解决方案简介

英特尔® 至强® 可扩展处理器
英特尔® Software Guard Extensions
英特尔® Secured Cloud Management Stack
英特尔® BigDL Privacy Preserving Machine Learning

基于英特尔® SGX 的安恒 AiLand 数据安全岛解决方案

概述

大数据已经成为企业推动数字化转型，释放数字化价值的重要方式。大数据在消费偏好洞察、业务预测分析、风险管控等方面的应用催生了业务创新，驱动了企业的快速发展。要充分发挥大数据平台的价值，需要打通多源数据，推动数据要素高效流通。在复杂的网络安全环境中，化解数据的安全隐患、保证数据的安全可信是打造繁荣数据市场的重要前提条件，这推动了机密计算方案的广泛应用。

为助力数据要素流通、赋能数据价值释放，安恒信息与英特尔公司强强联合，在大数据应用层面完成了与英特尔® Software Guard Extensions（英特尔® SGX）技术的深度适配，推出了安恒 AiLand 数据安全岛平台和隐私计算一体机。该方案具备高效、稳定、安全、方便、快捷等优势，可以帮助用户在加强数据安全性的基础上，实现数据的自由流动，赋能广告营销、消费者数据洞察、联邦计算等应用场景。

背景：数据安全成为数据要素流通市场发展的重要前提

在业务发展过程中，组织积累了海量的结构化和非结构化数据，这些数据已经成为组织最有价值的资产之一。行业报告显示，大数据平台的数据存储量在 2019~2024 年将以 26% 的年复合增长率（CAGR）高速增长[1]。在挖掘数据价值的同时，越来越多的组织探索将数据作为重要的产业要素，在市场中进行配置与流通，从而满足更多市场主体对于数据的需求，推动数字经济的发展。

在此背景下，数据要素流通市场得到了快速发展，数据要素资源规模持续扩大，数据交易市场日趋繁荣。在数据要素流通的过程中，数据安全是重要的前提与保障，只有充分化解数据泄露、数据滥用、数据篡改等数据安全风险，才能给予数据要素市场各参与主体的信心，保护其权益，提升数据要素流通的深度与广度。用户希望能够利用机密计算等技术方案，化解以下安全挑战：

- 在传统的数据流通模式中，数据交付后脱离数据服务方控制，可能导致数据泄露、数据不当利用、数据篡改等风险，影响数据要素流通的积极性。
- 传统数据流通模式往往采用大量的手动、非标准化流程，导致数据要素流通无法满足可追溯、可审计的需求。
- 在数据要素流通中，传统的数据安全解决方案更多的聚焦于保护静态和传输中的数据，却难以保护使用中的数据，带来了一定的安全隐患。
- 传统方案在构建安全防线时，往往不会将特权代码排除在外，使得整个系统存在较大的攻击面，可能被网络攻击者所利用。

解决方案：基于英特尔® SGX 的安恒 AiLand 数据安全岛

安恒 AiLand 数据安全岛平台是一个专注于保障数据安全流通，致力于解决数据共享过程中的安全、信任和隐私保护问题的机密计算平台。通过综合应用大数据可信执行环境、MPC 和联邦学习等多种隐私计算前沿技术，配合关键行为数字验签和区块链审计技术，这一平台可实现共享数据的所有权和使用权分离，确保原始数据的“可用不可见”、“可用不可取”，保障多方数据联合计算过程的可靠、可控和可溯。

[1] 数据援引自《IDC MarketScape：中国大数据管理平台厂商评估，2020》。

安恒信息与英特尔公司合作，在大数据应用层面与英特尔® SGX 完成了深度适配，提供了高效、稳定、安全、方便、快捷的数据市场安全保障能力。该方案采用数据要素全生命周期加密、区块链、机密计算、BDTee（大数据可信执行环境）、数字验签和全业务流程追踪审计技术，提供了一整套数据市场安全保障能力。安恒支持在隐私计算一体机中集成安恒 AiLand 数据安全岛平台，实现软硬件的协同交付。

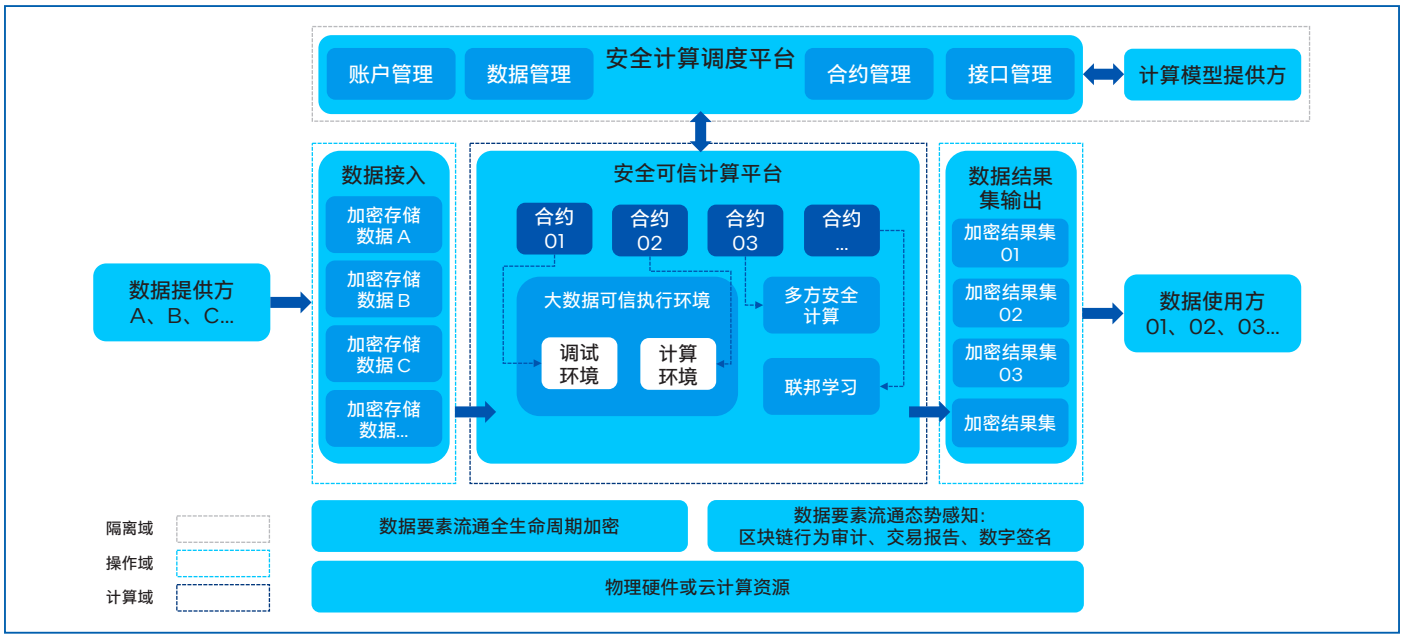

图 1. 安恒 AiLand 数据安全岛平台应用流程

有别于传统的对存储和传输中的数据进行加密的技术，机密计算技术指由具备通用计算能力的硬件提供可信执行环境（TEE）来实现的技术，能够对使用中的数据提供安全保护。安恒 AiLand 数据安全岛平台架构如图 2 所示。

图 2. 安恒 AiLand 数据安全岛平台系统架构

在底层支撑层，安恒 AiLand 数据安全岛平台依托新一代英特尔® 至强® 可扩展处理器，能够充分利用处理器强大的算力与丰富的扩展能力，支撑机密计算平台的高效运行。处理器支持英特尔® SGX 技术，将可信执行环境与安恒 AiLand 数据安全岛机密计算应用系统的计算任务、数据合约绑定，为用户提供了从硬件到软件的，数据全生命周期的安全保护。此外，新一代英特尔® 至强® 可扩展处理器具备丰富的扩展功能，能够为安恒 AiLand 数据安全岛平台提供高安全性、高运行效率、高稳定性的支撑。

第四代英特尔® 至强® 可扩展处理器通过创新架构增加了每个时钟周期的指令，每个插槽多达 60 个核心，支持 8 通道 DDR5 内存，有效提升了内存带宽与速度，并通过 PCIe 5.0（80 个通道）实现了更高的 PCIe 带宽提升。第四代英特尔® 至强® 可扩展处理器提供了出色性能和安全性，可根据用户的业务需求进行扩展。借助内置的加速器，用户可以在 AI、分析、云和微服务、网络、数据库、存储等类型的工作负载中获得优化的性能。通过与强大的生态系统相结合，第四代英特尔® 至强® 可扩展处理器能够帮助用户构建更加高效、安全的基础设施。

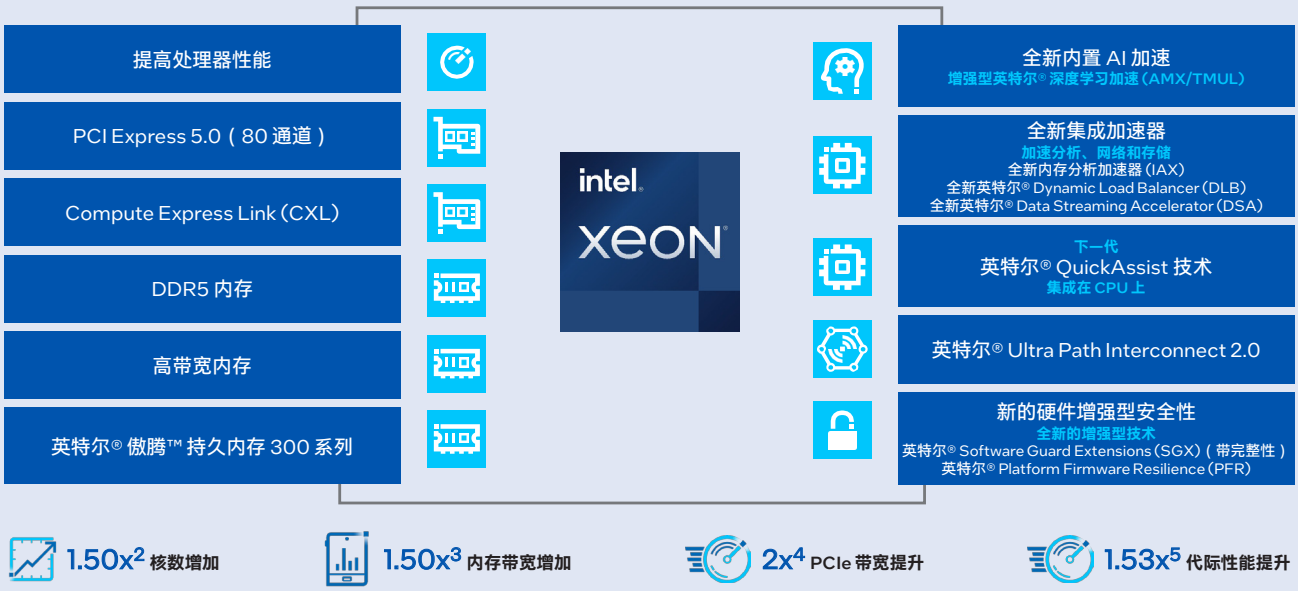

图 3. 第四代英特尔® 至强® 可扩展处理器提供多种优势

安全支撑系统为安恒 AiLand 数据安全岛平台核心组件运行时安全性提供保障，该系统由英特尔® SGX 技术提供支持。作为应用最广泛的机密计算方案之一，英特尔® SGX 能够帮助用户构建基于硬件的数据中心可信执行环境 (TEE)，通过将特权代码排除在受信任的范围之外，英特尔® SGX 能够更有效地抵御多种类型的攻击。它可显著加强数据安全，满足对于机密计算的广泛需求。

英特尔® SGX 提供了一种基于硬件的内存加密机制，将内存中的特定应用代码和数据隔离开来。它允许为用户级代码分配专用内存区域 — 飞地 (Enclave)，以免受到拥有更高权限的进程的影响。除了有助于防御基于软件的攻击外，英特尔® SGX 的验证机制还能够帮助用户确保应用程序所在的飞地是一个真正的英特尔® SGX 环境，不会受到相关攻击和篡改。

为了增加大规模部署的灵活性，英特尔基于当前业内典型的云基础架构管理平台 OpenStack 以及 Kubernetes 等，全面集成了英特尔® SGX 的安全功能，推出了基于英特尔® SGX 的安全云管理解决方案：英特尔® Secured Cloud Management Stack，帮助云计算用户更好地防范云端安全风险并实现快速部署。

该方案能够支持用户在云端以简单灵活的方式使用英特尔® SGX 功能，更有效地保护云端的实例（包括虚拟机、裸金属服务器以

[2] 数据来源自第四代英特尔® 至强® 可扩展处理器的最大核数（60 核）与第三代英特尔® 至强® 可扩展处理器的最大核数（40 核）的比较。

[3] 详细配置信息请访问：intel.com/processorclaims，选择“第四代英特尔® 至强® 可扩展处理器”，查看编号“G2”。实际性能受使用情况、配置和其他因素的差异影响。

[4] 数据来源自第四代英特尔® 至强® 可扩展处理器（80 条 PCIe 5.0 通道）与第三代英特尔® 至强® 可扩展处理器（64 条 PCIe 4.0 通道）的比较。

[5] 详细配置信息请访问：intel.com/processorclaims，选择“第四代英特尔® 至强® 可扩展处理器”，查看编号“G1”。实际性能受使用情况、配置和其他因素的差异影响。

及 Kubernetes 集群中的 Pod），使运行于上述实例中的应用获得芯片级的数据安全保护能力。此外，这一方案还实现了对整个安全云基础架构的自动化部署，支持在云端对英特尔® SGX 进行完备的资源管理，并提供相应实例的生命周期管理能力。基于上述能力，该方案能够赋能大数据、联邦学习、可信多方计算、安全密钥管理等应用，帮助用户更好地保护云端数据。

构建在英特尔® Secured Cloud Management Stack 安全云管理解决方案之上的安全支撑系统，能够通过机密虚机、机密裸机、机密容器等技术，为程序和数据提供安全的执行环境，其提供了如下关键能力：

- 基于硬件安全启动功能构建的系统可信模块，为安恒 AiLand 数据安全岛平台上运行的系统提供了系统层面的可信保证。
- 基于硬件远程证明、安全隔离的合约可信模块，可以为安恒 AiLand 数据安全岛平台上运行的应用程序与数据提供可信保障。
- 基于硬件安全存储、安全通信、密码运算、数据封装的数据全生命周期加密模块，可以为应用系统中的数据提供硬件级别的数据安全保护。
- 基于硬件密钥管理的密钥管理和身份认证模块，可以为业务系统提供安全、灵活的用户管理功能。

在基础架构支撑层，包括安全支撑系统、性能支撑系统和大数据平台支撑系统，大数据平台支撑系统构建在安全支撑系统和性能支撑系统之上，为上层安恒 AiLand 安全岛机密计算中台提供大数据计算、存储的能力。大数据平台应用了英特尔® BigDL PPML 框架，该框架基于英特尔® SGX/TDX 技术，为大数据分析和人工智能应用提供了端到端的安全和隐私保护。BigDL PPML 提供了一个可以运行标准大数据应用的环境，能够帮助现有的大数据/分布式应用无缝迁移到端到端安全环境中，并且强化每个环节的安全性。在此基础上，PPML 也提供了安全参数聚集、隐私求交和联邦学习等高阶功能，帮助行业客户打破数据孤岛，进一步实现数据赋能。

应用实践

基于英特尔® SGX 的安恒 AiLand 数据安全岛平台提供了如下重要价值：

- 通过英特尔® SGX 减少了可信执行环境的攻击面，提升了芯片算力，为各种应用领域提供了可信的底层支撑。
- 结合硬件及软件，保证了数据全生命周期的安全。硬件层面基于英特尔处理器，软件层面使用安恒信息独立开发的安恒 AiLand 数据安全岛数据互联平台，安全层面由安恒信息多维度的网络安全防护系统进行保障，满足了企业对 IT 设施和软件严格的安全性要求。
- 机密计算技术与密钥管理和身份认证绑定，为每个用户的身份验证及数据安全保护提供安全保护功能。
- 机密计算技术与数据合约绑定，为每个计算任务创建独立的可信环境，使不同合约之间的数据完全隔离，最终实现数据的“可用不可见”、“可用不可取”，保障多源多方数据安全计算的可靠、可控和可溯。
- 机密计算技术与其他隐私计算平台结合，提供安全、可信、快速执行计算任务的基础，可为安恒 AiLand 数据安全岛其他隐私计算平台提供底层支撑。其他隐私计算平台包括安全多方计算平台、联邦学习平台等。
- 可信执行环境内的操作被详细审计和记录，并保存在区块链上，实现操作监控和历史回放，方便后续事件溯源。

目前，机密计算技术正处在迅速发展的阶段，安恒 AiLand 数据安全岛平台已经在互联网、金融、教育、零售和政务等各垂直领域得到了广泛应用，实现了对于数据资产和隐私数据的全生命周期保护，满足了客户对于数据安全流通的要求，提供了基于安全、信任和隐私保护的海量数据市场化解决方案。

案例：某互联网视频企业为品牌方客户提供个性化的广告投放服务。客户期望通过第三方独立单位的数据验证广告位投放的精准性和有效率。为了保护各方数据安全并实现数据共享，该企业采用了安恒 AiLand 数据安全岛平台，通过中立的隐私计算平台保护用户的个人隐私数据以及各方数据资产，确保数据验证的可控、可审计，同时保证数据验证模型可审核。

图 4. 某互联网视频企业通过安恒 AiLand 数据安全岛平台保证多方数据安全

通过该方案的实施，该互联网视频企业能够在确保数据安全和隐私保护的前提下，按照品牌方客户的要求，进行精准广告投放，提升广告收益和服务品质。品牌方客户得以有效地评估广告投放的精准性，增加品牌曝光率。

展望

在数据要素市场日趋繁荣、网络安全环境不断复杂化的今天，通过机密计算等方式来降低数据安全隐患、提升数据要素市场主体信任度已经迫在眉睫。安恒 AiLand 数据安全岛平台通过采用新一代英特尔® 至强® 可扩展处理器，以及英特尔® SGX 等关键技术，提供了软硬件融合的一站式机密计算解决方案，帮助用户提升数据安全、保证数据验证的可控、可审计，推动数据要素市场的快速发展。

未来，安恒信息还将基于英特尔® Secured Cloud Management Stack 2.0 版本对方案进行优化。该版本将英特尔® SGX 与 Kubernetes 容器管理平台集成，并提供基于主流大数据组件以及数据流的工具，为客户提供大数据场景下的 SGX 应用参考。此外，该版本还将围绕远程认证服务，结合密钥管理，为用户提供应用层面的安全设计参考架构。通过应用英特尔® Secured Cloud Management Stack 2.0 版本，安恒信息将增强数据安全管理能力，满足数据要素市场对于机密计算的要求。

关于安恒信息

杭州安恒信息技术股份有限公司（简称：安恒信息）成立于 2007 年，自成立以来一直专注于网络信息安全领域，公司秉承“构建安全可信的数字世界”的企业使命，以数字经济的安全基石为企业定位，将“诚信正直、成就客户，责任至上，开放创新，以人为本，共同成长”作为企业的价值观，致力于成为全球领先的数字安全企业。

关于英特尔

英特尔（NASDAQ: INTC）作为行业引领者，创造改变世界的技术，推动全球进步并让生活丰富多彩。在摩尔定律的启迪下，我们不断致力于推进半导体设计与制造，帮助我们的客户应对最重大的挑战。通过将智能融入云、网络、边缘和各种计算设备，我们释放数据潜能，助力商业和社会变得更美好。如需了解英特尔创新的更多信息，请访问英特尔中国新闻中心 newsroom.intel.cn 以及官方网站 intel.cn。

intel®