案例研究

深度学习
安全计算

机密计算助力深度学习安全及能力兼得

本文探讨英特尔® 软件防护扩展 (英特尔® Software Guard Extensions，以下简称英特尔® SGX) 如何参与构建百度 MesaTEE* 安全计算平台，与百度飞桨 (PaddlePaddle) 开源深度学习平台联动，实现为深度学习定制的机密计算能力，并展望了其在多个领域被应用的可能性和潜力。

引言

这是一个以大数据和人工智能技术驱动的新时代。各行各业都已认识到数据的意义，并期待不断开发数据的巨大价值潜力。在这一过程中，数据的流动和聚合成为了近年来不断被关注的话题。随着数据不断膨胀和多元化，越来越多企业渴望聚合更多来源、更多维度和更高质量的数据，通过深度学习等先进技术对其加以利用。然而，在众多敏感数据被传输、分享和处理的过程中，对数据安全的担忧日益凸显。与此同时，在全球及中国，越来越严格的数据安全法规也在不断出台，为企业合规性提出了挑战。

为兼顾数据共享与数据安全需求，实现机密计算，英特尔从第 6 代英特尔® 酷睿™ 处理器平台开始引入了英特尔® 软件防护扩展 (英特尔® Software Guard Extensions，以下简称英特尔® SGX) 技术。作为一个基于硬件的安全解决方案，英特尔 SGX 绕过操作系统和虚拟机软件层，帮助将敏感的程序代码和数据加载到指定的受 CPU 保护的内存分区“飞地” (enclave) 里，提供更强的保护以防止其被泄露或更改。

本文探讨英特尔 SGX 如何参与构建百度 MesaTEE* 安全计算平台，与百度飞桨 (PaddlePaddle) 开源深度学习平台联动，实现为深度学习定制的机密计算能力，并展望了其在多个领域被应用的可能性和潜力。

打造百度 PaddlePaddle 机密深度学习平台

关于 PaddlePaddle

深度学习被誉为人工智能时代的“操作系统”。作为中国知名的科技企业，百度多年前就展开了对深度学习的研究。百度飞桨 (PaddlePaddle) 是百度在深度学习领域布局的重要产品。作为云端托管的分布式开源深度学习平台，PaddlePaddle 致力于让深度学习技术的创新与应用更简单，在中国拥有活跃的开发者社区生态，提供丰富的官方支持模型集合，并提供全类型的高性能部署和集成方案供开发者使用，目前已广泛应用于工业、农业、服务业等。

自2016年开源以来，PaddlePaddle不断优化和升级。近两年来，为帮助各行各业的企业以更安全的方式应用深度学习模型发掘数据联合的价值，PaddlePaddle在自身生态系统内构建出了软硬件两种实现机密计算的解决方案。

其中，软件解决方案基于MPC (Secure Multi-Party Computation) 密码学算法来实现，其核心是开源联邦学习框架PaddleFL。PaddleFL提供很多联邦学习策略及其在计算机视觉、自然语言处理、推荐算法等领域的应用。此外，PaddleFL还提供传统机器学习训练策略的应用，例如多任务学习、联邦学习环境下的迁移学习。依靠着PaddlePaddle的大规模分布式训练和Kubernetes对训练任务的弹性调度能力，PaddleFL可以基于全栈开源软件轻松地部署。

而硬件解决方案则基于TEE (Trusted Execution Environment) 可信执行环境来实现，其核心是百度安全计算服务框架MesaTEE。MesaTEE提供基于英特尔SGX等硬件保护的TEE执行环境，免除了软件层面的密文操作，执行速度快且能对抗服务端恶意攻击模型。

MesaTEE 与 SGX

2018年9月，百度安全联手英特尔发布了MesaTEE——基于SGX技术，全部使用内存安全的Rust语言开发的内存安全可信计算平台。MesaTEE分成商用版(MesaTEE)和社区版(Teaclave)。后者于2019年中期在GitHub上开源，同年年底捐献Apache基金会，并更名为Teaclave，成为Apache社区孵化器项目。商业版MesaTEE基于ApacheTeaclave开发，为厂商客户提供深度定制的商用解决方案，不仅支持基于英特尔SGX的TEE计算引擎，而且独创了协同机密计算引擎。这两种计算引擎让隐私保护的大数据分析及机器学习成为可能。MesaTEE在隐私保护的前提下，打破了产业链上下游既有的数据壁垒，有效解决数据流通与协作过程中的合法合规、数据安全问题，能充分激发数据要素价值，实现数据“价值”与“知识”开放与共享，真正做到“数据可用不可见”。

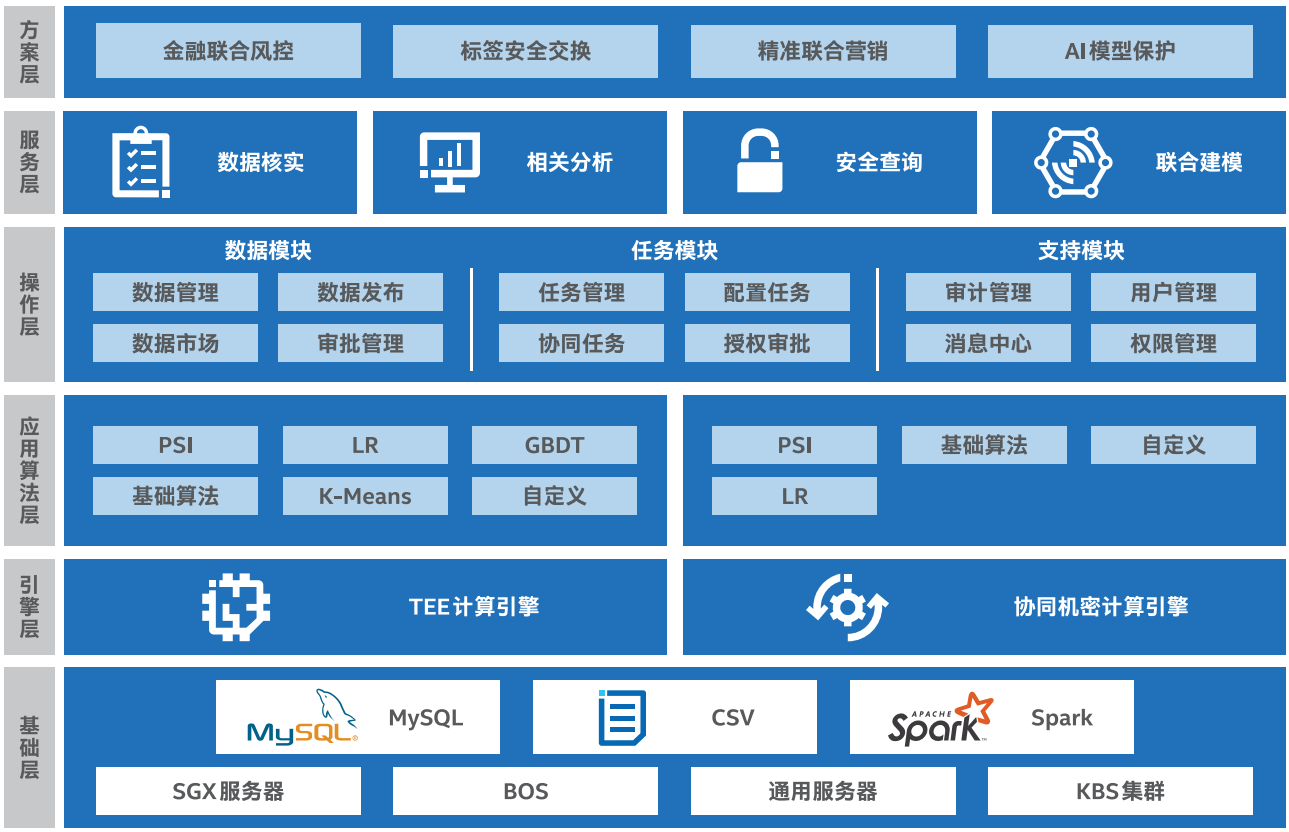

图1. 百度MesaTEE整体架构

MesaTEE 与 PaddlePaddle

作为一个通用的机密计算平台，MesaTEE整体完全运行在TEE可信环境中，且完全使用Rust语言撰写，能够做到从数据上传、数据处理到结果获取的全流程保护。此外，MesaTEE也是一个多方任务协作平台，能通过任务方式（类似于合同方式）来管理合作流程，确保执行流程不受外界干扰。这意味着参与方能在隐私信息不泄露的前提下，公平地完成任务协作，达成共识后获取到各自所需的计算结果或模型。

用户场景的多样性导致在实际应用中需要权衡安全、功能、性能甚至习惯等诸多因素。为此，MesaTEE将安全等级划分为5级。L1为最低安全等级，提供最全的功能支持和最快的速度，但在安全上有所妥协。L5为最高安全等级，提供更全面的安全防护，限制了功能及实现方式，其运算性能和功能相比其他等级将有所妥协。在默认情况下，MesaTEE提供L5最高级别的数据安全防护以及在运算速度上的平衡。为了适应不同应用场景和安全等级要求，MesaTEE可通过支持Executor插件的形式提供其它类型的执行环境，包括SCONE、Occlum和Graphene等TEE执行环境。

为将PaddlePaddle运行在类似LibOS的TEE环境，需要对其底层运行库进行改造。英特尔SGX的enclave是一个资源受限环境，严格限制了系统调用、数据进出、网络访问及内存等。原生的PaddlePaddle使用glibc，但并未考虑到在资源受限的环境中运行，导致glibc在迁移到TEE环境时遭遇种种障碍，甚至需要裁剪及补丁，且难以维护，在TEE中仅有非常少数厂家支持。相比之下，大部分厂家选择使用musl（为受限环境全新撰写且实现了POSIX接口底层的运行库）作为TEE和上层程序的调用接口。为运行在已有的TEE环境中，PaddlePaddle联合百度安全适配了底层调用接口库，并提供了WITH_MUSL编译选项，以及全自动化的编译脚本。PaddlePaddle将持续对底层运行库进行安全审计，修复潜在安全风险。目前，此修改已完全向PaddlePaddle社区开放并将长期维护。

作为协作平台和任务调度者，MesaTEE以Executor插件的形式将PaddlePaddle作为其一种任务执行环境，将特定的深度学习任务投递到PaddlePaddle的TEE运行环境中执行。此外，MesaTEE还联合了不同的TEE厂商，适配其远程证明(Remote Attestation)流程的正确性，并且整合至通信协议上，确保其运行环境的安全性是可度量的。在文件访问方面，支持S3等远程文件存储协议，文件内容全部使用密文存储。另有一套特殊文件系统，用于为PaddlePaddle在不改变使用方式的前提下，在训练过程中在TEE中访问所需密文，但在TEE外无论从磁盘、内存或网络通信上都不存在途径可以窥查其计算内容，从而抵抗恶意攻击模型，确保整体安全性。

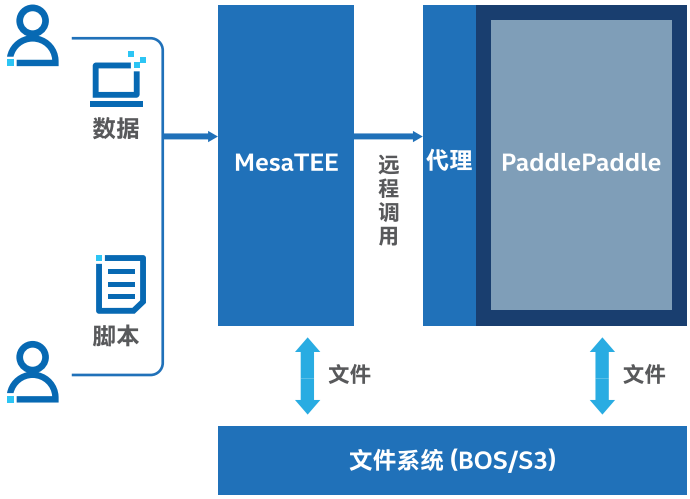

图2. PaddlePaddle与MesaTEE的联动

方案优势

借助MesaTEE来实现硬件级PaddlePaddle机密深度学习能力的解决方案拥有多重优势：

A. **高效：** 借助硬件级的英特尔SGX技术，百度PaddlePaddle得以更高速地实现在嵌入式TEE环境中的运行。搭载新一代英特尔® 至强® 可扩展处理器时的运行速度快。此外，硬件级解决方案排除了网络限制，避免了网络故障导致大型训练任务中断的风险。

B. **低成本：** 拥有低成本的优势是不言而喻的。传统上，为提升数据安全性，很多企业会投入购买诸如专用加密设备一类的解决方案。PaddlePaddle与TEE环境的结合仿佛一个巨大的分布式的加密设备，而使用兼容英特尔处理器的用户在使用时无需付出额外成本。

C. **简单易上手：** 对开发者而言仅需3步即可运行，安装时间可以缩短至3分钟。[1]

D. **支持多种容器：** 能支持大多数SGX TEE容器，包括SCONE、Occlum和Graphene等。

百度 PaddlePaddle 机密深度学习平台应用示例

在各行各业，随着数据量的指数级增长，数据格式的丰富（文本、图片、音频、多媒体等），传统的机器学习已无法满足很多场景下的模型需求，而深度学习正在展现出明显的优势。同时，为打破数据提供方、建模方与使用方之间彼此割裂的障碍，机密计算势在必行。PaddlePaddle 将深度学习平台与机密计算能力有机结合，响应了业界趋势，能够在众多领域发挥重要作用。

医疗影像筛查

医疗影像筛查的对象是影像（即图片），而非传统意义上的特征向量。在识别图片时，传统机器学习技术往往采用图像处理与机器学习相结合的方式，不仅效率低下，而且无法应对庞大的图形数据量。深度学习技术的发展推动了医疗影像识别能力质的飞跃。它借助计算机视觉，实现了从特征提取到整体图像识别的完整一体化识别方式，大幅提升了医疗影像识别的效率和精准度，能快速实现医疗影像的分类、识别、定位、检测、分割等任务。

然而，深度学习虽然解答了技术手段问题，却未能解决现实场景中的操作问题。一个成功的医疗影像筛查模型需要以大量的病患医疗影像数据为基础展开模型训练，必然涉及大量个人隐私，对数据安全性提出了极高的要求。再者，当多家医疗机构共同访问一个模型平台时，也希望对各自病患的信息进行严格保护，避免被他方窃取。此外，模型开发方，不论是第三方还是医疗机构本身，也希望保护自己的模型，实现利益最大化。显然，机密计算将是具备隐私保护能力的完整医疗影像筛查解决方案中不可或缺的一环。

在 TEE 中运行的 PaddlePaddle 能很好地解决以上种种问题。目前已有一套眼底图像血管分割系统充分利用 PaddlePaddle 深度学习框架，克服了眼底图像噪声大、视网膜血管结构复杂多变等障碍，实现了对眼底图像中血管特征的实时提取，对辅助医疗人员诊断眼科疾病、心脑血管疾病等具有重要作用。而借助 PaddlePaddle 开发的肺炎 CT 影像分析模型可以高效地完成病灶检测识别和病灶轮廓勾画，并通过一定的后处理代码，分析输出肺部病灶的数量、体积、病灶占比等全套定量指标。该系统借助深度学习算法模型，训练了所收集到的高分辨率和低分辨率 CT 影像数据，能很好地适应不同等级 CT 影像设备采集的检查数据，有望为医疗资源受限和医疗水平偏低的基层医院提供有效的肺炎辅助诊断工具。更重要的是，在当前疫情诊疗的关键时期，该系统能有效帮助临床医生缓解工作压力，加快患者诊疗速度，为缓解医疗资源不足和取得抗疫的最终胜利提供助力。同时，借助机密计算能力，这些医疗影像筛查系统还能充分保护病患隐私，消除数据提供方、建模方与使用方之间的隔阂，在医疗行业数据泄露频繁、数据使用效率低的大背景下，为智能医疗的未来开辟了新的道路。

金融风险控制

风险控制是金融行业的根基。以信贷风险评估为例，其主旨是对借贷人的还款能力和信用等级进行详实的分析、评估和预测。传统以来，金融机构以简单的二维数字型数据来勾勒借贷人画像，并使用机器学习技术展开建模和分析。深度学习技术的日趋成熟为信贷风险评估开拓了全新的可能。深度学习模型能突破传统机器学习技术的局限，高效利用语音识别、图像识别等方式，将多媒体数据和流数据纳入模型，比如支付数据（第三方支付方）、消费数据（零售商及电商平台）、信贷数据（第三方信贷机构），甚至是社交人脉（社交平台）、工作履历（招聘平台）、旅游出行信息（出行平台）等。

传统上，建立一个信贷风险评估模型需要采用分布式系统模式，将以上种种数据整合到其中一方。但从数据提供方角度而言，这些用户隐私数据敏感性很高，并且可能受到法律保护不允许流通。这导致现实场景中，金融行业数据孤岛情况非常普遍。数据的提供方、建模方、评估方和使用方之间彼此割裂。为实现数据聚合，引入机密计算技术是必然的发展趋势。

通过在 TEE 中运行的 PaddlePaddle 深度学习平台，金融机构将得以安全地与更多数据源合作，获得更多维的用户画像数据，打造出更健壮的信贷风险评估模式。PaddlePaddle 机密深度学习平台将大幅提振各方信心、避免数据泄露风险、划分数据所有权、帮助数据合规流动，一站式解决了多方共享及使用敏感数据的种种痛点，满足金融技术对挖掘数据共享和聚合价值的迫切渴望。

展望

2020年12月，全新的PaddlePaddle 2.0版本将正式开放，届时会推出多项重要的升级和特色，包括在TEE环境中实现所有已有的PaddlePaddle功能，并提供musl的预编译版本，供用户在TEE环境中直接安装和使用。

在前文介绍的MesaTEE和PaddlePaddle之外，百度还在更高层面布局了点石大数据开放平台。百度点石融合了百度大数据全栈技术能力，将复杂多样的大数据工具打通适配，形成数据处理、加工与应用的一站式开发服务。面向数据提供者、系统集成商、独立软件开发商、咨询公司、模型开发商等不同类型的合作伙伴，点石提供独具特色的解决方案，精准满足客户与伙伴需求。

在英特尔方面，全新一代英特尔®至强®可扩展处理器将会搭载升级后的英特尔SGX技术，其EPC内存将从现在的单路128 MB跃升至512 GB，助SGX TEE环境内的机密计算性能一举迈上全新台阶。

此外，拥有多年合作关系的英特尔与百度还将继续携手开拓创新，利用英特尔的技术，为百度智能方面的业务、平台、产品和服务带来高性能和出色功能，共同服务业界生态。

intel®

[1] 性能表现数据来自百度。如欲了解这些测试的更多细节，请与百度联络。英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。

英特尔技术特性和优势取决于系统配置，并可能需要支持的硬件、软件或服务得以激活。产品性能会基于系统配置有所变化。没有任何产品或组件是绝对安全的。更多信息请从原始设备制造商或零售商处获得，或请见intel.com。

描述的成本降低情景均旨在特定情况和配置中举例说明特定英特尔产品如何影响未来成本并提供成本节约。情况均不同。英特尔不保证任何成本或成本降低。