Global Computing Consortium
全 球 计 算 联 盟

机密计算白皮书

Confidential Computing White Paper 2024

全球计算联盟
机密计算专业委员会

指导专家组组长

冯登国院士

指导专家

姚相振	刘林超	秦　宇	张　侃	王骏超	张亚光
张　磊	金意儿	吴　烨	夏虞斌	王小航	谢秋华
刘　静	王惠莅				

编写专家

葛小宇	张　瑞	李　振	李博文	黄　江	严志超
虞　刚	牛博强	李光辉	张　亮	司兵松	庞　婷
严敏瑞	于　攀	胡科开	唐　文	刘　钢	许小兵
鲍　鹏	李煳桦	华佳烽	张　尧	刘敬彬	李向锋
王琼霄	陶立峰	张振永	王吾冰	陈浩栋	宋雨筱
黄　淼	马　姚	李莹威	陈小春	孙　亮	傅　瑜
王　莹	张殷乾	李　帜	王　龑	涂长茂	彭晓川
肖　军	罗　翀	王　震	任　彤	谭　琳	张　磊
贾宝军	俞锦浩	孙　琪	王　帅	朱　域	牛健宇
糜泽羽	李鼎基	李明煜	陈世武	马　威	肖　波
熊　毅	惠　静	苗福友	羡喻杰	陈凌潇	周建平
黄梓锋	赵宇航				

编写单位

华为技术有限公司

中国科学院软件所

北京国家金融科技认证中心

中国工商银行

南湖实验室

中国民生银行

天翼云科技有限公司

抖音集团有限公司

北京数字认证股份有限公司

杭州安恒信息技术股份有限公司

北京冲量在线科技有限公司

北京信安世纪科技股份有限公司

昆仑太科（北京）技术股份有限公司

中国联合网络通信集团有限公司

南方科技大学

杭州锘崴信息科技有限公司

北京天融信网络安全技术有限公司

希奥端（深圳）计算技术有限公司

上海交通大学

飞腾信息技术有限公司

超聚变数字技术有限公司

麒麟软件有限公司

统信软件技术有限公司

安谋科技（中国）有限公司

（以上排名不分先后）

序　言》

数据是数字时代的基础性战略资源与关键性生产要素，其安全问题受到国际社会的广泛关注。数据安全威胁总体呈现出事件频度密集化、攻击损失扩大化、威胁类型多样化的态势。

总体来讲，数据保护涉及数据的三种不同状态：

一是传输时的数据（data in transit），其安全保护措施主要有加密、信息隐藏、SSL/TLS、IPSec、VPN和HTTPS等。

二是存储时的数据（data at rest），其安全保护措施主要有加密、访问控制、安全数据库、数据容灾备份等。

三是使用中的数据（data in use），其安全保护包括其在内存、处理器中进行计算时的机密性和完整性保护。数据使用安全问题的本质是安全计算问题，这就要求CPU、GPU、DPU等能够支撑安全计算功能。

当前，数据使用安全问题需求迫切。例如，针对云应用的每种攻击模式（包括虚拟机逃逸、容器逃逸、固件损坏和内部威胁）都使用了不同的攻击技术，但它们的共性是被攻击对象都是使用中的代码或数据。而传统的保护数据在传输或存储中的安全措施无法处理云场景下敏感数据在使用中的数据安全。机密计算是目前为止最为现实的一种数据使用安全技术，本质上是一种密态计算技术。

我之所以非常关注机密计算，主要原因有四：

一是机密计算可视为可信计算发展的新阶段。可信计算重点以TPM/TCM为基础，建立一种信任传递体系以保证系统实体按照预期的行为执行。这样的机制无法防御数据在运行时受到的攻击，因此，需要一个与外界隔离的安全容器对敏感数据进行处理，避免攻击者读取其所使用的内存空间，机密计算中的可信执行环境（TEE）就是这样的容器。TEE通过软硬件协同既能保护敏感数据，又能保留与常规执行环境之间的算力共享。

二是机密计算是实现内生安全（也称为本原安全）的一种新途径。内生安全是指系统固有的安全能力，在系统建设时就从底层同步考虑其具备的安全能力。机密计算是一种从体系结构层面解决安全问题的技术，可从硬件、系统和应用等不同层面解决安全问题，从而实现内生安全。

三是机密计算是解决数据使用安全的一种现实方法。目前除了机密计算之外，还有很多其他数据使用安全技术，如同态加密、安全多方计算、联邦学习等，有的安全性高而性能低，有的安全性低而性能高。例如，同态加密尤其是全同态加密是一种理想的数据使用安全技术，但离实用化还有距离；联邦学习的实用化程度较高但安全性仍有待提高。

四是机密计算是实现高性能安全技术的重要支撑。很多安全技术的性能不能满足实际应用需求，可通过机密计算大大提升其性能，使其实用化。例如，基于TEE可设计并快速实现全同态加密、安全多方计算、函数加密和零知识证明等安全机制。

为了推动机密计算产业高质量发展、标准化、生态繁荣并加速应用落地，2024年9月19日，全球计算联盟机密计算专业委员会正式成立。这个委员会成立之初，就力争推出一本高质量的《机密计算白皮书（2024）》，旨在简明揭示机密计算的本质，分析机密计算的发展现状，展望机密计算的未来发展趋势，为机密计算研发人员、行业用户等提供参考。我相信，随着专业委员会的发展壮大，人们对机密计算认识水平的提高，《机密计算白皮书》的质量会越来越高、内容会越来越丰富

冯登国

中国科学院院士

2024年10月于北京

目 录 》

CONTENTS

目 录 》

CONTENTS

第四章　机密计算应用案例

第五章　机密计算评测体系

引 言

在数字化浪潮的席卷之下，数据已成为推动社会进步与经济发展的不可或缺的力量。然而，数据的广泛流通与深度应用也伴随着前所未有的安全风险。传统的数据安全技术主要作用于数据存储和传输阶段，而对于使用中的数据缺乏保护。这一缺口在处理敏感数据时尤为明显，亟需一种新的技术来解决数据使用过程中的安全性问题，实现数据安全与数据价值利用的平衡。

机密计算是一种基于硬件保护使用中数据的安全技术，2019年Gartner首次将机密计算纳入云安全技术曲线，并将其视为重点关注的技术领域。机密计算生态飞速发展，已广泛应用于金融、政务、医疗等各行各业。

本白皮书旨在阐明机密计算技术本质，分析机密计算发展现状及趋势，为机密计算研发人员、行业用户等提供机密计算技术框架和评测体系参考，并给出典型场景中的机密计算应用案例，加强技术落地信心。通过对机密计算技术的全面了解，读者将能够认识其在数据安全领域的潜力，并在实际应用中实现更高水平的安全保障。

第一章
机密计算概述 》

1.1 产业背景

在数字化浪潮席卷全球的今天，随着云计算、大数据、人工智能等前沿技术的深度融合与广泛应用，数据已成为驱动数字经济及社会发展的关键生产资料。全球多个国家和地区对数据安全与隐私保护给予高度重视，纷纷出台相关法律法规及政策要求，明确指示数据安全与发展并重，依法保障数据的可信流通与数据价值的充分利用，主要的法律法规政策文件要求总结如表1所示。

而诸如数据加解密等传统的数据安全技术主要作用在数据的传输和存储环节，偏向于静态数据的保护，难以抵御数据在使用过程中面临的安全威胁。面对这一严峻挑战，产业界迫切需要一种创新的技术方案，在保障数据高效流通与利用的同时，筑起坚不可摧的安全防线，保护使用中数据的机密性和完整性。

正是在这样的产业背景下，机密计算技术应运而生，它以独特的理念与先进的技术架构，保障数据在被处理和分析的过程中仍能保持机密性和完整性，不仅为数据的可信流通和价值挖掘提供了有力保障，也为数字经济的发展注入了新的活力。

表1 主要的数据安全法律法规政策文件

国家或地区	法律法规政策文件	生效时间	相关要求
中国	《中华人民共和国数据安全法》	2021年9月1日	强调数据安全与开发利用并重，保护个人、组织与数据有关权益，同时保障数据依法有序自由流动。
	《中华人民共和国个人信息保护法》	2021年11月1日	强调个人信息在数据流通过程中的安全合规。
	《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》	2022年12月2日	建立数据可信流通体系，增强数据的可用、可信、可流通、可追溯水平。强化数据安全保障体系建设，把安全贯穿数据攻击、流通、使用全过程。
	《关于促进数据安全产业发展的指导意见》	2023年1月3日	推进新型计算模式和网络架构下数据安全基础理论和技术研究，支持后量子密码算法、密态计算等技术在数据安全产业的发展应用。

续表　　表1 主要的数据安全法律法规政策文件

	《网络数据安全管理条例》	2025年1月1日	强调数据开发利用与保障数据安全并重，加强数据安全防护能力建设，保障数据依法有序自由流动。
美国	《加州隐私权法案》（CPRA）	2023年1月1日	要求企业对个人数据采取“合理的安全措施”。
欧盟	《通用数据保护条例》（GDPR）修订建议	待定	强调数据保护设计和默认保护，推动数据在使用中的隐私保护。
	《关于公平访问和使用数据的统一规则的条例》	2024年1月11日	数据持有者可采用适当的技术保护措施，包括智能合约和加密，以防止对数据（包括元数据）的未经授权访问。

1.2 概念及属性

机密计算是一种保护使用中数据安全的计算范式，其核心原理是利用可信执行环境硬件，构建出具备安全隔离、内存加密、远程证明、数据封装等的计算环境，使得机密计算环境内运行的代码和数据免于非可信特权软件（包括操作系统和虚拟机监控器等）的窥探和篡改，保护使用中数据的机密性与完整性。

机密计算大多具备以下属性：

1.隔离：机密计算使用硬件TEE技术保护数据，通过硬件的强安全隔离限制任何特权软件对TEE内数据的直接访问或篡改。

2.内存加密：对内存数据加密保护，防止未经授权的访问。

3.远程证明：允许验证者通过可信度量及远程证明，对机密计算环境的初始状态进行验证，确保状态正确性和完整性。

4.数据封装（sealing）：基于硬件根密钥及应用程序的完整性度量值等生成封装密钥，基于封装密钥加密保护应用程序的数据，使得数据的机密性与应用程序自身的完整性产生关联。

1.3 参与角色

机密计算的参与角色如图1所示，具体包括：

- 算力提供方：提供机密计算算力环境。
- 服务提供方：提供机密计算环境分布式管理、机密计算应用批量部署及资源监测等服务。
- 应用提供方：提供在机密计算环境中运行的应用程序。
- 数据提供方：向机密计算环境传递计算任务所需要的数据。
- 结果需求方：提供具体的计算需求，包括需运行的程序、程序运行时所需计算的数据等，并获取相应的计算结果。

注：实际业务场景中可能是一个参与方承担上述多种角色。

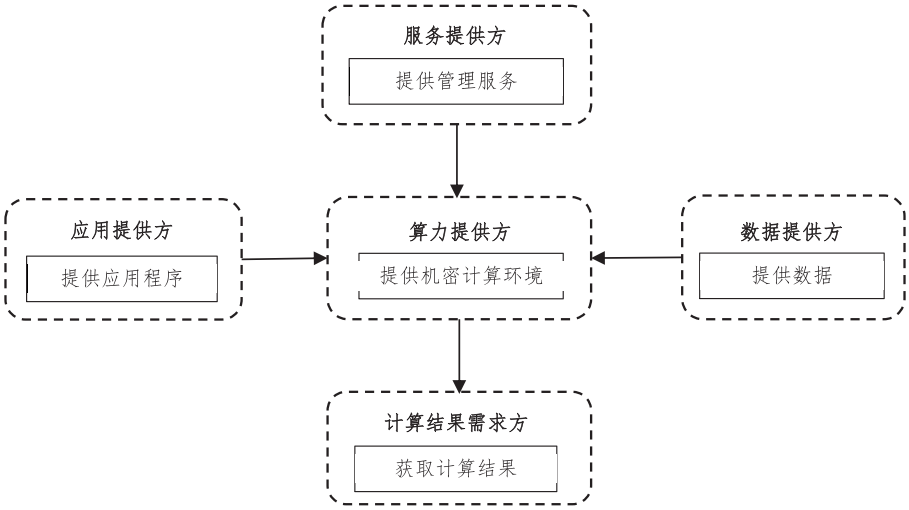

图1 机密计算参与角色

第二章

机密计算发展现状及趋势》

2.1 代际演进

近二十年来，机密计算技术蓬勃发展，多家芯片厂商分别提出了基于其处理器体系架构的机密计算技术方案，机密计算发展历程如图2所示。

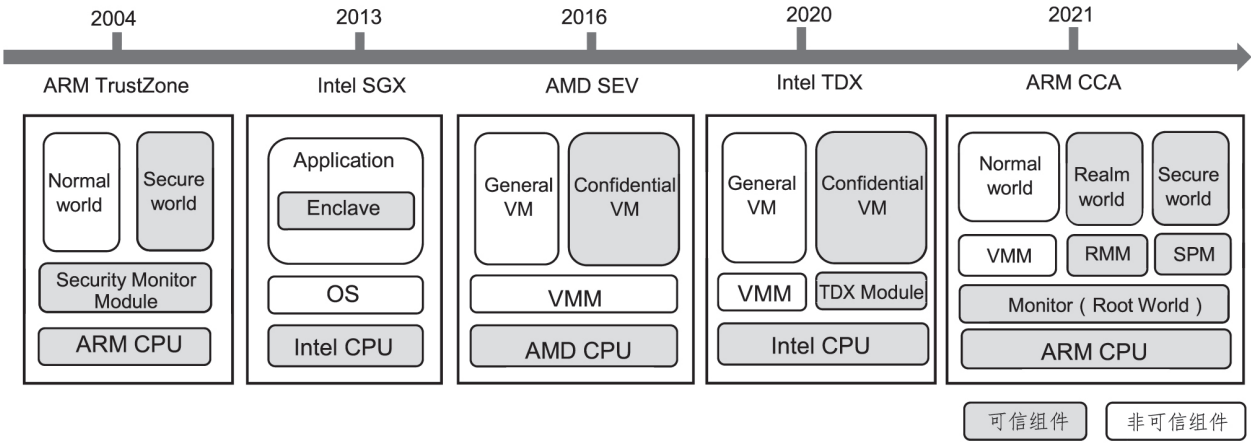

图2 机密计算技术发展历程

2002年，ARM提出TrustZone技术，被普遍认为是第一代机密计算技术。TrustZone通过分时复用将处理器区分为两种运行状态，即Secure World和Normal World，每种运行状态有物理隔离的寄存器、缓存、内存页表等，并在Secure World内运行可信操作系统和可信应用。Secure World拥有更高的权限，Secure World可以访问Normal World的代码及数据，而Normal World无法直接访问Secure World的代码及数据。

2013年，英特尔提出了基于x86架构的安全扩展SGX，提供用户空间的TEE。通过一组新的指令集扩展与内存加密机制，SGX实现了程序之间的隔离运行，保障了用户关键代码和数据的机密性与完整性。

2016年，AMD推出了支持SEV技术的EPYC处理器，并分别在2017年和2020年分别发布了第二和第三代SEV技术，即SEV-ES和SEV-SNP。SEV通过密钥透明加密每个虚拟机的内存，有效地保护了机密计算虚拟机内存中数据的机密性。SEV还支持远程证明，可以向虚拟机所有者证明虚拟机的OVMF的完整性。

2020年，英特尔发布了TDX技术，提出了基于虚拟机抽象的机密计算技术，保护虚拟机内存数据的机密性和完整性。Intel TDX引入了高权限的TDX模块，介于Guest客户机与外部不可信VMM之间，负责检查机密计算虚拟机和外部不可信VMM之间的交互。

2021年，ARM发布了CCA技术白皮书，定义了新一代ARM架构机密计算技术。ARM CCA引入了领域管理扩展(RME)，在TrustZone的Normal World和Secure World之外增加了Realm World和Root World。RMM是Realm World的管理组件，通过与Normal World 虚拟化管理软件交互管理机密计算虚拟机的运

行，为机密计算虚拟机提供相互隔离的运行环境，将其中的工作负载与Normal World、Secure World隔离开来，并支持内存加密，还支持通过远程或本地证明来度量和验证机密计算虚拟机的初始状态。SPM是Secure World的管理组件，Monitor是Root World的管理组件。

本白皮书将机密计算发展历程总结为机密计算1.0、机密计算2.0和未来的机密计算3.0三个阶段，如图3所示。

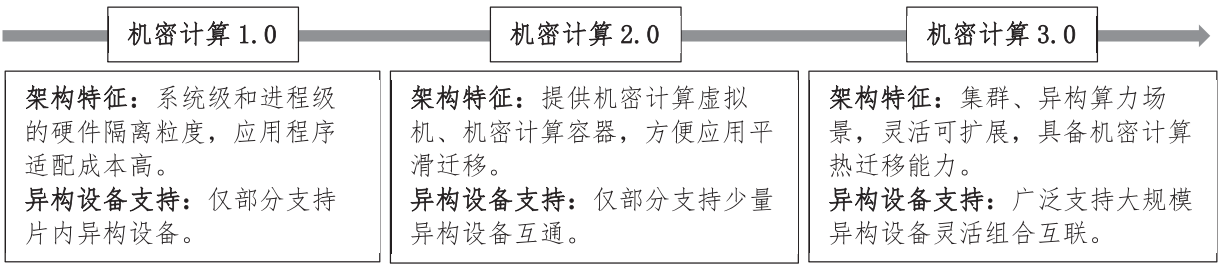

图3 机密计算代际演进

在机密计算1.0阶段，主要是系统级和进程级的硬件隔离技术，仅部分支持片内异构设备互通。例如，ARM TrustZone通过NS状态位区分安全世界、非安全世界，与片内异构处理器核互通。此阶段的机密计算技术易用性较弱，需要应用程序做较多的适配改造才能运行在机密计算环境。

在机密计算2.0阶段，基于硬件的虚拟机级机密计算技术被提出，并已成为当前机密计算的主流形式，仅部分支持少量异构设备互通。此阶段的机密计算与云计算具有较好的兼容性，允许在单一物理机器上运行多个机密计算虚拟机，由机密计算虚拟化管理软件提供不同机密计算虚拟机之间的隔离与管理。同时，部分机密计算虚拟机能够通过TEE-IO与AI加速卡、SSD等异构设备互通。

机密计算技术正处于蓬勃发展阶段，朝着机密计算3.0稳步前进。未来，硬件架构的异构性、软件生态的兼容性，与大模型等热点技术的交叉融合等，将是影响机密计算发展的重要因素。**在机密计算3.0阶段，TEE的异构可扩展性将成为一个重要特性，除了CPU具有机密计算能力外，设备侧和互联侧也将支持机密计算能力，将实现大规模的CPU及XPU之间机密计算环境互联，同时，机密计算虚拟机也能够根据资源利用率，灵活地热迁移，更好地支持大模型训练与推理等大规模应用。**

随着机密计算的代际演进，国内外产业界和学术界通过开源等多种形式推动机密计算的生态建设和落地部署。为了推动机密计算的大规模落地应用，Linux基金会于2019年8月宣布成立“机密计算联盟”（Confidential Computing Consortium，CCC），以开源合作的方式构建机密计算生态。CCC成员包括了国外的ARM、AMD、Intel、IBM、红帽、英伟达、微软、谷歌、Meta，以及国内的阿里、百度、字节跳动、华为等科技巨头。此外，机密计算已经逐渐在国内外云平台部署使用，例如，微软Azure云、亚马逊AWS、谷歌云、阿里云、腾讯云、华为云等都分别推出了基于机密计算的云服务。此外，国内外学者也提出了众多创新技术，以解决机密计算技术在密码机、数据库、机器学习、多方安全计算等场景

内应用的挑战。例如，学术界提出的基于ARM SEL2技术的TwinVisor系统和基于RISC-V架构的TEE系统Keystone、Sanctum、Penglai，产业界提出的基于ARM SEL2的virtCCA等。

2.2 标准现状

目前，各行各业、国际国内都很关注机密计算标准的研究与制订，已发布和在研的机密计算标准如表2所示。

表2 机密计算相关标准总结

标准类型	标准组织	标准名称	主要内容简介
国家标准	TC260	GB/T《网络安全技术 机密计算通用框架》（国家标准计划号：20230246-T-469，报批稿）	给出了机密计算相关的术语定义、参与角色、通用框架及必要的组件和功能、机密计算基础的安全服务和交互机制，以及虚拟化部署模式，作为机密计算技术的顶层设计，为后续机密计算其他标准制定奠定基础。
国家标准	TC260	GB/T 41388-2022《信息安全技术 可信执行环境 基本安全规范》	给出了TEE系统整体技术架构、硬件要求、安全启动过程基本要求、可信虚拟化、可信操作系统、可信应用与服务管理基本要求、可信服务基本功能及要求、跨平台应用中间件、可信应用架构及安全要求、测试评测方法的相关技术要求，标准适用于指导TEE系统的设计、生产及测试。
	TC260	GB/T 42572-2023《信息安全技术 可信执行环境服务规范》	提出了TEE服务的技术框架及主要功能构成，规定了相关安全技术要求及测试评测方法，适用于TEE服务的设计、开发、测试等。设备制造商、系统软件提供商、检测机构和科研机构等TEE服务参与方可参照执行。

续表　　表2 机密计算相关标准总结

行业标准	CCSA	《隐私计算 可信执行环境产品性能要求和测试方法》（征求意见稿）	规定了基于TEE的数据计算平台性能相应的测试方法，包括技术要求、测试维度、测试场景等内容，涵盖了在基础运算、联合建模、联合预测等常见算法场景中测试TEE产品的性能、性能相关的安全性、准确性三大测试维度的测试方法。该标准为机密计算相关产品的性能测试提供了相应的参考。
	CCSA	《隐私计算 可信执行环境产品安全要求和测试方法》（征求意见稿）	规定了基于TEE产品的安全要求和相应的测试方法，包括技术要求、测试维度、测试场景等内容，本标准对TEE产品的系统安全、数据流通安全、流程安全、应用算法安全、审计安全、认证安全、存证安全、密码应用安全、通信安全、模型安全等部分进行了规范。
国际标准	ISO/IEC JTC1/SC27	17603《cybersecurity-confidential computing》PWI	阐述机密计算的概念、产业成熟度、与既有标准的关系、标准化的必要性以及推荐的标准体系设计。
	ISO/IEC JTC1/SC27	25093《cybersecurity-confidential computing-part1:overview and concept》NP（WD阶段）	给出机密计算的概念、基本属性、核心机制及调度模型等。
	IETF	RFC 9397《Trusted Execution Environment Provisioning (TEEP) Architecture》(July 2023)	该体系结构文件规范了TEE的配置协议，该协议用于管理在TEE中运行的可信应用程序的生命周期。机密计算技术可参考此文稿，指导用户将数据和应用部署在机密计算环境中。

续表　　表2 机密计算相关标准总结

	IETF	RFC 9334《Remote ATtestation ProcedureS (RATS)》	提供了一个与处理器体系结构、证明内容和协议无关的通用远程证明模型。
	IEEE	P2952 《Standard for Secure Computing Based on Trusted Execution Environment》（August 2023）	标准规定了基于TEE的安全计算系统的框架，以及通用安全计算平台在隔离、保密、兼容性、性能、可用性和安全方面的技术要求。还规定了安全计算技术的使用案例和场景。本标准对于机密计算相关标准的编制有着重要的参考意义。
团体标准	CESA	T/CESA 1229-2022《服务器机密计算参考架构及通用要求》	标准旨在从最终产品和开发过程的角度出发，建立系统化的机密计算定义和统一框架，清晰地描述机密计算服务中各种参与角色的安全责任，提出机密计算角色、角色安全职责、安全功能组件以及他们之间的关系，指导机密计算参与者进行机密计算服务规划时的安全评估与设计。
	GP	TEE System Architecture v1.3 | GPD_SPE_009	阐述了符合Global Platform Protection Profiles和功能规范定义的TEE安全认证和功能合规性。本文档总结了这两个领域的各个方面，为读者提供了Global Platform TEE的安全性和潜在功能的概述。
	GP	《TEE Management Framework: Open Trust Protocol (OTrP) Profile Version 1.1》（OTrP，Open Trust Protocol Profile）	OTrP仅针对于Global Platform定义下的TEE，对于非GP的TEE，可参考TEEP协议。采用Global Platform TEE架构的机密计算技术可参考此标准对可信应用进行管理与配置。
	PCI-SIG	TDISP（TEE Device Interface Security Protocol）	定义了一种用于可信I/O虚拟化的架构，规范了TVM和Device之间如何建立信任关系，Host和Device之间的互联安全以及如何以可信的方式将TDI与TVM绑定或分离。

机密计算技术框架以及机密计算依赖的TEE、可信度量、远程证明等关键技术都已进行标准化，为了推广机密计算大规模应用，还需要在统一服务接口、统一远程证明、跨设备互联安全及测评体系等方面进一步完善标准体系。

2.3 发展趋势

2.3.1 虚拟化

通过云计算与机密计算技术融合，一方面可提高云计算服务的可信度，另一方面可降低用户在云环境下使用机密计算的门槛。新一代机密计算如AMD SEV、Intel TDX、ARM CCA等正向机密计算虚拟机方向演进，能够支持虚拟机、容器在TEE内运行。

2.3.2 集群化

随着算力需求规模增长，机密计算也将从单节点向集群化发展，需要考虑集群中异构服务器节点的机密计算环境统一纳管、机密计算虚拟机及容器等跨节点迁移以及诸多不同节点中机密计算环境的高效、统一可信度量与远程证明等问题。

2.3.3 异构互联

目前，大多数机密计算基于CPU TEE，然而，随着人工智能等应用的出现，需要异构计算资源（如GPU、NPU、TPU、FPGA等）协同完成模型训练、模型微调与模型推理等任务，因此，需要将异构计算资源纳入机密计算的安全边界，实现异构计算资源之间灵活组合建立机密互联，构建异构资源协同的机密计算环境。

2.3.4 易用性提升

新一代机密计算技术在硬件架构和机密计算操作系统方面进行了优化，进一步提升了机密计算的易用性。例如，蚂蚁集团开发的Occlum[4]机密计算操作系统使现有应用能够直接运行在机密计算环境中，openEuler社区的secGear[5]和蚂蚁集团的HyperEnclave[6]等机密计算中间件，可以屏蔽硬件差异，使现有应用可以运行在不同技术路线的机密计算环境中，大幅降低了应用迁移和开发的成本。

2.3.5 性能优化

安全方案的落地应用，离不开对性能的权衡，当前机密计算方案应用过程中，不少行业用户首先考虑应用机密计算方案造成的性能影响，尤其是AI场景，算力昂贵，性能影响即为经济损失，机密计算相关研发人员也在努力进行性能优化，更好地推动机密计算方案端到端应用。

2.3.6 协同发展

协同发展、交叉研究是机密计算领域的一大特色，需要机密计算与密码技术、隐私增强技术、安全协议、可信计算技术、容器和微服务安全等的协同发展、交叉融合，最终实现对国计民生相关数据的安全保护与价值利用。

第三章
机密计算参考框架》

3.1 参考框架

机密计算参考框架主要包括机密计算环境、机密计算管理服务以及机密计算应用生态，分别由机密计算算力提供方、服务提供方以及应用提供方提供，多方协同发展机密计算生态体系，如图4所示。同时，业界也有观点将机密计算环境及机密计算管理服务的集合视为机密计算平台，应用提供方可直接基于机密计算平台更高效、便捷地开发部署机密计算应用。

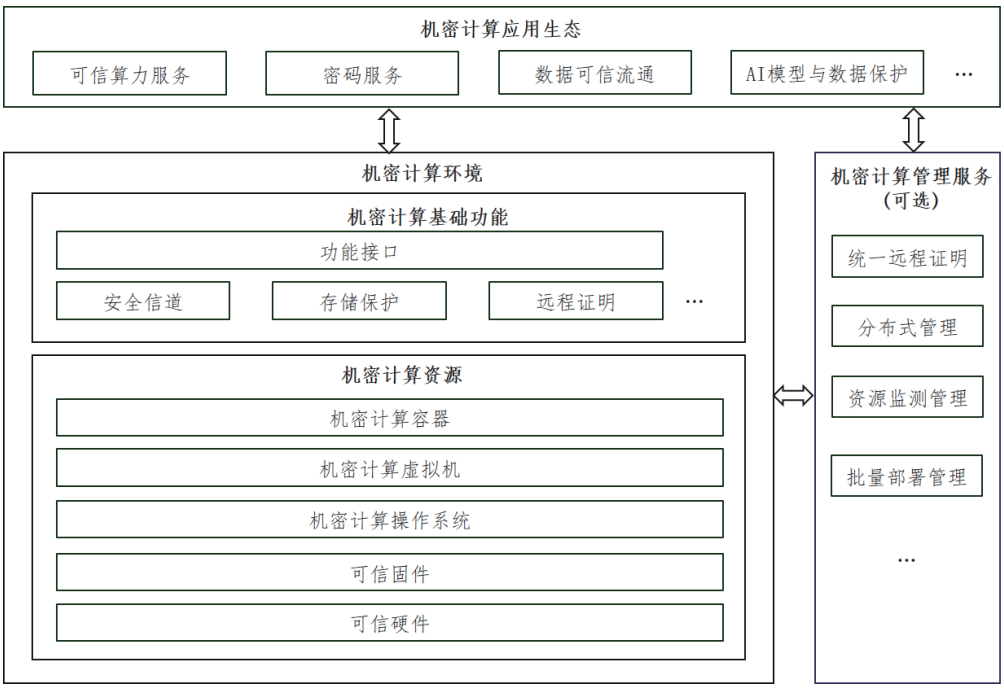

图4 机密计算参考框架

1.机密计算环境

机密计算环境主要包括机密计算资源和机密计算基础功能，各部分具体组成如下：

a）机密计算资源：以可信硬件、可信固件、机密计算操作系统为基础，可能存在机密计算物理服务器（可选包含机密计算容器）、机密计算虚拟机（可选包含机密计算容器）等多种形态。

b）机密计算基础功能：包括安全信道、存储保护、远程证明等基础功能以及基本的功能接口。安全信道功能的目的是基于密码技术保障数据导入和导出机密计算环境的安全性。存储保护功能的目的是加密存储用户数据，这些数据只能由授权访问机密计算环境的实体访问或修改。远程证明功能的目的是供应用提供方等验证机密计算环境的可信状态，验证通过后，才导入应用和数据或允许不同应用之间通信。

2.机密计算管理服务

机密计算管理服务是为了支撑机密计算在分布式、虚拟化等不同架构的计算系统中规模化应用的管理服务。核心作用是要屏蔽硬件架构差异，面向应用提供通用的统一远程证明、分布式管理、资源监测管理、批量部署管理等管理类服务。

3.机密计算应用生态

机密计算应用生态旨在由应用软件研发单位围绕各行业用户需求，面向行业用户业务场景，基于机密计算环境开发各类具体的机密计算应用。典型应用场景主要包括可信算力服务、数据可信流通、密码服务、多方数据协同、AI模型与数据保护等。

3.2 部署模式

目前机密计算的部署形态比较丰富，可以基于物理服务器机密计算环境直接部署应用系统，也可以在物理服务器中部署机密计算虚拟机，进而在机密计算虚拟机中部署应用系统。同时，无论是在物理服务器形态的机密计算环境，还是在虚拟机形态的机密计算环境中都可以容器化部署应用系统。本白皮书给出最典型的两种部署模式，为相关参与方部署应用机密计算提供参考。

3.2.1 机密计算虚拟机

机密计算虚拟机部署视图如图5所示。在该部署模式中，除了安全状态的CPU核、安全隔离内存等可信硬件之外，主要涉及机密计算虚拟化管理软件、密钥管理系统、远程证明服务和机密计算操作系统四个重要组件。机密计算虚拟化管理软件主要用于创建管理配置机密计算虚拟机资源，密钥管理系统组件中存储着系统镜像的加密密钥，远程证明服务提供证明机密计算环境的验证服务，机密计算操作系统即为机密计算虚拟机中的操作系统。

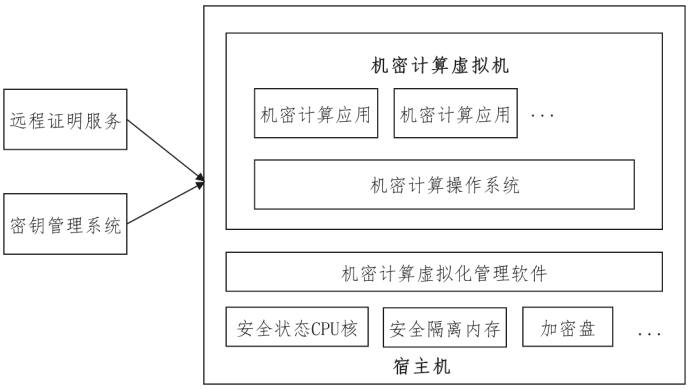

图5 机密计算虚拟机部署模式

在该部署模式下，租户首先对文件系统及应用镜像等进行加密，并将密钥保存到密钥管理系统中。整个虚拟机的启动将分为两个过程，在启动初期，租户首先加载操作系统内核，其次向密钥管理系统发起密钥请求，此时密钥管理系统将通过远程证明的方式确认宿主机机密计算环境符合预期，从而将密钥通过加密链路发送给机密计算虚拟机，解密文件系统及应用镜像，验证其完整性并挂载到加密盘。在完成解密后，系统将切换根目录到加密盘，从而加载用户文件系统最终完成虚拟机的启动。此时用户即可像使用普通虚拟机一样，在虚拟机中部署应用系统，而应用系统相关数据需要静态存储时，可以将数据直接存储到加密盘，基于加密盘的加密方案加密数据，也可以借助机密计算环境的存储保护功能，将数据加密后再存储到加密盘。

3.2.2 机密计算容器

机密计算容器的部署视图如图6所示。该部署模式与机密计算虚拟机相比，增加与容器相关的组件，包括容器调度软件、机密计算容器运行时软件和镜像仓库。

机密计算容器的形态与普通容器的形态不同，机密计算容器实际也运行在机密计算虚拟机中，通过机密计算容器运行时软件来控制相关容器负载的启动维护工作。具体地，用户需要配置容器的启动策略并下发给容器调度软件，调度软件将按照用户策略，动态创建机密计算虚拟机，并在机密计算虚拟机中执行用户策略，拉取用户指定的容器镜像，并将其启动。此时，用户的容器应用即完成了部署。在此过程中，用户可通过远程证明的方式，获取机密计算环境以及策略文件的度量值，并验证机密计算环境的完整性。此后，用户也可向密钥管理系统获取密钥，从而进行加密盘挂载、加密数据解密等操作。

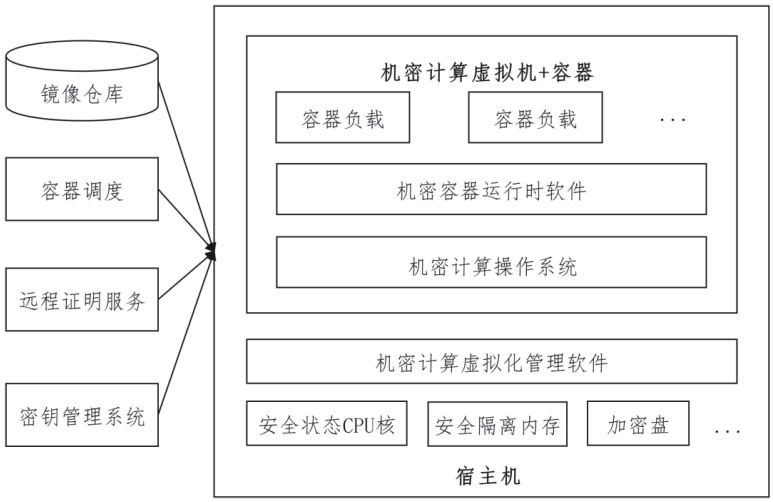

图6 机密计算容器部署模式

第四章
机密计算应用案例》

4.1 可信算力服务

可信算力服务是指基于机密计算环境提供安全可信的算力租用服务，保护算力需求方数据资产安全，使其放心租用算力，降低算力环境搭建成本，典型细分场景包括安全云主机、东数西算等。

4.1.1 机密计算云主机

4.1.1.1 场景描述

在公有云场景中，租户需要将自身数据上传到云服务器中运算处理，而云服务器由云服务提供商运维管理，可能存在恶意管理员滥用其运维管理账号权限窃取租户数据的风险，需借助机密计算技术构建机密计算云主机保障租户数据安全。

4.1.1.2 需求分析

在传统的云计算应用场景下，云平台管理员掌握对云主机进行运维管理等诸多账号权限，而传统的数据加密技术只能保障数据传输、存储过程安全，亟需一种数据安全技术能够保障云主机中的租户数据无法被虚拟化管理软件、宿主机操作系统、云平台管理员等获取，打消租户敏感数据上云的安全疑虑。

4.1.1.3 技术方案

机密计算云主机方案架构如图7所示，将通过可信硬件保护云主机内存数据，且仅在验证云主机环境的可信状态后，才导入数据，帮助租户防止云服务提供商、管理员或其他租户访问机密计算云主机中的数据，并且不会改变租户既有的应用系统架构。

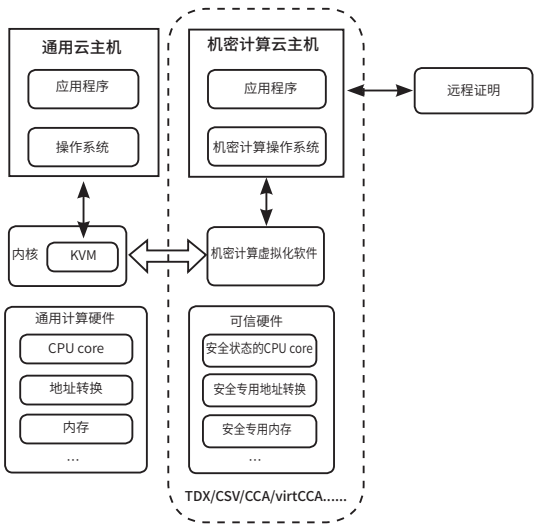

图7 机密计算云主机方案架构

机密计算云主机构建过程如下：

（1）加密镜像部署：租户将机密计算云主机OS文件系统打包成镜像，并加密存储进宿主机，通过加密保护，防范云主机文件系统遭篡改、替换等。

（2）构建机密计算环境：在宿主机中建立TEE，该环境与运行租户应用程序系统的其余部分隔离（包含机密计算云主机资源分配）。

（3）可信验证：租户对TEE内的资源环境（OS kernel、堆栈等）进行可信度量和远程证明（把OS kernel拷贝到TEE）。

（4）文件系统部署：TEE资源环境验证通过后，租户在TEE环境内解密镜像文件，部署文件系统，至此，完成机密计算云主机创建。

（5）接收和发送数据：应用程序将加密数据加载到机密计算云主机中，对其进行解密，执行租户应用程序，对生成的数据进行加密，然后发送。

与通用云主机相比，机密计算云主机具有如下安全能力：

（1）可信验证：基于可信根实现云主机的启动完整性度量与远程证明。

（2）内存数据保护：提供了云主机内存的强隔离机制，并借助密码学方法保护机密性和完整性。

（3）硬件隔离及访问控制：机密计算云主机由机密计算虚拟化软件管控，虚拟化管理软件、宿主机操作系统及管理员都无权限访问机密计算云主机内的租户数据。

4.1.2 东数西算

4.1.2.1 场景描述

依靠高速传输网络将东部发达地区产生的数据传输到西部数据中心进行分析和计算，最后再把计算结果传回东部；或者是东部企业产生的温冷数据，利用高速网络传输至西部数据中心备份，数据服务的提供、价值实现环节仍保持在东部地区。

4.1.2.2 需求分析

用户使用算力网络进行数据存储和计算，需要对存储和使用中的敏感数据提供安全防护。如果算力节点中存储的用户数据未被加密，可能存在被恶意篡改、窥探、泄露等安全风险。

既有技术存在以下两方面的问题：

（1）传统的数据加密技术，将整个数据块进行对称加密存储，当需要使用数据执行计算任务时，要将整个数据块解密成明文。数据加密后可用性差，无法满足用户多样化的算力任务需求，且数据以明文形式在内存中出现，存在数据泄露风险。

（2）联邦学习、多方安全计算、同态加密等基于密文计算的方式实现，性能降低幅度较大，与传统明文计算相比有百倍的性能差距。

因此，如何在保护数据安全的同时，提供可用性更强、更高效的计算和存储服务成为东数西算面临的一个难题。

4.1.2.3 技术方案

基于机密计算的东数西算安全计算平台架构，如图8所示。

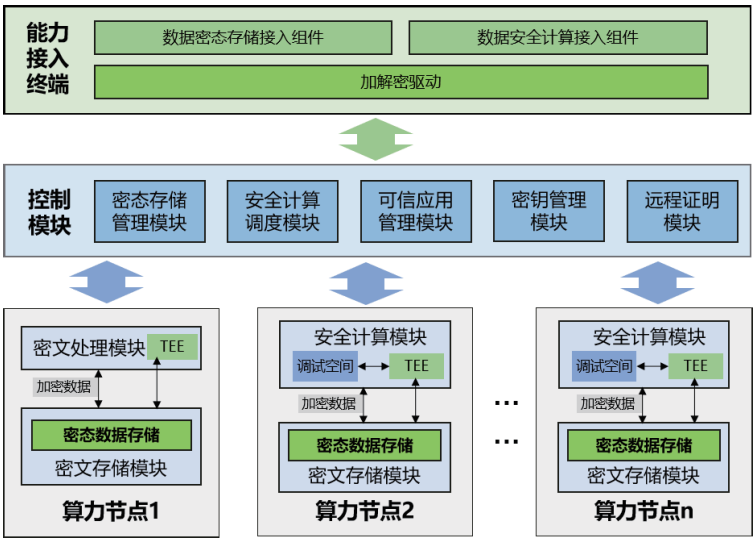

图8 存储与安全计算系统架构图

整体方案由能力接入终端、控制模块和算力节点三部分组成。

能力接入终端上可部署数据密态存储接入组件和数据安全计算接入组件，这两种组件分别接入加解密驱动模块，对与控制模块交互的数据进行加解密操作。

控制模块主要包括密态存储管理模块、安全计算调度模块、可信应用管理模块、密钥管理模块和远程证明模块。密态存储管理模块主要是对数据进行密态存储和增删改查等操作的处理和资源管理。安全计算调度模块主要是对计算任务进行数据处理、代码调试、任务配置和管理等。可信应用管理模块主要是实现对算力节点上TEE应用的生命周期管理。密钥管理模块主要实现对系统中用户的公私钥对、数据加密密钥，进行生成、分配、更新和管理等功能。远程证明模块主要完成对算力节点环境安全提供验证。

算力节点上可部署密文处理和安全计算两种功能模块。密文处理模块主要是依据加密算法存储密态数据，对数据进行创建、插入、检索、删除等操作，同时对不同加密状态和要求的操作，分配TEE或REE资源进行执行。安全计算模块主要是依据调试环境中调试完成的任务执行脚本，将密态存储的数据集导入机密计算环境中，执行安全计算任务，输出密态计算结果等。

存储与安全计算系统业务流程如图9所示。

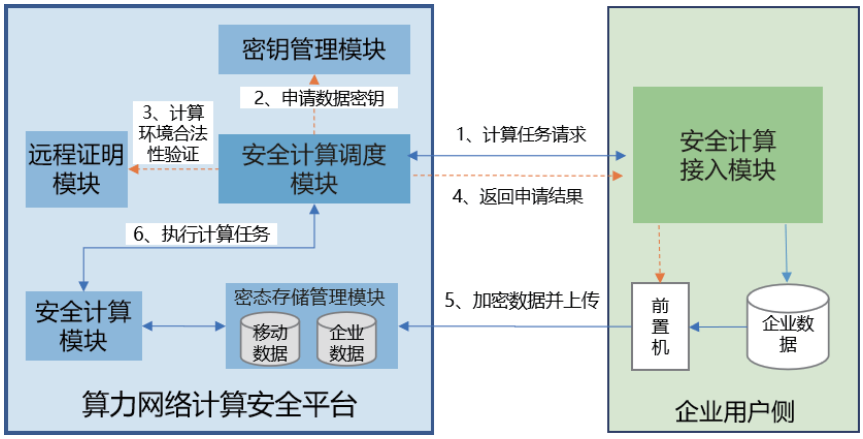

图9 存储与安全计算系统业务流程图

企业调用安全计算接入模块向算力网络计算安全平台提交计算任务请求，并挑战计算安全平台机密计算模块的合法性；安全计算调度模块向密钥管理模块申请数据密钥，远程证明模块处理企业对计算安全平台机密计算模块合法性的挑战，处理完成后，计算安全平台返回任务申请结果；安全计算接入模块基于密钥加密数据，并将数据上传/更新到算力网络计算安全子平台存储系统给定目录中；计算安全平台执行计算任务，若需要回传计算结果则返回计算结果。

4.2 密码服务

本白皮书所提密码服务是指基于机密计算环境，构建数字签名验签、数据加密及密钥管理等密码服务，实现密码服务与业务应用共用计算资源，高效互通，相对传统外挂式密码服务，存在降低适配对接工作量、实现业务应用敏捷上线等优势。

4.2.1 敏捷密码服务

4.2.1.1 场景描述

敏捷密码服务可以与应用系统灵活适配、安全且高效，将更好地提升密码技术对于信息系统的安全防护支撑作用，能够支持以用户/业务应用为颗粒度的安全保护。机密计算为构建敏捷密码服务提供了技术可行性。

4.2.1.2 需求分析

当前主流的、安全的密码技术应用，是使用具有一定资质的密码产品（如商用密码产品、CMVP密码模块等）。其中，密码硬件设备（如密码机、密码卡等）是当前广泛采用的密码供给方式。密码硬件设备具有功能/性能明确、安全边界清晰等特点，但是存在功能及部署位置固化，无法快速适配应用的功能需求变更，无法在虚拟化/云化部署下，随业务应用动态迁移、扩容/缩容等局限性。密码云、密码服务平

台等密码服务解决方案可以外部密码服务的形式部署，适应云计算业务场景需求，但是业务应用与密码服务之间需要建立数据连接（如网络通信），使得业务应用与密码服务之前存在安全暴露面，也增加了密码调用的通信及时间开销。此外，对于底层密码硬件设备无法支持的功能，依然无法快速适配应用的功能需求变更。

为有效支撑信息系统多元化的密码应用需求，敏捷密码服务应具有以下能力：

（1）**密码功能安全：**这是密码服务的基本要求，密码运算、密钥安全、密码功能访问等应用符合相关法律法规及技术标准要求。

（2）**业务伴生：**密码功能与信息系统近地部署，对信息系统的部署方式无特定限制（如本地、私有云/公有云部署），密码功能可随业务进行迁移。

（3）**密码敏捷：**密码功能（如算法、协议）可根据应用系统业务需求及密码技术演进（如抗量子密码算法）等需求，实现高效、安全的更新与部署。

（4）**以用户/业务为中心的数据安全保护粒度：**支持用户可控的数据安全，如使用用户指定的密钥进行数据加解密操作、提供用户签名私钥的安全保障等。

4.2.1.3 技术方案

在机密计算节点上实现的密码服务如图10所示，主要包含在TEE侧的可信密码服务模块、在REE侧的通用密码服务模块及SDK三个部分构成。其中，通用密码服务模块实现REE与TEE侧可信密码服务的通信，SDK由REE侧的业务应用集成实现对密码服务的具体功能调用。此外，可以在本机节点，或节点外部配置密码服务管理模块（系统）实现对密码服务的管理与配置；密码服务管理模块（系统）可支持同时对多个机密计算节点的密码服务进行统一管理，以实现密码服务的分布式部署及云部署支持。

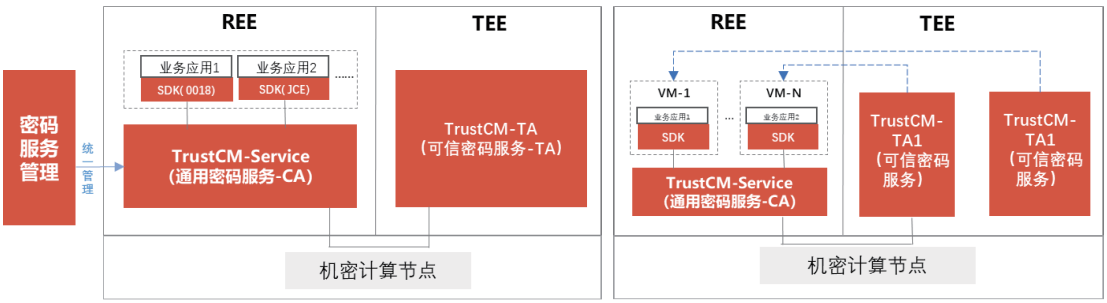

图10 基于机密计算的密码服务架构

4.2.2 密码管控平台

4.2.2.1 场景描述

传统的银行数据中心密码资源大多依赖外挂的密码设备，存在无法集中管控、难以弹性扩容以及难以

与云原生应用适配等问题。随着机密计算技术与密码技术的融合，基于TEE的密码模块作为一种新型的密码应用解决方案，在解决外挂式密码设备存在的问题的同时，衍生出了对基于TEE的密码资源的管控需求。

4.2.2.2 需求分析

银行信息系统大规模应用基于TEE的密码计算资源，需将多台设备的多个TA作为密码资源池进行集中管理。需考虑和解决以下痛点问题：

（1）**部署管理：**银行信息系统的存量设备和增量设备不确定是否支持TEE能力，需对设备硬件环境进行监测和管理。设备可能来自不同厂商，需要一套统一的策略在不同厂商的设备上部署安装TA，同时能够对安装/卸载过程进行管理。

（2）**密钥监测：**不同的业务应用可能调用不同的TA，每个业务应用使用的密钥数量存在差异，每个TA所能存储和使用的密钥数量也有所不同，需要实时监控每个TA的密钥数量并在密钥数量达到阈值时进行告警。

（3）**密钥分发：**部分业务场景中需要使用密钥管理系统分发密钥，TA无法充当密钥管理系统的角色，需要一个管理平台承担密码分发的任务。

（4）**监控告警：**每个TA接收到的运算请求量不同，TA部署在主机的TEE中，和REE共享硬件资源，需对TA的资源占用率进行实时监控和告警。

4.2.2.3 技术方案

密码资源管控平台技术方案架构如图11所示，由以下五部分组成：部署在中心服务器的部署管理平台和监管告警平台，部署在应用服务器的Agent、客户端应用CA和密码应用TA。其中，部署管理平台提供Agent注册发现、TEE环境检测、TA安装/卸载、License管理、Agent升级、TA升级等服务。监管告警平台提供密钥监控、资源监控、性能监控、密钥导入、生成证书请求、证书导入、策略下发等服务。部署在应用服务器上的Agent和管理平台通信，执行在应用服务器安装/卸载TA，并将应用服务器的环境信息及TA相关信息自动上报部署管理平台。客户端应用CA负责和TA通信，共同为业务应用提供密码服务。

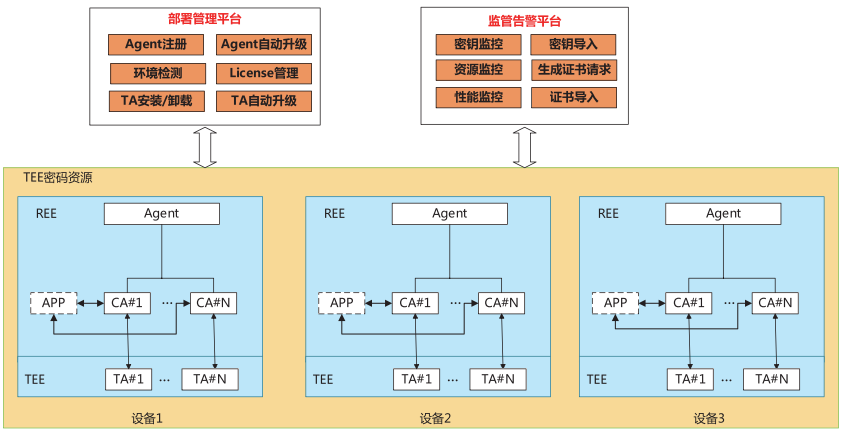

图11 密码管控平台技术架构

4.3 数据可信流通

数据可信流通是指计算结果需求方下发需求，数据提供方将数据以密文形式导入机密计算环境，按照需求运算出计算结果，再落盘加密存储，在保护数据安全、掌握数据主权的条件下，实现数据流通与共享。

4.3.1 金融业务风控

4.3.1.1 场景描述

本场景主要目的是在消费贷业务中，综合利用多维数据进行信贷风险控制。数据需求方与数据拥有方可能跨域，例如，在开发测试环境使用生产数据，在办公环境使用生产数据等情况。

4.3.1.2 需求分析

本场景中构建技术方案需满足如下需求：

（1）**兼容性：**需要支持通用的计算框架，如深度学习框架、Spark大数据分析计算引擎等。

（2）**安全与隐私：**需要遵从《数据安全法》、《个人信息保护法》，保护敏感数据流转、处理过程中的机密性和隐私性。

（3）**高性能：**在保障数据安全的同时，保障对整体信贷风险评估计算过程带来性能损耗在20%以内。

4.3.1.3 技术方案

以图12为例，因为业务需要，数据需求方需要使用数据进行业务分析或者建模，向业务部门申请数仓中的数据时，会关联数据并将脱敏后数据或数据的一些统计量分析结果提供给业务部门。但是，目前采用打标签方案进行此流程，会导致在数据格式不规范的情况下无法正确的关联数据。

因此，提出基于机密计算的解决方案如下：

（1）数据管理方将数据元上传至机密计算平台，并发布。

（2）数据需求方在机密计算平台上查看相关数据样例，根据需求请求数据的使用权，并选择使用需要的算法；数据管理方对此申请进行身份验证以及授权；通过后，数据进入机密计算模块进行计算；并根据需求，数据展示可进行脱敏处理。

（3）数据需求方获得所需结果，并无法感知原始数据以及计算过程。

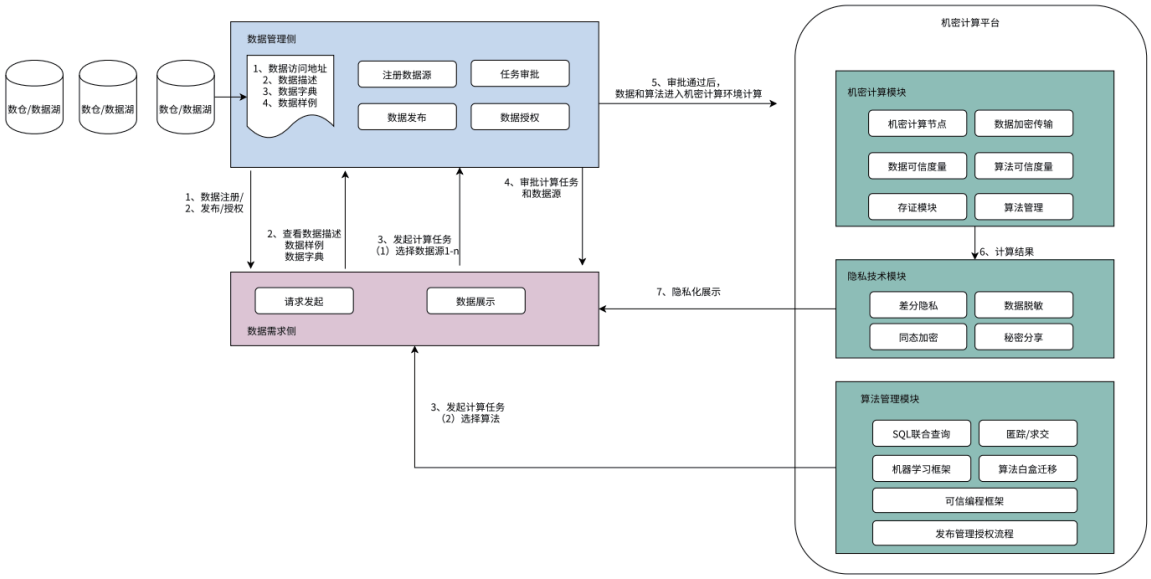

图12 数据流通以及业务需求流程图

4.3.2 政务数据共享

4.3.2.1 场景描述

如图13所示，政务不同部门间需通过对大量敏感数据共享使用、融合分析，以促进政务信息资源跨地区、跨层级、跨部门的畅通流动和业务的高效协同，但同时要求保障数据安全及隐私保护与出域安全可控，符合数据安全相关法律法规要求。

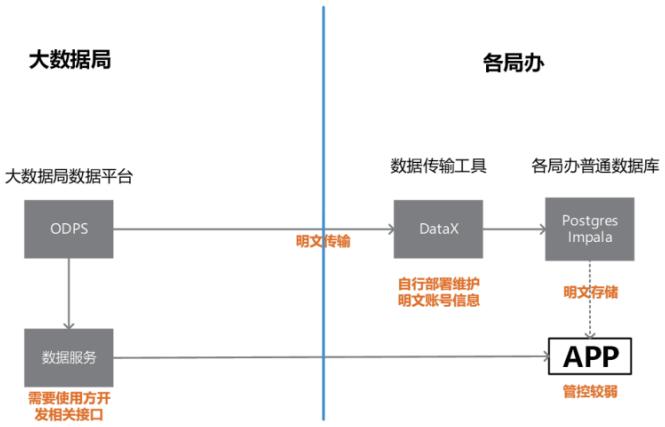

图13 政务数据共享场景示例

4.3.2.2 需求分析

目前政务数据的分享通常通过申请审批直接明文导入局办数据库或在大数据局的数据平台开发数据服务，将数据转化为可调用接口等方式，这些方式存在诸多痛点问题：

（1）**数据安全保护弱：**数据分享到各局办后通常无法提供高强度的数据安全保障，存在数据明文传输、存储、粗放式权限管控、管理员滥用操作权限等威胁，导致数据泄露等风险。

（2）**数据管控弱：**大数据局对已分享出域的数据无法再进行管控。

（3）**开发成本高：**数据服务分享方式需要额外开发，不兼容原始应用，增加数据使用成本。

4.3.2.3 技术方案

基于机密计算的政务数据共享技术方案如图14所示，由以下四部分组成：部署在数据提供方域内的应用签名服务与密钥管理服务，以及部署在数据使用方域内的加密数据库和机密计算容器集群。该方案中加密数据库和业务应用均运行在机密计算环境中，保障数据库与业务应用相关数据的全流程（存储、使用、传输态）机密性，任何明文数据无法被泄露,从而解决数据分享后安全保护弱的问题。同时对加密数据库程序和业务应用程序都进行可信度量，数据提供方可通过远程证明，验证相关程序是否运行在真实可信的机密计算环境，只有合法授权的应用程序才能够获取到使用数据的权限，并且可利用白名单随时禁止业务应用使用特定的数据，从而解决数据分享后无法管控问题。最后利用机密计算容器技术，业务应用可无缝的将应用以容器的方式运行在机密计算环境中，基本没有额外开发需求，从而解决开发成本高问题。

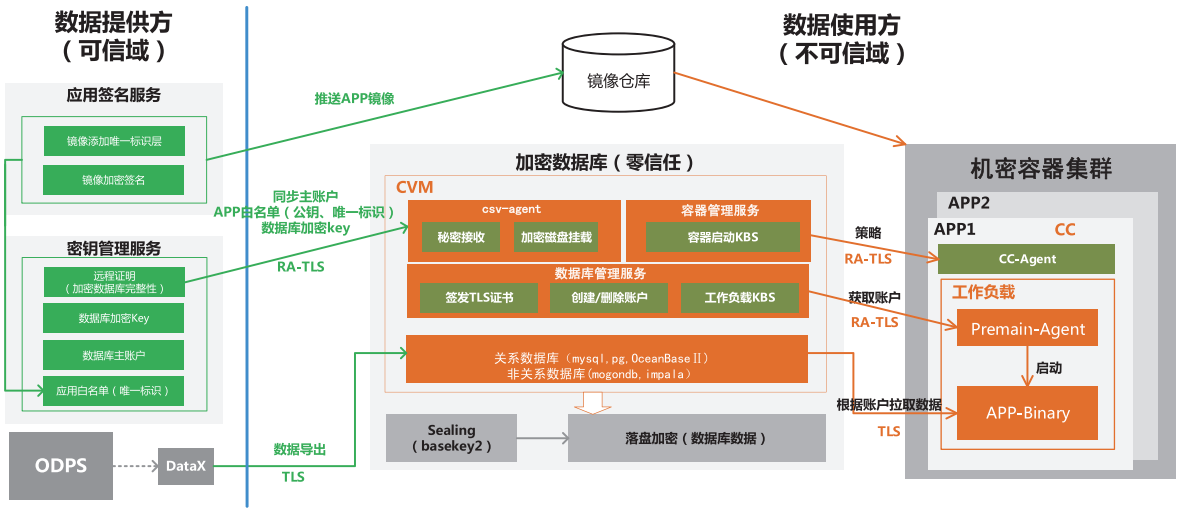

图14 基于机密计算的政务数据共享方案

4.3.3 联合建模预测

4.3.3.1 场景描述

本业务场景主要是通过在边缘节点基于机密计算技术保障数据安全的同时，进行数据预处理，并协同云端算力平台，多个边缘计算节点联合建模，基于千万条用户数据进行模型训练，保障模型预测用户点击广告的概率，实现精准营销。

4.3.3.2 需求分析

在运营商边缘计算业务中，工厂、港口、园区等用户存在着大量算力需求，计算节点需要面对海量边缘设备接入，对于涉及到用户高敏感数据的边缘设备节点，面临着数据泄露或数据被截获的风险，无法及时传输敏感数据来完成计算节点的训练和预测业务。目前边缘计算设备有地域分布广、算力多元泛在、数据海量异构、接入协议种类多的特性，在敏感信息采集和传输过程中有以下痛点：

（1）**边缘设备数据保护弱：**边缘计算设备由于地域分布广，离用户侧近且易被物理接触，易泄露已采集信息。

（2）**多方协作安全保障差：**多个数据提供方和数据计算方在联合计算时，数据传输过程和数据计算过程保障差，如何解决在多个参与方协同的环境下，实现多源数据跨域协作计算，保障多方协作过程中敏感数据信息的安全是一个难题。

4.3.3.3 技术方案

（1）边缘计算数据流转平台

保障数据在整个计算环境内不被窃取，满足客户对隐私数据处理的需求，从边缘基础设施安全到边缘安全服务，体系化构建边缘计算安全防护体系，基于机密计算的数据流转平台架构，如图15所示。

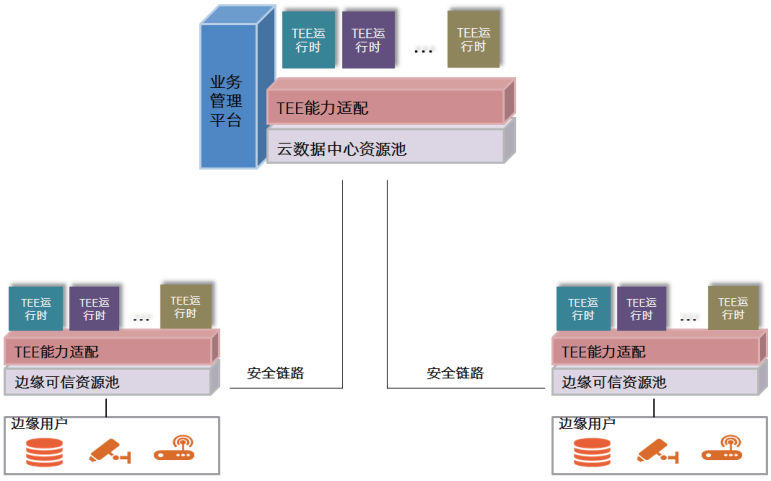

图15 数据流转平台架构图

依托于MEC平台架构，机密计算云平台采用中心-边缘的网络架构，中心节点与边缘节点采用专线网络的连接方式。在实际部署过程中，业务管理平台集中部署于云数据中心资源池端，管理平台根据业务实际需求进行资源编排和能力部署，TEE能力适配模块部署于云数据中心资源池端和各边缘数据中心端，用于构建TEE计算单元，如机密计算虚拟机、机密计算容器等。

该方案是给用户提供边缘机密计算环境节点，用户本身管理自身业务，实现防止数据泄露和篡改，解决了需求分析中的第一个问题。

（2）边缘计算业务-多方联合建模

该方案将机密计算技术与机器学习相结合，采用数据加密传输、加密存储的方式处理数据，在机密计算环境下通过训练用户数据来构建机器学习算法模型，再基于模型预测用户点击广告的概率，达到精准营销效果。

多方联合建模技术方案总体可分为数据传输模块和数据计算模块。数据传输模块是用于不同节点间的加密传输数据集，数据计算模块运行在计算节点上，用于数据计算、训练机器学习算法模型和基于模型预测结果。

数据计算模块分为联合训练任务和联合预测任务，训练任务主要在计算节点的TEE环境运行，以保证程序的机密性和完整性。训练任务流程图如图16所示，中间各关键节点会记录至审计日志。

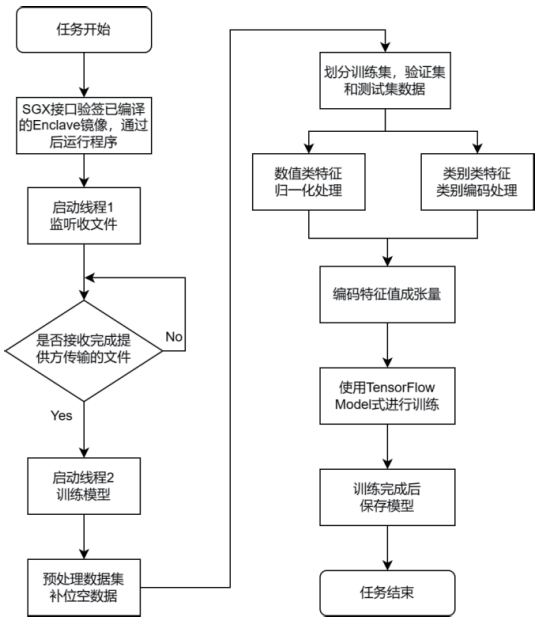

图16 训练任务流程图

多个数据方通过加密隧道向计算节点传输数据文件；任务发起方发起训练任务指令，计算节点接收指令，开始验证接收数据文件的完整性，验证通过后则解密数据文件，多方数据经处理和整合后开始训练任务，完成后加密保存模型，通过加密隧道再传给任务发起方。

联合预测任务是基于训练任务得到的模型和多方待预测数据进行广告点击率批量预测。在加载任务镜像前，系统对已编译好的镜像进行验证，通过后再加载并运行程序，确保上述计算过程运行在机密计算环境中。多个数据提供方均通过加密隧道向计算节点传送待预测数据，预测结果再返回给有权限的结果方。使用数据集前通过SHA256算法验证数据完整性，验证通过后再对数据进行处理。

4.3.4 安全联邦学习

4.3.4.1 应用场景

目前业界常用的多个数据方协同开展数据训练，基本都是通过联邦学习实现，而普通的联邦学习还是存在一些风险和问题，包括通过中间结果反推原始数据，无法支撑数据预处理阶段和模型评估过程的隐私安全等。为了弥补普通联邦学习技术中存在的不足，学术界和工业界提出了安全联邦学习概念。安全联邦学习是将传统联邦学习与TEE、多方安全计算、密码学等其他技术相结合，根据场景侧重点发挥各技术路线的优势，综合应用相关技术实现的解决方案。其中，TEE有相对较高的执行效率、较高的处理能力，应用较为广泛。

4.3.4.2 需求分析

安全联邦学习不仅要保证数据、代码、模型的机密性和完整性，还要支持多个互不信任的客户端进行协同训练。

4.3.4.3 技术方案

在安全联邦学习中，客户端可在TEE内进行本地训练，确保输入数据和训练代码的安全性，如图17所示。为了管理和协调客户端之间的机器学习协同训练，在安全联邦学习中添加一个受信任的管理组件，它根据所有客户端之间的协议来维护安全策略并约定对全局训练计算、全局训练模型以及使用的代码和输入数据的访问控制，可以自动透明地执行远程证明，确保本地计算运行正确的代码，正确的数据，并在正确的平台上执行。客户端只有在成功执行远程证明后才可以参加全局训练。

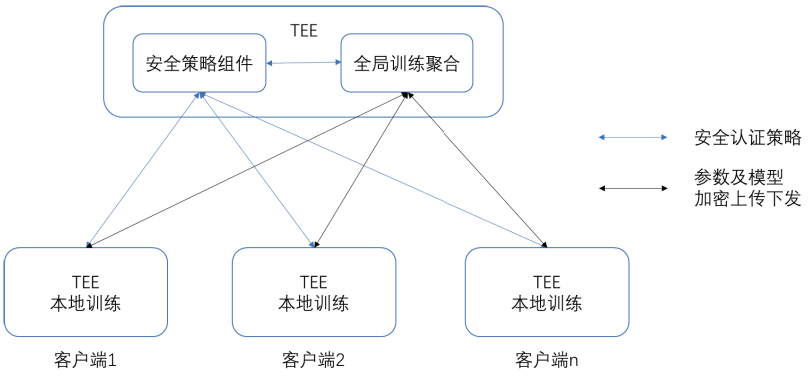

图17 基于TEE的安全联邦学习架构

在横向联邦学习中，每个参与方需要根据自有数据进行独立训练，并将中间参数传递给服务端进行聚合，然后生成新模型再次下发给参与方进行下一轮计算。可将参与方和服务端都部署在TEE环境中。参与方在各自的TEE本地训练其模型，然后将模型参数发送到聚合器进行聚合。然后，聚合器将更新的模型参数发送回客户端进行进一步训练。在参与方TEE和服务端TEE之间可通过数字信封或其他加密方式进行数据传递，在整个过程中，TEE同时承担了加解密和隔离计算的功能，可以在不损失计算效率的前提下大

幅度提高联邦学习算法的安全性。

在纵向联邦学习中，它主要用于处理不同参与方拥有相同用户但属性不同的数据的情况。各参与方拥有属性的数据会被输入到下层网络中，得到中间结果（embedding），发送给拥有标签的参与方（leader方），而不拥有标签的参与方则被称作follower方。Leader方使用embedding和标签来训练上层网络，再将算出的梯度回传给各个参与方用以训练下层网络。通过TEE环境可以将网络中的关键层屏蔽，可以使该层计算难以被反推，从而保证纵向联邦学习训练和推理过程的数据安全。

4.4 AI模型与数据保护

基于机密计算环境进行大模型微调、推理等，在保护AI模型及数据资产机密性和完整性的条件下实现AI模型及数据价值变现。

4.4.1 个人隐私云

4.4.1.1 场景描述

个人隐私云服务核心应用场景如图18所示。当用户在使用智能设备执行高强度计算任务时，如图像生成、邮件摘要、日程安排等，端侧算力有限，个人隐私云允许在云端基于更大的基础模型执行这些任务，同时保护用户隐私数据安全，无需暴露或存储用户数据。

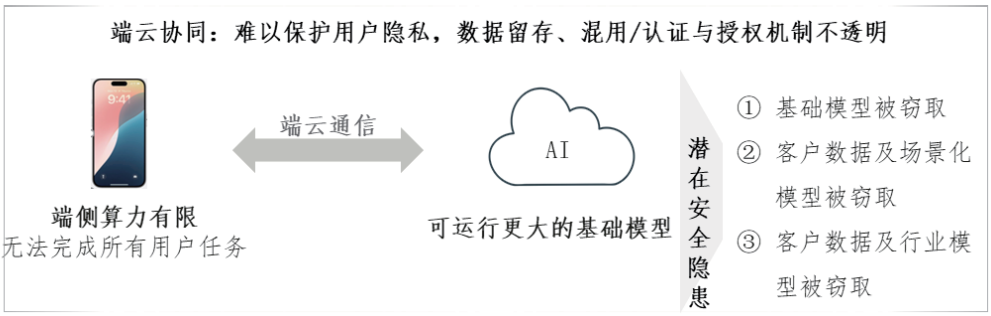

图18 个人隐私云核心应用场景

4.4.1.2 需求分析

该场景的安全需求如下：

（1）**隐私保护需求：**随着数据泄露事件的频发，用户对个人隐私保护的关注度持续提升。个人隐私云中，确保用户数据的安全和隐私成为首要问题。

（2）**高效计算需求：**AI技术的快速发展使得越来越多的复杂任务需要在云端进行处理。然而，传统的云计算服务在隐私保护方面存在诸多不足。个人隐私云通过提供安全、高效的云计算环境，满足了用户对高效计算能力的迫切需求。

（3）**透明可审计性需求：**为了建立用户信任，个人隐私云还需提供透明度和可审计性保障。使用用户能够方便地获取相关信息，验证服务器运行情况，确保自己的数据得到了妥善保护。

4.4.1.3 技术方案

符合上述场景需求的典型技术方案如图19所示。方案核心组成描述如下：

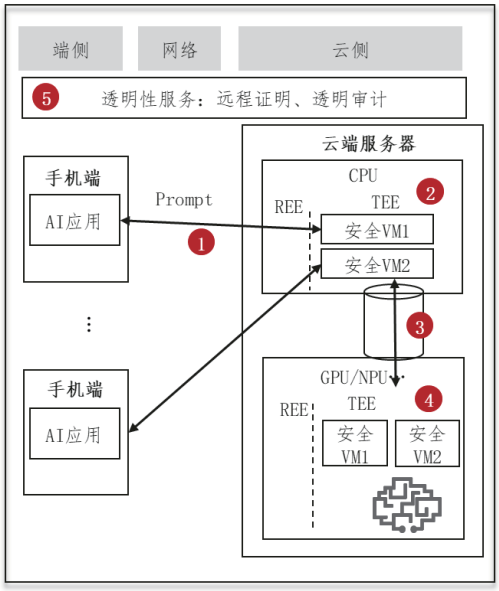

图19 个人隐私云技术方案

（1）**通信加密：**手机端隐私数据（含用户提示词Prompt）加密上传至云端服务器。

（2）**机密计算虚拟机：**为了确保用户数据在传输和处理过程中的安全性，个人隐私云服务会在云端服务器中建立机密计算虚拟机，在机密计算虚拟机中解密用户隐私数据，支撑大模型推理运行。

（3）**机密互联：**涉及需要AI加速处理器协同处理的算子及相关隐私数据，通过机密互联信道传输至AI加速处理器侧协同运算，机密互联信道能够保障其中传输的数据仅可被安全世界的授权进程访问，且能够通过加密等手段保障数据机密性和完整性。

（4）**异构可信执行环境：**AI加速处理器侧通过硬件隔离及访问控制等机制构建与CPU侧机密计算虚拟机互联的可信执行环境，保障用户隐私数据被加载到AI加速处理器侧依然能够保障机密性和完整性，CPU侧非可信特权软件及恶意程序无法访问AI加速处理器侧可信执行环境内的数据和代码。在AI加速处理器侧可信执行环境中推理获得的计算结果通过机密互联安全传输至CPU侧机密计算虚拟机内，加密后传回手机端。推理任务执行结束，机密计算虚拟机及AI加速处理器侧可信执行环境内缓存的数据均被及时删除。

（5）**透明性服务：**除在（1）-（4）描述的核心步骤之外，用户可通过远程证明验证云端服务器的可信状态，可通过透明日志审计云端推理任务执行对用户数据的调度过程。

4.4.2 AI模型微调安全

4.4.2.1 场景描述

该案例主要是在通用的人工智能微调应用部署中，为AI模型微调提供机密计算环境，保护AI模型及微调数据的机密性和完整性。

4.4.2.2 需求分析

人工智能模型在微调过程中，通常会存在以下客观事实：

（1）微调使用的数据通常是企业花费了极高的成本通过标注、治理获得的高价值数据。

（2）多数企业需要租用公有算力资源完成模型的微调训练任务。

（3）完成微调任务的模型是企业的高价值资产。

基于上述事实，AI模型微调过程中通常有如下安全需求：

（1）精调数据的保护。

（2）精调模型的保护。

4.4.2.3 技术方案

如图20所示，该方案通过与具备AI加速能力的硬件联动，将传统CPU侧的机密计算能力扩充到了AI加速硬件上，构建了面向AI模型训练和微调的机密计算环境。在此基础上，将机密计算环境与AI（大模型）开发和运维环境相结合，使得用户可以灵活地在机密计算环境之上高效地开发、运行各类大语言模型、多模态大模型。同时，通过结合基于机密计算的密钥管理系统、身份认证与鉴权、数据密封、远程证明、数据落盘加密等模块能力，确保了数据和模型全生命周期的安全性，实现了对精调数据和精调模型的保护。

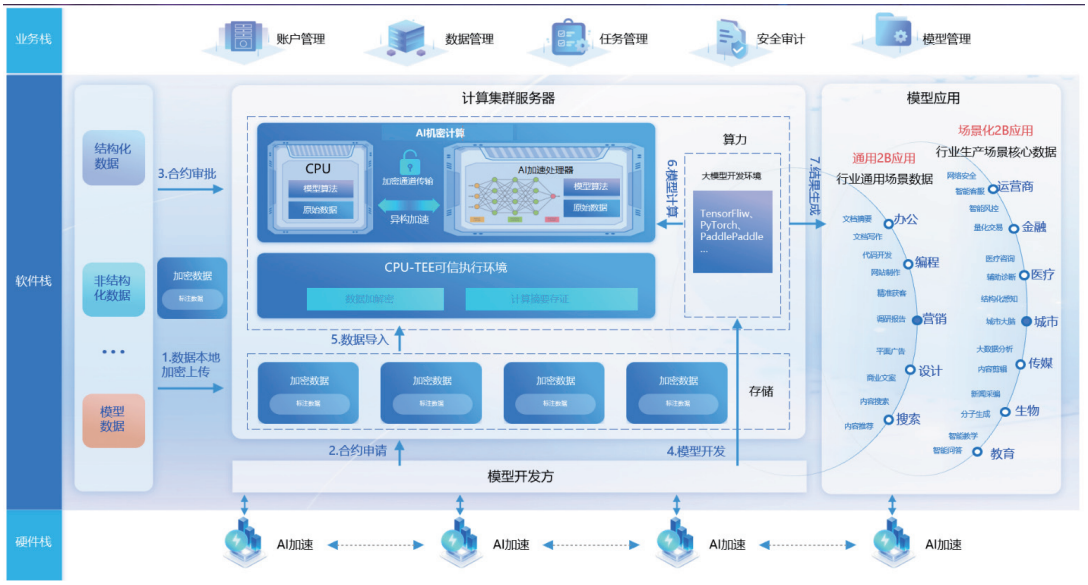

图20 AI模型微调安全架构

第五章
机密计算评测体系》

5.1 评测流程

机密计算相关产品的评测流程如图21所示。本文将对机密计算相关评测对象、评测指标及评测方法等展开介绍。

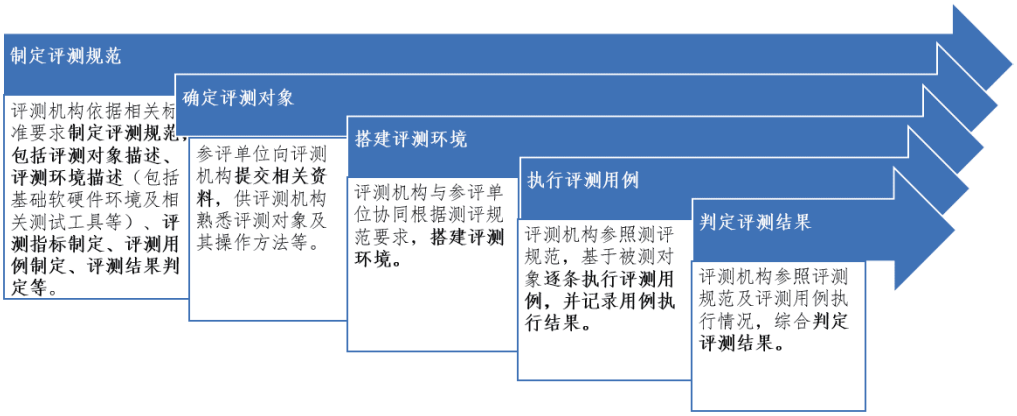

图21 机密计算评测流程

5.2 评测对象

为了最大化满足相关供应商不同产品的评测需求，对机密计算的评测对象进行了分类，如图22所示。

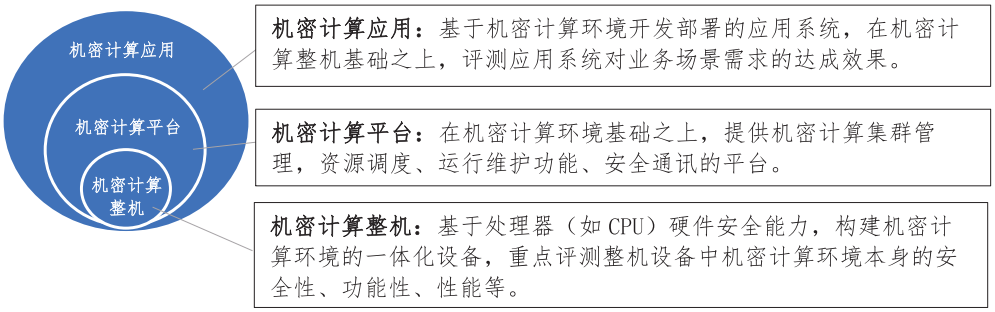

图22 机密计算评测对象

5.3 评测指标

5.3.1 机密计算整机

建议从以下维度对机密计算整机开展评测：

（a）**安全性：**评测机密计算整机是否具备系统软硬件隔离、安全启动、远程证明等安全能力。

（b）**功能性：**评测机密计算整机是否具备安全信道、存储保护、密码硬件加速和异构设备互联等功能，需要同时评测各安全功能实现的完备性及正确性。

（c）**性能：**评测机密计算整机中关键操作对系统运行整体的性能影响。

（d）**兼容性：**评测是否能够兼容主流服务器操作系统及开发语言和开发环境。

（e）**易用性：**评测对开发包和开发工具的支持情况、应用开发、部署升级维护的简易程度等。

5.3.2 机密计算平台

建议从以下维度对机密计算平台开展评测：

（a）**安全性：**评测被测对象是否已完整集成底层整机的安全能力。

（b）**功能：**针对管理型平台对象，是否支持机密计算资源的管理能力，是否支持迁移切换，故障恢复，运维监控等能力，自动化调优和分配能力，针对中间件型平台对象，对下是否提供了完整的原生机密资源的整合能力，对上是否提供了足够的服务支持库和应用开发资源。

（c）**性能：**评测被测对象对系统运行产生的额外开销。

（d）**兼容性：**评测被测对象是否支持多种异构机密计算资源的接入和管理，是否与多种OS运行时环境兼容等。

5.3.3 机密计算应用

建议在机密计算整机及平台基础之上，根据不同场景机密计算应用要解决的问题，有侧重点的评测不同场景机密计算的应用效果。建议从以下维度对机密计算应用开展评测：

（a）**安全性：**首先评测机密计算应用是否已完整利用机密计算平台或整机的安全能力；其次围绕不同应用的安全目标，评测其核心安全目标达成情况，例如，对于数据可信流通类应用，首先评测数据流通过程中，数据机密性、完整性保护效果。

（b）**功能：**根据不同的应用类型定义细节指标进行评测，例如对于可信算力服务类应用，围绕机密计算算力资源虚拟化、虚拟资源可信验证、异构算力互联等进行评测；对于AI模型与数据保护类应用，围绕AI训练或推理任务工作流程，对模型及数据运行态保护效果等进行评测，对于密码服务类应用，围绕密钥保密性，算法支持能力，算法的可扩展能力等方面进行评测。

（c）**性能：**根据不同应用类型定义业务目标强相关的性能指标。

5.4 评测方法

实际评测执行过程中，以技术测试为主，材料审核为辅，例如，可通过部署Qemu仿真器测试机密计算环境之外的普通虚拟机能否访问机密计算虚拟机中的数据。少量通用的或者难以通过技术验证的测试用例，可通过审阅参评单位提供的权威机构出具的检测报告或者产品技术文档来支撑判断用例通过情况。

关于最终评测结果的判定，可通过在评测规范中确立打分框架，包括各项指标的权重，各条用例的得分等，最终对不同评测指标得分加权求和等方式得出评测分数，也可进一步对评测分数划分等级，总之需要确定出归一化的评测结果，支撑行业用户选型参考。

5.5 评测结果应用

评测结果应用过程可参考图23。建议根据不同应用场景及系统架构面临的安全威胁、评测对象受损造成的影响等，明确评测对象并参考评测内容建议进行测评，并通过划分级别或打分对测评结果进一步处理，结合业务场景及安全需求进行产品选型。

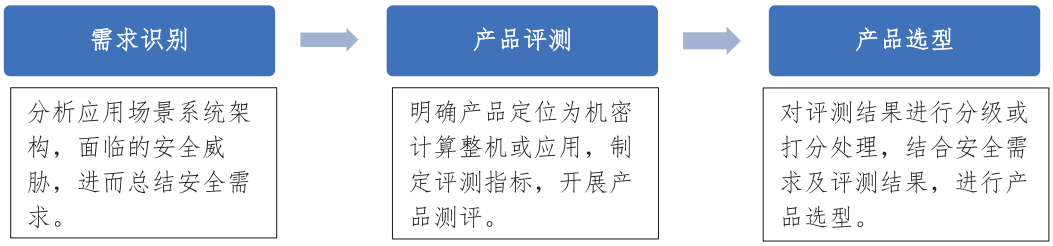

图23 评测结果应用示意

如图24所示面向不同应用场景，安全需求是不同的，受攻击影响范围越大、在非受控环境使用或者面向公众用户使用，则应选择更加安全的产品或解决方案。

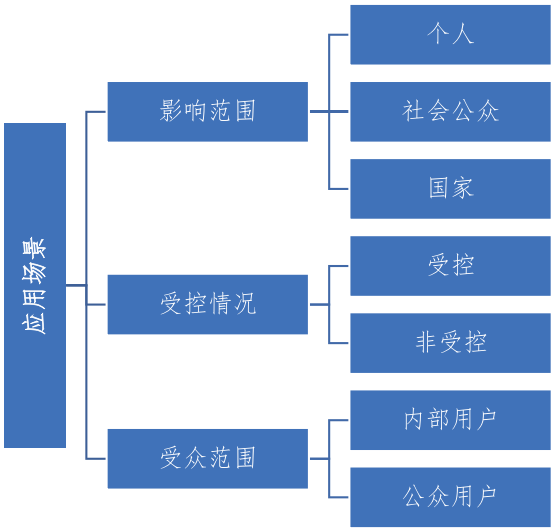

图24 应用场景分析

总结与展望》

本白皮书深入探讨了机密计算技术的核心原理、发展现状，总结了机密计算代际演进历程，研判了机密计算的发展趋势，并给出了机密计算参考框架以及面向不同场景的应用案例及评测体系，为机密计算的应用推广提供参考。

展望未来，机密计算技术将迎来更加广阔的发展空间和机遇。随着技术的不断演进和创新，机密计算将在以下几个方面实现新的突破和进展

（1）**技术创新与融合：**未来，机密计算技术将与其他先进技术如人工智能、后量子密码等深度融合，推动技术创新和升级。这种融合将进一步提升机密计算的性能、效率和安全，为用户提供更加优质的服务。

（2）**生态协作与共荣：**随着技术的不断成熟和应用场景的不断拓展，机密计算将在更多领域发挥重要作用。机密计算算力提供方、应用提供方与服务提供方等将更加紧密协作，围绕不同领域不同场景的产业需求，共同建设更加丰富、安全、高效的机密计算应用方案，做大产业生态。

（3）**标准化与规范化：**随着机密计算应用落地进入深水区，标准化和规范化将成为推动其发展的重要力量。通过制定机密计算统一服务接口、统一远程证明、互联互通协议等标准，促进不同厂商和产品之间的互操作和兼容性，降低用户的使用成本和维护难度。同时，标准化和规范化将有助于提升机密计算技术的整体安全性和可靠性。

（4）**政策引导与支撑：**监管部门的政策引导和规范，将促进机密计算的规范化发展，确保其安全合规运营，获得用户和监管部门的充分信任。随着机密计算应用落地推广、标准化与规范化推进，政府部门将逐渐在相关政策发文中，认可机密计算技术作为保障数据安全及可信流通的关键技术，并建立机密计算相关产品的检测认证制度。

（5）**市场需求与产业发展：**随着用户对数据安全需求的不断提升，机密计算将成为越来越多企业的必备技术之一，并演进出诸多可商用落地的产品及解决方案。这将推动机密计算产业的快速发展和壮大，形成更加完善的产业链和生态系统。

附录A 缩略语

英文缩写	英文全称	中文全称
AI	Artificial Intelligence	人工智能
CCC	Confidential Computing Consortium	机密计算联盟
CPU	Central Processing Unit	中央处理单元
CMVP	Cryptographic Module Validation Program	密码模块认证计划
CVM	Confidential Virtual Machine	机密计算虚拟机或机密虚拟机
FPGA	Field Programmable Gate Array	现场可编程逻辑门阵列
GPU	Graphics Processing Unit	图形处理器
KMS	Key Management System	密钥管理系统
KVM	Kernel-based Virtual Machine	内核虚拟机
MaaS	Model as a Service	模型即服务
MEC	Multi-access Edge Computing	多接入边缘计算
NPU	Neural network Processing Unit	神经网络处理器
OS	Operating System	操作系统
OVMF	Open Virtual Machine Firmware	开放虚拟机固件
PWI	Pre Work Item	预工作项目
QoS	Quality of Service	服务质量
REE	Rich Execution Environment	富执行环境
RME	Realm Management Extension	领域管理扩展
RMM	Realm Management Monitor	领域管理监视器
SDK	Software Development Kit	软件开发工具包

续表 附录A 缩略语

SEV	Secure Encrypted Virtualization	安全加密虚拟化
SEV-ES	Secure Encrypted Virtualization - Encrypted State	安全加密虚拟化 -加密状态
SEV-SNP	Secure Encrypted Virtualization - Secure Nested Paging	安全加密虚拟化 - 安全嵌套分页
SGX	Software Guard Extensions	软件防护扩展
SMMU	System Memory Management Unit	系统内存管理单元
TA	Trusted Application	可信应用
TDI	TEE Device Interface	TEE设备接口
TDISP	TEE Device Interface Security Protocol	TEE设备接口安全协议
TEE	Trusted Execution Environment	可信执行环境
TCB	Trusted Computing Base	可信计算基
TCM	Trusted Cryptography Module	可信密码模块
TDX	Trust Domain Extensions	可信域扩展
TLS	Transport Layer Security	传输层安全
TPM	Trusted Platform Module	可信平台模块
TPU	Tensor Processing Unit	张量处理器
TSB	Trusted Software Base	可信软件基
TVM	Trusted Execution Environments Virtual Machine	TEE虚拟机

参考文献 》

[1] 冯登国.《机密计算发展现状与趋势》.信息安全研究，2024年1月

[2] 李为，冯伟，秦宇，冯登国.《基于动态完整性度量的机密计算运行时监控方案》. 计算机研究与发展，2024年61卷10期

[3] 徐涛, 孔帅迪, 刘才华, 李时.《异构机密计算综述》.吉林大学学报 (工学版)，2024年3月

[4] Occlum: https://occlum.io/

[5] secGear: https://www.openeuler.org/zh/other/projects/secgear/

[6] HyperEnclave: https://juejin.cn/post/7435636363795841087

[7] Dengguo Feng, YuQin, WeiFeng, WeiLi, Ketong Shang, Hongzhan Ma. Survey of research on confidential computing. IET Communications. 2024

[8] Shijun Zhao, Qianying Zhang, Yu Qin, Wei Feng, and Dengguo Feng, Minimal Kernel: An Operating System Architecture for TEE to Resist Board Level Physical Attacks. USENIX Association 2019

[9] CCC, CCC-Tech-Analysis-Confidential-Computing-V1 2023

[10] CCC, Common Terminology for Confidential Computing 2023

[11] CCC, Confidential Computing-The Next Frontier in Data Security 2021

[12] IEEE Spectrum, What is Confidential Computing 2020

[13] NIST IR 8320D, Hardware Enable Security: Hardware-Based Confidential Computing 2023

[14] NIST IR 8320, Hardware Enable Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases 2022

[15] Arm, Arm TrustZone for AArch64, 2022

[16] Arm, Arm Confidential Computing Architecture, 2022

[17] Arm, Arm Realm Management Extension (RME) System Architecture, 2021

[18] Arm, The Realm Management Extension (RME), for Armv9-A, 2021

[19] Intel, Intel Trust Domain Extensions, 2021

[20] Intel, Overview of Intel Software Guard Extension, 2016

[21] Dayeol Lee, David Kohlbrenner, Shweta Shinde, Krste Asanovi, Dawn Song, Keystone: An Open Framework for Architecting Trusted Execution Environments, 2022

[22] Kaplan David, Protecting VM Register State with SEV-ES, 2017

[23] Advanced Micro Devices, Inc. AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More, 2020

[24] AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More 2020

[25] Microsoft. Confidential computing within an AI accelerator.2023

[26] NVIDIA. Nvidia confidential computing. 2024

Global Computing Consortium

全　球　计　算　联　盟

联盟官微

www.gccorg.com

联盟官网