

智能体三级演进重构互联网运行逻辑

本报记者 李洋

人工智能(AI)技术的爆发式发展,正在推动行业从“模型创新”向“场景落地”加速转型。在这一进程中,如何让生成式AI突破技术边界、实现规模化应用?在近日举行的2025中国互联网大会上,中国工程院原副院长、中国互联网协会原理事长邬贺铨认为,智能体(AI Agent)的三级演进——从智能体到智能体协同群(Agentic AI)再到覆盖更广的智联网,这不仅是AI技术落地的关键路径,更将重构互联网的运行逻辑。

邬贺铨表示,AI正在从“被动响应的工具”升级为“主动协作的伙伴”,推动互联网从“用户主导操作”迈入“智能体自主执行+人类监督决策”的新阶段,而人的角色也将从“操作者”转型为“AI行为决策者”,技术与需求的双重驱动将为通用AI的实现筑牢根基。

从单一智能体到智联网

邬贺铨认为,智能体应该是“大模型+记忆系统+工具调用+规划能力”构成的闭环系统,不仅能执行任务,还可通过反馈反思结果。

“生成式AI根据提示词生成内容,缺乏持续目标跟进,只能被动回应,不具备主动发起任务和对物理世界的感悟能力,仅起到‘助手’作用,推广变现较难;而智能体是面向特定场景、基于大模型,通过感知—思考—调用工具—行动闭环生成的软件程序,可在限定数字环境中执行目标导向任务。但智能体仍缺乏因果推理能力,处理时间变量和复杂关系问题时不稳定,且对提示设计高度敏感,影响任务可行性。”邬贺铨表示,为此需要进一步从智能体发展到智能体协同群。

本报讯(记者 孙立彬)近日,国际数据公司(IDC)发布的《中国物联网安全市场份额》报告显示,2024年,中国物联网安全市场整体规模约在21.3亿元。在终端设备持续增长、行业数字化转型加快,特别是国家政策日益强化安全合规要求的背景下,物联网安全建设正逐步迈向体系化、常态化,其市场整体保持稳中有进的发展态势。

IDC中国机器人与物联网领域研究经理李君兰表示,在万物智联时代,安全已成为系统稳定运行与业务持续发展的基础能力。随着终端数量激增与场景不断扩展,物联网安全



据介绍,智能体协同群新增中心化编排层,可协调封闭系统内具有统一复杂目标的多智能体合作,通过共享记忆库实现知识的继承与反思,打造多智能体协作生态。“不过,智能体协同群仍未解决AI的语义模糊性和不可预测性,多智能体协同甚至可能放大错误。”邬贺铨补充道,因此还需要向智联网(Internet of Agents)发展,借助区块链、联邦学习等分布式协议实现开放式异构智能体间跨域协作,使其能在开放环境中广泛应用,起到“数字化身”作用。

“智能体、智能体协同群和智联网,是生成式AI走向应用落地的重要环节也是过渡到通用AI的必要阶段。”邬贺铨认为,技术迭代与市场需求将推动智能体从单一个体走向多智能体协同,从“工具辅助”升级为“自主协作”,最终向智联网演进。

邬贺铨表示,在应用层面,智能体时代的互联网在2B和2C领域均有广阔空间。2B领域可

通过“智能体即服务”提供低代码平台或嵌入药物研发、供应链管理场景;2C领域则能实现行程规划、智能家居控制等功能。

安全与智能的博弈

随着数字化、智能化深入业务核心,新的问题随之浮现。

360集团创始人周鸿祎坦言,AI带来的新挑战主要有两个:一是大模型本身具有随机性,如同人一样会犯错、有幻觉,还可能被人用自然语言套路导致泄露数据,传统的防火墙、杀毒软件对此无效;二是黑客会利用智能体规模化攻击,把黑客经验训练成智能体,自动规划攻击、找漏洞、调用工具,这使得对抗从人与人变成人与机器、算法、算力的对抗。

周鸿祎认为,需用“以模制模”的思路加以应对:一方面,用安全大模型做“大模型卫士”,理解大模型的输入输出,以此解决大模型自身的安全问题;另一方面,训练安全专家智能体,用智

能体对抗攻击智能体,弥补安全专家的不足。“安全防护是动态演进的,不可能一劳永逸。”

奇安信集团副总裁韩永刚认为,AI的发展给网络安全带来“双重性”——既要保护AI自身安全,也要利用AI提升安全防御能力。

韩永刚进一步解释称,AI安全与传统安全存在本质区别,其风险不仅存在于研发测试环境,数据与应用层面,未来还将延伸至认知领域与智能体交互中。例如,多智能体协同场景下,智能体需在不同接口、应用与数据间“游走”,其身份认证与权限管控至关重要。因此,从算力平台到大模型应用,构建“大模型卫士”与安全围栏,已成为当务之急。

另一方面,AI也是安全能力的“增量”,能突破传统安全模式的局限,实现人工难以完成的高效防御。通过AI赋能,漏洞挖掘的效率能大幅提高;AI在情报发现、自动化渗透测试中能发挥关

键作用,尤其是在安全运营这一对技术和人力消耗最大的环节,通过增量学习、思维链模式、多智能体协同,能显著提升专业研判、响应处置的效率。不过,AI目前仍以辅助为主,无法完全替代安全专家,但能让专家效率大幅度提升。

人机协同推动科技向善

“智能体时代,人该怎么做才能不被替代,成为超级个体”?对于这一问题,周鸿祎认为,技术进步总会淘汰一些岗位,关键是主动拥抱AI、学会用AI的人淘汰不会用的人。智能体时代,人的角色要从操作者变成智能体管理者,规划和协调智能体的工作,替它们做决定。

对此,零一万物联合创始人马杰认为核心是人机协同。例如,游戏开发行业过去大团队才能做精美游戏,现在小团队可以用AI生成美术、音乐等素材。“这不是AI抢工作,而是会用AI的人能做更多事。对于年轻人而言,未来不是AI夺走工作,而是会用AI的人将更有竞争力。”

硅基智能创始人司马华鹏表示,向善的应用有更大市场,能用商业逻辑推动“良币驱逐劣币”,避免AI被用来挑拨关系、考验人性。

马杰举例说,AI带来了技术平权,让小企业和个人都能用上好的AI技术。在乡村振兴方面,偏远地区可通过互联网和AI获取优质的农业技术指导、电商渠道等资源;在普惠医疗上,AI辅助诊断、远程医疗能通过网络延伸到基层,弥补资源不均。

在数字经济加速渗透的今天,互联网作为新质生产力的引擎,正在与人工智能、实体经济深度交织,催生出新的技术变革与应用场景。

中国物联网安全市场规模突破21亿元

正在覆盖感知、传输、数据、应用与平台等全链路环节。未来,用户将从合规驱动转向价值导向,更加重视安全对业务连续性、数据可信性与系统韧性的支撑作用。物联网安全将加速与AI、平台生态及行业场景深度融合,构建“原生安全”体系,成为推动可信物联网发展的关键底座。

当前,中国物联网安全市场以软硬件一体化方案为主,产品供给主要聚焦在边界安

全、接入安全和安全管理平台三大核心方向。

边界安全作为物联网防护体系的第一道防线,是企业优先部署的核心环节,目前市场规模超过5.6亿元;接入安全依托物联网终端设备数量的持续扩张,具备广泛的应用基础和显著的增长潜力,市场规模约5.5亿元;安全管理平台在统一数据采集、集中管理与安全态势感知方面发挥关键作用,正逐步成为系统化安全建设的重

要支撑,市场规模约为5.4亿元。此外,值得关注的是,物联网安全服务市场规模持续增长,收入占比翻倍,反映出服务化趋势正在初步显现。

从行业应用层面看,物联网安全市场正顺应物联网应用日益碎片化的发展特征,安全防护的场景化、多样化趋势持续加快。面对多类型感知设备、多源异构数据以及复杂多变的业务场景,市场对于差异化、定制化的安全防护策略提

出了更高要求。整体看,视频类物联设备的安全防护仍是当前行业关注的重点。

政府作为物联网安全建设的主导力量,持续推动城市治理、公共安全等领域的体系化部署,市场规模达10.6亿元,在整体市场中占据核心地位。与此同时,交通、金融、教育、电力、医疗等重点行业的安全投入也在不断加大,带动物联网安全应用不断向纵深发展,覆盖场景日益多样化、复杂化。