机密计算平台

产品简介

腾讯云

文档目录

产品简介

产品概述

最近更新时间：2022-12-09 10:13:35

什么是机密计算平台

机密计算平台（Confidential Computing Platform，CCP）是一款腾讯云推出的基于可信执行环境（Trusted Execution Environment，TEE）打造的隐私安全基础平台，可以为用户提供机密计算轻松接入，服务托管，一站式运维等功能，实现端到端全生命周期保护用户数据的机密性和完整性，满足用户多应用多业务多场景的安全需求。

产品功能

命令行工具

机密计算平台提供命令行工具，令用户的应用或容器镜像直接适配到机密计算环境中，无需重编译即可低门槛接入。

低门槛接入

用户无需对业务进行改造，即可轻松快速接入机密计算平台，保护用户数据的机密性和完整性。

唯一私钥

机密计算平台集成了密钥管理系统（KMS ）的密钥管理服务，用户使用机密计算服务时，会生成唯一私钥用于加密镜像，在密文传输到 TEE 可信环境中再解密运算。

可信执行环境

可信执行环境技术（TEE）提供了可行的技术支持，其核心思想是以可信硬件为载体，提供硬件级强安全隔离和通用计算环境，数据仅在隔离的安全区“飞地”（Enclave）内才进行解密并计算，数据在离开“飞地”（Enclave）之前会被自动加密，离开“飞地”（Enclave）后无法接触数据明文内容。

产品优势

最近更新时间：2022-12-09 10:44:42

安全性高

应用程序运行在高度隔离的硬件飞地环境，保证了用户数据的“使用中”安全，解耦了对云平台的信任依赖，实现了应用的安全自治。

易用性强

平台提供适配工具，令用户的应用或容器镜像直接适配到机密计算环境中，无需重编译即可低门槛接入。

集中化密钥管理

支持通过 API、SDK 及已经对接的云产品接入腾讯云密钥管理系统（KMS ）服务，并使用 KMS 集中管理业务应用的密钥策略，无论这些业务应用是在腾讯云或是腾讯云外。

安全环境

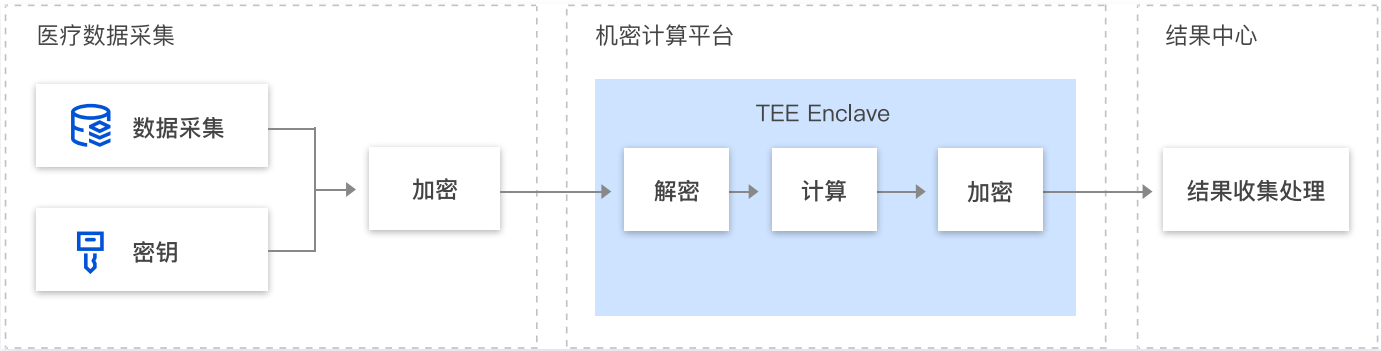
密钥管理系统（KMS）使用经过第三方认证的硬件安全模块 HSM 来生成和保护密钥，保障用户主密钥的创建、管理等操作都将在HSM 硬件中进行，能够保障用户的明文主密钥。

应用场景

最近更新时间：2022-12-09 10:13:35

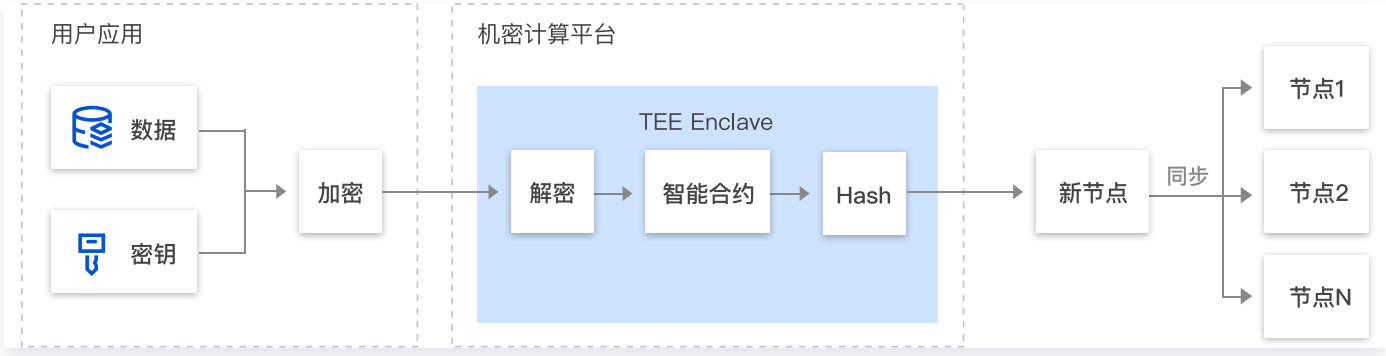
医疗隐私保护

- 痛点：医疗数据是私密性很高的数据类型，医疗采集后会进行加密，数据库中均是密文的状态，但加密后的数据很难支持计算，引用明文数据进行计算又存在隐私问题。
- 方案：将密文传入 TEE 中进行解密计算，将计算结果重加密，用户可以在 TEE 中部署指定算法，同时支持完整性验证，机密计算平台可帮助用户管控 TEE 的边界，当 TEE 在任务结束后，提供方法证明其被彻底销毁/重置。



区块链智能合约

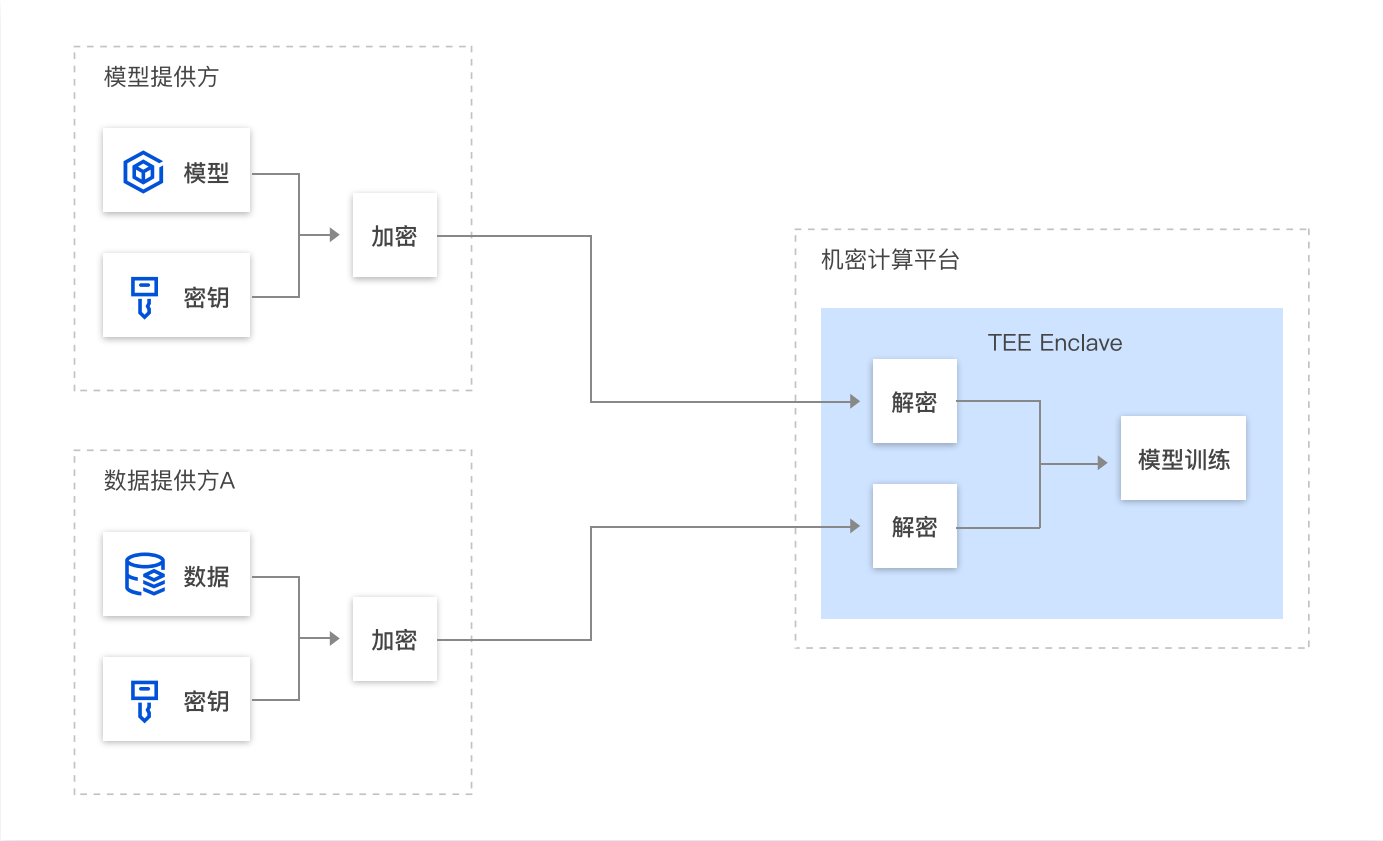
- 痛点：当用户传输电子合约时，以往多数以明文的形式传输或者以明文数据的形式在服务端进行运算，且无法识别验签。通过机密计算平台可实现密文传输，在可信环境内再解密验签，且可信环境下分为多节点，有效避免数据泄露等风险问题。
- 方案：用户可通过接入机密计算平台实现合同流转全流程的节点见证，真实可溯源，规避不透明性；密钥加密传输到可信环境内再解密签署大大降低了内容泄密的风险，区块链智能合同能有效溯源验证签署人的身份信息。



模型训练

- 痛点：模型训练的过程往往伴随许多的数据传输，且模型和数据结合使用需要有足够安全的环境，以往传输过程没有加密或者运算环境无法高度可信。机密计算集成了 TEE 可信环境，保证运行环境的安全性同时还能够提供加密功能，密文传输提高模型训练环境的整体防泄密。

- 方案：通过机密工具可实现系统零改造接入机密计算平台，用户通过调用 API 实现对机密运算环境的管理与控制，一体化的加密集成提高了传输安全性的同时，还降低了模型与数据传输过程的泄密风险，大大提升建模效率。



多方联合建模

- 痛点：企业各部门数据相互独立存储、各自定义，部门间的数据无法进行连接互动，形成数据孤岛。现有的共同建模和模型分享局限于性能，且支持算法有限。
- 方案：训练算法部署在 TEE 中，数据方将密文数据传入 TEE，解密后进行训练，验证整个 TEE 生命周期，确保 TEE 完整性，且在任务完成后销毁。