



金融服务业新一代数据共享：
运用五大技术加强隐私保护、解锁全新价值

引言

在金融服务行业中的数据共享是存在矛盾的。一方面，数据共享有助于打击交易欺诈，帮助金融机构为客户提供更加个性化的建议并检测系统性风险；另一方面，客户对于各机构如何存储和使用其数据亦变得愈发谨慎。目前，欧盟《通用数据保护条例》（General Data Protection Regulation）、英国推行开放式银行等相关改革举措均表明监管机构亦持相同态度。

数据共享能够为金融服务业带来巨大价值，但保护隐私和机密性更是每个金融机构的重要职责。

自2015年以来，德勤一直与世界经济论坛合作，致力于探究金融服务业中的变革力量。世界经济论坛另一份《*Navigating uncharted waters: A roadmap to responsible innovation with AI in financial service*》报告中探讨了隐私和数据共享间权责义务的竞争关系。这促使我们进一步审视新技术，探索新方法，以期助力金融机构在不影响隐私和机密保护的前提下，发掘数据共享价值。

隐私增强技术

本报告探讨了五项关键“隐私增强技术”：



本报告概述了各类技术的工作原理、可解决的数据共享问题类型以及适用的金融服务子行业。



差分隐私

人们普遍认为对个人身份信息进行匿名化处理足以保护客户隐私，然而事实并非如此。

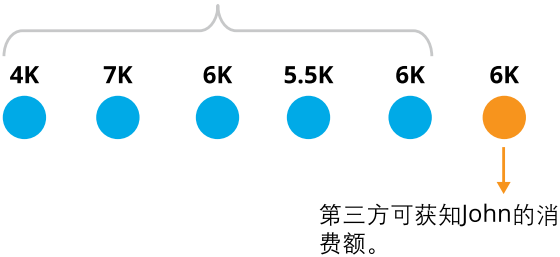
为什么这么说呢？我们假设John在某个人理财咨询应用程序上共享了自己银行账户信息。该应用可帮助客户更轻松的管理其支出，并可与同类客户进行比较。John在该应用上将自己每年在酒吧的支出与所在地区同年龄段人群的平均值进行比较，得到如下结果：“在该邮政编码对应的地区，25-29岁男性通常每年在酒吧消费5,750美元。”

但假如有恶意用户想知道John在酒吧的花费，该人可通过诸如将自己的地址信息改为与John所在地区相应年龄段人群的统计信息相匹配。更改地址后再次查询系统，在知道一部分输入数据的情况下（即恶意用户掌握的信息），与其他数据（如人口普查数据）进行交叉对比，他就可以推断出John在酒吧的支出，从而侵犯到John的隐私。

为防止这种侵犯隐私的行为，系统可使用差分隐私来计算为达预期的隐私保护级别所需的噪声量，然后在平均值计算中加入噪声（随机数）。例如，可以用一个随机数代替某客户的消费额，从而改变平均值，使恶意用户无法通过逆向工程分析得到输入数据，同时又可为诚实的用户提供有用的统计数据。

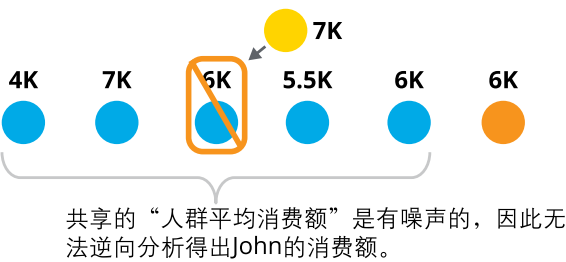
不使用差分隐私：

第三方知道一些人的消费额以及相应人群的平均消费额



使用差分隐私：

将其中一个输入数据删除并采用一个随机数代替



差分隐私应用前景巨大，尤其适用于零售银行、保险公司、支付服务提供商等持敏感个人信息的机构，能使机构在不侵犯客户隐私的情况下，整合并分析敏感信息。

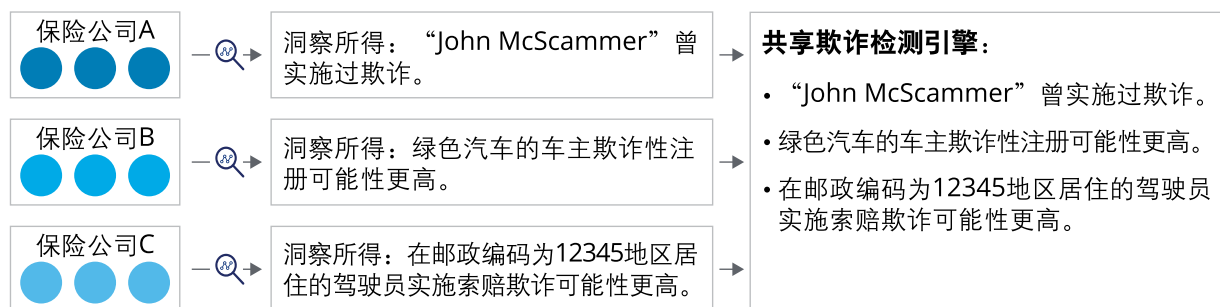


联合分析

有时，决策所需的数据分散在多个数据源中（例如，反欺诈监测数据分布在多家银行）。对此，将分散在各银行的数据归集到一个大型数据库中进行分析可能会更加轻松高效，但如果机构的内部数据是受不同司法管辖区约束而分布式存储的，则有关隐私保护规定可能会限制数据跨区域传输。再如，数据在各机构间共享，客户可能会反对其个人信息向第三方披露，同时，机构对第三方如何处理这些数据也有所顾虑，尤其，当发现这些数据被第三方向竞争对手披露。

解决这些问题的一种方法是分别分析每个数据集，并构建各自独立的模型，再将这些决策模型整合到一个汇总系统中，这种技术称为联合分析。例如，一些保险公司希望跨机构合作进行反欺诈检测，各保险机构可独立分析数据，然后共享所得洞察。如此，既可从彼此的分析研究中受益，其客户隐私也不会收到威胁。

使用差分隐私：



这项技术已嵌入许多企业的分析系统中。例如，大型技术公司使用联合分析（以及其他隐私增强技术）改进其智能手机操作系统键盘输入的“单词联想”功能。

金融机构可采用联合分析来打破关键壁垒、从多个私有数据集中获取洞察。例如，联合分析可以令保险公司鼓励客户更多使用互联网设备（如汽车追踪器和健康监测器）提升客户的负责任行为，而不必担心个人信息泄露。同时，保险公司仍可从客户的数据中获取汇总洞察。在支付和保险等行业，联合分析也可用于提高安全性，例如用于建立通用反欺诈检测网络，各参与机构均不用担心内部数据被对手获取。



同态加密

有时，金融机构（或其客户）希望聘请第三方进行数据分析。第三方可能拥有该机构没有的辅助性数据或专有分析技术。但是，第三方作为数据所有者或管理者可能因基于权限不足或者担心数据安全问题，而无法共享这些数据和技术。

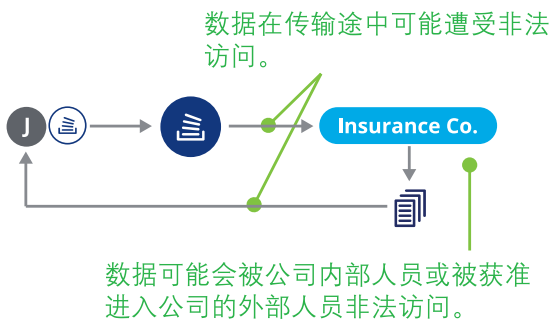
同态加密可通过对数据进行加密来弥合这种差距，从而在不获知基础信息的情况下对数据进行分析。使用同态加密无需先解密数据。除原定接收方外，任何人都无法读取分析结果。

假设John Doe想要分析自己的病历以确定是否存在任何潜在的健康风险。其健康保险提供商的技术服务部门能够进行这种分析，但是John Doe希望自身的健康记录不被泄露。

借助同态加密，John Doe对数据进行加密并将其发送给保险公司，自己掌握解密密钥。保险公司技术部可通过模型直接对加密数据进行分析，而不必了解健康记录或结果的内容，然后再将两者返回给John Doe进行解密和读取。

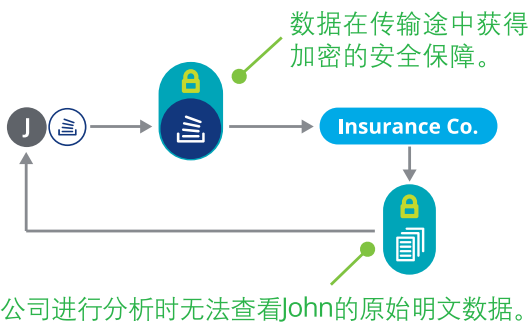
不使用同态加密：

John将自己的健康记录放入一个盒子，寄给分析公司，公司对记录进行分析，生成报告，并将报告寄回给John。



使用同态加密：

John在共享健康记录之前对其进行同态加密，使除他以外的任何人均难以查看数据或分析结果。



对于希望在云端或借助第三方分析敏感信息的金融机构而言，同态加密应用潜力巨大。如今，对于数据泄露、本地化要求和隐私监管的担忧使企业在选择数据分析方法上受限。但同态加密或能改变这一状况。通过采用同态加密，企业在使用数据时可切实确保数据加密与安全，防止数据泄露。

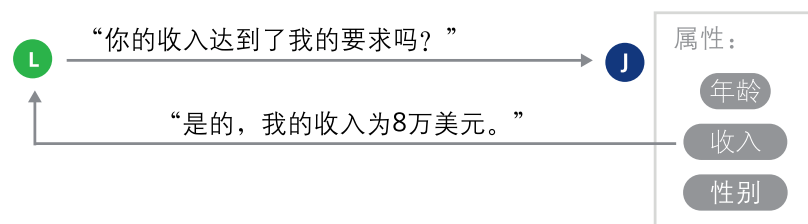


零知识证明

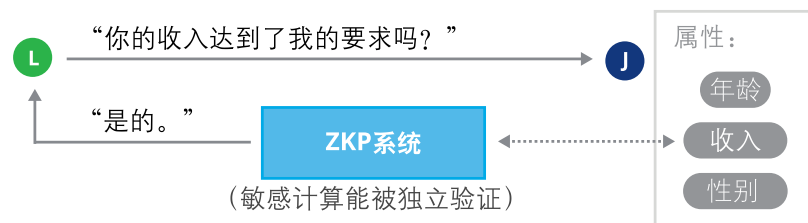
许多客户不愿透露除完成交易所必需内容以外的任何信息，以防这些信息被用于损害自身权益。例如，John须向房东证明自己有能力租用公寓，但为避免房东伺机提高租金，John不希望房东知道他的实际收入比房租最低要求高很多。

John的银行可使用零知识证明技术来为其提供帮助。通过使用零知识证明，银行采用数学方法向房东证实John的收入足以支付租金，同时不透露其实际收入。整个流程为自动化流程，John可以很快证明自己的租房资格，而无需银行人员介入。

不使用零知识证明：



使用零知识证明：



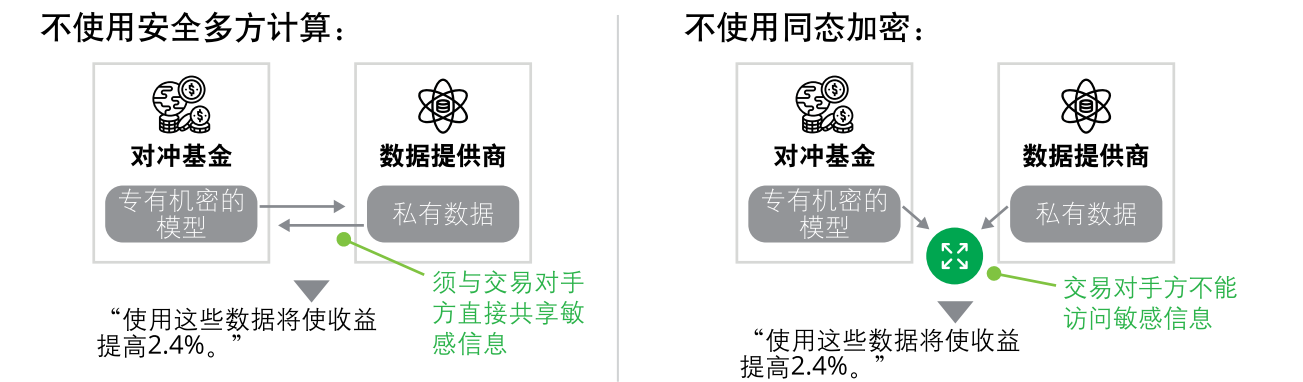
各种规模的机构正越来越多地将零知识证明技术应用于支付、基础设施、自主数字身份解决方案等方面。这种应用正广泛地推动机构向“零知识证明体系”转变。在此体系下，机构将其数据系统设定为仅能满足任务所需的最少信息，以保障其他数据的私密性。



安全多方计算

安全多方计算允许多家机构共同分析数据，同时确保任何一家机构都无法访问完整的数据集，从而降低数据泄露的风险。

假设：一家对冲基金试图从第三方数据提供商处购买数据，以提高其交易模型的质量。该基金希望在购买之前确知这些数据是有用的，但第三方数据提供商在收到付款之前又不愿共享其数据。传统方法是，第三方数据提供商向该对冲基金披露一组历史数据集（可能无法反映当前效用）或一组小样本数据（可能难以整合到对冲基金的模型中，从而无法准确反映数据的价值）。



采用安全多方计算技术可结合双方的敏感信息（对冲基金的模型和提供商的数据）来计算数据的价值，但同时任何一方都无法访问另一方的机密信息。通过这种方式，对冲基金可在了解更多信息后作出是否购买数据的决定，过程中双方的相互信任并非必要条件。各方还可独立审核安全多方计算系统，以保护其输入数据的隐私性。

简而言之，安全多方计算技术适用于：针对一个共同的问题，多个机构各自拥有一部分答案，但均不希望其他机构访问自身所持数据。安全多方计算技术在资本市场的运用相当典型，因为交易和投资各方为获取所需信息往往会涉及大量专有、敏感的数据。与联合分析一样，安全多方计算技术还有助于促进跨机构合作反欺诈检测网络的开发。

让隐私保护 更进一步

长期以来，金融机构一直在数据共享价值和
维护隐私与机密性之间做权衡。如今，这五
种新兴技术或能从根本上改变这一状况。

这些技术的共同点是能够使金融机构、客户和监管机构在不必共享底层数据的情况下，分析数据并共享相应洞察。大大降低数据共享风险，助力金融机构构建数据安全新方法，以客户、监管机构和社会各界都能够接受的方式解决其最大、最紧迫的问题。

本文为世界经济论坛与德勤合作编写的《**金融服务业新一代数据共享：利用隐私增强技术解锁全新价值**》报告概要。世界经济论坛将持续探索变革力量对金融服务行业的影响。欢迎您阅读报告全文，若您希望对报告进行更多更深入的探讨和交流，欢迎您随时与我们联系。



全球联系人

Bob Contri

金融服务业领导人

德勤全球

bcontri@deloitte.com

Rob Galaski

银行业及资本市场全球领导人

德勤管理咨询

rgalaski@deloitte.ca

作者

Ishani Majumdar

Omnia AI高级顾问

德勤加拿大

ismajumdar@deloitte.ca

Hemanth Soni

德勤摩立特高级顾问

德勤加拿大

hemasoni@deloitte.ca

还要感谢德勤加拿大Courtney Kidd Chubb和Denizhan Uykur为本报告提供的大力支持。

中国联系人

方烨

德勤中国金融服务业
风险咨询领导合伙人（中国大陆）
+86 21 6141 1569
yefang@deloitte.com.cn

薛梓源

德勤中国
网络安全及科技风险服务领导合伙人
+86 10 8520 7315
tonxue@deloitte.com.cn

郭仪雅

德勤中国
网络安全及科技风险服务，
金融服务业联合领导合伙人
+852 2852 6304
evakwok@deloitte.com.hk

何微

德勤中国
网络安全及科技风险服务合伙人
+86 755 3353 8697
vhe@deloitte.com.cn

Tony Wood

德勤中国金融服务业
风险咨询领导合伙人（中国香港）
+852 2852 6602
tonywood@deloitte.com.hk

何晓明

德勤中国
网络安全及科技风险服务，
金融服务业联合领导合伙人
+86 10 8512 5312
the@deloitte.com.cn

肖腾飞

德勤中国
网络安全及科技风险服务，
数据安全和隐私领导合伙人
+86 10 8512 5858
frankxiao@deloitte.com.cn

江玮

德勤中国
网络安全及科技风险服务合伙人
+86 21 2312 7088
davidjiang@deloitte.com.cn

关于德勤

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体。德勤有限公司并不向客户提供服务。请参阅www.deloitte.com/cn/about了解更多信息。

德勤亚太有限公司（即一家担保有限公司）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100座城市提供专业服务，包括奥克兰、曼谷、北京、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、大阪、上海、新加坡、悉尼、台北和东京。

德勤于1917年在上海设立办事处，德勤品牌由此进入中国。如今，德勤中国为中国本地和在华的跨国及高增长企业客户提供全面的审计及鉴证、管理咨询、财务咨询、风险咨询和税务服务。德勤中国持续致力为中国会计准则、税务制度及专业人才培养作出重要贡献。德勤中国是一家本土注册成立的中国专业服务机构，由德勤中国的合伙人所拥有。敬请访问www2.deloitte.com/cn/zh/social-media，通过我们的社交媒体平台，了解德勤在中国市场成就不凡的更多信息。

本通信中所含内容乃一般性信息，任何德勤有限公司、其成员所或它们的关联机构（统称为“德勤网络”）并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。任何德勤网络内的机构均不对任何方因使用本通信而导致的任何损失承担责任。

©2019。欲了解更多信息，请联系德勤中国。
Designed by CoRe Creative Services. RITM0374219



这是环保纸印刷品