蚂蚁集团

隐私计算最佳实践

Gartner

隐私计算最佳实践

1 概述

隐私计算：隐私保护前提下链接数据孤岛

满足数据安全、隐私保护和监管合规前提下，链接数据孤岛，实现多方协同释放数据要素价值，是当前大数据技术发展应用的一大难题，而隐私计算正是解决这一难题的技术方案。隐私计算又称为隐私增强计算、隐私保护计算，是目前业界认可的、能在数据要素流通融合中有效保护数据隐私的信息技术。

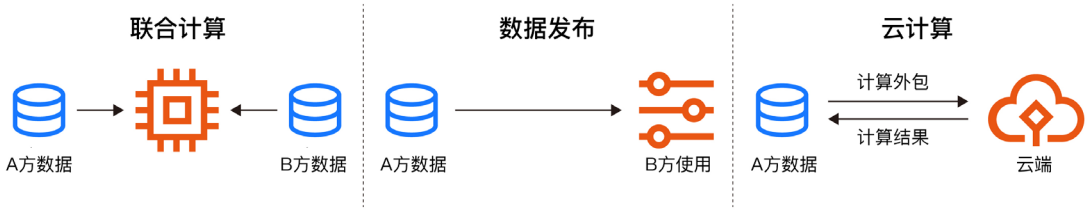
随着各国隐私保护法规的陆续出台、隐私保护意识的觉醒，近年来欧洲、美国、中国、日本、韩国等国家和地区加快了对隐私计算的研发和商用步伐。隐私计算在业内已经应用于金融、科研、医疗等十多个行业，在联合机器学习、联合统计、联合科研、数据发布、外包数据计算、外包数据查询等应用中保护数据隐私。

隐私计算作为一个快速发展的领域，其技术复杂发展快，其技术和应用还不被很多期望采用隐私计算的机构和个人熟知，而隐私计算技术和产品的选型并不是一个简单事情。本文将主要探讨隐私计算场景、技术选型、产品选型等话题，给隐私计算潜在使用者提供隐私计算实践的参考。

2 隐私计算应用和场景

图示1

隐私计算三大场景



资料来源: 蚂蚁集团

隐私计算可用于数据流通的三大类典型应用（联合计算、数据发布、云计算），保护其中的敏感数据。在联合计算中，多方联合基于他们的数据完成指定的计算，如基于多方数据的建模、统计分析。在数据发布中，数据方将其数据提供给一个或多方使用方，使用方可以对数据进行各种分析和计算。在云计算中，数据方将其数据交给云，利用云端丰富的计算和存储资源对其数据进行加工处理。这里，数据和计算都是广义的概念，数据包括数据集、查询条件、机器学习模型参数、计算逻辑等，计算包括机器学习建模推理、统计、查询等。

隐私计算的这三大类应用中，联合计算由于其需求广、隐私保护的难度大，是近年来业内最为关注的。本文将重点介绍联合计算中的隐私计算。

下面以金融、医疗、政务行业场景举例介绍隐私计算应用。

2.1 金融场景

金融是数据要素密集行业，同时也在多方数据协同、释放数据价值的过程中存在诸多痛点。

隐私计算防范多头借贷。互联网金融行业中，多头借贷用户的信贷逾期风险是普通客户的3到4倍，贷款申请者每多申请一家机构，违约的概率就上升20%。如何对贷款申请者的多头借贷风险进行准确评估成为行业风控的重要一环。多个行业机构可以通过隐私计算共同搭建行业安全数据联盟，让参与方通过安全查询获取风险黑名单、多头贷款、多头逾期、多头查询在内的风控数据，也可以支持多方不输出明细数据即可进行联合安全建模、联合风险预测，形成行业内的联防联控方案，大大降低企业经营风险。隐私计算保证了查询方只能获取联盟内的统计数据，而无法获知任一参与方的明细数据，保证各方自有数据的安全。

金融行业联合风控提升风险识别能力。银行个人信贷要提升风险识别能力，既需要充分挖掘自身数据的价值，也需要引入外部数据。在离线建模阶段，银行与数据服务商采用隐私计算联合双方样本进行机器学习训练，银行得到风控模型。在在线推理阶段，银行将模型加密部署，保障模型及查询结果安全。

提升保险理赔效率。随着越来越多的传统医院投入互联网怀抱，移动医疗与保险的结合也展现出广阔的前景。但是，在目前的商业医疗保险理赔过程中，参保人必须带齐所有表单、医疗收据、病历等资料到保险公司提交申请，或者手工拍照后通过保险公司APP将资料上传给理赔平台并发起理赔申请，整个过程效率低、程序繁琐，需要等待多天才能获得理赔。为了提高用户体验，增加用户粘性，提高患者整体的就医支付能力，不少商业保险公司开始搭建"商保快赔通道"，但是在关键的医疗数据使用上，由于院方出于对医疗数据安全的担忧，不愿意直接把敏感的医疗数据开放给商保快赔平台，导致众多"商保快赔通道"在接入医院时难度较大。参与计算的医院和保险公司在各自私域内部署隐私计算节点，进行联合理赔模型和策略训练，验证效果后，将理赔计算逻辑部署在医院域的隐私计算节点上。在患者就诊结束后申请理赔，医院对理赔申请人的原始就医数据进行理赔计算，输出理赔计算结果，最大程度的保护了医疗数据，同时也降低医院接入的难度。

2.2 医疗场景

医疗数据是个人隐私的最后防线，自身具有高价值与隐私性强等特点，隐私保护与充分发挥其巨大的价值是一对始终存在的矛盾。而隐私计算的出现化解了这一矛盾进而在医疗领域前景广阔。

隐私计算支持医疗行业联合科研。通过机器学习对大规模病例数据进行深度挖掘，可提高医疗科研与病情推断的效率，促进整个医疗服务的精确度和效率的提升。但是单个医疗机构的数据样本有限，需要联合多机构的病例数据进行联合建模。而病例数据属于个人隐私范畴，收集个人隐私信息容易面临合规风险。同时医疗健康行业知识产权竞争十分激烈，出于商业利益保护，数据共享会导致数据持有机构失去原有竞争优势。多家医院和医疗科研机构可在本地部署隐私计算节点，将进行联合计算的数据对接到各自私域的隐私计算节点上，通过联合隐私统计等可保障医疗数据不离开私有域的前提下，进行疾病的联合统计分析。此外，还可通过联合机器学习进行病情推断提升医疗服务效率和准确度。

2.3 政务场景

政务场景也是隐私计算的重要场景。通过隐私计算，一是可以打通政府各部门的数据，从而为民众提供更为便捷、智能的服务；二是可以融合各方数据到政务场景中，例如城市大脑的场景，更多的数据为城市的交通、市政设施规划、安全、商业发展等各个方面治理水平的提升提供了强劲的动力；三是可以把政府数据安全地开放给产业，助力产业的发展。

3 隐私计算技术选型推荐

隐私计算并非单一的技术，而是包含多种隐私保护技术，涉及密码学、安全硬件、信息论、分布式计算等多个学科。隐私计算基于其实现隐私保护的原理可分为密码学、可信执行环境、信息混淆脱敏、分布式计算四类路线，其中的主要代表技术有多方安全计算、差分隐私、匿名化、联邦学习等。这些技术在可支持的计算、隐私保护的维度、隐私保护强度、安全性、性能等方面有较大差异，分别适合不同的应用和场景。有时也需要结合使用两种或多种技术来满足应用需求。

- 密码学路线代表技术是多方安全计算MPC(secure Multi-Party Computation)。这一路线是在密态下进行数据的计算、检索等处理，这一过程中输入数据、中间结果处于密态不暴露，只输出最终结果。
- 可信执行环境TEE(Trusted Execution Environment)其方法是通过可信的抗篡改的软硬件构建一个可信的安全环境，数据在该环境中由可信的程序进行处理。
- 信息混淆脱敏路线的主要代表是匿名化和差分隐私。其方法是通过加噪、删除、泛化等信息处理手段对数据处理后再输出。
- 分布式计算路线的代表是联邦学习。大多分布式计算任务原始数据不需要对外输出，只需输出本地基于原始数据计算的中间结果。与把各方数据汇聚在一起再计算的集中式计算方法相比，大为减少了原始信息的泄露，但仍有中间结果信息泄露。

MPC和TEE是用于联合计算的主要技术。他们都可以支持多方数据的各种计算，除了可以保护各方数据隐私，还可以只让指定方获得计算结果或结果的一部分。而且每次计算都需要各方的配合协作，因此各方可以很好控制数据的用途（参与了什么计算任务）、用量（参与了几次计算、哪些字段参与了计算），容易实施数据最小化使用原则，防止数据滥用和非授权使用。

下面总结对比隐私计算各技术路线代表技术，并给出技术选型推荐。技术路线的具体分析请参见附录。

总体而言，多方安全计算、可信执行环境可用于各种类型的联合计算、外包计算，两者在安全强度和性能上各有取舍；联邦学习适用于对结果管控无要求的联合建模；混淆脱敏可用于数据发布，还可辅助多方安全计算、可信执行环境用于联合计算。

技术路线建议。从联合计算的功能丰富性出发，联合计算的隐私计算产品必须采用MPC或TEE技术路线，辅以信息脱敏和混淆技术，增强隐私保护。在某些建模情况下（模型不需要控制，可接受信息泄露），可以采用联邦学习作为补充。如何在MPC和TEE之间选择？MPC和TEE在安全强度和性能方面各有优势。MPC的安全强度更高，但性能比TEE差。为了灵活支持各种场景，理想的PPC产品应该支持MPC和TEE双引擎。允许用户灵活选择引擎，并以相同的方式操作PPC产品。

路线	输入隐私	中间计算隐私	结果隐私	数据用法 用量管控	结果管控	性能	优缺点	适合应用
MPC	Y	Y	N	Y	Y	低到中	优点：高安全、高隐私、高管控 缺点：性能	1. 高安全的联合计算 2. 外包计算（要求多个计算服务商） 3. 用于联邦学习：梯度安全计算，减少信息泄露
TEE	Y	Y	N	Y	Y	高	优点：高隐私、高管控、高性能 缺点：依赖特定硬件和硬件厂商的可信度	1. 中安全、高性能的联合计算 2. 外包计算
混淆脱敏	Y	Y	Y	N	N	高	优点：高性能 缺点：低管控；难平衡隐私保护、数据可用性的矛盾	1. 数据发布 2. 联合计算：配合其他路线使用，减少结果泄露敏感信息
联邦学习	Y	N	N	Y	N	中	优点：易开发实现 缺点：结果管控弱，中间信息泄露（一般需结合其他路线减少信息泄露）	联合计算中的联合建模，且模型可公开给各参与方

4 隐私计算产品选型

随着《数据安全法》、《个人信息保法》陆续出台，很多机构都开始关注隐私计算，希望借助隐私计算解决机构间联合计算中的隐私保护问题。面对市场上参差不齐的隐私计算产品，该如何选择？下文从功能、技术路线、审计、集成交付、性能、安全5个维度给出选型建议。

4.1 功能是否覆盖常见联合计算

联合机器学习：需要关注隐私计算产品是否有特征处理与分析能力、模型算法支持情况、模型效果评估指标。对模型文件有保护诉求机构需关注模型文件是否能加密保护防止被窃取。 以及模型预测针对模型结果以及底层变量稳定性监控，保障模型服务稳定性。

联合统计分析：需关注支持算子是否满足需求，有在线调度需求机构需关注定时调度能力。另外，SQL灵活度非常高，SQL安全校验非常关键，需关注产品是否有安全校验能力。

自定义脚本：针对多样定制化计算需求，需关注隐私计算产品是否支持自定义计算逻辑，编译成安全计算脚本执行。

匹配撞库：需关注支持的数据量以及性能，计算结果对接能力。

匿名查询：需大批量匿名查询性能以及是否具备查询计量功能。

4.2 是否支持审计

在很多应用场景，需要对计算数据、过程、结果进行追踪审计。例如央行21年3月发布的《人工智能算法金融应用评价规范》中要求银行人工智能算法中用到的数据、采用的模型、模型的参数以及计算结果等具备可追溯可审计。另外在个人信息使用场景，使用个人信息必须获得个人授权，机构如何证明数据使用已获得个人权限。诸如此类需要进行多方共识或是监管审计的场景，机构在进行隐私计算选型的时候，需关注是否具备区块链存证审计能力。

4.3 系统集成与交付能力

账号对接：机构内部一般都有自己的账号管理系统，机构内部账号是否能方便的与隐私计算产品对接，并能对账号操作进行审计。一是提升机构内部使用体验，而是对账号进行安全管控。

日志对接：针对机构内部对操作员产品操作和业务日志进行管理、监控和运维需求，隐私计算产品应支持方便的日志对接能力，方便机构根据自身需求搭建日志管理审计平台。

数据对接：在进行数据合作时，机构数据如何方便对接到隐私计算产品，并能对不同级别数据进行不同授权管理。隐私计算产品应支持数据库、文件、API等多种数据接入形式。

交付能力：对机构不同交付诉求，隐私计算产品是否具备多样化交付能力。例如针对有自建隐私计算平台的机构，是否有封装好的隐私计算API。有安全性以及性能有更高要求机构，是否有一体机交付。

4.4 性能

离线计算性能：离线隐私计算功能一般包含联合机器学习、联合统计分析、联合策略、安全匹配等功能，随着隐私计算场景越来越丰富，以及对计算时效要求越来越高，隐私计算产品是否能支持大规模分布式安全计算和硬件加速。

在线计算性能：模型预测、策略服务、匿名查询等隐私计算在线生产应用场景，需关注请求量以及时延，同时关注隐私计算产品在线配套监控预警机制是否完善，确保在线服务稳定。

4.5 隐私保护

只要使用了隐私计算技术，就可以高枕无忧，不担心隐私数据泄露吗？事实并非如此。主要有以下4方面的原因：

- 采用的隐私计算技术的隐私保护能力与需求不匹配。如前文所述，每种隐私计算技术的隐私保护能力各不相同。需要采用合适的技术，有时还需要结合采用多种技术。

- 采用的隐私计算算法的安全强度不足，易被攻破。例如，一些隐私计算算法不能抵抗参与方的合谋攻击，任两个参与方合谋就可获得其他参与方的输入数据。如果参与方合谋的可能性大，需要采用技术手段防范这一攻击，或者换用安全强度更高的算法。

- 权限控制不严。如果管控不严，合作方有可能超范围超期限发起联合计算任务。

- 缺乏对恶意脚本、恶意输入的防范。以通过SQL脚本进行联合统计为例。由于SQL的灵活性，脚本可能输出的是对方的原始数据而非基于双方数据的统计结果。即使以隐私计算的方式执行该SQL，也破坏了数据隐私。

针对上述风险，隐私计算产品应合理选择隐私计算技术和算法，实施严格精细的权限控制，并采用技术手段检测和防范恶意脚本、恶意输入。

5 总结与展望

隐私计算应用的行业和场景广泛，然而其应用也面临巨大的挑战。隐私计算技术复杂，包含多种技术路线和具体算法，他们在功能、性能、隐私保护强度、安全强度上各不相同，需要合理进行技术选型。作为链接数据孤岛的工具，隐私计算产品要服务好应用，只具备隐私保护能力是不够的，还需要具备计算类型丰富、高性能、可审计、易集成、易交付、安全可信等特性。要同时达到这些特性挑战非常巨大，尤其是想同时达到计算类型丰富、高性能、高安全几乎是不可能的。为了提升这些特性，业内除了继续改进和发展隐私计算技术外，也在积极结合多种隐私计算技术，引入区块链、分布式集群加速、一体机软硬件加速等技术。

附录 隐私计算技术路线分析

密码学路线

密码学路线包括多方安全计算MPC、同态加密、可搜索加密等，代表技术是多方安全计算。这一路线是在密态下进行数据的计算、检索等处理，这一过程中输入数据、中间结果处于密态不暴露，只输出最终结果。其中，MPC采用诸如秘密分享、混淆电路、同态加密等密码学技术将多方的明文数据转换到密态下进行计算，最后将密态结果转换回明文结果。

MPC可以支持多方数据的各种计算，除了可以保护各方数据隐私，还可以只让指定方获得计算结果或结果的一部分。而且采用MPC的每次计算都需要各方的配合协作，因此各方可以很好控制数据的用途（参与了什么计算任务）、用量（参与了几次计算、哪些字段参与了计算），容易实施数据最小化使用原则，防止数据滥用和非授权使用。MPC还有个可选特性，可以验证计算的正确性。

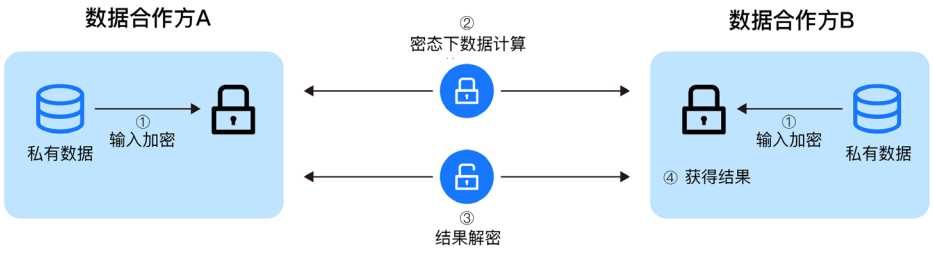
密码学路线中的同态加密技术除了可以用于构建MPC、实现多方联合计算的隐私保护，还可以用于安全外包计算，让云端无法看到外包的敏感私有数据。同态加密缺点在于性能较差，对复杂逻辑的计算还不实用。另一方面，MPC也能用于安全外包计算，但要求有多个计算服务商（例如云提供商）：数据方将其数据采用秘密分享技术将拆分后发给多个计算服务商，计算服务商之间采用MPC技术进行联合计算。

可信执行环境路线

可信执行环境TEE其方法是通过可信的抗篡改的软硬件构建一个可信的安全环境，数据在该环境中由可信的程序进行处理。该环境具备一定抵抗外界窃取数据、篡改数据、篡改程序的能力。目前较为成熟的可信执行环境方案有SGX、Trustzone、HyperEnclave等。

图示2

多方安全计算路线的隐私计算



资料来源：蚂蚁集团

与MPC一样，TEE同样支持任意计算逻辑，可实现数据隐私保护、结果输出可控、计算正确性校验。两者的差异源于实现机制的不同，TEE依赖于特定软硬件的安全性，MPC依赖于密码算法的安全性。前者的安全性相对弱些，需要在有TEE硬件环境才能使用，但由于是在安全环境下进行明文计算，其性能远高于MPC的密态下运算。

信息混淆脱敏路线

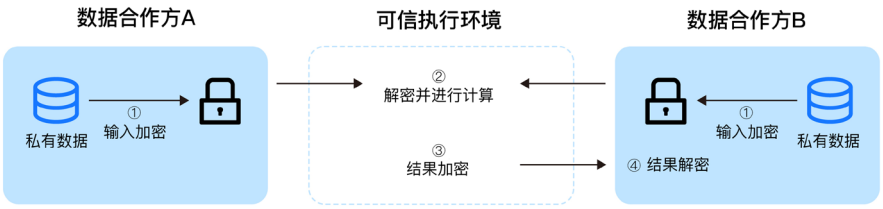
信息混淆脱敏路线的主要代表是匿名化和差分隐私。其方法是通过加噪、删除、泛化等信息处理手段对数据处理后再输出。其中，匿名化是对数据中的标识信息、准标识信息进行处理后再输出，防止从输出的数据关联到具体个人。而差分隐私一般用于多人数据的计算中，通过在计算结果中引入噪声，防止从结果中推出具体个人的信息。引入噪声的方式可以是在结果中直接加噪，也可以是在计算的输入或中间结果中加噪。

信息混淆脱敏适合于数据发布的场景。例如，医学主管单位将采集的个人数据/疫情数据匿名化和脱敏后公开发布，供广大医疗机构研究，供各机构和民众做好防疫工作。在这样的场景下，数据的合理用途非常广、用量非常大，MPC或TEE使用成本高、权限管控太严，限制了数据的流通和利用。而信息混淆脱敏路线具备低成本、高性能、实现简易的优势。缺点是难平衡隐私保护和数据可用性的矛盾：混淆脱敏去除了部分信息（或降低了部分信息精度），而某些计算和分析可能需要使用这些信息（或需要使用高精度的信息）。在这种情况下，就还需要采用MPC或TEE。

信息混淆脱敏另一大用途是结合其他隐私技术路线（如，MPC、TEE）使用，减少从结果中得到敏感信息。MPC、TEE可以保护输入数据、中间计算结果不泄露。但是如果最终计算结果包含敏感信息，则还需要采用信息混淆脱敏处理后再输出最终结果。

图示3

可信执行环境路线的隐私计算



资料来源：蚂蚁集团

图示4

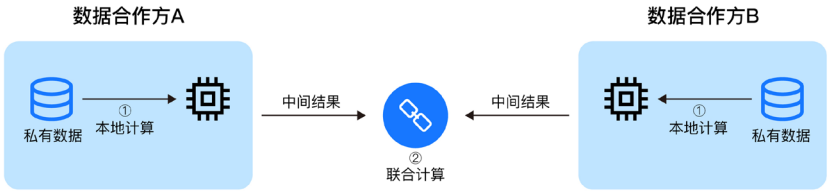
混淆脱敏路线的隐私计算

资料来源：蚂蚁集团

分布式计算路线

图示5

分布式计算路线的隐私计算



资料来源: 蚂蚁集团

分布式计算路线的代表是联邦学习。大多分布式计算任务原始数据不需要对外输出，只需输出本地基于原始数据计算的中间结果。与把各方数据汇聚在一起再计算的集中式计算方法相比，大为减少了原始信息的泄露。但与MPC、TEE方式相比隐私保护弱，额外泄露了中间结果信息。

联邦学习沿用了传统分布式机器学习的参数服务器-工作服务器架构。这一架构中，一个中心服务器作为参数服务器协调多个数据方的服务器(作为工作服务器)进行联合机器学习训练，各工作服务器基于本地数据计算出的梯度信息交给参数服务器进行汇聚，参数服务器将最新迭代的模型参数下方给各工作服务器。这一架构缺乏对计算结果的管控，即任一参与方都能得到模型参数。

联邦学习另一个弱点是计算中间信息（梯度）的泄露，多项研究表明该泄露有暴露原始数据敏感信息的风险。为了减少梯度信息泄露，联邦学习一般采用MPC或者差分隐私技术进行各方梯度的汇聚。相对于整个建模过程都在密态下计算的纯MPC路线，联邦学习只在梯度计算中引入MPC密态运算，在研发实现上更为容易。

资料来源: 蚂蚁集团

Gartner的研究

2021年最主要的战略技术趋势：隐私增强计算

隐私增强计算能够实现数据变现和隐私保护场景，这是以前的方法无法做到的。IT领导者需要理解PEC如何支持其机密性和隐私用例。

概述

机会

- 隐私增强计算（PEC）对使用中的数据进行保护。针对在处理和分析中必须对数据保密的用例，以及即使数据本身不具有机密性，算法仍必须保密的用例，PEC能够提供支持。它能够实现数据变现和隐私保护场景，这是以前的方法无法做到的。

- PEC是许多技术的总称，每项技术都有不同的安全和隐私保证。它们可以单独使用，也可以组合使用以提高效力。具体选择哪项技术，取决于用例和执行要求。

- 各项技术业已成熟，相应的商业实现已经上市。计算机处理器和超大规模云提供商已有可用的可信执行环境。越来越多供应商提供安全多方计算和同态加密产品。

建议

负责技术、信息和恢复力风险的IT领导者应：

- 通过评估需要将高度敏感的个人数据用于数据变现、欺诈分析和商业智能用例的数据处理活动，确定PEC的候选对象。

- 将在数据处理和分析过程中需要保证数据和/或算法安全的更普遍用例的PEC机会纳入考虑。

- 评估差分隐私、同态加密、安全多方计算、可信执行环境和其他方法对这些用例的有效性和实施需求的差异，以确保它们适用于用例及必需的安全和隐私保证。

战略规划设想

到2025年，50%的大型组织将采用隐私增强计算来处理不可信环境和多方数据分析用例中的数据。

分析

企业需要了解什么

此项研究是Gartner2021年最主要的战略技术趋势的一部分。

隐私增强计算执行指南（下载）。

数据共享需求的增加，从数据中释放价值的前所未有的渴望和机会，以及国际数据驻留限制，都是保护使用中的数据的强大驱动力。随着不同国家/地区（包括欧盟[1]、英国和美国[2]）的法律发展，如果没有额外的隐私保护机制，可识别数据就无法跨境共享或转移。

此外，许多数据分析和商业智能用例服务于次要目的（即获取个人数据的主要目的以外的目的），这往往导致需要匿名处理数据。商业秘密或出口限制信息等其他机密数据，在机密性方面具有相似的要求，即使更广义的隐私要求不适用。PEC技术能为使用中的数据提供隐私和机密性保护，从而为扩大业务活动提供保障，并促进数据的分析和国际传输。它还能减少现有合规和其他隐私风险，而此类风险目前可能妨碍对（公有）云的采用。

PEC技术（参见图1）不提供加强隐私保护和确保数据机密性的单一方法。相反，它是各种不同技术的统称，这些技术能单独应用，也能与其他技术组合使用，这取决于当前的用例。许多PEC技术已列入2020年隐私技术成熟度曲线；这些技术尚未孤立地超越期望膨胀期的顶峰，但它们组合起来就能构成未来几年的一致趋势。

描述

PEC包含三种类型的技术，这些技术可用于确保数据处理和数据分析的安全性，从而保护数据：

第一种技术提供了一个可处理或分析敏感数据的可信环境。它包括可信第三方和硬件可信执行环境（也称为机密计算）。

第二种技术以分散方式执行处理和分析。它包括联合机器学习和隐私感知机器学习。

第三种方式在处理或分析之前转换数据和算法。它包括差分隐私、同态加密、安全多方计算、零知识证明、私有集合交集和私有信息检索。

每种技术都提供了特定的保密性和隐私保障，有些技术还可以结合起来以获得更大的功效。

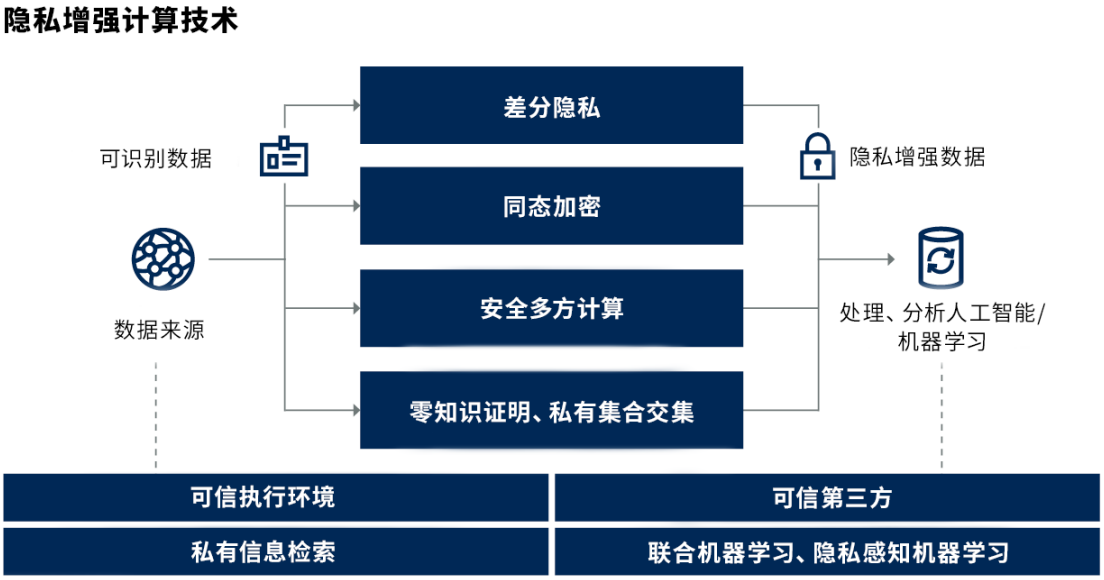
成为趋势的原因

全球数据保护立法日趋成熟，随着个人数据不可阻挡的普及，每个处理个人数据的组织都面临着越来越高的隐私和不合规风险。与此同时，各组织现在都已意识到其数据存储库的潜在经济效益。

在不可信环境中处理数据以及执行多方数据共享和分析的需求正在迅速增长。分析引擎和架构的复杂性日益增加，这就要求提供符合设计的隐私保护功能，而不是一种固定的方法。与常见的静态数据安全控制不同，隐私增强计算可以保护使用中的数据，从而实现前面所述的用例，同时保持机密性或隐私性。因此，组织可以实施以前由于隐私或安全顾虑而无法实施的数据处理和分析。

图示1

隐私增强计算技术



资料来源：Gartner
740641_C

Gartner

影响

超大规模云提供商已经开始提供可信的执行环境。组织可以利用它们在云环境中提供增强的安全性和隐私性。其他技术，例如同态加密、安全多方计算和私人信息检索，已经从学术研究项目转向商业解决方案。这些采用还处于早期阶段，但在欺诈分析、情报业务、金融和医疗保健领域都有实施。这些实现形式遵循以下两种用例模式之一：

第三方组织分析一个或多个组织的数据，而这些组织不提供对其数据的完全访问权限。

多个组织将其数据汇集在一起进行联合分析，而无需访问彼此的底层数据。

行动

通过评估需要将高度敏感的个人数据用于数据变现、欺诈分析和商业智能使用案例的数据处理活动，确定隐私增强计算的候选对象。

评估差分隐私、同态加密、安全多方计算、可信执行环境和其他方法对这些用例的有效性和实施需求的差异。

关于Gartner 2021年最主要的战略技术趋势

此趋势是我们的2021年最主要的战略技术趋势之一。趋势和技术并不孤立存在；它们彼此加强，以实现以人为本、位置灵活和韧性交付（参见图2）。您应了解这些趋势中的每种趋势，以确定它们对您组织的适用性。

图示2

2021年最主要的战略技术趋势：隐私增强计算

资料来源：Gartner
740641_C

Gartner

依据

[1] 关于案例C-311/18——"数据保护专员诉Facebook Ireland Ltd.和Maximillian Schrems, EDPB"中欧盟法院判决的常见问题。

[2] 除现行《澄清境外合法使用数据法案》(CLOUD Act) 外，新的法律可能继续破坏公平竞争的环境或影响评估和可行技术替代方案。示例包括《消除滥用和严重忽视互动技术法案》(EARN IT Act) 和2020年《合法访问加密数据法案》(LAED 2020 Act)。

资料来源：Gartner研究笔记G00740641，
Ramon Krikken，Bart Willemsen，2021年1月12日1