支持互联互通的隐私计算网关设计与实现

叶剑，李文
中国联合网络通信有限公司软件研究院，北京 100176

摘要
基于国内外隐私计算发展现状，总结了隐私计算互联互通研究进程。运用系统架构视角，阐述互联互通技术的“应用层、协议层、通信层”三层次实现路径。针对目前互联互通平台计算原理复杂、架构多样化等特点，创新性地提出Adaptation机制互联互通框架。通过关键技术的设计和实现，在保证原有功能实现的基础上，解决了不同架构的兼容问题。通过传统机器学习、横向联邦、纵向联邦具体实验场景，针对数据量、特征分布等维度，验证了Adaptation框架下互联互通可信网关的有效性和合理性。

关键词
隐私计算；互联互通；系统架构；联邦学习；可信网关

中图分类号：TP311.52 文献标志码：A doi: 10.11959/j.issn.2096-0271.2023072

Design and implementation of trusted gateway for privacy-preserving interconnection

YE Jian, LI Wen
China United Network Communications Co., Ltd., Beijing 100176, China

Abstract
Based on the current development status of privacy computing both domestically and internationally, this paper summarizes the research progress in the field of privacy computing interconnectivity. Utilizing a systemic architecture perspective, it elaborates on the implementation pathways of interconnectivity technology across three levels: the "application layer, protocol layer, and communication layer". Considering the complexities arising from the current characteristics of interconnectivity platforms, including intricate computational principles and diverse architectures, an innovative Adaptation mechanism is proposed as an interconnectivity framework. Through the design and implementation of key technologies, this framework not only ensures the realization of existing functionalities but also addresses the compatibility issues posed by different architectures. By means of experiments conducted in various scenarios encompassing traditional machine learning, horizontal federated learning, and vertical federated learning, and

considering dimensions such as data volume and feature distribution, the effectiveness and viability of the trustworthy interconnectivity gateway under the Adaptation framework have been demonstrated.

Key words
privacy-preserving computation, interconnection, system architecture, federated learning, trusted gateway

0 引言

随着隐私计算技术[1]的发展，众多技术服务供应商相继推出了多种基于不同架构的隐私计算系统。这些系统不仅为自家生态提供服务，还被应用于金融机构、政府机构等领域，它们通过隐私计算技术实现了“数据可用不可见[2]”。然而，不同隐私计算平台基于各异架构或算法原理构建，并且这些平台多为封闭架构，导致其间的有效互联互通受限，将“数据孤岛”演变成了“数据群岛”[3]。在实际应用中，作为数据使用方，往往需在与多个数据机构合作时，配置多套不同的隐私计算平台，以实现与多家数据提供机构的数据交流。这无疑严重增加了系统建设和运营成本，因此，实现互联互通逐渐成为隐私计算在实际应用中新兴的挑战。此外，在推广隐私计算技术的过程中，不同隐私计算技术平台之间的互通问题也成为限制其推广应用的重要障碍。

1 互联互通发展历程

隐私计算是指在保护数据不外泄的前提下，进行数据分析与计算的一类信息技术[4]，涵盖了数据科学、密码学、人工智能等多个技术领域。随着隐私计算技术的不断进步，隐私计算的互联互通问题日益凸显。所谓隐私计算互联互通，即在不同系统架构下，通过统一规范的接口和交互协议，实现跨隐私计算平台的数据、算法和算力的互动与协同，为用户共同完成同一隐私计算任务提供技术支持[5]。隐私计算平台互联互通的发展历程可以概括为3个阶段。

第一个阶段：不同厂商的隐私计算平台初级互联互通。

在隐私计算平台的实际应用中，数据提供机构常根据已有平台或正在研发中的隐私计算系统，为其数据应用的机构客户配置隐私计算平台。此时，隐私计算厂商需要进行一对一的技术对接，确保双方的平台相互适配。这一过程需要统一的节点管理、资源管理，以及特定算法的流程设计。因此，在这一阶段，以“通”为目标的一对一平台互联互通在业务推动下是可以实现的。在此过程中，不同隐私计算平台会选择双方都认可的标准算法，由一方主导进行技术对接，从而实现隐私计算平台的互联互通。

第二个阶段：不同厂商的隐私计算平台高级互联互通。

随着隐私计算业务规模的不断扩大，各个隐私计算厂商在为客户提供服务时将面临更加复杂的互通需求。虽然初级互联互通的实施已经初见成效，但是在开发规模、使用流程等方面仍然存在一系列挑战。鉴于此，隐私计算厂商开始探索隐私计算平台的高级互联互通，这一阶段旨在通过制定不同厂商之间的互通规范或方法，明确相互间的通信协议、报文封装以及加密算法等内容，从更高层面实现不同厂商隐私计算平台之间的互通。

第三个阶段：行业统一的互联互通标

准规范。

不同隐私计算厂商各自采用独立的隐私计算架构，导致了不同的“数据孤岛”存在并独立运行。随着隐私计算应用的普及，互联互通问题逐渐成为行业发展的重要制约因素。因此，制定一套行业统一的互联互通标准规范，已成为推动行业发展的大势所趋。

通过制定行业互联互通的标准，实现通信协议、报文格式等内容的规范化，从而在统一的通信渠道上促成不同隐私计算平台之间的互动。

2 互联互通难点

隐私计算技术的原理异常复杂，且平台架构存在多样性。因此，实现隐私计算平台之间的互联互通，不仅需要解决不同架构的问题，还必须确保对原有功能的完整保留，同时确保对不同架构的兼容性。这种复杂性为实现互联互通带来了严峻的挑战。

首要的挑战在于实现原理的多样性。不同隐私计算技术供应商拥有自己的核心知识产权，而不同的算法设计影响着数据计算逻辑和数据交互流程。不同算法设计原理的差异导致了各个隐私计算平台之间无法互通的问题。此外，隐私计算平台的通信模块、加密组件、资源管理、任务管理、模型管理、节点管理、授权管理等功能组件在不同技术服务提供商之间存在差异，这些差异是由技术积累和场景应用的不同造成的。因此，隐私计算平台底层实现原理的多样性成为互联互通的首要难题。

其次，不同厂商间的差异也是互联互通的难点。由于众多厂商参与，如何实现多家隐私计算平台的互联互通也变得异常复杂。

3 实现路径

隐私计算技术是解决数据流通与数据隐私保护之间矛盾的关键技术，随着隐私计算在大规模应用中的推广，隐私计算平台之间的互联互通变得尤为关键。为此，本文着眼于隐私计算平台的架构来探讨实现互联互通的途径。

从系统架构的角度来看，隐私计算平台可以被划分为3个关键层次：应用层、算法层和原语层。这些层次分别承担不同的隐私计算功能，互联互通的实现同样也应从这3个层次出发。因此，从架构的角度来看，隐私计算平台的互联互通可以划分为应用层互联互通、算法层互联互通和原语层互联互通[6]。

应用层互联互通指的是不同的隐私计算平台能够在应用层面实现系统管理功能的互通，例如节点发现、资源管理等，从而在不同平台之间实现业务层的互联互通。

算法层互联互通涉及不同隐私计算平台在技术服务厂商之间建立特定算法原理的标准设计方式。这种算法实现的原理在各个隐私计算平台中是透明的，不同厂商可以根据自身的技术栈实现同一种算法的设计以及交互流程，从而实现不同隐私计算平台之间的互通。

原语层互联互通。不同隐私计算平台往往采用不同的算法或协议实现方式。无论采用何种隐私计算技术方案，都可以将算法或协议拆分为最小粒度的计算原语。以安全多方计算采用的ABY3秘密分享协议为例，互通参与方需要按照该协议的原理定义流程，进行原始数据的密文拆分，在密文基础上实现加密计算算子。

借助协议原理，可以在每个步骤中分别实现计算原语的抽象和定义，在不同隐私计

算平台之间对计算原语进行各自的实现，从而在原语层次上实现互联互通。进一步地，可以基于底层计算原语的中层算法实现以及上层应用服务实现，实现平台之间的互联互通。

异构隐私计算平台在3个层面上实现互联互通，必须在互联互通协议的流程设计和代码实现方面进行落实。由于流程与代码均来自不同厂商的实现，各家的开放程度也不尽相同。因此，基于流程和代码实现方式的差异，可以将其分为3种不同的实现方式：协议互联、SDK互联和Client互联。

本文创新地提出了Adaptation机制，以实现异构隐私计算平台的应用层和算法层的互联互通。

4 系统设计

4.1 设计目标

本系统设计的核心目标在于解决异构隐私计算平台在应用层和算法层之间的互联互通问题，以促进联邦学习[7]平台之间的协同增益，从而满足互通和能力扩展的需求。TrustGate网关中Adaptation机制主要通过Adaptation模块借助适配器机制在应用层实现异构隐私计算平台的适配，通过映射引擎与算法管理在算法层进一步实现异构隐私计算平台之间的互通。最终集成了TrustGate网关的FATE、SecretFlow等异构隐私计算平台，在应用层和算法层实现了互联互通。

4.2 架构设计

互联互通Adaptation模块如图1所示，TrustGate网关中Adaptation模块的架构设计旨在实现隐私计算平台的互联互通。后文详细阐述了其Adaptation互联机制的实现原理。

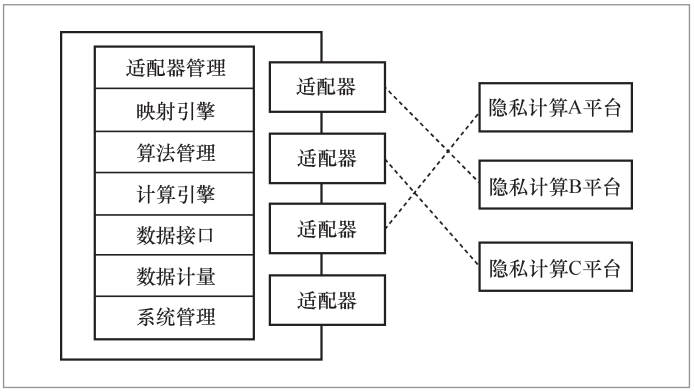


图1 互联互通 Adaptation 模块

Adaptation模块涵盖了多项关键功能，包括适配器管理、映射引擎、算法管理、计算引擎、数据接口、数据计量以及系统管理。通过适配器管理，该模块实现了对不同隐私计算平台客户端的配置。利用多样的适配器，成功促成了与异构隐私计算平台客户端在应用层的互联互通。接着，通过映射引擎的协同运作，实现了不同隐私计算平台之间算法参数的同步，从而在算法层面实现了跨平台的互联互通。这种设计不仅在应用层面，而且在算法层面实现了不同隐私计算平台之间的互通。Adaptation模块在强调了安全性、可控性以及可计量性的同时，具备了实现跨平台互联互通和灵活扩展的特点。

在应用层互联互通方面，Adaptation模块具备众多适配器，每个适配器针对其他异构隐私计算平台进行适配，从而实现异构平台间的互联互通和统一资源管理。适配器管理包括节点管理、资源管理等功能。

节点管理的主要功能是管理不同隐私计算平台的节点，支持隐私计算平台节点的创建、编辑和删除。节点基本信息（如名称、描述、端口、平台等）可以进行维护管理，同时支持节点详细信息（如任务详情等）的展示和搜索查询功能。

资源管理用于实现应用层异构隐私计

算平台之间各类资源的有效管理。

在算法层互联互通方面，Adaptation模块借助映射引擎和算法管理，实现了基于同一算法的异构隐私计算平台之间参数的相互传递和互联互通。

具体包括：

- 不同隐私计算平台的适配，实现互联互通；
- 算法数据和参数的路由；
- 参数的同步；
- 任务状态的同步。

因此，Adaptation模块在算法层面实现了互联互通。

综上所述，TrustGate网关中Adaptation模块借助适配器管理、映射引擎和算法管理，成功实现了FATE、SecretFlow等异构隐私计算平台在应用层和算法层的互联互通。

5 系统实现

5.1 实现架构

本文设计了一个多层结合的松耦合系统架构，如**图2**所示，该系统架构集成了联邦学习、区块链、大数据等技术平台。平台搭建在大数据平台上，依靠大数据资源平台的算力、存储、网络等资源。数据存储在HDFS上，使用Spark计算资源。平台主要由TrustGate、SecretFlow、FATEClient和WebManager四大部分组成。

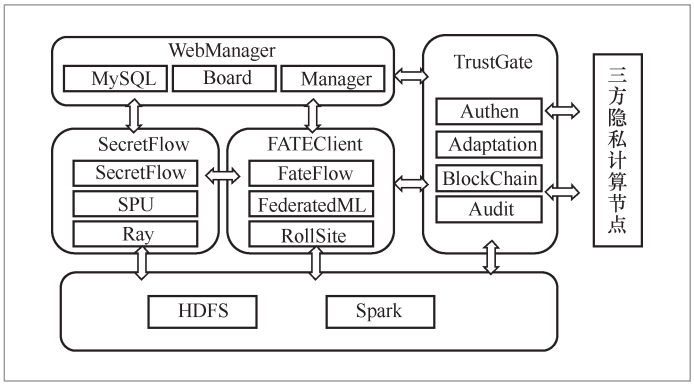


图 2 松耦合系统架构

TrustGate网关负责与外部系统对接、隐私计算平台的互联互通适配和可信存证等逻辑的实现。Adaptation模块是TrustGate网关的重要组成部分，主要负责异构平台的互联互通。

SecretFlow负责联邦学习各种多方安全计算（secure multi-party computation，MPC）算子库、加密算法库、安全求交、特征工程等一系列隐私计算相关功能组件的实现。

FATEClient负责FATE[8]协议的接入和转化，实现与FATE类节点的互联。

WebManager负责各类管理数据的存储与流程管理及可视化展示。

5.2 跨平台架构解析

关于隐私计算跨平台互联互通的设计，可以采用“底层通信-中间层交互-顶层应用”的方法来制定实现路径。

（1）应用层

在明确定义通信需求和互联协议栈的基础上，需要定义在跨平台隐私计算任务的实现过程中的协同管理要求和具体场景的实现流程。这不仅涵盖了跨平台任务的编排、调度、执行、监控和存证等统一规则，还包括对不同类型计算任务的实现流程的规范约定。

（2）协议层（交互层）

在协议层，可以从节点、资源和算法执行3个维度出发，进一步明确跨平台交互过程中各个环节的规范流程和要求，包括但不限于发现、认证、申请、授权、连接调用、信息交换和状态同步等。

(3)通信层

在通信层，需要规范化涉及平台间通信的各个方面，包括通信框架的选择、通信接口的定义、数据格式的规范以及传输机制的制定。

值得注意的是，整个互联互通的适配将在TrustGate的Adaptation模块中实现，该模块将负责平台之间的协调与适配。以上方法能够更好地设计和实现隐私计算跨平台互联互通的架构。

5.3 功能验证

本文使用集成TrustGate网关的FATE与SecretFlow隐私计算平台验证互联互通的有效性，开展基于“单移转融”业务场景数据的联合建模训练，并对联邦学习建模效果进行评估。使用联邦学习机器算法建立二分类模型，预测出潜在的单移转融用户。

(1)特征选取

基本信息：业务行为、用户价值、终端类型、用户交往圈。

(2)模型训练

安全求交：对数据样本进行分割，模拟两方数据，通过RSA加密算法，进行安全求交。

算法选择：通过纵向逻辑LR算法和SecureBoost算法效果比对，最终选择SecureBoost算法。

模型优化：对关键参数调优，如树深度、子节点个数等，输出最优模型。

(3)效果比对

不同样本数量：对样本进行横向分割，对比建模效果及预测数据。

不同特征数量：对样本进行纵向分割，对比建模效果及预测数据。

5.3.1 横向联邦场景

集成TrustGate互联互通网关的隐私计算平台横向联邦[9]实验结果见**表1**，对比发现F1值随数据变化趋势不明显，曲线下面积(area under the curve，AUC)随数据体量逐渐变大。

如**图3**所示，拟合曲线符合实际情况，在单边数据由50万条逐渐变大的情况，AUC逐渐增大，增大趋势逐渐降低。

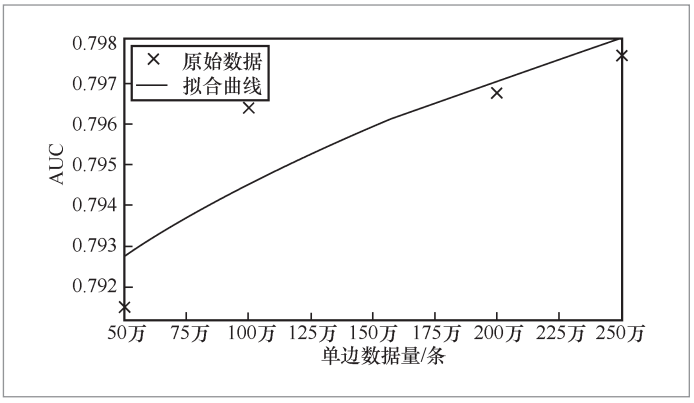


图 3 集成 TrustGate 互联互通网关的隐私计算平台横向联邦实验结果对比分析

表 1 集成 TrustGate 互联互通网关的隐私计算平台横向联邦实验结果

样本数量/条	host方特征个数/重要特征个数	guest方特征个数/重要特征个数	AUC	Precision	Recall	F1值	阈值(取最好的指标即可)
100万(每侧50万)	41	41	0.791519	0.5323	0.231	0.322295	0.79
200万(每侧100万)	41	41	0.796426	0.5755	0.226	0.324828	0.71
400万(每侧200万)	41	41	0.79676	0.5416	0.2346	0.327377	0.7
500万(每侧250万)	41	41	0.797694	0.4887	0.2378	0.328208	0.68

5.3.2 纵向联邦场景

（1）纵向联邦学习随数据量变化趋势

纵向联邦随数据量变化实验结果见**表2**。建模效果：集成TrustGate互联互通网关的隐私计算平台，纵向联邦场景[10]下，模型AUC、F1值随训练样本增加而逐渐增大，分别如**图4**、**图5**所示。

表 2 纵向联邦随数据量变化实验结果

样本数量/条	AUC	Precision	Recall	F1值
50万训练/500万验证	0.805648	0.608	0.215	0.318766
200万训练/500万验证	0.808	0.57	0.24	0.339472
500万训练/500万验证	0.817468	0.62	0.255	0.361701

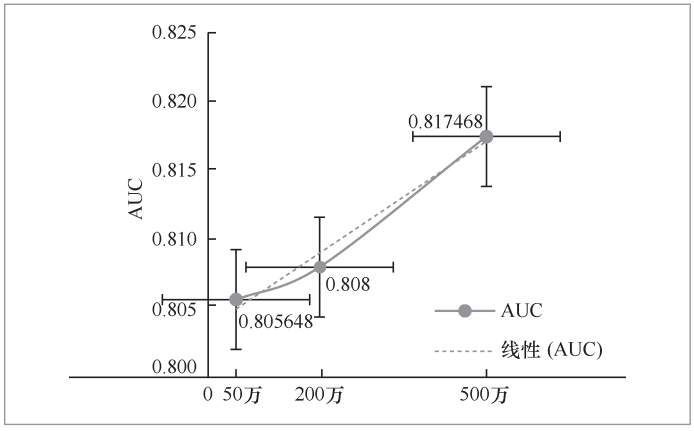


图 4 纵向联邦随数据量变化实验 AUC 变化趋势

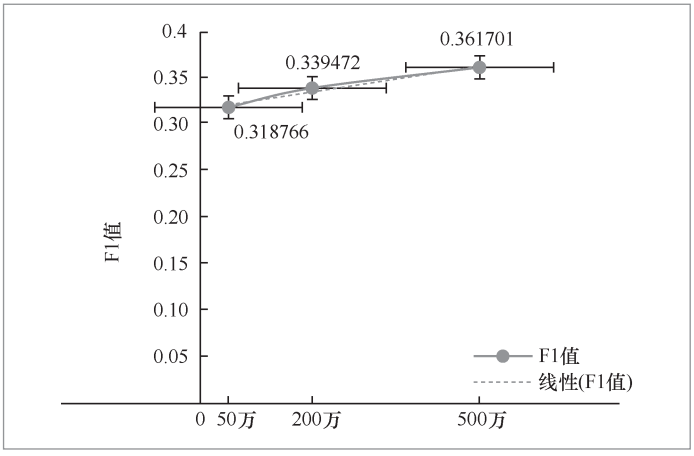


图 5 纵向联邦随数据量变化实验 F1 值变化趋势

实验结论：集成TrustGate互联互通网关的隐私计算平台，纵向联邦学习与普通机器学习一样，随训练样本的增加，模型效果随之提升。

（2）纵向联邦学习随特征维度增加变化趋势

纵向联邦学习随特征维度增加实验结果见**表3**。建模效果：模型AUC、F1值随训练样本特征维度增加而逐渐增大，分别如**图6**、**图7**所示。

实验结论：集成TrustGate互联互通网关的隐私计算平台，纵向联邦学习与普通机器学习一样，随训练样本特征维度增加，模型效果随之提升。

（3）纵向联邦学习随重要特征分布变化趋势

纵向联邦学习随重要特征分布实验结果见**表4**。建模效果：模型AUC、F1值基本稳定，分别如**图8**、**图9**所示。

实验结论：集成TrustGate互联互通网关的隐私计算平台，纵向联邦学习训练结果与重要特征分布在哪方无关。

5.4 性能验证

使用集成TrustGate网关的FATE与SecretFlow隐私计算平台互联互通，开展性能测试。按照隐私计算产品性能测评标准化研究方案，在特定硬件资源、特定数据集、特定算法要求和特定结果要求条件下，模拟实际需求场景，通过性能测试，测试隐私计算平台准确性指标。

隐私计算平台严格遵守隐私保护原则，确保用户输入数据保密，各计算方中间数据私密，全局中间数据未暴露。在联合建模联邦学习中，采取有效措施保护本地梯度等敏感信息，杜绝泄露。整合TrustGate网关的FATE隐私计算平台继

表 3 纵向联邦学习随特征维度增加实验结果

样本数量/条	host方特征个数	guest方特征个数	AUC	Precision	Recall	F1值
500万训练/500万验证	5	5	0.734017	0.309	0.248	0.275305
500万训练/500万验证	10	10	0.785428	0.396	0.246	0.303039
500万训练/500万验证	15	15	0.785723	0.394	0.244	0.301387
500万训练/500万验证	20	20	0.789237	0.454	0.244	0.317558

表 4 纵向联邦学习随重要特征分布实验结果

样本数量/条	重要特征分布	AUC	Precision	Recall	F1值
500万训练/500万验证	12个重要特征均不在标签方	0.789234	0.4995	0.229	0.314305
500万训练/500万验证	3个重要特征在标签方	0.789238	0.454	0.2441	0.31756
500万训练/500万验证	6个重要特征在标签方	0.789238	0.454	0.2441	0.317553
500万训练/500万验证	12个重要特征均在标签方	0.789239	0.454	0.2441	0.317562

续支持差分隐私技术，通过引入噪声，使个体数据贡献难以确定，在模型训练中降低泄露风险。FATE运用差分隐私确保模型训练隐私，同时支持同态加密技术，允许加密状态下计算，保护数据隐私。FATE应用同态加密在加密状态下执行计算任务，进一步维护数据隐私。

根据准确性评估要求，依然选取“单移转融”真实联合建模场景，使用TrustGate网关Adaptation模块实现互联互通网关的隐私计算平台和与传统机器学习算法程序，在保证样本数据集、特征选择和训练参数一致的前提下分别进行建模训练。若该产品通过隐私计算得到的模型的评价指标（如AUC和KS值）和相对应的明文机器学习训练得到的基准模型的评价指标保持在规定的误差范围内，则表示通过核验。

实验验证传统数据集中式建模与TrustGate互联互通网关隐私计算平台联邦学习效果。同样本同特征与同样本不同特征两种维度的建模效果及预测数据比对实验结果见**表5**，AUC与F1值的变化趋势分别如**图10**、**图11**所示。

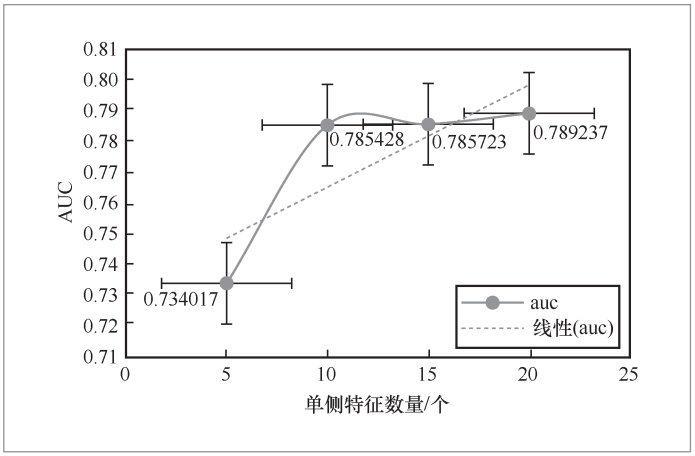


图 6 纵向联邦学习随特征维度增加实验 AUC 变化趋势

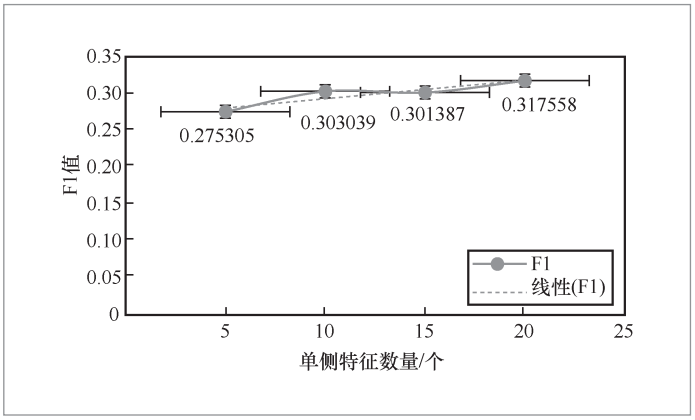


图 7 纵向联邦学习随特征维度增加实验 F1 值变化趋势

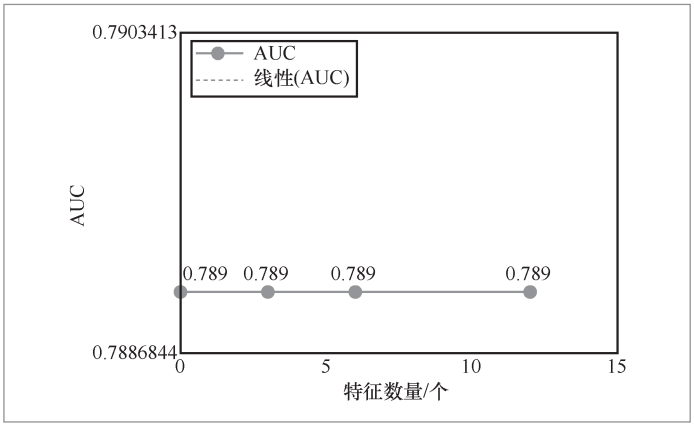


图 8 纵向联邦学习随重要特征分布实验 AUC 变化趋势

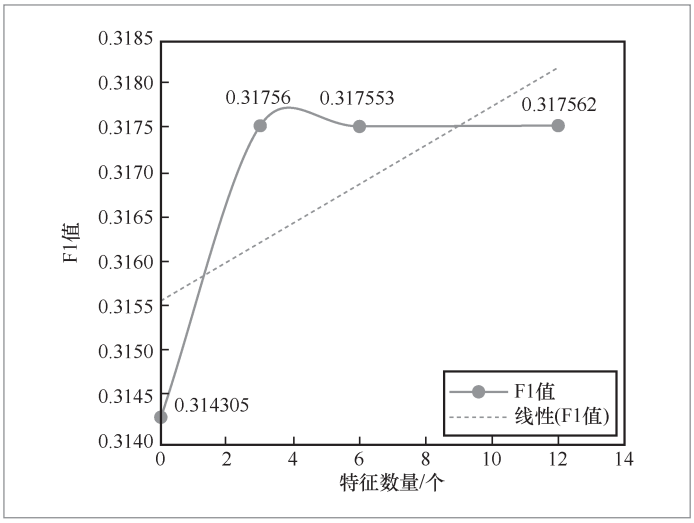


图 9 纵向联邦学习随重要特征分布实验 F1 值变化趋势

建模效果如下。

AUC值：传统建模（20个特征）<联邦学习（41个特征）<传统建模（41个特征）。

F1值：传统建模（20个特征）<联邦学习（41个特征）<传统建模（41个特征）。

实验结论：集成TrustGate互联互通网关的隐私计算平台联邦学习的效果接近于全特征机器学习。相比于半特征建模，无论是F1值、还是AUC，效果均有显著提升。

5.5 实验结论

从上述实验结果可以观察到，通过集成TrustGate网关的FATE与SecretFlow隐私计算互联互通平台在功能和性能两个方面都经过了验证。

TrustGate网关的引入实现了FATE与SecretFlow隐私计算平台之间的有效互联互通，成功地展现了在“单移转融”场景下横向联邦和纵向联邦的实验。在相同的样本量下，普通模型训练的效果与整体联邦学习效果相差无几。随着特征维度的增加，联邦模型训练的效果逐渐提升。

此次验证实验是在集成TrustGate网关的FATE框架基础上进行的，成功地验证了数据的不可见性、数据的可信存证、数据的可计量性以及互联互通等多个方面。其中，数据不可见性、数据可信存证和数据可计量性的验证均取得了预期效果。为了实现互联互通，本文引入了Adaptation框架，有效地实现了异构联邦学习平台之间的互操作性，部分实验也获得了预期的积极结果。

基于实验结果的分析，本次验证实验顺利达成了预期目标，充分证明了互联互通网关的有效性。因此，本文提出的技术方案在实际可行性方面具备了明确的支撑。

表 5 TrustGate 互联互通网关隐私计算平台联邦学习与集中式机器学习建模效果比对实验结果

对比项	样本	特征个数/个	AUC	Precision	Recall	F1值
互联互通网关隐私计算平台	200万训练/500万验证	41	0.792	0.502	0.225	0.311
传统建模（全特征）	200万训练/500万验证	41	0.796	0.536	0.223	0.315
传统建模（半特征）	200万训练/500万验证	20	0.779	0.452	0.184	0.241

6 结束语

隐私计算技术已经在数据安全交互和协同中发挥了积极的作用，得到了快速发展和越来越多的应用。面向未来更加广泛深入的规模应用和构建良好产业生态的需求，隐私计算技术还需要在提升效率、降低开销、开展安全保障的评估和评测、扩展适配更多算法和协议、实现不同框架的兼容和互联互通等方面进行深入研究。

（1）促进不同技术框架和产品之间互联互通

针对目前业界隐私计算技术框架众多、彼此无法互通协作的突出问题，迫切需要解决不同技术框架和产品之间的互联互通问题。一个机构无须部署多个系统，而是通过一套服务，与外部各种机构进行大数据协同的连接合作。对于企业或实体，研究跨行业跨平台的转换和对接技术，实现最大限度的互联互通，让各方基于数据实现更好的合作。

（2）推进国际国内隐私计算技术的标准化

当前，国内外众多标准化组织已开始制定或发布以框架和功能为主的隐私计算相关技术标准。相关技术标准已经开始从基础的功能标准向产品性能、安全性等方向拓展，加速构建更加完善的隐私计算技术标准体系。中国移动已牵头或参与在TMF、IEEE 以及国内的全国信息安全标准化技术委员会、CCSA等标准化组织设立13个标准，重点围绕隐私计算在技术框架的互联互通、安全评估与测试、数据价值评估和激励机制以及未来通信网络中的应用场景等方面开展标准制定工作。

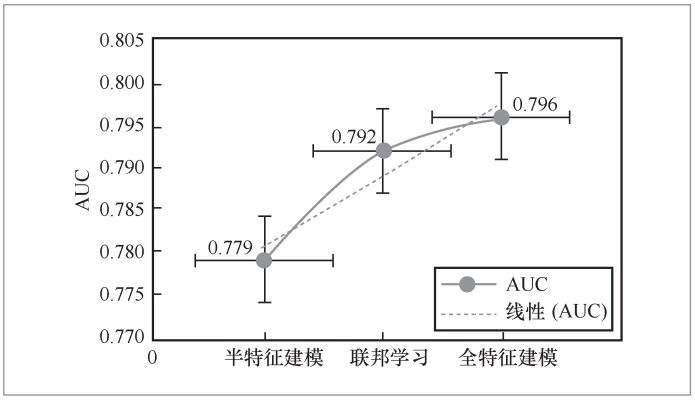


图 10 TrustGate 互联互通网关隐私计算平台联邦学习与集中式机器学习建模效果比对实验结果 AUC 变化趋势

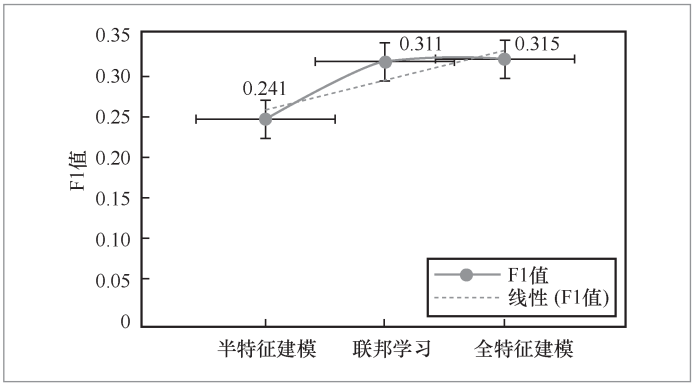


图 11 TrustGate 互联互通网关隐私计算平台联邦学习与集中式机器学习建模效果比对实验结果 F1 值变化趋势

参考文献:

[1] UN Global Working Group on Big Data. UN handbook on privacy- preserving computation techniques[R]. 2019.

[2] 隐私计算联盟，中国信息通信研究院. 隐私计算应用研究报告(2022年)[R]. 2022.
Privacy Computing Alliance, China Academy of Information and Communications Technology. Research report on privacy computing applications (2022)[R]. 2022.

[3] 王思源，闫树. 隐私计算面临的挑战与发展趋势浅析[J]. 通信世界，2022(2)：19-21.
WANG S Y, YAN S. Challenges and development trends of privacy computing[J]. Communications World,

2022(2): 19–21.

[4] 隐私计算联盟, 中国信息通信研究院. 隐私计算白皮书[R]. 2021.
Privacy Computing Alliance, China Academy of Information and Communications Technology. Privacy computing white paper[R]. 2021.

[5] 吕艾临, 闫树. 隐私计算跨平台互联互通的若干思考[J]. 信息通信技术与政策, 2022(5): 2–6.
LYU A L, YAN S. Some thoughts on cross–platform interconnection of privacy preserving computing[J]. Information and Communications Technology and Policy, 2022(5): 2–6.

[6] 姚明, 何浩, 李博, 等. 隐私计算跨平台互联互通研究与实践[J]. 中国科技信息, 2022(16): 140–143.
YAO M, HE H, LI B, et al. Research and practice on cross–platform interconnection of privacy computing[J]. China Science and Technology Information, 2022(16): 140–143.

[7] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication–efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. [S.l.:s.n.], 2017: 1273–1282.

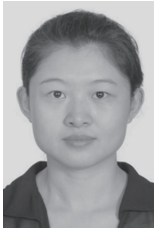
[8] LIU Y, FAN T, CHEN T J, et al. FATE: an industrial grade platform for collaborative learning with data protection[J]. Journal of Machine Learning Research, 2021, 22(226): 1–6.

[9] KAIROUZ P, AVENT B, MCMAHAN H B, et al. Advances and open problems in federated learning[J]. Foundations and Trends® in Machine Learning, 2021, 14(1/2): 1–210.

[10] FENG S, YU H. Multi–participant multi–class vertical federated learning[EB]. arXiv preprint, 2020, arXiv: 2001.11154.

作者简介

叶剑(1976–), 男, 中国联合网络通信有限公司软件研究院高级工程师, 主要研究方向为大数据技术、数据挖掘、数据安全、人工智能、数据治理等。



李文(1991–), 女, 中国联合网络通信有限公司西安软件研究院助理工程师, 主要研究方向为可视化大数据分析、大数据治理、数据安全等。

收稿日期: 2023–07–05