隐私计算是确保数据安全的最优解

□ 科普时报记者 **陈 杰**

大数据时代，数据在各行各业释放的价值越来越重要，而打破数据孤岛、共享数据信息更是实现数据价值的重要前提。但因数据涉及到隐私，在使用价值与安全同等重要的情况下，如何合法合规的使用数据，成为互联网产业企业面临的重大难题。

“目前来看，隐私计算是数据安全与隐私保护的最优解决方案。”平安科技（深圳）有限公司副总工程师王健宗接受记者采访时表示，不过由于受安全性以及合规性等多方因素的影响，目前这一技术的应用还处于测试阶段，大规模运用的案例相对较少。

确保数据“可用不可见”

所谓隐私计算，是在处理和分析数据的过程中，能保持数据的不透明、不泄露、无法被计算方法以及其他非授权方获取。从技术角度来看，隐私计算是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系，实现数据的“可用不可见”，其中关键技术包括联邦学习、多方安全计算、安全求交、匿踪查询、差分隐私、同态加密等。

王健宗表示，隐私计算目前在全球还没有成熟的解决方案，大部分项目处于验证性测试阶段，难以实现大规模生产应用。“从数据层面来看，隐私计算需要将各行各业的数据规范化，数据的格式、关键字等都要一致，算法平台才可以有效运作；而在算法层面，则需要有足够的响应速度，隐私计算在商业上才有使用价值。”

尽管隐私计算技术还未被大规模运用，但在市场的需求下，入场的玩家却并不少，不仅有互联网大厂布局，一些金融机构与创业公司也都相继入场。目前，隐私技术的参与者主要有三类，分别是互联网大厂如蚂蚁、腾讯、百度、字节跳动，金融机构或金融垂直行业公司如平安科技、微众银行、同盾科技，创业公司如光之树、富数科技、矩阵元等等。

同盾科技已经提出了天启可信AI开放操作系统，并在隐私计算技术落地案例极少的当下，同盾科技已协助某国有大型商业银行围绕着企业级数据分级分类、敏感信息保护等行业及监管关注的焦点问题展开咨询以及落地工作。

平安科技则是基于联邦学习、多方安全计算等核心技术，提供面向数据隐私安全保护的一站式综合解决方案服务。目前，平安科技的蜂巢联邦智能隐私计算平台已经成为解决当下数据难题与隐私保护的一大利器，助力企业建设跨企业、跨数据、跨领域的大数据AI生态。

视觉中国供图

王健宗表示，基于行业内各个异构平台存在着无法直接互通建模的问题与挑战，蜂巢平台联合外部互联网机构，完成了行业内第一例打破异构平台壁垒，通过约定标准化参数与通信协议，实现跨平台互联互通的案例。

催生千亿规模“蓝海市场”

下半年，《国数据安全法》和《个人信息保护法》正式开始实施，终于让数据安全和个人信息安全有了立法保障，也将“一揽子授权”“强制同意”等过度收集用户个人信息的行为将被限制。而早在2020年末，国家发改委等四部委就联合发布指导意见，提出数据是国家基础战略性资源和重要生产要素，要加强数据中心、数据资源的顶层统筹和要素流通，强化大数据安全保障。

监管之下，基于数据使用机构对数据安全与隐私保护的需求，隐私计算产业的发展进入春天。腾讯发布的《深潜数据蓝海：隐私计算行业研究报告》指出，隐私计算机构的营业收入主要分为两大类，一是传统的软件销售和服务收入，二是通过隐私计算平台上的业务运营产生的利润分成。据推算，未来三年，我国隐私计算系统的销售和服务收入规模有望触达100—200亿元的空间市场，而在平台运营分润的模式下，仅消费金融业务就能撬动千亿市场规模。

“隐私计算是解决数据隐私之痛，释放数据市场巨大经济价值的关键，必然具有极大发展空间。”王健宗表示，在法律法规、行业政策等顶层设计不断迭代完善下，数据安全和隐私保护合规要求将更加明确，进而牵引隐私计算市场潜力释放。技术方面，算法优化和硬件提升会提高隐私计算技术的可用性，将进一步促进数据市场快速发展。未来，数据市场将会出现一批依托隐私计算的平台型公司，开辟数据运营商模式，充当数据存储，交换和价值挖掘的核心媒介，从数据密集型行业切入，摸清行业痛点，再从预算充足、数字化程度高的头部企业渗透到中小客户，后期可通过数据交换或SaaS服务收费模式盈利。

随着大量行业企业的入局，隐私计算的春天已然到来，但不容忽视的一点是，隐私计算若要撬动千亿市场，还需要克服多重难点。

行业人士认为，隐私计算落地过程中还需要更好的工具，更好地解释安全性，以及生态能力更加结合业务场景。当下的隐私计算相关技尚处于萌芽与上升阶段，最终真正成熟实现可用的技术状态还需时日，但未来可期。

作为数据安全与隐私保护的最优解决方案，隐私计算要早日实现为数字社会、数字经济的全面发展赋能，只有通过技术的迭代、政策的革新和市场的发育与健全，才能在数据安全与个人隐私保护方面砌起一道坚如磐石的高墙。

让我国拥有自己的开源操作系统根基

□ 科普时报记者 **马爱平**

日前，在操作系统产业峰会2021上，华为携社区全体伙伴将欧拉开源操作系统（openEuler，简称“欧拉”）捐赠给开放原子开源基金会。此举对操作系统产业发展具有何深远意义？未来将如何持续融合欧拉最新技术和能力落地？

“欧拉自2019年正式开源以来，麒麟软件等业界伙伴与华为一起积极建设和维护。2021年9月，欧拉的全新发布是中国开源操作系统社区的里程碑，在欧拉开源社区，聚集着近万名开发者，近百个特别兴趣小组，它是一个开放的、共创协同的社区。将欧拉捐赠给第三方开放原子开源基金会，社区将更开放和更加具有活力，所以此次捐赠让中国操作系统有了自己的根，大家能够在一个相对共性的根技术上面，再去开发各自不同领域的具体版本，这对于中国操作系统有着重要的意义。”麒麟软件高级副总经理韩乃平在接受记者采访时表示。

在韩乃平看来，一个社区的成长，或者开源文化的成长包括开源社区代码的贡献、开源文化打造、开源人才培养、开源生态构建、以及呈现给用户的开源应用选择和开源服务等。

韩乃平介绍，麒麟软件在欧拉社区签约CLA超过150人，后续还将加大投入更多的社区人才贡献社区。在开源代码贡献方面，麒麟软件在欧拉社区涉及到桌面、云原生、分布式存储、AI、大数据和高可用等多个领域，还发起成立了高可用组、虚拟化组、轻量化桌面组、容器组等多个组，贡献领域包括桌面、服务器、安全云原生、人工智能、大数据等众多方面。

麒麟软件已是除华为外欧拉社区第一大代码贡献者。一个好的开源项目成功最关键的要素之一是应用。应用层面，麒麟软件基于社区推出的新版银河麒麟操作系统已经在政务、金融、能源、交通等多个领域得到了广泛的应用，部分行业还进入了核心应用。当前，银河麒麟操作系统在桌面和服务器端累计适配软硬件超过20万款。这些软硬件包括了数据库、中间件、上层开放环境，行业应用和下层的服务器、国产CPU整机、外设、存储等，实现了同源支持国际和国内主流CPU平台。银河麒麟操作系统的生态体系已形成体系有序发展。

“未来，我们既要把自身的生态做好，在认证广度和数量上进一步扩大，也要把欧拉社区做好。一方面要开发更丰富的贴近产业需求的应用场景，另一方面要打造更好的开源版本和基于开源版本的通用商业软件。”韩乃平说。

创新是所有科技型企业永恒的主题。“当前我们有几项重点工作。”韩乃平表示，第一，对欧拉社区而言，麒麟软件和华为等社区伙伴一起，积累并贡献优秀的产品技术，持续创新，持续贡献。对麒麟软件而言，把欧拉作为一个自主创新的根社区，基于这些根技术，我们要做一些商业增值，在产业生态和本地化服务方面做好服务，使它成为最活跃的根社区。

AI正快速向认知智能迈进

□ 科普时报记者 **陈 杰**

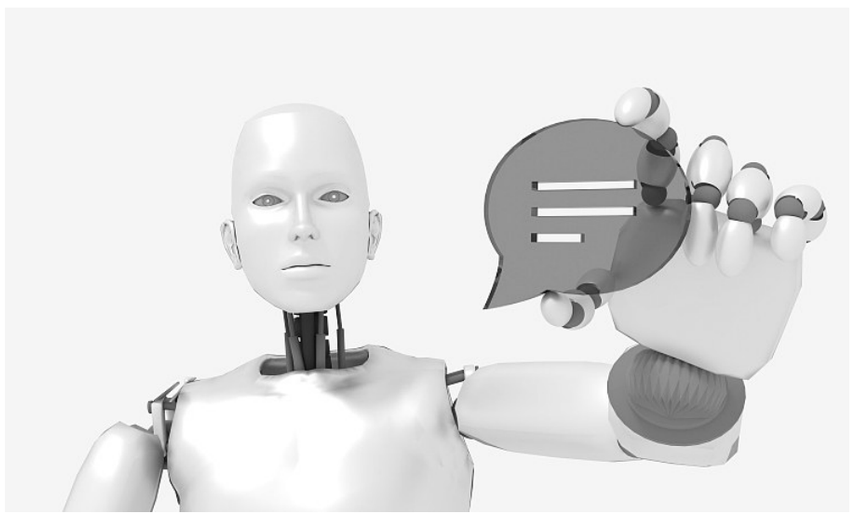
数字经济时代，人工智能已经成为重要基础设施，已具备同各行各业结合的能力，越来越多的行业和领域都在进行不同层次的智能化升级。当然，人工智能本身也在不断迭代升级。基于多层人工神经网络的深度学习是目前人工智能最有效的学习算法，深度学习在识别（感知智能）上已有突破，但在理解（认知智能）上还有局限性。

目前来看，人工智能的发展方向从感知智能向认知智能快速推进中，自然语言识别技术及预训练模型便成为AI领域中的热门赛道。一时间，超大规模的预训练模型成为全球人工智能技术研发的热点和竞争的焦点。

不过，一直由腾讯、搜狗、华为、阿里达摩院等巨头轮番霸榜的权威中文语言识别评测基准（CLUE）榜单，最近却被一家创业公司的轻量化预训练模型刷榜。

日前，澜舟科技的孟子轻量化预训练模型以十亿参数完成了此前百亿、千亿参数模型刷新的纪录，首战登顶中CLUE榜单。此外，在HICOOL2021全球创业大赛中，孟子新一代认知服务引擎项目也从全球48个国家和地区的4018个项目中脱颖而出，获得人工智能和金融赛道第一名。

澜舟科技创始人兼CEO周明表示，过去的两三年里，预训练模型在自然语言领域得到非常广泛的重视，各大公司学校都开展了预训练模型的研究，趋势就是预训练模型越大越好。“但也存在一个问题，就是模型越大训练的成本就越高，在提供服务的时候也要求客户的机器设备能力也要非常大，从而导致很多硬件能力低的中小企业用不起这些重量级预训练模型。”



视觉中国供图

基于这一痛点，澜舟科技一直在考虑能不能把模型做得小一点，提高训练速度的同时也降低使用成本，名为孟子的轻量化预训练模型应运而生。

周明表示，孟子轻量化的预训练模型是利用大规模的语料库，以无监督的方式的训练一个大规模的语言模型，这个语言模型输入一个句子或一个片段，基本上可以定义出每一个词和每个句子的语义，可以应用在机器翻译、问答搜索等场景。“在预训练基础上，澜舟科技开发了新一代的机器翻译、文本生成和行业搜索引擎等技术，并通过产业合作实现了技术落地。”

当前，企业的数字化转型和智能化转型，也已经随着人工智能的发展从感知智能推进到认知智能，企业需要从大数据中获取信息，然后在知识图谱和和产业规则的基础上进行推理，最后形成的业务报表并对流程作出趋势判断等等。这种强烈的需求加上预训练模型的技术发展，认知智能赛道必然会迎来一个新的飞跃。

不过周明坦言，虽然预训练模型充分利用大数据来建立语言模型，但是在做多轮对话或者需要对趋势作出判定，或者依赖知识图谱进行推理方面，认知智能目前还差强人意。“人脑在处理熟悉的事情时往往依赖数据和直觉，速度快但缺乏解释性，这类似与训练模型或深度学习；而在处理不熟悉事情时往往依赖规则、逻辑和推理，速度较慢，但是具备可解释性，更像是符号计算。当下的深度学习可以思考，如何通过一个模型将二者的优势结合，也就是数据和知识融合起来寻找解决思路。”

2纳米制程让摩尔定律得以延续

计算机行业长久以来一直受到摩尔定律的支配——半导体电路中的晶体管数量每两年就会翻一番。但是随着芯片制程的不断缩小，传统的摩尔定律正面临失效的危机，特别是在芯片产业进入5纳米制程之后，传统的硅芯片已经趋近于极限了。

不过，近日从IBM传来好消息，比DNA单链还小的全球首颗2纳米芯片亮相，性能比当前主流的7纳米提升45%，能耗则是减少75%。若是采用2nm工艺打造手机芯片，手机续航时间可以增长至之前的四倍。未来，手机用户只需四天充一次电即可。

早在2014年，IBM就宣告退出芯片制造赛道。但事实上，蓝色巨人并没有放弃先进芯片制程工艺芯片的研发。通过与AMD、三星等企业合作，IBM接连在多个工艺节点，率先推出测试芯片。此此，借助2纳米制程工艺，IBM成功将500亿个晶圆体容纳在了指甲大小的芯片上。

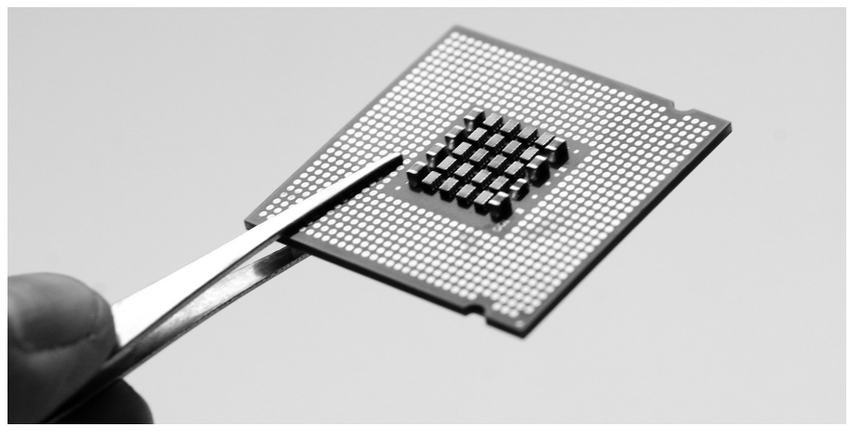
据悉，按照计划三星、台积电两家企业将会在2025年前后，实现2纳米芯片量产。而英特尔此前也公布了芯片技术升级路线图，表示会在2025年前后发布等效于2纳米技术的2A工艺。

相比7纳米芯片，2纳米制程芯片除了可以应用在手机等消费电子设备上，还可以用在边缘计算、太空探索、5G/6G等领域。借助这一新工艺帮助，人们的生活水准有望获得大幅提升。毕竟，未来社会必然会向着智能化方向发展，而设备的智能程度，很大程度都是取决于芯片的制程工艺级别。从该角度来看，2纳米技术其实可以帮助智能化产业实现更加快速的发展。

2纳米芯片亮相，对于整个半导体产业都有非常重要的意义。虽然短期内，2纳米工艺芯片无法规模量产，但通过展示2纳米工艺芯片在标准300毫米硅晶圆上蚀刻真实芯片的过程，证明了摩尔定律的延续性。

当然，业界对于摩尔定律在半导体界还能延续多久并不乐观，因为1纳米之后才是半导体产业的极限和关键所在。

为什么1纳米是极限呢？所谓的半导体芯片就是能表示“0”和“1”这两种状态，因而称为半导体。但小于7纳米时随着物理结构上硅晶体管间的距离越来越小，会逐渐出现量子隧穿效应，电子不再停留在预期的逻辑门内表示“0”和“1”，而是连续地从一个门流向下一个门。此时的硅晶体管不再可能处于关闭状态，半导体也就变成了全导体，自然也就无法完成芯片的基本功能了。



视觉中国供图

单纯从材料性能角度考虑，硅并不是最好的半导体芯片材料，但是硅最大的好处就是便宜，原料成本十分低廉。因此，芯片制程在逐渐逼近硅晶片的1纳米极限的时候，除了提高工艺之外，世界各地的顶尖实验室也开始考虑使用其他材料代替硅的可能性。（科文）

2022年IEEE最高等级会员名单公布

11月24日，国际电气和电子工程师协会（IEEE）公布了2022年新晋最高等级会员（Fellow）名单。新增名单中，265位学者入选，华人学者有83位，占比31.3%，国内AI领域多人入选。

其中，百度首席技术官王海峰以及百度计算机视觉首席架构师王井东入选，入选理由分别为在自然语言处理和人工智能技术方面的贡献和引领、对视觉内容理解和检索作出贡献。王海峰现任百度首席技术官、深度学习技术及应用国家工程实验室主任，是自然语言处理领域最重要的国际学术组织ACL全球首位华人主席，ACL会士，ACL亚太分会创始主席；王井东今年9月加入百度，在此之前曾任微软亚洲研究院视觉计算组首席研究员。研究领域为计算机视觉、深度学习及多媒体。目前研究的问题包括神经网络结构的设计、行人姿势估计、图像分割、目标检测以及多媒体搜索等。

除此之外，AI领域入选的学者还包括清华大学信息科学技术学院副院长汪玉，入选理由为对领域专用加速器设计作出了贡献；阿里巴巴集团副总裁李飞飞，入选理由为对数据库查询处理和优化以及云数据库系统作出贡献；嬴彻科技CTO杨睿刚，入选理由为对3D计算机视觉和自动驾驶作出贡献。

国际电气和电子工程师协会（IEEE）是国际性的电子技术与信息科学工程师的学会。1963年1月1日建会，在160多个国家中拥有42万多位会员和39个专业分学会，引领着信号和信息处理、电力、电子、计算机、通信、控制、遥感、生物医学、智能交通和太空等技术领域的最新发展方向。

IEEE Fellow为学会最高等级会员，是IEEE授予成员的最高荣誉，每年由IEEE同行专家在拥有高级或终身等级的会员中遴选约300名左右，当选人数不超过IEEE当年会员总人数的千分之一。当选人需要对工程科学技术的进步或应用作出重大贡献，为社会带来重大价值。

（韩阳）

安全报告：终端安全形势愈发严峻

近日，亚信安全发布的《2021年第三季度网络安全威胁报告》（简称“报告”）显示，第三季度勒索病毒总量小幅提升，且攻击靶心开始向政府和医疗行业移动。此外，PE病毒、后门木马、僵尸网络、钓鱼网站、Web威胁、高危漏洞等皆有增长，终端安全形势依旧严峻。

报告的“勒索病毒月检测图”显示，第三季度勒索病毒总量较上一季度有小幅度上升。此外，勒索病毒针对发展中国家发起的攻击数量开始增加。在勒索病毒数量上升的同时，遭受攻击的行业变化。其中，政府及医疗行业由于其业务连续可用的高要求，对感染勒索病毒后支付赎金的可能性较大，因此也更容易遭到黑客的锁定成为被攻击的目标。另外，勒索病毒也将目标瞄准全球各大公司，索要巨额赎金。

今年第3季度检测到的病毒类型中，PE（感染型病毒）数量在所有检测病毒类型中所占比重最大，占到总检测数量的25%。此外，报告还对三季度出现“新、热”威胁进行了分析。亚信安全截获了隐藏在激活工具下MLXG病毒，此病毒会检测安全软件运行情况，并释放加密文件解密执行，通过修改国内用户常用浏览器设置来诱导用户访问自身推广站点，之后还会释放恶意驱动并注册为服务，以此常驻于系统当中。目前，亚信安全已经推出专杀工具，并建议用户避免使用盗版系统、激活工具等，同时部署终端安全产品并及时更新组件及特征库。

报告还包括了最新的安卓平台病毒、WEB安全威胁情况、TOP 10恶意URL和钓鱼网站分析。通过对不断变化的威胁环境情报共享，用户不仅可以用来打击当下的网络攻击，并预测新出现的威胁，还能以此为依据为网络安全战略方向调整提供精准导向。

（雷远方）