中国联通
China unicom

机密计算共享数据价值白皮书

中国联通研究院
中国联通网络安全研究院
下一代互联网宽带业务应用国家工程研究中心

2023 年 11 月

版权声明

目录

前 言

本白皮书围绕数据安全的发展与产业需求，介绍中国联通云机密计算平台实践案例。

本白皮书起草单位：中国联合网络通信有限公司研究院（中国联通网络安全研究院、下一代互联网宽带业务应用国家工程研究中心）、英特尔（中国）有限公司。

编写组成员：

侯乐、徐雷、王莹、贾宝军、杨双仕、胡慧、陶冶、曹咪、胡自强、马建伟、田莉。

一 背景

随着数字经济发展和数字技术变革，数据成为继土地、劳动、资本等之后人类又一重要生产要素。数据流通带来的价值越来越受到重视，与此同时，数据流通暴露出的安全风险问题也备受关注。2023年1月，工信部等十六部门联合发布了《关于促进数据安全产业发展的指导意见》，进一步明确要加强隐私计算、数据流转分析等关键技术攻关。

在政策扶持、需求刺激、应用升级等多方因素的驱动下，我国网络安全产业呈现高速发展态势，上中下游都有相关企业提供产品和服务，产业链逐步完善。在数据流通和交易领域，产业链上中下游企业需要深度合作，通过各方数据协同计算，更好地释放数据价值。面对跨机构、跨行业的联合分析、联合建模等应用，需要频繁的数据共享和数据融合，要求数据安全高效协作，这对多方数据系统的全链条安全可控提出了更高要求。

中国联通作为数字信息基础设施的建设者和运营者，拥有大规模的网络和IT基础设施资源，运营着海量高价值数据。如何高效发挥数据资源价值，是运营商面对的最大挑战。中国联通高度重视数据安全治理工作，不断创新安全产品，沉淀服务能力，纵深推进数字化转型。

本文介绍了中国联通研究院项目团队研发的云机密计算平台及

其安全算力供给功能，分析了当前机密计算技术的主要需求与挑战。简要介绍了中国联通云机密计算平台的研发进展与阶段性成果，以及联合英特尔开展的功能验证和性能测试分析。文末对机密计算应用于商业生产的前景和社会价值进行了展望。

二 业务及技术需求

当前，在金融、互联网、工业互联网及汽车等领域，数据协作与数据融合的需求越来越普遍，但伴随而来的数据窃取、隐私泄露等事件也显著增多，数据安全引起政府和各行业的关注。面对数据安全问题，各数据所有方普遍采取了相对保守的策略，对数据共享使用顾虑很多。数据生产方为了自身的数据安全，主动或被动地限制数据的流动和使用，使得数据价值变现变得困难重重。如何稳妥地处理好数据保护和数据利用之间的关系，是业内共同面对的难题。

近些年，行业专家们开展了如多方安全计算、联邦学习等隐私计算数据处理技术的研究，取得了一定进展，同时也遇到一些使用问题，如性能问题、业务可用性问题等。在平衡数据安全性和性能两方面考量中，业内需要寻找一种性能损失较少，能提供较高安全性的解决方案。纵观数据在整个生命周期中的保护，在处于静态（At-Rest）和传输态（In-Transit）时的保护措施较多，而在使用态（In-Use）保护措施相应不足。现有安全防护技术如 HTTPS、IPSec、TLS、FTPS、磁盘加密等数据加密技术，大多是针对网络传输和静态数据存储阶段的数据安全保护，可以对传输中和静态的数据提供有效的保护手段。而在核心数据和隐私数据使用、运行阶段，不管是传统基础设施还是云计算基础设施，对计算环境都缺乏有效的安全可信保护能力。需要特别强调的是，公有云作为云计算的主流型态，其开放的运行模型势必会增加风险暴露面，会带来更多的安全隐患。由此，解决数据运算

过程中的安全问题迫在眉睫。

面对产业发展需求和数据安全挑战，中国联通研究院安全研发团队聚焦云化机密计算及可信验证能力提升，创新研发了基于硬件可信执行环境（TEE）的云机密计算平台，为数据运算过程提供隔离、加密和可信计算度量等功能，为数据计算提供可信安全底座，弥补了云平台机密计算算力的安全短板，助力中国联通推出更优秀的数据保护行业解决方案，服务行业企业数据共享与协作，促进数据价值持续释放。

三 云机密计算平台

3.1 平台介绍

中国联通云机密计算平台是在通用云平台基础上，基于硬件可信执行环境（TEE），实现机密计算虚拟机和虚拟容器提供的能力。平台实现了机密计算虚拟机、机密计算容器的生命周期管理，完成了对主机 TEE 计算能力的适配。目前平台构建了基于 Intel SGX 技术架构的资源池，用户可以很便利地使用机密计算虚拟机和容器，建立起基于 TEE 的数据运行环境。平台也考虑了多种架构的适配能力，后续还规划适配中科海光 CSV 的技术架构，也逐步对其他架构做进一步扩展。

在管理门户中，用户可自主创建机密计算虚拟机和虚拟容器，搭建所需的算力单元，目前支持 Intel SGX 和中科海光 CSV 两种架构模式。管理页面如下图所示：

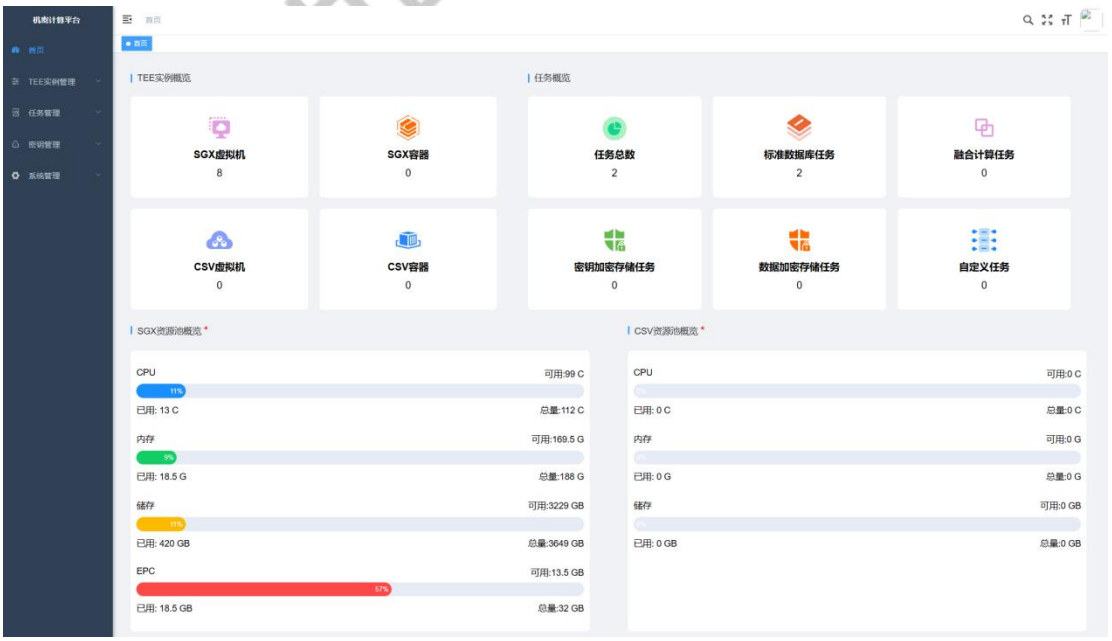

图 3-1 云机密计算平台界面图

3.2 架构和功能

3.2.1 平台架构

云机密计算平台架构基于支持 TEE 的底层硬件基础设施，根据应用环境可划分为两部分，第一部分是容器层面的应用支持（如图 3-2 所示），该部分基于 Gramine 等开源框架实现针对容器应用的安全隔离。

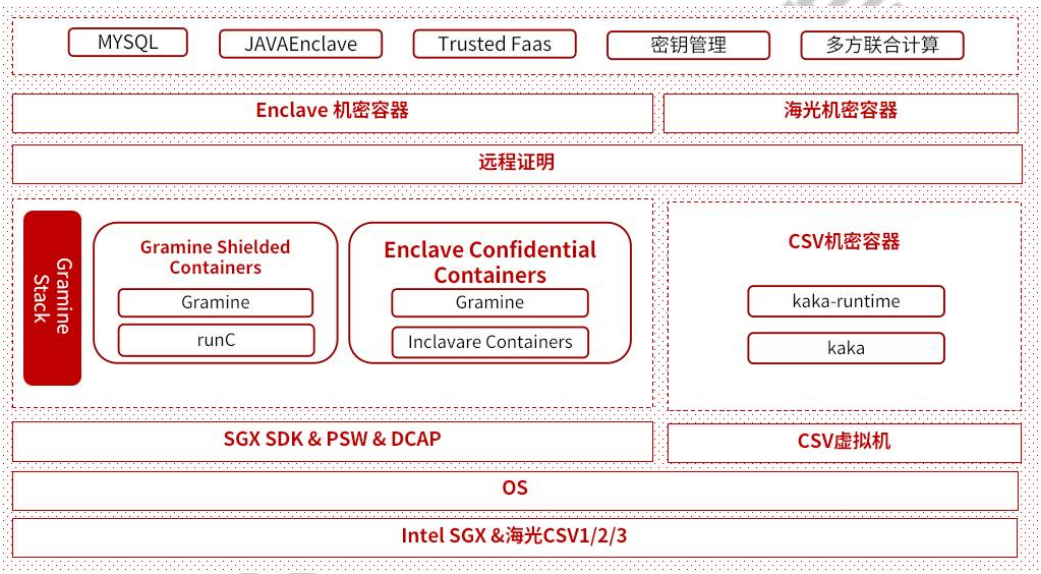

图 3-2 云机密计算平台容器资源池

第二部分是虚拟化层对隐私计算应用能力支持（如图 3-3 所示），该部分基于 KVM、Libvirtd 等技术对底层 TEE 进行适配，实现在虚拟机中机密计算的调用能力。

图 3-3 云机密计算平台虚拟机资源池

3.2.2 平台功能

云机密计算平台支持可视化创建 TEE 机密虚拟机环境和 TEE 机密容器环境，支持基于 TEE 的任务管理、环境验证、密钥管理、数据加密存储、多方联合计算、隐私查询等。具体功能示意图如图 3-4 所示。

图 3-4 云机密计算平台功能示意图

- **任务管理模块**

支持创建 TEE 机密计算环境，如 TEE 机密虚拟机、TEE 机密容器等，用于密钥管理、数据加密存储、多方联合计算、隐私查询。支持设置物理机及容器相关加密内存参数，通过脚本一键自动生成环境。

- **环境验证模块**

支持通过静态度量方式对 TEE 机密计算环境进行可信验证。

- **密钥管理模块**

支持创建 TEE 密钥管理能力，在 TEE 环境中实现密钥生命周期管理功能和机密虚拟机远程证明。

- **基于 TEE 的数据加密存储模块**

支持对 TEE 数据的加解密功能，支持数据加密存储于 TEE 环境内或将加密的数据存储在外部存储介质中，可消除内存泄漏等造成的数据安全隐患。

- **多方联合计算模块**

支持创建 TEE 多方联合计算任务，通过各参与方分发加密密钥与接口方式，实现多方数据汇交，根据相应算法执行计算任务，有效保护数据的安全性，防止原始数据泄露，同时，也可以满足企业间数据高效协作、联合计算的需求。

- **隐私查询模块**

支持创建 TEE 隐私查询任务，通过在 TEE 内部移植标准的数据库管理系统，支持基于 SQL 的数据查询功能，实现多方安全数据查询。

- **系统管理模块**

支持用户管理功能，实现用户在系统操作期间支持日志记录功能，在系统运行过程中，系统会对当前机密计算环境中各项指标实时监控，若出现指标异常情况会及时告警通知。

3.3 SGX 测试验证

3.3.1 测试范围

为了验证云机密计算平台数据保密性和机密计算对性能的影响，项目团队与 Intel 技术团队开展合作，围绕以下两方面开展了功能验证和性能测试：

（1）功能测试

针对普通环境与云机密计算平台机密实例环境，分别部署敏感应用（Redis 数据库），对比验证对内存数据的保密。

（2）性能测试

针对普通方式部署与云机密计算平台部署，分别测试以创建 TEE 机密虚拟机和 TEE 机密容器方式进行 AI 数据集运算的性能损失比。

3.3.2 功能测试

（1）测试过程

a. 普通环境下部署并运行 Redis，在 Gramine 机密容器中部署并运行 Redis；其中 Gramine 是轻量级的 LibOS，用户业务代码无需修改即可在其环境中运行，方便用户业务应用 SGX 特性；

b. 通过 redis-cli 工具向普通 Redis 和 Gramine Redis 写入键值；

c. 从上述对应的进程中拷贝内存数据至文件中；

d. 在内存文件中搜索步骤 b 中写入的键值信息。

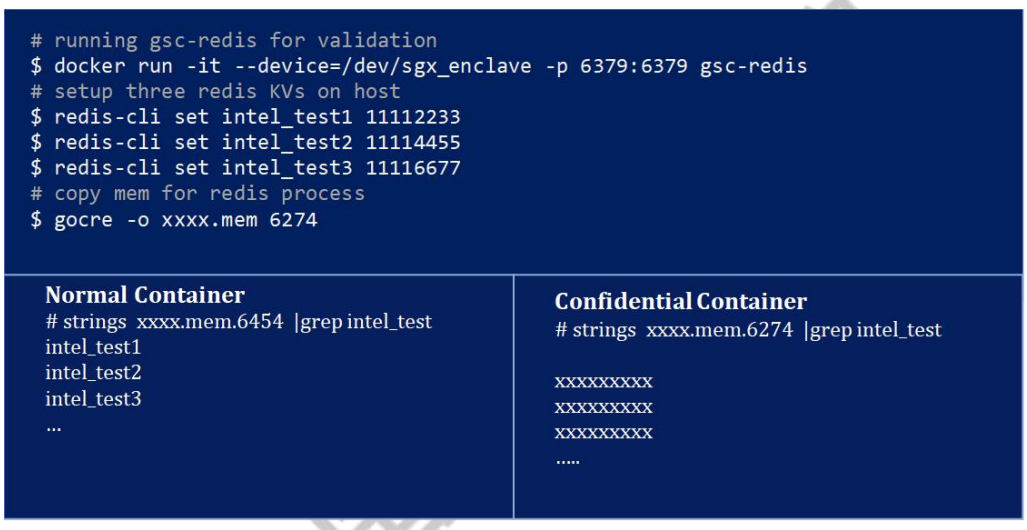

图 3-5 机密计算实例功能测试记录

（2）测试结果

如图 3-5，在普通容器 Redis 内存中可以搜索到先前存入的键值字符串，而在 Gramine 容器中则搜索不到存入的数据。

（3）结果分析

由于 SGX 的优势是对内存加密，存入 Redis 的数据是加密状态，因此，在内存密文中无法搜索到存入的字符串。

3.3.3 性能测试

在机密计算平台上的实例，分别进行虚拟机和容器性能测试。

针对虚拟机，分别在普通虚机和 Gramine 虚机中运行机器学习的推理程序，并同等的限制 CPU 使用核数。对于虚拟机，分别在普通容器和 Gramine 容器中运行机器学习的推理程序，并同等的限制 CPU 使用核数。

测试环境的硬件配置为 Intel(R) Xeon(R) Gold 6330 CPU @ 2.00GHz，操作系统为 Ubuntu 20.04，数据集为 150 万条数据，特征维度为 39 维。

（1）虚拟机

表 3-1 虚机运行程序对比

Within VM	CPU Core Number	SGX Enclave Size	Inference time	Memory
Normal	2 core	N/A	172s	2.1G
Gramine-sgx	2 core	32G	184s	0.6G

通过运行上述程序对比，SGX 虚机推理耗时较普通虚机耗时增加 6.98%；上表中其常规内存使用较低，原因是运行中的程序使用了 SGX Enclave 内存。

（2）容器

表 3-2 容器运行程序对比

Within Container	CPU Core Number	SGX Enclave Size	Inference time	Memory
docker	2 core	N/A	220s	2.1G
Gramine-docker	2 core	32G	244s	0.6G

通过运行上述程序对比，SGX 容器推理耗时较普通容器耗时增加 10.90%。

（3）结果分析

对比性能测试结果,虚拟机和容器场景的性能损失在 7-10%左右，因此,在一些处理重要数据,且性能敏感度需求不高的数据业务场景，基于硬件 TEE 的机密计算是一种可行的技术方案。

四 展望

目前，机密计算技术和应用仍处于产业发展早期，数据保护理念和技术体系成熟还需要市场的磨合。在公有云场景中，机密计算已得到落地应用，主要源于公有云的开放特性，用户对于数据保护的需求更为迫切。实际上，在私有云场景中也同样存在安全隐患，基于边界的安全防护已经不能满足当下的安全要求，很多安全事件都是由内部系统或管理缺陷引起的，在内部数据泄露问题上尤为突出。因此，私有云中处理重要数据的算力环境也需要安全加固，防范可能存在的数据窃取问题。虽然机密计算不能解决所有的安全问题，但是在数据防泄漏、防窃取方面，它是目前比较有效的一种安全技术。同时，芯片架构的加解密计算性能在逐步增强，这也将加快机密计算技术的应用落地。

随着跨企业、跨行业、跨国别合作日益深入，数据的协作共享越来越普遍，数据安全与治理日趋重要。在金融、互联网、工业互联网及汽车等行业，已经开启了小规模的协作和共享，同时也伴随出现了隐私数据泄露的危机。这就需要产业界共同寻求解决方案，探索包括机密计算在内的数据安全技术的应用，建立行业数据协作规范，完善立法和管理制度，共同激发数据价值，促进社会智能化发展和生产力水平的提高。

中国联通研究院已完成了云机密计算平台的初步研发，后续将持续完善平台功能，针对多方联合计算、隐私查询、边缘计算、人工智

能等业务场景开展应用实践，研究机密计算的行业解决方案。同时联合 Intel 等业界头部合作伙伴，发挥先进安全技术优势，进一步丰富机密计算应用场景，夯实数据安全治理能力，促进政府和各行业数据融合和数据价值实现。

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院致力于提高核心竞争力和增强核心功能，紧密围绕联网通信、算网数智两大类主业，按照 4+2+X 研发布局，开展面向 C3 网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国建设，大力发展战略性新兴产业，加快形成新质生产力。联通研究院现有员工 700 余人，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话： 010-87926100
邮编： 100176

中国联通研究院

中国联通泛终端技术