Deloitte.
Insights

人工智能隐私保护：同态加密和联邦学习有助于提升人工智能的隐私性和安全性

这两种现有的新兴技术可有效保护人工智能应用中所使用的数据，但目前的挑战在于如何增强其实际可行性

同态加密和联邦学习是两种不同但相关的技术，其目的均在于解决同一个问题：如何在执行机器学习等人工智能任务的过程中更好地确保隐私性和安全性？据德勤全球预测，由于这一问题的解决变得日益迫切，同态加密和联邦学习市场将在2022年实现两位数的增长，达到2.5亿美元以上。到2025年，该市场的规模有望超过5亿美元。[1]

数据越安全，人工智能的应用越广泛

同态加密和联邦学习均属隐私增强技术，[2]是提高人工智能隐私性和安全性的工具。基于同态加密技术，机器学习可使用加密状态下的数据；而其他情况下的机器学习则需要首先解密数据，增加了遭受攻击的风险。联邦学习将机器学习分配到本地或边缘设备，而非将所有数据保存在同一个地方，从而避免因某一次黑客攻击就泄露全部数据的情况，

这种情况在集中式机器学习中比较常见。同态加密和联邦学习并不相互排斥，两种技术可同时使用。

市场对提升人工智能应用隐私性和安全性的需求急速上涨，成为同态加密/联邦学习市场增长的主要驱动力。众所周知，人工智能是许多行业的关键技术，目前有多家企业对人工智能的隐私性和安全性给予了前所未有的关注。使用人工智能的企业将同态加密和联邦学习视为降低未来风险的方式。这对于使用人工智能的云计算企业来说尤其如此，因为它们需要面对数据的云端迁移和场外处理，而这两者都会带来潜在的隐私和安全问题。监管机构针对人工智能实施了新的监管方式[3]，同态加密和联邦学习或有助于企业更好地遵从这些监管规定。规模庞大的市场，尤其是医疗保健和公共安全市场，对人工智能的隐私性和安全性影响高度敏感，已开始探索研究同态加密和联邦学习，以解决相关问题。

监管机构针对人工智能实施了新的监管方式，同态加密和联邦学习或有助于企业更好地遵从这些监管规定。

同态加密和联邦学习都是相对较新的技术，比传统的人工智能解决方案更为复杂。两种技术虽然具有良好效能，但也存在一定缺点。使用同态加密进行计算比使用未加密数据计算要慢；联邦学习需要边缘设备配备更强大的处理器，同时也要求数据中心的核心硬件（用于安装主要的人工智能软件）和边缘设备（用于学习技术应用）之间能够建立快速且高度可靠的网络连接。（这里的“边缘设备”可以是智能手机或工厂里面距离机器人几百米的设备。）

然而相比前几年，如今使用这两种技术已变得更为容易。首先，随着Wi-Fi 6和5G无线技术速度和可靠性的提高，其应用也越来越广泛，这提高了依靠边缘设备的可行性。部分供应商发布了开源工具，非专业人员因此能够更加容易接触到技术的运作过程，从而降低了同态加密和联邦学习的使用难度。[4]但处理器成本/性能的改进才是可行性提高的真正原因。同态加密过去的计算速度比未加密计算慢万亿倍，但如今由于应用了新的专用处理器，部分情况下同态加密的计算速度仅比未加密计算慢20%。[5]与之类似，为联邦学习提供驱动的边缘处理器正变得功能更强、价格更低、应用更广泛。目前的全同态加密属处理器密集型，同态加密优化处理器的显著发展可大幅缩减时间和成本。[6]

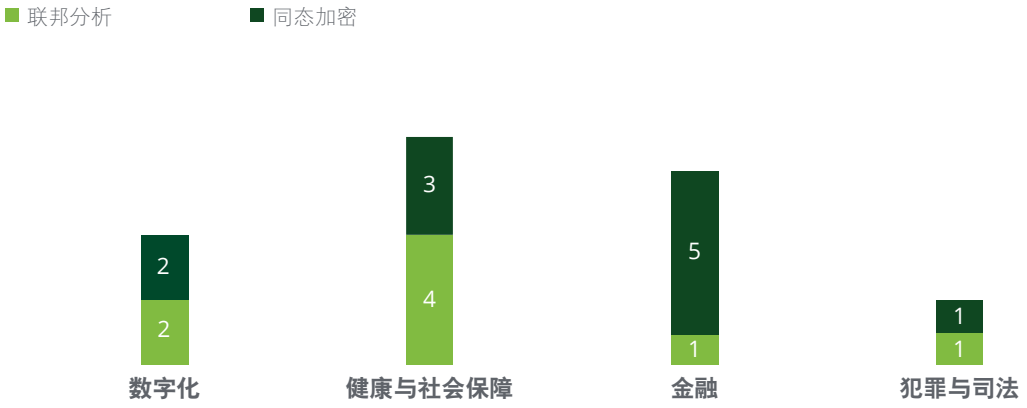
我们通常不会对同态加密和联邦学习这类市场价值较低的技术展开预测。我们打破惯例，部分原因在于这两种技术正处于关键转折点。全球监管机构纷纷开始针对人工智能制定规则；与此同时，虽然《通用数据保护条例》早在2016年就已发布，但这并非隐私监管的最终定音：每月都会有隐私相关的新规出台，且《通用数据保护条例》的执行也可能会提高到新水平。受这些监管规定的影响，供应商和用户可能会意识到，人工智能的使用将变得越发困难，这一情况将蔓延至更多的司法辖区和行业。而同态加密和联邦学习则可以帮助企业满足这些监管要求，极大地便利它们使用人工智能。

同态加密和联邦学习目前的用户是我们讨论这两种技术的另一个重要原因。从最近某隐私增强技术知识库的数据来看，目前公开发布的同态加密和联邦学习试点、产品和概念验证共计19项。这看起来似乎并不多，但开展这些项目的组织机构包括苹果、谷歌、微软、英伟达、IBM和英国国民医疗服务体系；用户和投资者包括美国国防部高级研究计划局、英特尔、甲骨文、万事达卡和加拿大丰业银行。参与这些早期项目的也是规模最大的行业领域。健康与社会保障以及金融行业在同态加密和联邦学习的使用方面处于领先地位。此外，这两种技术在数字化以及犯罪与司法领域的使用也较为突出（图1）。[7]

图1

同态加密和联邦学习正在吸引部分全球最大的企业及行业领域

不同行业领域公开发布的同态加密和联邦分析试点、产品和概念验证数量



资料来源：德勤对数据伦理和创新中心2021年《使用案例知识库》（Centre for Data Ethics and Innovation, Repository of use cases, 2021）[8]的分析

小结

随着部分全球最大的企业对同态加密和联邦学习的采用，对敏感数据的隐私性和安全性感兴趣的组织应持续关注这两种技术以及其他隐私增强技术的动态，虽然到2022年，对其中大部分组织机构而言，同态加密和联邦学习技术可能依然没有实用价值。最感兴趣的组织机构或团体可能包括：

- 云服务提供商和云服务用户 [9]
- 医疗保健、金融和公共部门等特别敏感的行业的组织，特别是犯罪和司法机构
- 希望与竞争对手分享和比较数据，但不会泄露最重要的知识产权的企业
- 首席信息安全官及其团队

与量子计算等其他新兴技术（见《2022 科技、传媒和电信行业预测》报告相关部分）一样，致力于探索同态加密和联邦学习的组织机构可采取以下举措，以有效制定未来规划：

了解对行业的冲击。同态加密和联邦学习等隐私增强技术可能为企业所在及邻近行业带来何种冲击？从战略、运营和竞争角度来看，人工智能的隐私性和安全性提高对企业有何意义？要理解这一点，领导者必须紧跟技术进步的步伐，并密切关注同行、竞争对手和生态系统合作伙伴如何开展相关的投资与实验。

制定战略。企业应当召集具备丰富的相关知识的专业人才，共同制定隐私增强技术战略。这一战略的现阶段策略可能是按兵不动，但领导者却可通过识别未来预示需要开始或加大投资与探索的触发事件（如竞争格局变化或技术发展），为应对未来挑战做好准备。企业应当指派兼具技能、知识和组织地位的人才在时机来临之时扛起战略执行的大旗。

关注技术和行业发展。同态加密和联邦分析战略应该随技术和市场态势的变化而演变。领导者应该根据这些变化相应调整企业战略，避免未能及时采取行动而与触发事件擦肩而过。

提前引入网络。网络安全通常在部署阶段才会被纳入人工智能流程。但企业可能希望在使用同态加密和联邦学习阶段就提前引入网络。这种人工智能与网络之间协作性更强的方法或有助于增强隐私性和安全性，同时将透明度和问责风险降至最低。

包括同态加密和联邦学习在内的隐私和安全技术都只是工具，而并非灵丹妙药。虽然没有什么工具是完美的，但同态加密和联邦学习能够在保护隐私和安全方面起到重要的助益作用。它们能够通过保护人工智能核心数据，扩大人工智能的用途，进而为个人、企业和社会带来积极影响。

尾注

1. Globe Newswire, “Federated learning solutions market research report by application, by vertical—Global forecast to 2025—Cumulative impact of COVID-19,” press release, May 14, 2021; MarketWatch, “Homomorphic encryption market size forecast 2021–2027,” August 2, 2021.
2. Holger Roth, Michael Zephyr, and Ahmed Harouni, “Federated learning with homomorphic encryption,” NVIDIA Developer blog, June 21, 2021.
3. 参见人工智能监管预测部分。
4. Sergio De Simone, “Google open-sources fully homomorphic encryption transpiler,” InfoQ, June 29, 2021; Flavio Bergamaschi, “IBM releases fully homomorphic encryption toolkit for MacOS and iOS; Linux and Android coming soon,” IBM Research Europe, June 4, 2020; Dennis Fisher, “Microsoft open sources SEAL homomorphic encryption library,” Decipher, December 3, 2018.
5. Roth, Zephyr, and Harouni, “Federated learning with homomorphic encryption.”
6. Scientific Computing World, “Optical accelerator enables fully Homomorphic Encryption”, August 25, 2021.
7. Centre for Data Ethics and Innovation, “PETS adoption guide: Repository of Use Cases”, accessed on October 6, 2021.
8. Ibid.
9. TechTarget, “Homomorphic encryption,” accessed October 6, 2021.

关于作者

Duncan Stewart | Canada | dunstewart@deloitte.ca

Duncan Stewart is the director of research for the Technology, Media & Telecommunications (TMT) industry for Deloitte Canada. He presents regularly at conferences and to companies on marketing, technology, consumer trends, and the longer-term TMT outlook.

Ariane Bucaille | France | abucaille@deloitte.fr

Ariane Bucaille is Deloitte's global Technology, Media & Telecommunications industry (TMT) industry and also leads the TMT practice and the TMT Audit practice in France. She has more than 20 years of experience and is a chartered and certified public accountant.

Gillian Crossan | United States | gicrossan@deloitte.com

Gillian Crossan is a principal in Risk & Financial Advisory, Deloitte & Touche LLP, and leads the global technology industry sector. She has been with Deloitte for more than 25 years and has worked across sectors including energy, health care, consumer products, and technology.

致谢

The authors would like to thank **Lukas Kruger** for his contributions to this chapter.

关于德勤科技、传媒和电信行业中心

德勤科技、传媒和电信行业 (TMT) 中心专注于研究并发表洞察，以帮助企业领导者清晰了解其业务选择。在新技术和新趋势背景下，本中心的研究将协助企业高管简化复杂的业务问题，并提出明智策略，提升企业长久竞争优势并赢得商业胜利。本中心将作为值得信赖的顾问，帮助高管更好地识别风险，获悉商业回报，赢取关键机遇，从而在快速变化的TMT环境中解决棘手挑战。

联系我们

了解有关科技、传媒和电信行业中心的更多信息并获取最新研究和洞察报告，请访问 www.deloitte.com/us/tmtcenter。

订阅

如您想接收TMT行业电子邮件，请访问https://my.deloitte.com/subscriptions.html，选择您感兴趣的领域进行订阅。

关注我们

敬请关注 @DeloitteTMT.

德勤科技、传媒和电信行业汇聚了全球最顶级的行业专家，组成全球最大的专业团队之一，协助各类形态和规模的企业在数字化时代蓬勃发展，成就辉煌。德勤科技、传媒和电信行业专家致力于为企业提供丰富的定制化服务，帮助他们顺应变革趋势，抢占行业先机，所服务的客户遍布全球，覆盖全价值链。敬请联系作者或访问www.deloitte.com，了解更多信息。

Deloitte.
Insights

敬请登陆 www.deloitte.com/insights 订阅德勤洞察最新资讯。

敬请关注 @DeloitteInsight

参与人员

编辑：Junko Kaji, Preetha Devan, Prodyut Ranjan Borah, Rupesh Bhat, Arpan Kumar Saha, Ribhu Ranjan, Emma Downey, Nairita Gangopadhyay, Blythe Hurley, and Aparna Prusty

创意：Jaime Austin, Sylvia Yoon Chang, Govindh Raj, Sanaa Saifi, and Rishwa Amarnath

推广：Maria Martin Cirujano

封面设计：Jaime Austin