行加密并调用应用层通信协议发送对方各自加密 ID；

——各参与方对对方单次加密 ID 使用己方大质数进行二次加密并发送给协调方；

——协调方对各二次加密 ID 求交集并将交集密文 ID 集合分发给各参与方；

——各参与方还原原始交集 ID。

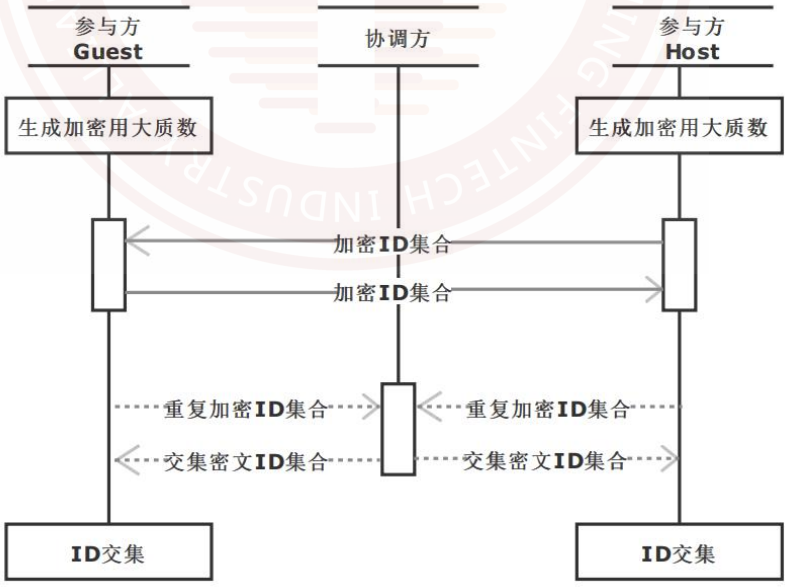

图 2 三方安全对齐的数据交换流程

1.1.5. 其他 PSI 方法

（1）基于不经意传输协议(OT)的实现

不经意传输(Oblivious transfer)是密码学中的一类协议，缩写为 OT，实现了数据提供方将潜在的许多信息中的一个传递给数据需求方，但对提供方所接收信息保持未知状态。

具体做法为双方通过不经意传输协议构造不经意伪随机函数，利用该函数对数据 id 进行变换后比对获取交集。

（2）基于混淆电路(GC)的实现

基于混乱电路的 PSI 协议主要思想有 2 种: 1)将元素映射到二进制向量，通过向量的与运算求集合交集; 2)通过电路解决隐私保护的元素相等性判断问题，然后通过集合中元素的两两比较以〇(n^2)复杂度计算集合交集。

目前主要实现方式有: 基于钥匙混乱点数的 PSI 协议实现，基于随机协议 OT 进行优化的 PSI 协议实现、基于不经意伪随机函数的 PSI 实现。

（3）基于同态加密(HE)的实现

使用全同态加密技术的 PSI 协议，通过拥有较小 集合的一方将自己的集合加密以后发送给另一方，而另一方负责基于密文求两个集合的交集，然后将结果交给对方解密。

用全同态加密实现 PSI 可以达到相对较小的交互复杂度，但它的计算复杂度通常非常高，导致协议效率低下。尽管混乱电路的 PSI 协议一般具有通用性、灵活性和可扩展性，但功能函数的

电路设计一般要求很大的门电路个数和电路，因此基于此技术的协议一般计算效率很低。

（4）基于秘密共享(SS)的实现

秘密共享(Secret Sharing)将秘密以适当的方式分为 n 份，每一份由不同的管理者持有，每个参与者无法单独恢复秘密，只有达到指定数目的参与者才能恢复秘密。构建秘密共享系统的关键是设计好的秘密拆分和恢复方式.第一个秘密共享方案是(t,n)门限秘密共享方案，由 Shamir 和 Blakley 分别在 1979 年各自独立提出，他们的方案分别是基于拉格朗日插值法和线性几何投影性质设计的.此后很多研究者提出了不同的秘密共享实现方法，如基于中国剩余定理的秘密共享策略、可验证的秘密共享等。秘密共享在密钥管理分布式数据安全领域有许多应用，如电子投票、密钥托管、电子支付协议等，可以防止密钥存储过于集中，是一种兼顾机密性和可靠性的方法。

（5）基于 Diffie-Hellman 的实现

双方将 id 作为 Diffie-Hellman 协议的输入，执行协议。

（6）基于对称加密的实现

可用于有中心参数服务器协助的联邦学习场景之中，各方将本地 id 经过对称密钥后的密文 id 发送至中心服务器，而中心服务器不知道该密钥，只对密文进行比对，返回相同的密文。

1.2. 联邦特征相关性

皮尔森相关系数也称皮尔森积矩相关系数(Pearson product-moment correlation coefficient)，是一种线性相关系数，是最常用的一种相关系数。皮尔森相关系数用来反映两个变量 X 和 Y 的线性相关程度，r 值介于-1 到 1 之间，绝对值越大表明相关性越强。

$$\rho_{x,y}=\frac{\operatorname{cov}(X,Y)}{\sigma_x\sigma_y}=\frac{E\left(\left(X-\mu_X\right)\left(Y-\mu_Y\right)\right)}{\sigma_X\sigma_Y}=\frac{E(XY)-E(X)E(Y)}{\sqrt{E\left(X^2\right)-E^2(X)}\sqrt{E\left(Y^2\right)-E^2(Y)}}$$

两个连续变量(X,Y)的皮尔森相关系数等于它们之间的协方差 cov(X,Y)除以它们各自标准差的乘积(σ_x, σ_y)。系数的取值总是在-1 到 1 之间，接近 0 的变量被称为无相关性，接近 1 或者-1 被称为具有强相关性。

1.2.1. 场景说明

应用于纵向联邦学习的特征相关性计算。

金融机构通常为应用需求方，用参与方 Guest 表示。其他机构通常为数据服务提供方，用参与方 Host 表示。应用于使用纵向联邦学习应用的数据准备过程，联邦应用需求方通过用户 ID 寻找与其他参与方之间的用户 ID 交集，即共同拥有的用户 ID 的集合。

1.2.2. 扩展安全要求

纵向联邦 Pearson 相关性训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方的特征数据;

——不泄露参与方的特征数据;

——除了结果之外，不泄漏任何额外信息。

1.2.3. 两方数据交换流程

金融机构通常为 Guest 方，用参与方 P1 表示。其他机构通常为提供数据服务的 Host 方，用参与方 P2 表示。纵向联邦 Pearson 相关性的计算数据交换流程如图 3-5 所示。数据交换流程应满足如下要求:

——所有参与方归一化本地特征数据，归一化方式为标准化，每一列特征减去本列特征的均值后除以标准差;

——用归一化后的本地特征数据执行 SPDZ 协议，依次交互;

——Guest 方归一化后的特征数据的 share 发送给 host 方;

——Host 方归一化后的特征数据的 share 发送给 Guest 方;

——双方根据 SPDZ 协议计算乘法三元组;

——双方根据 SPDZ 协议利用乘法三元组加密计算两方归一化矩阵的乘积;

——双方重建矩阵乘法结果。

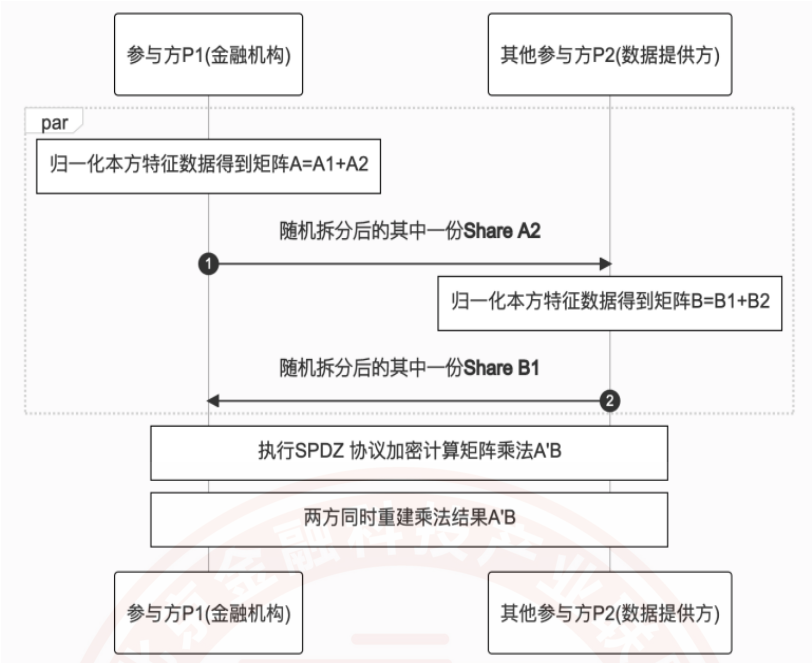

图 3 纵向联邦 Pearson 相关性的数据交换流程

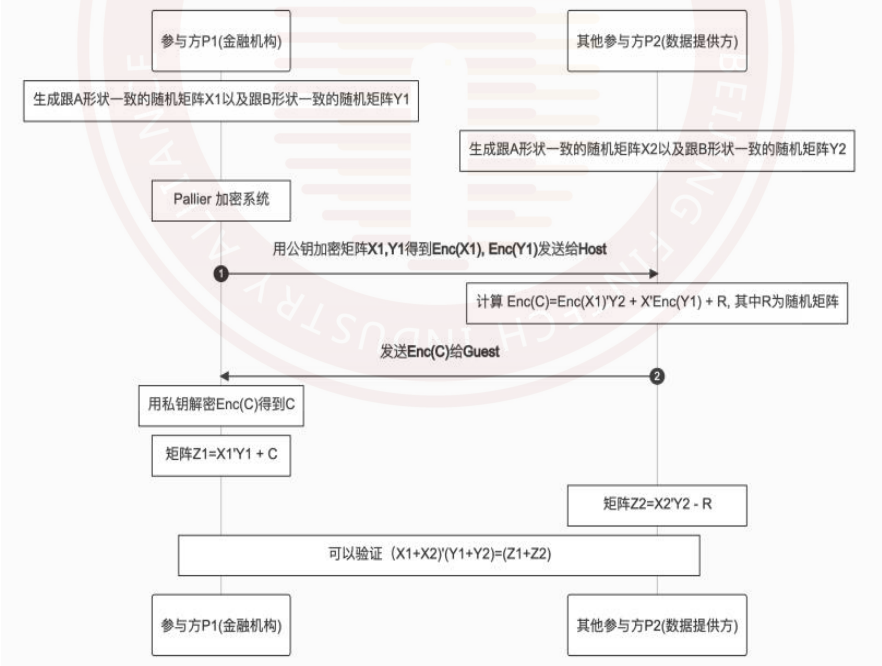

图 4 SPDZ 乘法三元组生成的数据交换流程

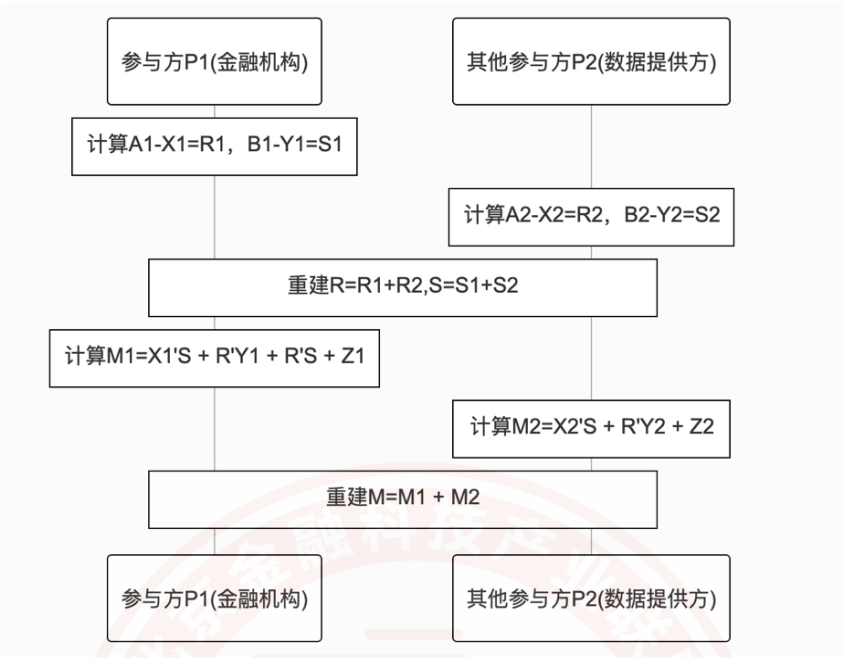

图 5 SPDZ 乘法的数据交换流程

1.2.4. 三方数据交换流程

金融机构通常为 Guest 方，用参与方 P1 表示。其他机构通常为提供数据服务的 Host 方，用参与方 P2 表示。可信第三方作为协助者 Arbiter。纵向联邦 Pearson 相关性的三方计算数据交换流程如图 6 所示。数据交换流程应满足如下要求:

——Arbiter 生成乘法三元组;

——Arbiter 将三元组数据分别发送给 Guest 和 Host;

——所有参与方归一化本地特征数据，归一化方式为标准化，每一列特征减去本列特征的均值后除以标准差;

——用归一化后的本地特征数据执行 SPDZ 协议，依次交互;

——Guest 方归一化后的特征数据的 share 发送给 host 方;

——Host 方归一化后的特征数据的 share 发送给 Guest 方;

——双方根据 SPDZ 协议计算乘法三元组;

——双方根据 SPDZ 协议利用乘法三元组加密计算两方归一化矩阵的乘积;

——双方重建矩阵乘法结果。

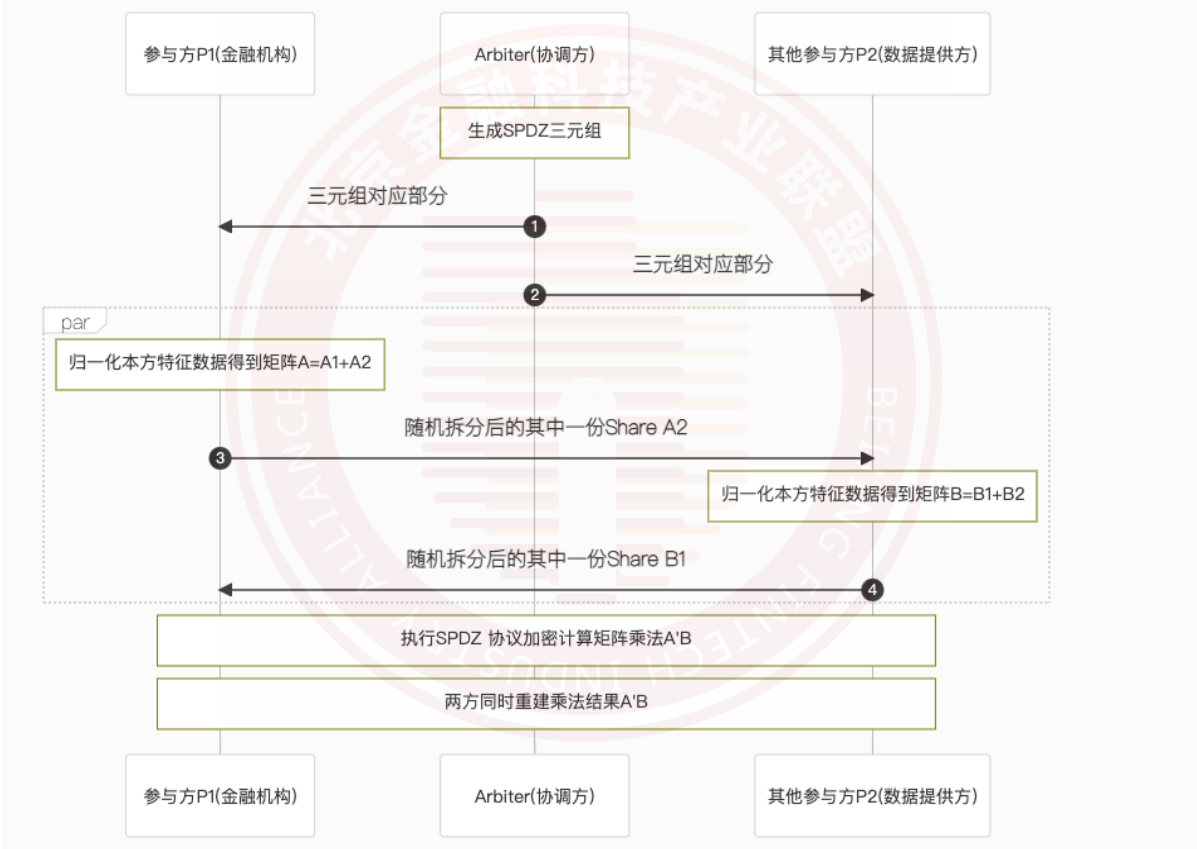

图 6 三方纵向联邦 Pearson 相关性的数据交换流程

1.3. 联邦分箱

1.3.1. 场景说明

应用于在金融应用场景建模之前的数据预处理过程，将连续特征离散化，离散化后的特征可以提高模型的鲁棒性。如果联邦分箱需要利用标签信息指导分箱过程，那么它就是一种有监督的联邦分箱。这种有监督的联邦分箱在纵向联邦中应用较多。

1.3.2. 扩展安全要求（纵向）

纵向联邦建模之前的数据预处理过程应满足如下扩展安全要求：

——不泄露参与方的特征数据；

——不泄露参与方的标签数据。

1.3.3. 两方数据交换流程

金融机构通常为数据需求方，拥有标签信息，用参与方 Guest（后简称 Guest）表示。其他机构作为服务提供方，需要利用金融机构方的标签信息进行特征选择，用参与方 Host（后简称 Host）表示。

基于信息价值的联邦特征最优分箱数据交换流程如图 7 所示。数据交换流程应满足如下要求：

——Guest 调用同态加密算法生成同态公私钥，并发送公钥和加密后的标签数据给 Host；

——Host 对本地特征进行较密集的等频分箱，并在密文空间上统计分箱中正负样本数密文，发送给 Guest，同时发送每个分箱的编号信息;

——Guest 解密每个分箱的统计信息得到正负样本数明文，可计算每个分箱信息价值 iv;

——Guest 构建最小堆树，合并使得 iv 值减少最少的两个分箱，生成新的分箱节点加入堆树中。重复此过程，直到满足终止条件,终止条件为达到预设分箱数或合并任何分箱后会超出预设分箱样本数;

——Guest 将最终合并后的边界分箱编号发送给 Host;

——Host 利用编号信息，还原最终真实分箱点。

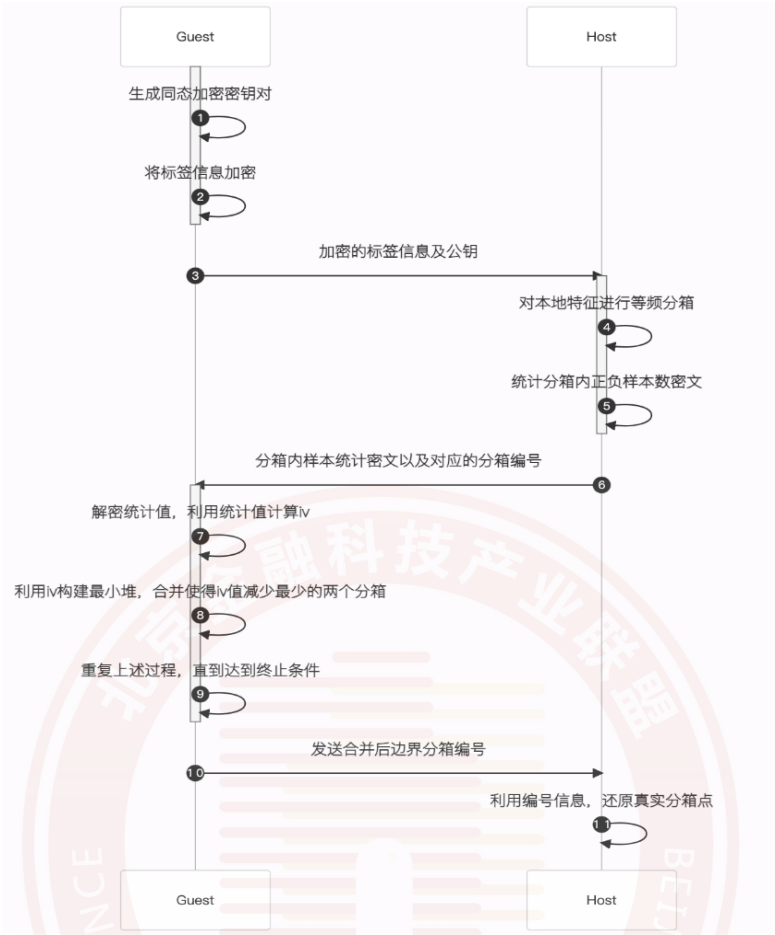

图 7 纵向联邦分箱的数据交换流程

1.3.4. 两方数据交换流程（卡方最优分箱）

数据需求方用 Guest 表示，Guest 为含有 Y 标签的一方。数据提供方用 Host 表示。纵向联邦分箱的计算流程如图 8 所示。计算流程的主要步骤包括:

——数据需求方 Guest 利用同态加密算法生成加密公私钥，并利用公钥对 Y 标签加密，同步加密标签给 Host;

——Host 对本方特征进行单边分箱，并对各箱进行编码，根据加密标签密态计算各箱正样本数量和负样本数量，同时将箱号编码和正负样本数同步给 Guest;

——Guest 解密得到每箱正负样本数的明文，计算每一箱的卡方值；

——Guest 将卡方值最小的区间合并，重复此过程直到达到合箱终止条件，终止条件为达到设定的最大分箱数或下一步分箱后每箱样本数低于设定的占比或下一步分箱后只包含正样本或负样本。同步最优分箱点编码给 Host；

——Host 根据分箱编码还原真实分箱点。

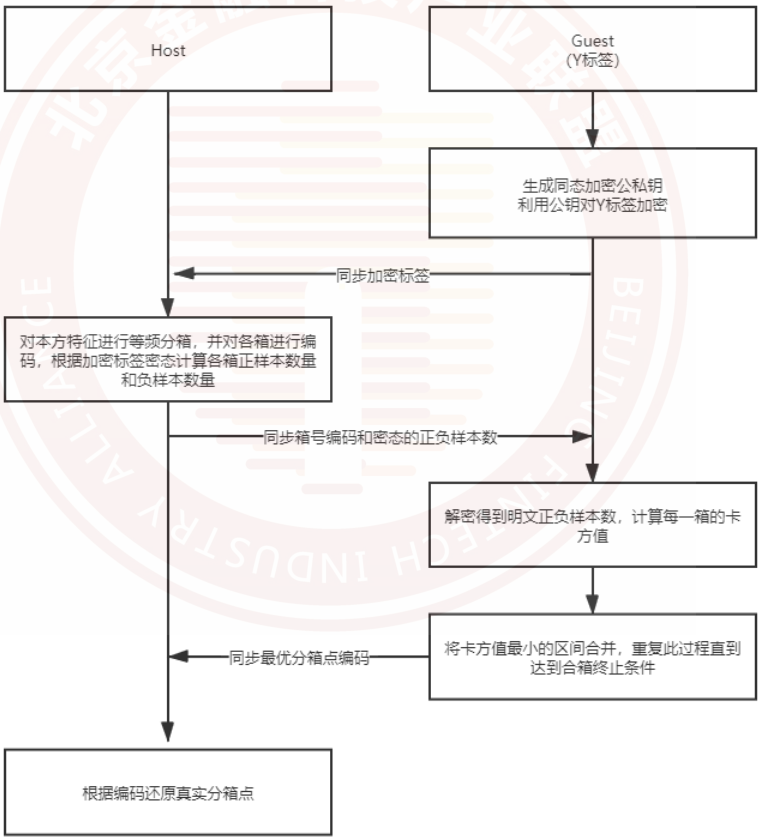

图 8 联邦卡方最优分箱的数据交换流程

1.3.5. 三方数据交换流程

金融机构通常为数据需求方，拥有标签信息，用参与方 Guest（后简称 Guest）表示。其他机构作为服务提供方，需要利用金融机构方的标签信息进行特征选择，用参与方 Host（后简称 Host）表示。可信第三方作为协助者 Arbiter。

基于信息价值的三方联邦特征最优分箱数据交换流程如图 A.9 所示。数据交换流程应满足如下要求：

——Arbiter 调用同态加密算法生成同态公私钥，并发送公钥给 Guest；

——Guest 加密自身标签，并将标签结果发送给 Host；

——Host 对本地特征进行较密集的等频分箱，并在密文空间上统计分箱中正负样本数密文，发送给 Arbiter，同时发送每个分箱的编号信息；

——Arbiter 解密每个分箱的统计信息得到正负样本数明文，可计算每个分箱信息价值 iv；

——Arbiter 构建最小堆树，合并使得 iv 值减少最少的两个分箱，生成新的分箱节点加入堆树中。重复此过程，直到满足终止条件，终止条件为达到预设分箱数或合并任何分箱后会超出预设分箱样本数；

——Arbiter 将最终合并后的边界分箱编号发送给 Host；

——Host 利用编号信息，还原最终真实分箱点。

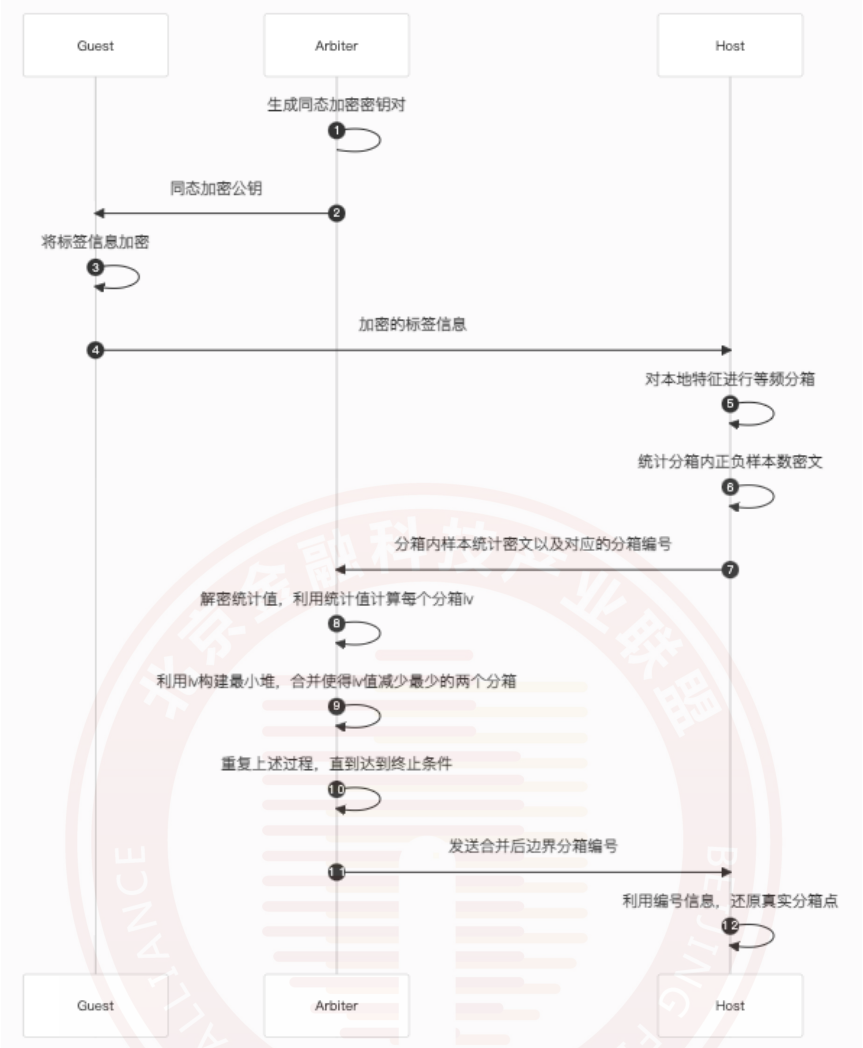

图 9 三方纵向联邦分箱的数据交换流程

1.3.6. 扩展安全要求（横向）

应用于横向联邦建模场景之前的数据预处理过程，将连续特征离散化，离散化后的特征可以提高模型的鲁棒性。模型训练前的联邦特征选择应满足如下扩展安全要求：

——不泄露参与方的特征数据；

——不泄露参与方的标签数据。

1.3.7. 三方数据交换流程

横向场景中，建模多方常常是拥有大量相同特征的机构。我们将任务发起方称之为 Guest，其余参与方称之为 Host（可存在多个），可信第三方作为协助者 Arbiter。

横向联邦分箱包含两个子协议，子协议一用于进行全局排序查询，子协议二用于联邦等频分箱。

横向联邦排序查询数据交换流程如图 10 所示。数据交换流程应满足如下要求：

——对于某一个请求值，Guest 和各 Host 方分别查询该值在本地的排序；

——Guest 和各 Host 方使用安全聚合方法，在 arbiter 中得到全局排序；

——Arbiter 将排序值传回 Guest 和各 Host 方。

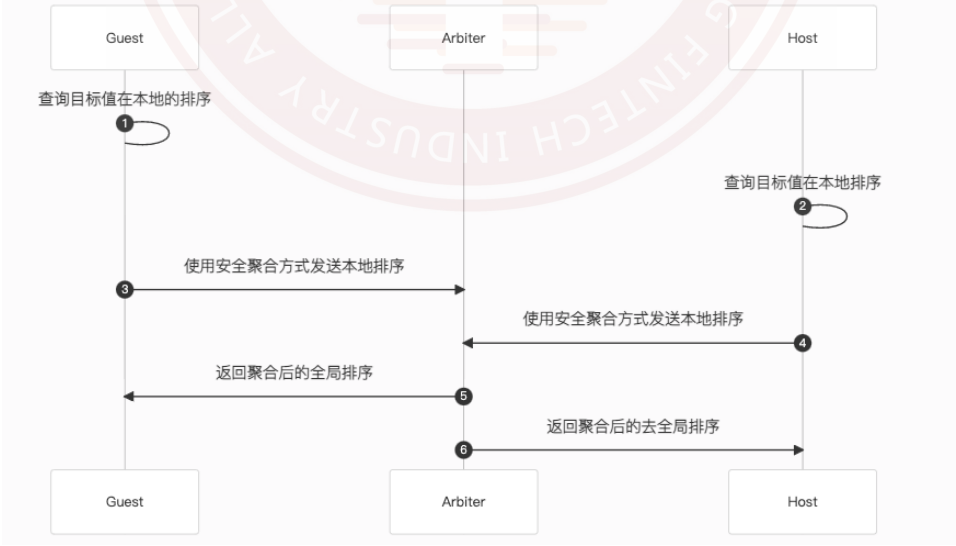

图 10 横向联邦特征分箱协议一的数据交换流程

注：该查询算法后续将被应用于横向联邦分箱算法中

横向联邦等频分箱数据交换流程如图 11 所示。数据交换流程应满足如下要求：

——Guest 和各 Host 使用安全聚合机制，由 arbiter 获得全局的最大值，最小值和总样本数；

——Arbiter 将最大值，最小值和样本总数发回 Guest 和各 Host 方；

——Guest 和各 Host 方在最大值和最小值之间，等频分割出目标分箱数个分割值，与对应的目标排序；

——Guest 和各 Host 方利用上述横向联邦排序查询方法，查询该值真实全局排序，并判断其是大于还是小于目标排序值；

——Guest 和各 Host 使用二分法，若大于目标值，查询该值与最小值的均值，否则查询该值与最大值的均值，并把最大或最小值设置为该值；

——重复上述过程，直到各分割点均处于可接受误差范围内。

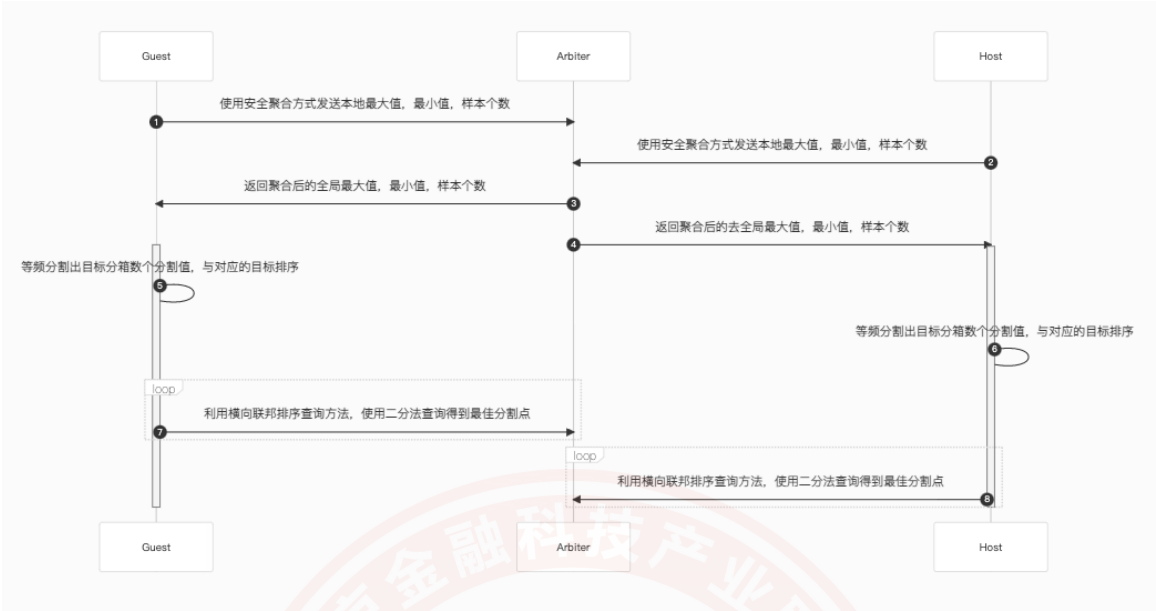

图 11 横向联邦特征分箱协议一的数据交换流程

1.4. 联邦特征选择

1.4.1. 场景说明

应用于模型训练前，通过算法筛选掉冗余或建模效果差的特征，从而提高建模效果以及加快训练速度。

1.4.2. 扩展安全要求

模型训练前的联邦特征选择应满足如下扩展安全要求：

——不泄露参与方的特征数据；

——不泄露参与方的标签数据。

1.4.3. 两方数据交换流程

金融机构通常为应用需求方拥有标签信息，用参与方 Guest（后简称 Guest）表示。其他机构作为服务提供方，需要利用金

融机构方的标签信息进行特征选择,用参与方 Host(后简称 Host)表示。

基于信息价值的联邦特征分箱数据交换流程如图 12 所示。数据交换流程应满足如下要求:

——Guest 调用同态加密算法生成同态公私钥,并发送公钥和加密后的标签数据给 Host;

——Host 在密文空间上统计每个分箱中正负样本数密文,发送给 Guest;

——Guest 解密每个分箱的统计信息得到正负样本数明文,计算信息价值 iv;

——对每个样本重复上述过程,Guest 方得到所有特征的 iv 信息;

——Guest 利用 iv 信息,选择合适的特征,并将属于 Host 方的特征编号发送回去。

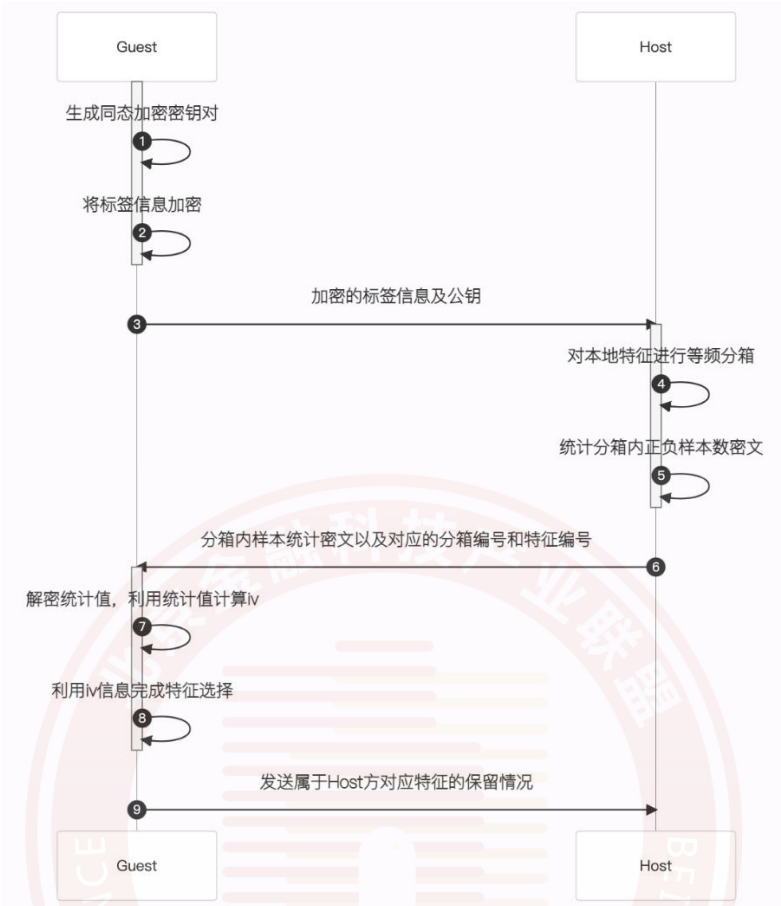

图 12 联邦选择的数据交换流程

1.4.4. 三方数据交换流程

金融机构通常为数据需求方，拥有标签信息，用参与方 Guest（后简称 Guest）表示。其他机构作为服务提供方，需要利用金融机构方的标签信息进行特征选择，用参与方 Host（后简称 Host）表示。可信第三方作为协助者 Arbiter。

基于信息价值的联邦特征分箱数据交换流程如图 13 所示。数据交换流程应满足如下要求：

——Arbiter 调用同态加密算法生成同态公私钥，并发送公钥给 Guest；

——Guest 加密标签信息，并发送给 Host;

——Host 在密文空间上统计每个分箱中正负样本数密文，发送给 Arbiter;

——Arbiter 解密每个分箱的统计信息得到正负样本数明文，计算信息价值 iv;

——对每个样本重复上述过程，Arbiter 方得到所有特征的 iv 信息;

——Arbiter 利用 iv 信息，选择合适的特征，并将属于 Host 方的特征编号发送回去。

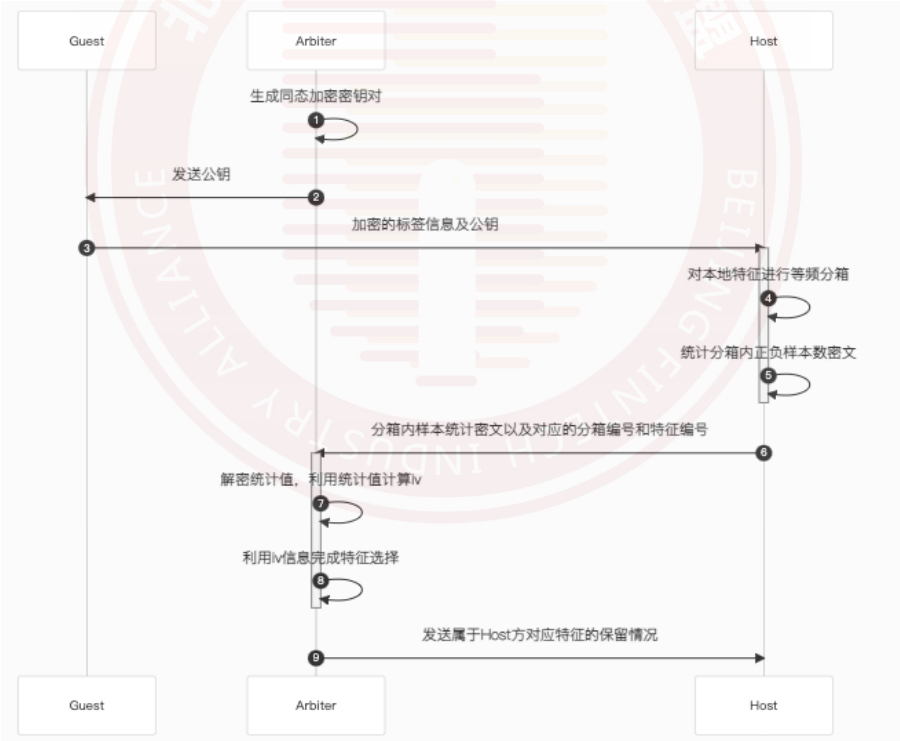

图 13 三方联邦选择的数据交换流程

1.5. 联邦特征编码

1.5.1. 场景说明

应用于横向联邦建模场景之前的数据预处理过程，特征编码可将字符型特征或者分类类型特征进行特征编码，有利于提升模型效果。

1.5.2. 扩展安全要求

模型训练前的联邦特征选择应满足如下扩展安全要求：

——不泄露参与方的特征数据；

——不泄露参与方的标签数据。

1.5.3. 三方数据交换流程

横向场景中，建模多方常常是拥有大量相同特征的机构。我们将任务发起方称之为 Guest，其余参与方称之为 Host（可存在多个），可信第三方作为协助者 Arbiter。

横向联邦特征独热编码交换流程如图 14 所示。数据交换流程应满足如下要求：

——Guest 和各 Host 将所需编码的特征名和出现过的特征值，发送给 Arbiter；

——Arbiter 聚合各方特征值，对所有出现过的特征值排序后，发回各方；

——Guest 和各 Host 各自对自身特征做独热编码。

图 14 横向联邦特征编码的数据交换流程

2. 联邦模型训练

2.1. 线性回归

2.1.1. 场景说明

应用于纵向联邦线性回归模型训练。

2.1.2. 扩展安全要求（纵向）

纵向联邦线性回归模型训练过程中的数据交换应满足如下扩展安全要求：

——不泄露参与方的特征数据；

——不泄露参与方的模型参数；

——不泄露标签数据。

2.1.3. 三方数据交换流程

金融机构通常为应用需求方，用参与方 Guest 表示。其他机构通常为数据服务提供方，用参与方 Host 表示。线性回归模型训练的数据交换流程如图 15 所示。数据交换流程应满足如下要求:

——协调方调用同态加密算法生成同态公私钥，并发送公钥给各参与方;

——参与方 Host 计算并使用公钥加密自有模型参数与特征点积 wx，发送给 Guest;

—— Guest 对 Host 发送加密点积与自有 wx 求和，结合标签计算加密残差[d]，并将其发送给参与方 Host;

——各参与方利用残差与点积计算加密梯度[g]，并将加密梯度发送给协调方;

——协调方解密各加密梯度，并发送给所有参与方，所有参与方更新模型参数。

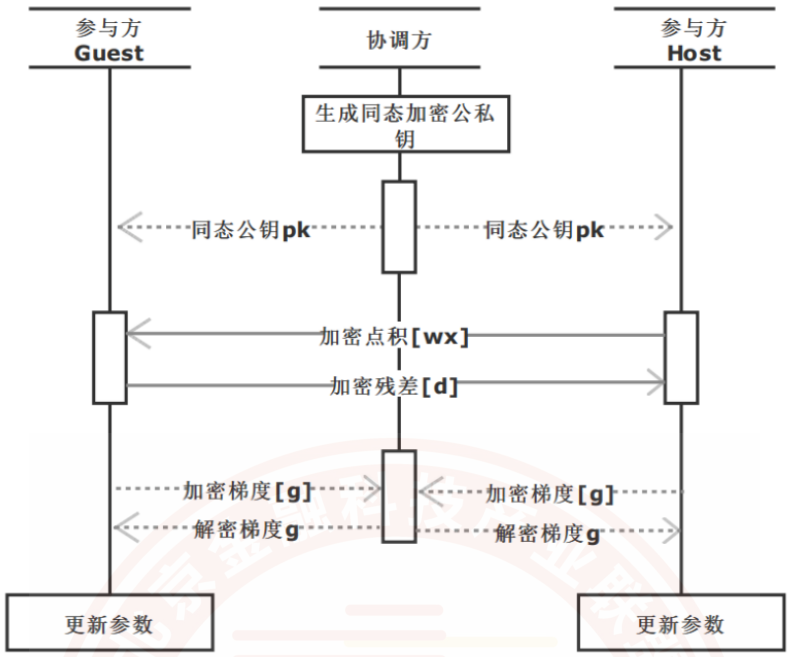

图 15 线性回归模型训练的数据交换流程

2.1.4. 两方数据交互流程

数据需求方用 Guest 表示，Guest 为含有 Y 标签的一方。数据提供方用 Host 表示。纵向联邦线性回归模型的算法流程如图 16 所示。算法流程的主要步骤包括:

——Guest 和 Host 分别利用同态加密算法生成本方的加密公私钥，并将公钥 pkA 和 pkB 同步给对方;

——Host 计算本方模型参数与特征的点积$w_A x_I^A$和部分损失，经 pkA 加密后同步给 Guest;

——Guest 计算本方点积及部分损失并用 pkA 加密。汇总两方部分损失得到 pkA 加密的损失值，并加入随机数 M; 结合标签数据计算得到 pkA 加密的中间结果 d，再利用 pkB 加密 d; 计算

得到 pkA 加密的 Guest 方梯度，并加入随机数 R。将上述三个结果同步给 Host;

——Host 利用本方私钥对损失值和 Guest 方梯度解密，同时根据中间结果 d 计算本方梯度，同步上述三个结果给 Guest;

——Guest 对损失和本方梯度消除随机数得到损失和梯度的明文结果后，判断模型是否收敛，同时更新本方参数；利用本方私钥对 Guest 方梯度解密，并将结果同步给 Guest;

——Guest 对本方梯度解密后更新本方参数。

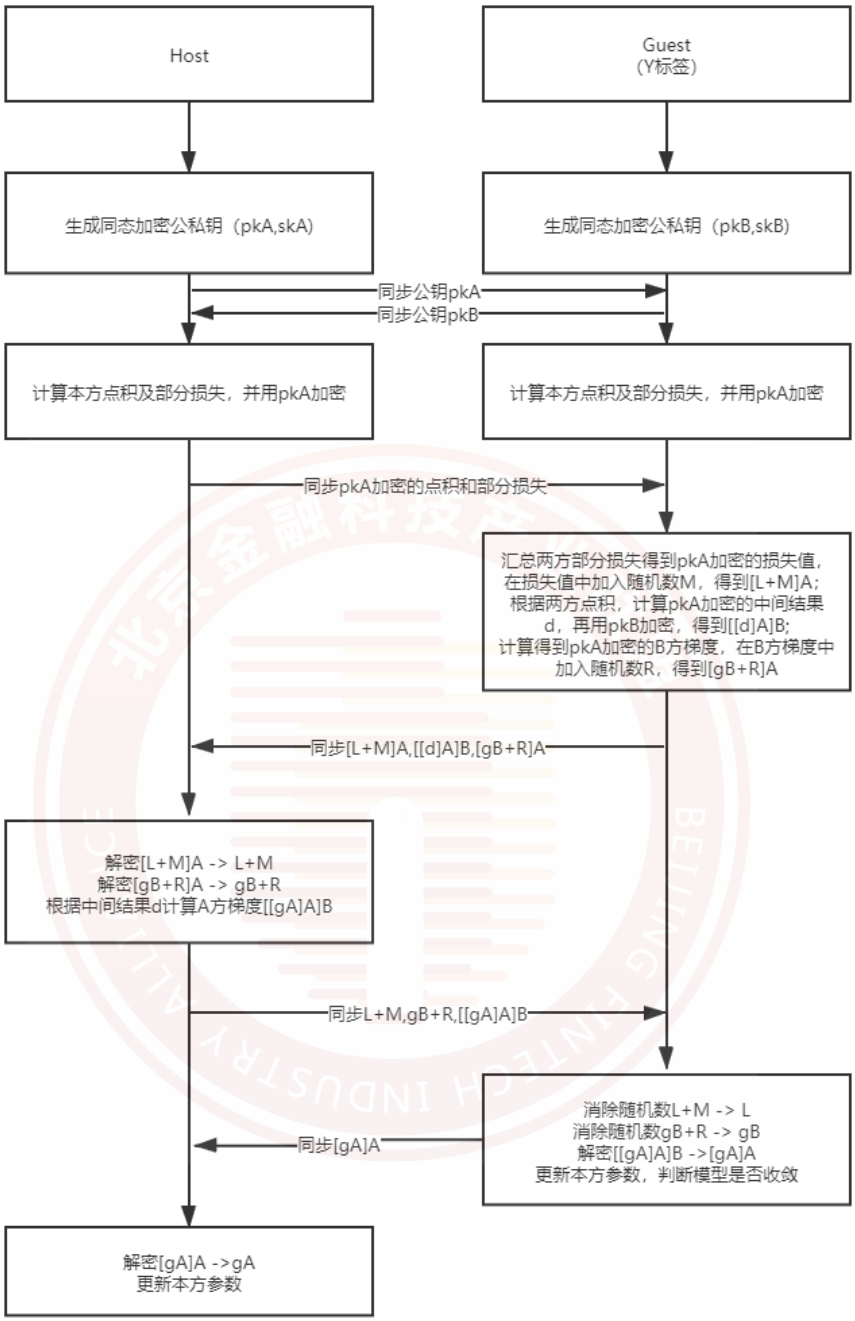

图 16 线性回归模型训练的数据交换流程

2.2. 逻辑回归

2.2.1. 场景说明

逻辑回归是风控领域最常用的模型，虽然逻辑比较简单，但是具备可解释性强，计算速度快的优点。逻辑回归其实是个分类问题。线性回归里 y 的范围是$(-\infty,\infty)$，而分类希望得到一个概率，它的范围是在 0 到 1 之间。因此需要在线性回归的基础之上做一个转换。本节先介绍一下无第三方的逻辑回归，逻辑回归一般采用对数损失，公式如下：

$$\mathrm{loss}=-\frac{1}{n}\sum_{i=1}^{n}y_i\log p\left(x_i\right)+\left(1-y_i\right)\log\left(1-p\left(x_i\right)\right)$$

其中$p=\frac{1}{1+e^{-wx}}$，$wx=w^Ax^A+w^Bx^B$。在纵向联邦学习模式下，各方之间梯度明文计算可以满足半诚实模型假定。如果需要满足恶意模型假定，两方场景下需要加一些特殊安全保护，梯度加上差分隐私干扰是常见技术手段。

2.2.2. 扩展安全要求（纵向）

纵向联邦逻辑回归模型训练过程中的数据交换应满足如下扩展安全要求：

——不泄露参与方的特征数据；

——不泄露参与方的模型参数;

——不泄露标签数据。

2.2.3. 三方数据交换流程

金融机构通常为应用需求方，用参与方 Guest 表示。其他机构通常为数据服务提供方，用参与方 Host 表示。逻辑回归模型训练的数据交换流程如图 17 所示。数据交换流程应满足如下要求:

——协调方调用同态加密算法生成同态公私钥，并发送公钥给各参与方;

——参与方 Host 计算并使用公钥加密自有模型参数与特征点积 wx，发送给 Guest;

—— Guest 对 Host 发送加密点积与自有 wx 求和，结合标签计算加密中间数值[d]，并将其发送给参与方 Host;

——各参与方利用加密中间数值与点积计算加密梯度[g]，并将加密梯度发送给协调方;

——协调方解密各加密梯度，并发送给所有参与方，所有参与方更新模型参数，满足半诚实模型假定。若需满足恶意模型，协调方加密计算梯度，并以密文发送给所有参与方，所有参与方解密更新模型参数。

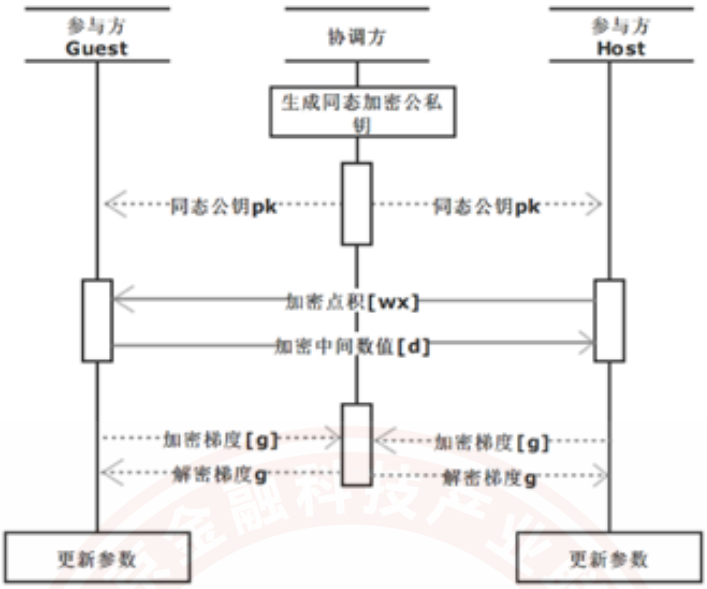

图 17 逻辑回归模型训练的数据交换流程

2.2.4. 扩展安全要求（横向）

横向联邦逻辑回归模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方的特征数据;

——不泄露标签数据。

2.2.5. 三方数据交换流程

金融机构通常为数据需求方，用参与方 Guest(后简称 Guest)表示。其他机构作为数据提供方，用参与方 Host(后简称 Host)表示。可信第三方作为协助者 Arbiter。

横向逻辑回归算法交换流程如图 18 所示。数据交换流程应满足如下要求:

——Guest 和各 Host 方各自利用自身数据，得到本地模型;

——Guest 和各 Host 利用安全聚合机制，将模型发送到 Arbiter;

——Arbiter 聚合各方模型，将聚合后的模型发送回各方;

——Guest 和各 Host 利用新一轮模型迭代计算;

——重复上述过程直到达到最大迭代次数或收敛。

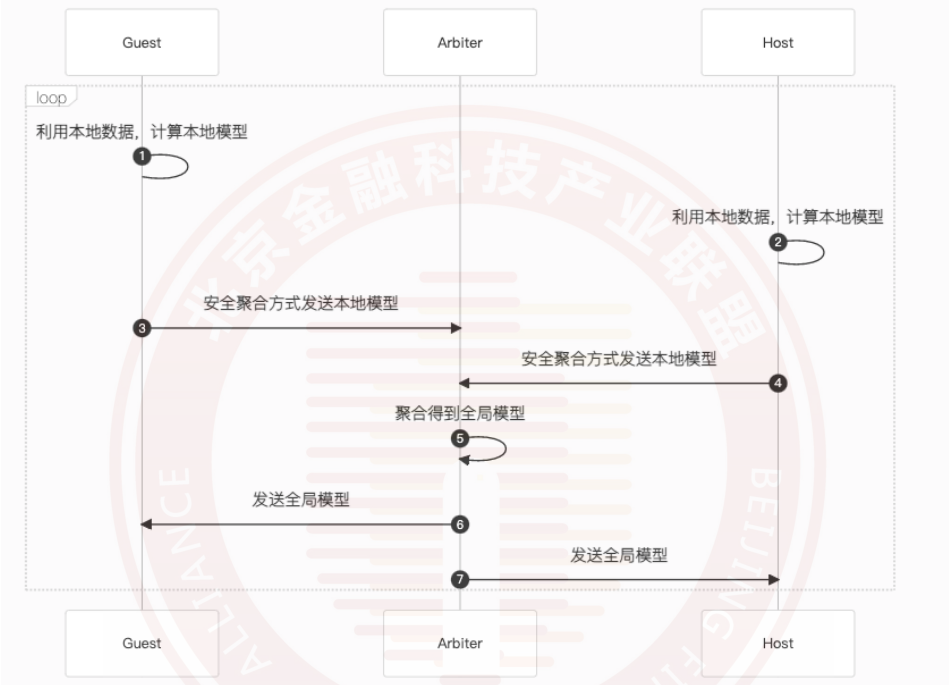

图 18 横向联邦逻辑回归模型训练的数据交换流程

2.3. 树模型

2.3.1. 场景说明

树模型既可以解决分类问题又可以处理回归问题，因而在机器学习中得到广泛应用。梯度提升决策树是一类实用性很强的树模型，在联邦梯度提升决策树中，各个参与方基于本地数据计算决策树的一阶导数和二阶导数，根据切分增益决定最佳特征和切分点。这一过程中需要对不同参与方的一阶导数和二阶导数做加

法，可以使用加性同态加密保护各个参与方的数据隐私在树模型构建过程中不泄露给其他参与方。

2.3.2. 扩展安全要求（纵向）

纵向联邦树模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方 Guest，Host 的特征数据;

——不泄露各个参与方的模型参数;

——不泄露 Guest 样本的一阶和二阶导数;

——不泄露 Guest 的标签数据。

2.3.3. 两方数据交换流程

树模型的数据交换包括两个子协议。子协议一的目的是在建立一颗树之前将一阶导数 gi 和二阶导数 hi 的密文从参与方 Guest 传输给参与方 Host; 子协议二在树的每颗节点处执行，输入各个参与方的候选切分点信息，输出该节点是否切分和最优切分点信息，根据该信息每个参与方可以生成左右子树或叶子节点。

子协议一的数据交换流程如图 19 所示。数据交换流程应满足如下要求:

——参与方 Guest 生成同态公私钥，加密每个样本对应的一阶导数和二阶导数，发送到参与方 Host;

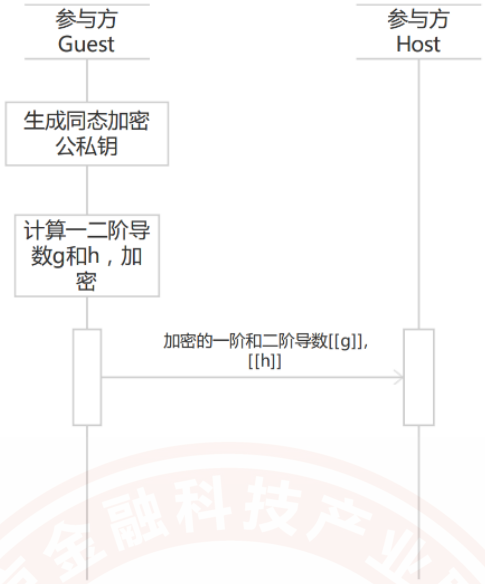

图 19 纵向提升树模型训练（两方）协议一的数据交换流程

子协议二的数据交换流程如图 20 所示。数据交换流程应满足如下要求：

——参与方 Host 将本方特征的候选切分点信息打乱编号，密文发送到参与方 Guest；

——参与方 Guest 解密接收到的密文，与本方候选切分点信息一起，分别计算每种切分的增益，判断该节点是否可以切分，若可以切分，则计算最优切分点信息。参与方 Guest 把节点是否切分的信息发送到 Host，若切分的特征位于 Host 方，则发送最优切分点编号给 Host，双方更新模型与样本划分。

图 20 纵向提升树模型训练（两方）协议二的数据交换流程

2.3.4. 三方数据交换流程

树模型的数据交换包括两个子协议。

子协议一的目的是在算法开始之前，联邦协调方将同态加密公钥分发给参与方 Guest。Guest 对样本一阶导数和二阶导数。在建立一颗树之前将一阶导数 gi 和二阶导数 hi 的密文从参与方 Guest 传输给参与方 Host。

子协议二在树的每颗节点处执行，联邦协调方获取参与方 Guest，Host 的候选切分点信息并解密，输出该节点是否切分和最优切分点信息，根据该信息决定每个参与方可以生成的左右子树或叶子节点，参与方根据协调方结果更新树模型。

子协议一的数据交换流程如图 21 所示。数据交换流程应满足如下要求：

——联邦协调方生成同态公私钥，发送到参与方 Guest；

——参与方 Guest 使用本地标签计算一阶导数与二阶导数，并使用同态加密公钥对一阶二阶导数进行加密，得到密文；

——参与方 Guest 将本方梯度密文发送至参与方 Host。

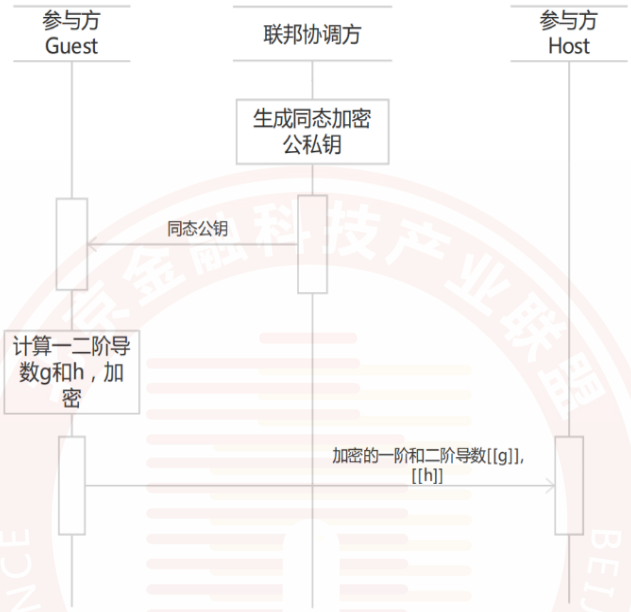

图 21 纵向提升树模型训练（三方）协议一的数据交换流程

子协议二的数据交换流程如图 22 所示。数据交换流程应满足如下要求：

——各个参与方使用本地标签一阶导数与二阶导数密文计算特征切分点，并将所有切分点顺序打乱并编号；

——各个参与方将切分点发送至联邦协调方；

——联邦协调方对切分点密文进行解密，比较切分点收益，得到最优切分点；

——联邦协调方将最优切分点编号告知所属参与方，该参与方使用切分点更新本地模型，并与其他参与方同步树结构与样本划分。

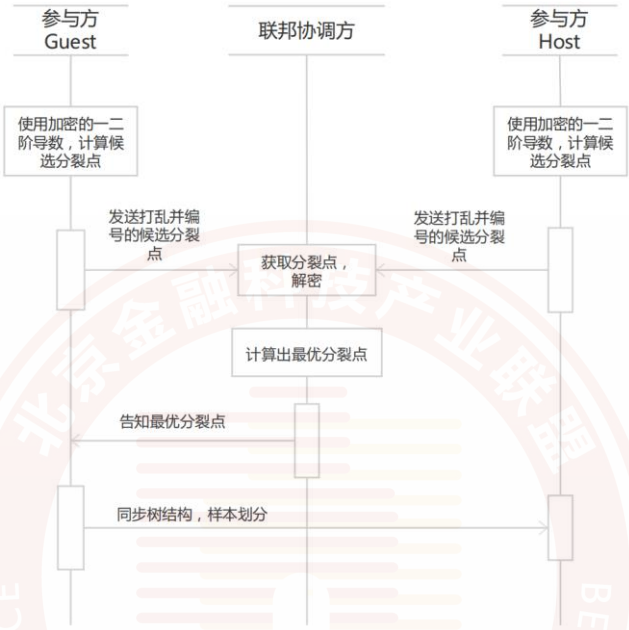

图 22 纵向提升树模型训练（三方）协议二的数据交换流程

2.3.5. 扩展安全要求（横向）

横向联邦树模型训练过程中的数据交换应满足如下扩展安全要求：

——不泄露各个参与方的特征数据；

——不泄露各个参与方的一阶和二阶导数；

——不泄露各个参与方的标签数据。

2.3.6. 三方数据交换流程

树模型的数据交换包括三个子协议。假设横向场景下有 n 个参与方 P1 到 Pn。

子协议一的目的是在算法开始之前，做好安全聚合所需的初始化工作； 子协议二的目的在树的每颗节点处执行， 各个参与方明文下计算样本一阶二阶梯度，汇总为直方图，所有参与方用持有所有的随机种子生成随机数混淆直方图中所有数值，发送给协调方。协调方汇总直方图，计算出最优分裂点，并将分裂点信息同步到各个参与方。

子协议一的数据交换流程如图 23 所示。数据交换流程应满足如下要求：

——参与方两两之间调用密钥交换协议，两两之间(Pi，Pj)得到一对相同随机数作 Rij 为种子

——各方保存交换得到的随机数

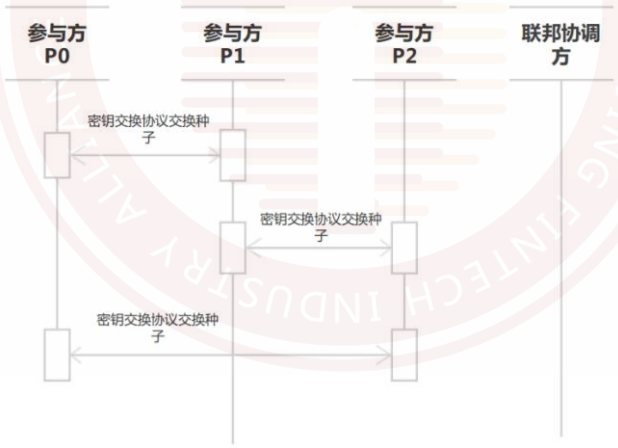

图 23 横向提升树模型训练协议一的数据交换流程

子协议二的数据交换流程如图 24 所示。数据交换流程应满足如下要求：

——各个参与方使用本地标签计算一阶和二阶导数，并由一阶二阶导数构建明文的直方图；

——各个参与方使用种子产生混淆数字，并用这些数字混淆直方图；

——各个参与方发送直方图至联邦协调方，联邦协调方将所有直方图相加，得到汇总直方图，根据汇总直方图计算出最优分裂点；

——联邦协调方将最优分裂点同步至各个参与方，参与方更新树模型。

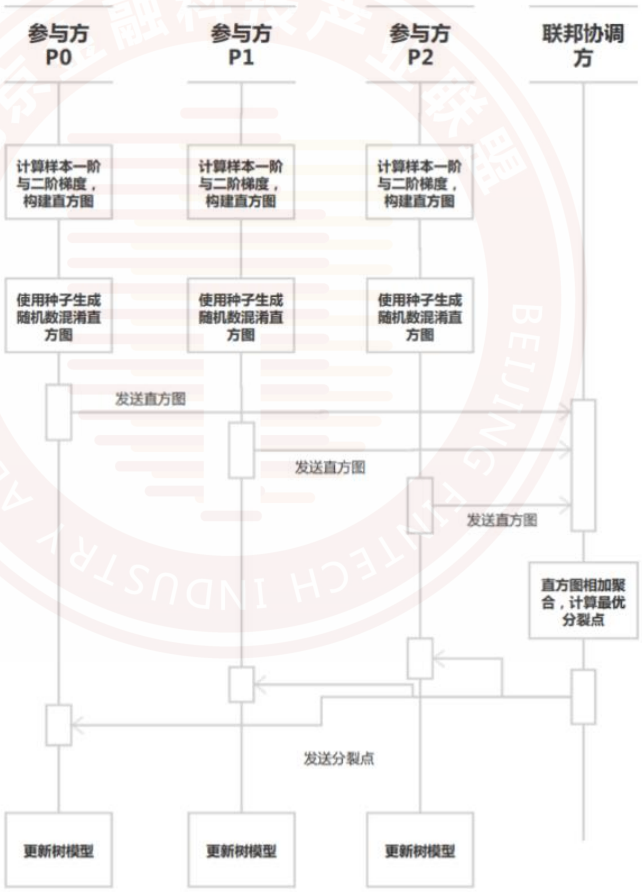

图 24 横向提升树模型训练协议二的数据交换流程

2.4. 神经网络模型

2.4.1. 场景说明

应用于纵向神经网络模型训练，纵向神经网络模型的训练算法有包含可信第三方（协调方）和无可信第三方（协调方）两种方法。 本节给出的是无可信第三方的数据交换协议。

2.4.2. 扩展安全要求（纵向）

纵向联邦神经网络模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露各参与方的特征数据;

——不泄露标签数据;

——不泄露各参与方的模型参数;

——不泄露不必要的梯度信息。

2.4.3. 两方数据交换流程

金融机构通常为数据需求方，具有特征数据和标签，用 Guest 来表示。其他机构通常为数据提供方，用参与方 Host 表示。神经网络一般分为前向传播和后向传播两个过程，涉及到两种协议交换。神经网络模型训练前向传播的数据交换流程如图 25 所示、后向传播的数据交换流程如图 26 所示。

A.前向传播数据交换流程应满足如下要求:

——Host 方对自己的数据，建立本方的底层神经网络模型，将原始数据经过底层神经网络模型后的输出 alpha 使用同态加密算法加密后发给 Guest;

——Guest 方对自己的数据，建立本方的底层神经网络模型，将原始数据经过底层神经网络模型后的输出传输到交互层；

——Guest 方维护交互层的模型，Guest 将[alpha]当成交互层 Host 模型输入，计算 Host 模型输出，同时加上白噪声后发给 Host，于此同时，将 Guest 底层模型的输出当作交互层 Guest 模型输入，计算 Guest 模型输出；

——Host 方解密 Guest 方的传输数据，并补充上累计噪声导致的模型输出缺失部分发给 Guest；

——Guest 将 Host 的发送结果去除白噪声与 Guest 交互层模型输出进行拼接，并当成顶层模型的输入，计算得到顶层模型输出结果。

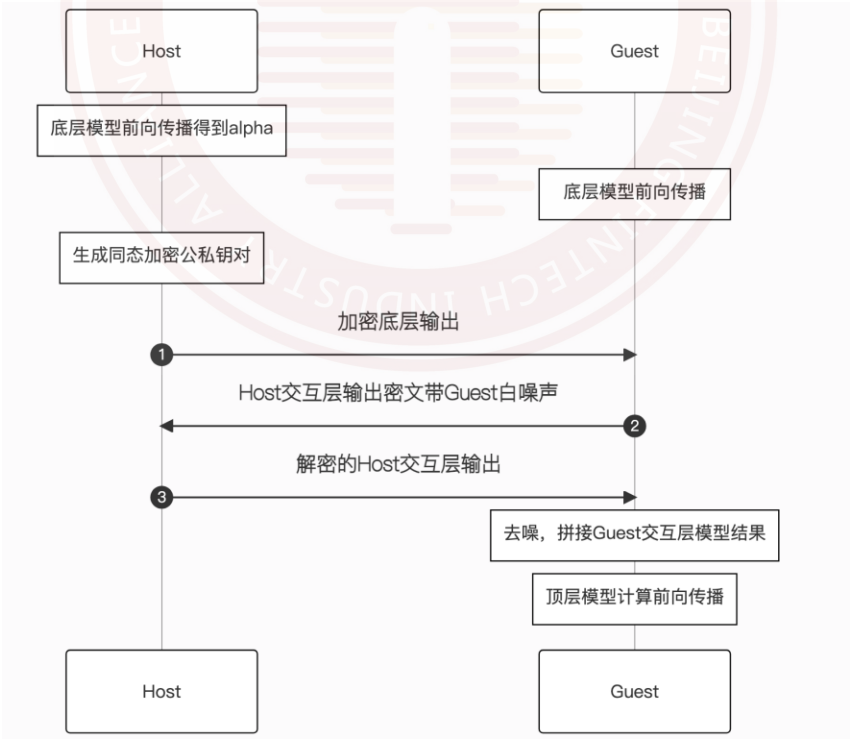

图 25 纵向联邦神经网络训练前向传播的数据交换流程

B.后向传播数据交换流程应满足如下要求:

——Guest 方结合标签 Y 和前向传播顶层的输出，计算和更新顶层模型，并将顶层模型的误差回传到交互层，并更新交互层 Guest 模型，和计算交互层 Guest 模型误差;

——Host 同步传输加密的累计噪声给 Guest;

——Guest 得到累计噪声后，计算 Host 交互层加密误差(顶层误差*(加密累计噪声 + 交互层 Host 模型）;

——Guest 计算交互层 Host 加密模型梯度(顶层误差*host 前向传播[alpha])，加上白噪声后传输给 Host 方;

——Host 解密 Guest 方传输过来的带噪声数据，并带上(自己方的噪声/学习率)并传输给 Guest，同时累计噪声更新(加上自己方的噪声);

——Guest 得到传输数据后直接更新交互层 Host 模型;

——Host、Guest 更新底层模型。

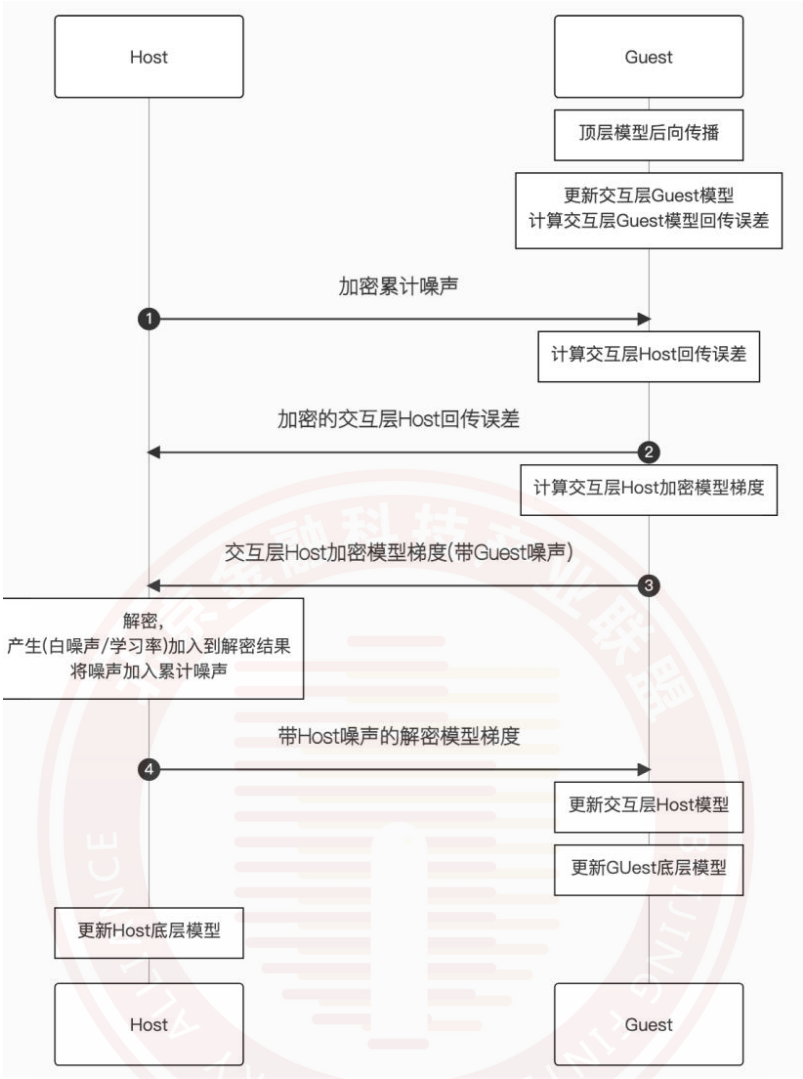

图 26 纵向联邦神经网络训练后向传播的数据交换流程

2.4.4. 扩展安全要求（横向）

横向联邦模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方的特征数据;

——不泄露单个参与方的梯度或者模型;

——不泄露标签数据。

2.4.5. 三方数据交换流程

金融机构通常为 Guest 方，用参与方 P1 表示。其他机构通常为提供数据服务的 Host 方，用参与方 P2-Pn 表示。横向神经网络模型训练的数据交换流程如图 27 所示。数据交换流程应满足如下要求:

——所有参与方 P1-Pn 调用安全密钥交换协议，两两之间（Pi，Pj）获取一对相同的随机数 rij;

——所有参与方用本地数据训练模型，得到当前轮的模型或者梯度;

——所以参与方 P1-Pn 用两两之间的随机数作为种子生成随机矩阵来混淆本地的梯度或者模型，发送给协调方;

——协调方计算聚合结果，之后发送给各参与方进行下一轮迭代金融机构通常为应用需求方。

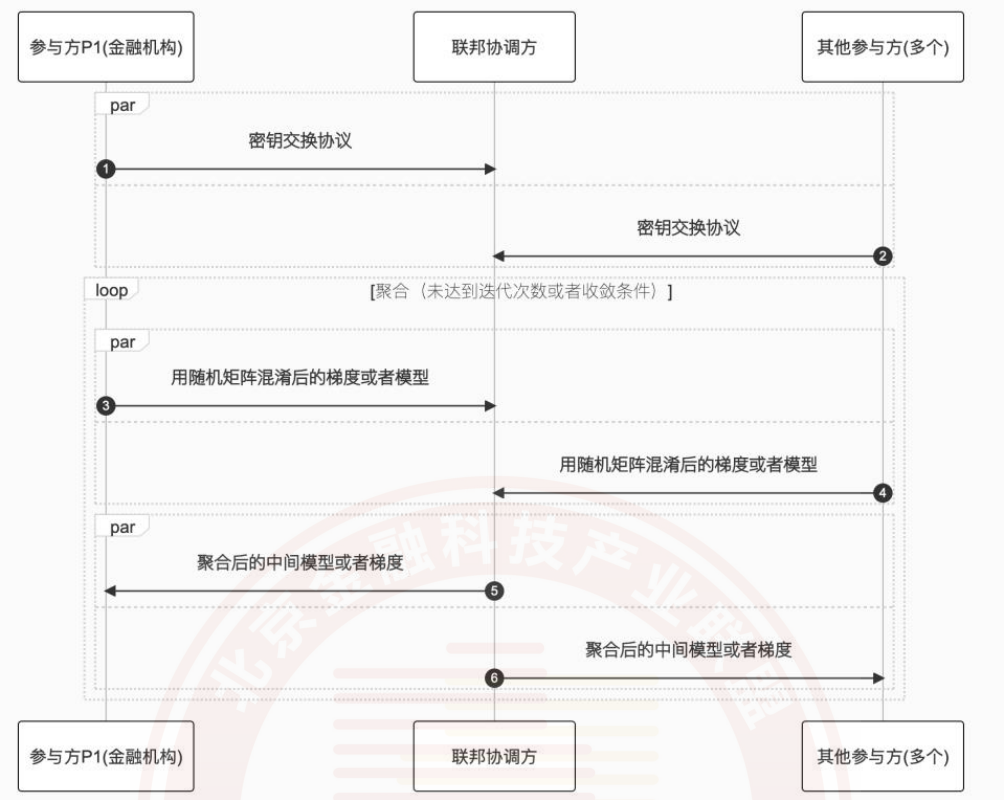

图 27 横向联邦神经网络训练的数据交换流程

3. 联邦模型推理

3.1. 线性回归推理

3.1.1. 场景说明

应用于纵向联邦线性回归模型推理

3.1.2. 扩展安全要求

纵向联邦线性回归模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方的特征数据;

——不泄露参与方的模型参数。

3.1.3. 数据交换流程

金融机构通常为应用需求方，用参与方 Guest 表示。其他机构通常为数据服务提供方，用参与方 Host 表示。线性回归模型推理的数据交换流应满足如下要求:

——参与方 Host 计算自有模型参数与特征点积 wx，发送给 Guest;

—— Guest 对 Host 发送点积与自有 wx 求和，得到推理结果。

线性回归模型推理的数据交换过程如图 28 所示。

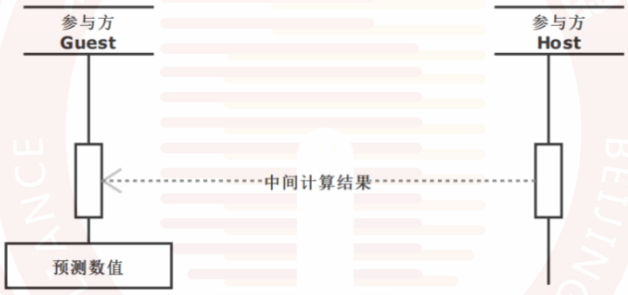

图 28 线性回归模型推理的数据交换流程

3.2. 逻辑回归推理

3.2.1. 场景说明

应用于纵向联邦逻辑回归模型推理

3.2.2. 扩展安全要求

纵向联邦逻辑回归模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方的特征数据;

——不泄露参与方的模型参数。

3.2.3. 数据交换流程

金融机构通常为应用需求方，用参与方 Guest 表示。其他机构通常为数据服务提供方，用参与方 Host 表示。逻辑回归模型推理的数据交换流应满足如下要求:

——参与方 Host 计算自有中间计算结果，发送给 Guest;

——Guest 对 Host 与己方中间计算结果求和，得到推理分数，根据设定阈值求得推理标签。

——Guest 对 Host 发送点积与自有 wx 求和，经过 sigmoid 函数后得到推理结果。

逻辑回归模型推理的数据交换流过程如图 29 所示。

图 29 逻辑回归模型推理的数据交换流程

3.3. 树模型推理

3.3.1. 场景说明

应用于梯度提升树模型推理

3.3.2. 扩展安全要求

纵向联邦树模型训练过程中的数据交换应满足如下扩展安全要求:

——不泄露参与方 Guest，Host 的特征数据;

——不泄露 Guest 方的推理结果;

——不泄露任何一方的模型参数;

3.3.3. 数据交换流程

树模型的数据交换包括一个子协议。

子协议一中，假设两方已对齐推理样本，从 Guest 方开始从根节点向下遍历，如果遇到使用 Host 方特征分裂的节点，则向 Host 方发起查询，得知方向后，向下遍历，直至达到根节点。

子协议一的数据交换流程如图 30 所示。数据交换流程应满足如下要求:

——Guest 从根开始往下遍历，如果遇到叶子节点，则向 host 发送停止变量;

——Guest 如果遇到 Host 节点，则发送该节点编号，Host 根据特征返回遍历方向;

——Host 收到停止变量后，各方停止推理。

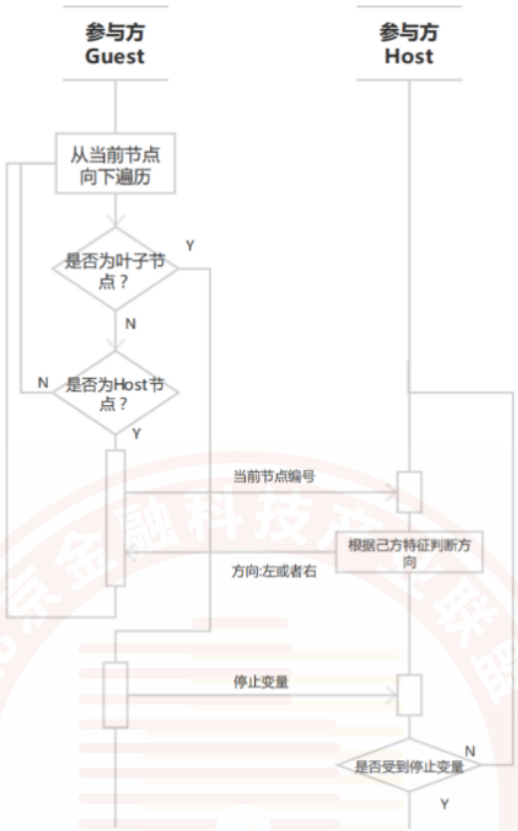

图 30 纵向梯度提升树模型推理的数据交换流程

3.4. 神经网络推理

3.4.1. 场景说明

应用于纵向联邦神经网络推理。

3.4.2. 扩展安全要求

纵向联邦神经网络推理应满足如下扩展安全要求:

——不泄露各参与方的特征数据;

——不泄露各参与方的模型参数;

——推理结果不能被非标签提供方(Host)获取。

3.4.3. 数据交换流程

金融机构通常为模型推理的发起方，用 Guest 来表示。其他机构通常为数据服务提供方，用参与方 Host 表示。纵向联邦神经网络模型推理的数据交换流程如图 31 所示，神经网络推理应满足如下要求:

——Host 方对自己的数据输入到本方的底层神经网络模型，将原始数据经过底层神经网络模型后的输出 alpha 使用同态加密算法加密后发给 Guest;

——Guest 方对自己的数据输入到本方的底层神经网络模型，将原始数据经过底层神经网络模型后的输出传输到交互层;

——Guest 将[alpha]当成交互层 Host 模型输入，计算 Host 模型输出，同时加上白噪声后发给 Host，于此同时，将 Guest 底层模型的输出当作交互层 Guest 模型输入，计算 Guest 模型输出;

——Host 方解密 Guest 方的传输数据，并补充上累计噪声导致的模型输出缺失部分发给 Guest;

——Guest 将 Host 的发送结果去除白噪声与 Guest 交互层模型输出进行拼接，并当成顶层模型的输入，计算得到上层模型输出结果即为推理的结果。

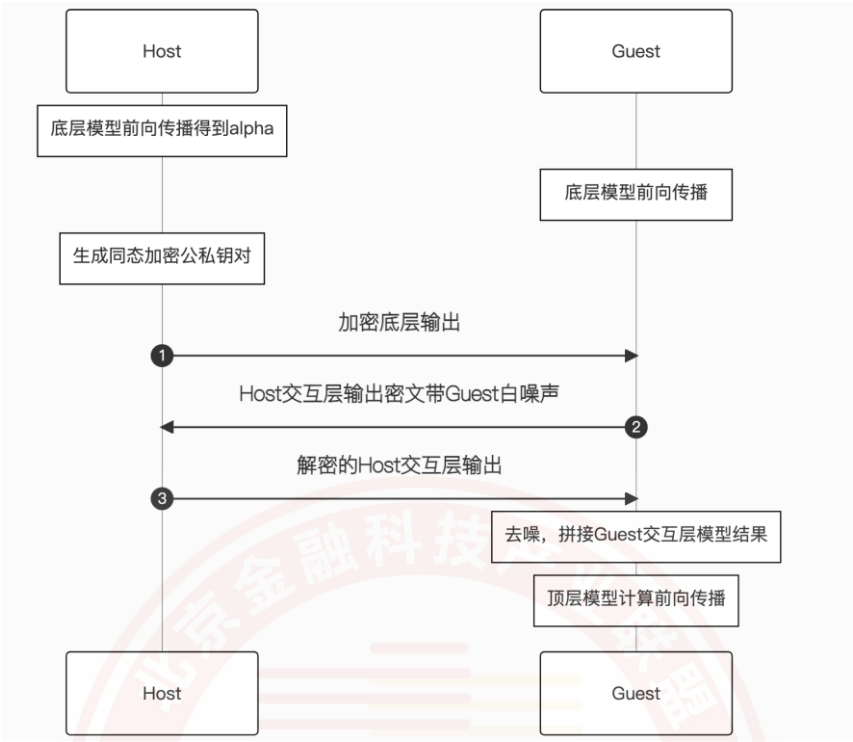

图 31 纵向联邦神经网络模型推理的数据交换流程