隐私计算

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2022-05-10 10:45:49

腾讯云隐私计算（Privacy Computing）是腾讯云推出的以联邦学习（FL）、安全多方计算（MPC）、可信执行环境（TEE）等隐私数据保护技术为基础的隐私计算平台，产品针对机器学习算法进行定制化的隐私保护改造，保证原始数据不出本地即可完成联合建模，同时支持安全多方 PSI（隐私保护集合求交技术）、安全隐私查询、安全统计分析，提供基于硬件的 TEE 可信执行环境。通过腾讯云隐私计算，各合作机构既能保障数据安全，又能发挥数据最大价值，很好地解决了业界数据孤岛的难题。

产品功能

腾讯云隐私计算平台包含了联邦学习（FL）、安全多方计算（MPC）、可信执行环境（TEE）3个部分，平台目前提供了节点管理、数据接入、安全求交、特征工程、数据分析、模型训练、模型管理等功能。

节点管理

在完成隐私计算平台部署后，需要在前端控制台进行隐私计算节点注册，用户可以添加、删除节点，在添加节点时会进行节点校验，校验通过的节点之间即可开始数据合作。

数据接入

腾讯云隐私计算平台可以直接对接大数据生态，支持分布式文件存储系统 HDFS 及本地文件系统，能够灵活地适应用户的实际情况。在整个流程中都不涉及用户数据上传，仅是在平台注册数据。

数据检测

在注册数据流程中需要进行数据本地检测，检测数据格式是否符合规范。例如，是否使用相同的用户 ID 主键、是否是相同的时间粒度、是否使用相同的加密方法等，只有双方/多方数据都符合规范才能进行数据合作。

安全求交

在纵向联邦场景中，模型训练之前都需要基于交集 ID 准备数据，安全求交可以轻松帮助合作双方进行 ID 对齐。在 ID 敏感的场景，依托于隐私求交及首创的非对称联邦技术，平台还能有效解决样本 ID 交集泄露的问题。

特征工程

特征工程是模型训练中必不可少的环节，通过联邦定制化改造，平台已经支持分箱、特征过滤、OneHot、缺失值填充、单变量衍生等主流特征工程。

数据分析

在联邦模型训练过程中，算法人员通常都需要对入模特征的统计分布、相关性等作出深入了解。针对多方数据，在保护各方数据隐私的前提下，做统计、相关性等联合数据分析。

模型训练

本平台目前支持 LR、XGBoost 两种算法，基于联邦学习协议对算法进行定制化改造从而达到无损的模型训练效果，基本已满足主流的纵向联邦场景。同时，平台正在适配 MLP、DSSM（双塔）、Deep&Wide 等算法，从而能更好的支持大数据量的推荐场景。

模型管理

模型训练完成后会生成对应的模型实例，在算法人员调试模型的过程中一般会生成多个模型实例，模型管理能帮助算法人员更好地对比模型参数和效果数据，从而有针对性地优化模型。模型管理包括删除模型、查看日志、模型上线、模型下线等功能。

在线服务

模型训练完成后就需要将其发布上线供业务侧实时调用，同时在线服务还实现了实时匿名查询等功能，能避免因为查询而暴露真实客户 ID。

调用统计

统计合作双方机器学习模型和安全查询调用次数，方便进行统计结算。

产品优势

最近更新时间：2022-01-12 14:07:32

产品安全性

平台不接触客户原始数据，合作方之间只传递中间加密参数，从框架和算法层均保障无任何中间第三方参与。

产品稳定性

产品基于 K8s 集群可做到灵活扩展，最大化保障平台稳定性。

产品性能

基于 Apache Spark、Apache Pulsar，产品计算性能和网络性能优异，并且可以适配不同场景的不同训练量级横向扩展资源，保证性能稳定可控。

专业机构背书

2019年获取信通院首批安全多方计算认证，当年一共只有5家公司获得该证书；2020年又获取了联邦学习和安全多方计算双认证。

应用场景

最近更新时间：2022-05-10 10:45:56

跨机构数据合作场景

在银行、保险、政务、教育、电商等众多行业的业务场景中，都会涉及到跨机构、跨部门的数据合作，但数据隐私泄露问题又是一个长期无法逾越的障碍。腾讯云隐私计算平台正好完美地解决了这个问题，只需在合作方之间传递加密中间参数即可完成联合建模，最大化保障了合作方之间的数据安全。

银行信贷场景

在银行信贷业务整个闭环中，从引流阶段的营销服务，到贷前、贷中、贷后全面风控服务，腾讯云隐私计算平台衔接各方数据能力，在保障各方数据隐私安全的基础上助力银行信贷业务顺利展开。

保险业务场景

在保险业务整个闭环中，从引流阶段的营销服务到核保、赔付的全面风控服务，腾讯云隐私计算平台衔接各方数据能力，在保障各方数据隐私安全的基础上助力保险业务顺利展开。

政务数据开放场景

在某些政务大数据应用场景中，例如政数局需要开放数据赋能银行、高校及其它企业，但又不能直接输出数据。在这种情况下腾讯云隐私计算平台正好作为一个完美的平台解决方案帮助政数局数据开发业务顺利展开。

在线教育营销场景

最近两年在线教育突飞猛进，营销获客及优化引流质量就成了在线教育机构的重中之重，腾讯云隐私计算平台正好能够衔接各方数据能力，在保障各方数据隐私安全的基础上助力教育营销业务顺利展开。

广告 RTA 场景

RTA（实时应用程序接口 Real Time API）是主流网络媒体向其广告主开放的一项流量精选技术，允许广告主以实时接口方式控制每一个媒体广告展示机会是否参与竞价。但并非每个广告主都具备有效的数据能力，腾讯云隐私计算平台恰好能够衔接各方数据能力，在保障数据隐私安全的基础上助力广告主优化用户质量。
"