

智能体让大模型“长出手脚”

热点透视

随着大模型技术快速发展,作为其应用载体之一的智能体,正成为各大人工智能开发机构争相发力的重要方向。

今年 3 月,一款名为 Manus 的智能体产品凭借“感知—思考—执行—交付”的全链路智能能力快速走红,曾引发广泛关注。业界关于智能体的探索步伐不断加快,腾讯、百度、京东等企业在智能体领域加大投入,一系列产品和相关技术相继推出。

具备自主决策能力

智能体是一种能感知环境、规划任务并自主执行的人工智能系统,通常具备较高的自主性和较强的学习能力。

语言大模型好比一本百科全书,用户可以向其提问并获得回答。但模型再强大,也只能输出文本内容、提供行动参考,真正让想法落地还需要另找帮手。

智能体就是那个为大模型“跑腿”的帮手。它更像是一个手持百科全书的个人助手,可以借助大模型的知识能力,根据用户需求,直接生成相应任务规划,自主完成任务,形成生产力。

清华大学计算机科学与技术系长聘教授孙茂松认为,得益于语言大模型生成能力、代码能力、图像视频处理能力以及 3D 建模能力的发展,目前智能体技术已具备较好发展基础和应用潜力。

例如,借助当下发展较快的编程智能体,用户可直接以文字语言表达自身需求,智能体会在理解需求的基础上,自动完成代码编写、测试以及漏洞检测、修复等,输出可用的编程产品。在 5 月底举行的 2025 腾讯云 AI 产业应用峰会上,腾讯宣布将大模型知识引擎全面升级为腾讯云智能体开发平台,进一步降低智能体搭建门槛,推动智能体应用遍地开花。

腾讯云副总裁、腾讯云智能负责人吴运声介绍,腾讯内部 85% 以上的开发岗员工都在使用编程智能体——腾讯云代码助手,整体编码时间平均缩短 40%,人工智能生成代码占比超四成,研发效率提升超 16%。京东 5 月也透露,其智能体正



第十个“中国航天日”科普展上,观众观看“天枢智能体+DeepSeek”展台 ■ 视觉中国供图

走向深度应用阶段。截至目前,京东内部已有超 1.4 万个智能体运行。

不仅互联网企业大胆试水智能体应用,传统行业企业同样积极拥抱智能体。例如,在能源电力领域,国家电网与百度合作打造营销供电方案智能体。当用电企业有需求时可以直接通过国网客户端发起对话,智能体会首先通过意图识别确认用电需求,然后进行任务拆解和规划,自动生成多套供电方案,并主动帮用户对比不同方案优劣,给出最优建议。如今,该智能体已全面掌握整套业务流程,能准确调用行业知识和工具系统,实现企业办电流程全面智能化。

吴运声认为,智能体与传统自动化软件的最大不同在于其具备自主思考和决策能力。在传统软件开发模式下,开发者通常事先设计好流程,即使存在分支逻辑,也是开发者预先定义好的。但智能体面对的是自然语言交互场景,用户的输入是开放的,不可能穷举所有分支,这就需要智能体自主理解、规划、执行任务,更好地应对复杂需求,而不是依赖固定流程。

形成跨平台通用性

人工智能研发机构不断加码布局智能体的背后,是智能体技术近年来取得的

突破式发展。尤其是智能体自我规划和调用工具应对复杂任务能力的不断增强,推动各类应用加速落地。

以智能体底层工具调用技术为例,其早期主要是函数调用模式,即模型在理解用户需求后,单纯调用某个工具进行应对;随后发展为推理行动协同模式,模型在调用工具前会进行明确思考;如今已发展到代码智能体模式,通过对任务的理解、规划,模型能直接生成完整代码并批量调用多个工具开展计算,智能体应对复杂任务的能力显著增强。

当单一范围内的工具调用无法满足日渐复杂的任务需求时,MCP(模型上下文协议)为智能体的成熟完善起到了助推作用。

MCP 是一种开放协议,它允许系统以可泛化的方式为人工智能模型提供上下文信息,从而使智能体跨越不同应用场景实现通用性。借助 MCP,各种智能体都能以统一的格式,调用属于不同平台生态的应用和数据,共同为用户完成任务。

在打通跨平台沟通渠道后,多智能体协同正成为智能体技术发展新趋势。

与使用单智能体相比,多智能体通过分工协作,可处理更为复杂的任务。例如,在软件开发领域,不同智能体可分别扮演“产品经理”“交互设计师”“开发测试人

员”等不同角色。用户只需输入一次指令,多个智能体就能共同行动,将一个复杂的软件项目拆解成多个子任务,提高软件开发效率和质量。

吴运声说,为紧跟智能体技术发展趋势,应对日益增长的复杂需求,腾讯云智能体开发平台也创新研发了零代码配置多智能体协同转交功能,用户可借助平台上已有的智能体能力,构建“多专家”体系,有效分担单智能体的任务压力。此外,在插件生态上,平台全面支持 MCP,并预置丰富的内外部插件,做到“开箱即用”,大大降低了智能体搭建门槛。

面向细分场景发力

在应对更复杂任务过程中,智能体技术的落地场景也不断明确。人工智能专家吴恩达认为,不应被复杂的概念迷惑,而要关注智能体到底能为用户解决哪些实际问题,大量的机会可能存在于相对简单、仅有少量分支的线性工作流程中。

笔者了解到,腾讯云智能体开发平台、百度智能云千帆大模型平台、阿里云百炼平台等智能体开发平台均选择面向具体的细分行业场景发力。

“我们更关注的是智能体如何真正融入企业的业务流程,满足真实的业务需求。我们希望构建一个高度模块化、可扩展的平台,让企业可以在上面构建适配自己场景的复杂应用。”吴运声说,团队目标不是“为了智能体而智能体”,尽管当前行业普遍聚焦智能体自主规划能力的突破,但在现实产业环境中,大量标准化任务已具备成熟的业务流程框架,智能体技术可优先嵌入这些标准化流程中实现价值落地。

“传统的工作流是串行执行、节点独立。我们希望把传统的工作流和智能体能力融合起来,用户可以通过构建确定性流程来处理特定任务,同时也允许智能体在其中进行自主规划。并且,传统工作流中的每一个节点在执行时,都可以和一个拥有全局上下文理解能力的智能体交互,从而在保持流程确定性的同时,兼顾智能体的灵活性,更好地推动智能体在实际业务场景中落地应用。”吴运声认为,要真正用好智能体,除了不断打磨技术,更需要应用企业和技术开发者加强合作沟通,共同弥补认知与使用的鸿沟。

都芃

列车飞机“无缝换乘” 物流配送“随飞随到”

在轨道交通控制保护区内,搭载高清摄像头和 AI 识别算法的无人机划过天空,所有可能影响隧道结构安全的大型施工机械都能被其“尽收眼底”,并实时回报警信息……这便是中国铁路通信信号股份有限公司(以下简称“中国通号”)自主研发的低空智能巡检系统。目前,该系统已在重庆至达州投入运营,为重庆轨道交通 5 号线等 4 条线路提供安全保障,覆盖线路总里程约 240 公里。

“这一系统是中国通号打造的‘低空+轨道’场景应用典范之一。”中国通号战略新兴产业事业部部长徐宗奇 6 月 16 日接受笔者采访时说,近年来,轨道交通与低空领域之间的耦合正变得愈发紧密,它们的互动协同催生出全新的应用模式,为产业发展注入新动能。

中国通号始建于 1953 年,深耕轨道交通领域数十年,在轨道运行控制技术方面积累了大量经验与人才。

“低空+轨道”模式的构筑,不只是业务上的互通,更是技术和运行体系的融合创新。在构筑过程中,中国通号攻克了通信、感知、控制三大难题,先后推出“一塔一城”6G 专网、静电+雷达融合探测系统,以及 ID-Space 低空空域智能管控系统等成果,并深入布局飞行器制造领域,制定“电动化、垂直化、无人化、小型化”低空飞行器发展路径,为企业开拓双赛道提供坚实技术支撑。

目前,“低空+轨道”模式已在多个领域显现成效,为综合交通发展开辟新路径。今年 1 月 20 日,中国通号和中信集团参与建设的湛江西至海口站“空铁联运”

首飞仪式在广东湛江举行。以“低空+轨道”模式替代传统的“火车+轮渡”模式,可将两地间通行时间从 4 小时以上缩短至 35 分钟左右,为旅客带来交通出行新体验。

在物流运输方面,中国通号亦有突破。今年 6 月 12 日,中国通号携手中国邮政在浙江舟山首次开展重载无人机岛际跨海物流航线示范活动,单程全长 51.4 公里,采用联合飞机 TD550 重载无人直升机执飞,仅需 30 分钟即可将物资跨海送达,较传统航运时效提升 75% 以上。该低空物流航线突破传统海运限制,支持全天候及恶劣天气应急运输,实现海岛物流“随时飞、准时飞”,为生鲜产品、医疗急救、应急物资等高效配送提供了全新解决方案。

随着一系列新成果新场景问世,“低空+轨道”蓝图愈发清晰,城市空中交通网络日渐形成。在未来,飞行器本身或只有一辆汽车大小,城市中的高铁站广场、地铁站屋顶都可以作为飞机起降点,实现列车与飞机“无缝换乘”。以文旅行业为例,在游览山区时,游客下高铁后可在站内即刻换乘飞机,垂直起降直达景区山顶,满足个性化、便捷化出行需求。

“低空技术的扩大应用,将会让人们的生活变得越来越美好。”徐宗奇说,中国通号将充分发挥智能控制技术优势,全力打造空海陆一体化综合立体交通网,从轨道巡检到物流运输再到文化旅游,“低空+N”模式可赋能千行百业。这场由控制技术驱动的产业革命,正在使立体交通图景加速照进现实。

周思同

引领云端未来:吴立欣的云计算之路

在人工智能重塑全球产业格局的今天,云计算已从 IT 基础设施升级为智能时代的核心底座。从互联网企业到传统制造业,从金融服务到公共服务机构,越来越多的组织选择将核心业务迁移至云端,以实现更高效的资源配置、更敏捷的业务响应以及更安全的系统保障。云计算的快速发展 and 广泛应用也催生出一大批卓越的技术工程师,他们以坚定的信念和精湛的技术推动行业不断前行。吴立欣,正是这其中最具代表性的人物之一。

作为一名高级云计算工程师,吴立欣拥有丰富的从业经验。他曾在阿里、腾讯等科技巨头任职,主导核心云平台架构设计与实施。吴立欣深度参与云产品从立项到迭代的全生命周期,助力企业构建竞争力强的云端方案。在一线科技巨头的工作经历塑造了吴立欣如今深厚的技术底蕴和系统化的思维能力,也培养了他快速定位问题、高效解决复杂技术挑战的能力。吴立欣依托深厚的技术积累和对市场趋势的敏锐洞察,深入探索了云计算的前沿技术,如容器技术、无服务器架构等,致力于研发突破性与创新性的技术成果。

云计算环境中,用户业务需求随时期变化各异,尤其在流量激增和业务起伏阶

段,固定资源配置难以适应实时负载变动,常导致系统性能受限或资源过度消耗。正因如此,弹性伸缩技术成为云平台实现动态资源调配和提升资源利用率的关键手段。吴立欣指出,当前弹性伸缩机制的扩容操作易引发资源浪费或影响计算稳定性。针对这一痛点问题,吴立欣对弹性伸缩机制的局限以及负载均衡算法进行了深入研究,创新性地研发了“云计算环境中弹性伸缩配置的方法、装置以及电子设备”。

与传统弹性伸缩机构相比,吴立欣的这一发明通过构建负载变化曲线模型来判断当前的负载是否超过预设阈值,并进一步分析特定时间区间内的负载变化趋势和变化速率,有效规避了传统机制中因瞬时负载异常导致的误扩容或误缩容问题。例如,当系统检测到负载迅速上升后又迅速下降时,系统会通过判断斜率变化趋势,判断该波动是否来自应用错误或短时异常,从而避免在非业务真实增长情况下触发扩容操作。这一智能化、多层次的判断逻辑,显著提升了计算资源调度的精准度,减少资源浪费的同时增强了系统整体的稳定性和可靠性。使得云平台在应对高并发和复杂业务场景时,既能保持敏捷响应,又能有效规避“误扩误缩”带来的成本和稳定性风险,真正实现了弹性计

算的“智能调度”和“按需供给”。

目前,吴立欣的这项专利技术已在多个行业和领域中投入使用,产生了积极而广泛的影响,获得了企业用户和技术同行的高度评价。在电商、在线教育、金融科技等对高并发、高可用性要求极高的行业场景中,通过部署智能化弹性伸缩方案,企业能够根据业务负载的实际波动灵活调整计算资源。例如,AHPA 方案能够根据历史时序数据进行主动预测,提前扩容,避免弹性滞后,并根据实时数据动态调整预测结果,兼容周期变动等场景,这种策略显著提升了系统的响应速度和运行效率。根据多个企业的反馈,采纳该方案后,企业不仅有效规避了因资源不足导致的系统拥堵和服务中断问题,还成功避免了过度扩容引发的资源浪费。通过实施资源动态调配和技术创新,企业显著降低了资源冗余成本,同时,通过流程再造和持续改进,实现了服务效率的提升和 SLA 达标率的稳步增长。随着该技术的不断推广和深化应用,其影响力正持续扩大,逐步成为云计算资源管理领域的技术新范式。

吴立欣不仅是技术创新的践行者,更是理念的传播者和行业变革的推动者。他



高级云计算工程师吴立欣 ■ 受访者供图

常说:“技术的真正价值不在于参数的堆砌,而在于是否能实际性地服务于业务、服务于人。”在未来,随着云计算不断向智能化、自主化方向发展,云平台的资源配置与调度机制,将在智能化、自主化的浪潮中迎接更多未知的挑战。

谢添

创新杂谈

人工智能浪潮奔涌向前,带来前所未有的发展机遇,也带来不容忽视的风险挑战。“声音克隆”导致电信诈骗防不胜防,“换脸视频”引发的造谣诽谤时有发生,“AI 幻觉”让生成内容真假难辨……今天,技术的“双刃剑”效应愈发具象化。经济合作与发展组织数据显示,2024 年 AI 风险事件总数比 2022 年增加了约 21.8 倍,并呈快速发展态势。

有人认为,当下正值 AI 抢位发展关键期,不应做过多限制;有人则觉得,技术问题会随发展自行得到解决,不必过早干涉。其实不然。要看到,一方面,“先放手后治理”,可能让“小风险”逐步叠加,变为“大问题”,治理代价会更大;另一方面,规范并不等于“设限”,如果放任技术沿着有违公序良俗、有悖产业规律的方向狂奔,有可能导致错失发展良机。重视 AI 安全,不是给这辆车疾驰向未来的列车套上枷锁,而是铺平轨道,让其沿着健康可持续的方向,跑得更快、更稳。

习近平总书记指出:“要把握人工智能发展趋势和规律,加紧制定完善相关法律法规、政策制度、应用规范、伦理准则,构建技术监测、风险预警、应急响应体系,确保人工智能安全、可靠、可控。”落实好这一重要要求,才能平衡技术发展与安全,推动人工智能更好造福社会。

技术每前进一步,治理就要跟进一步。时时有边界,技术方能在合理框架内有序前行,不越界;规矩跟得上,技术才会在正确轨道上稳健发展,不逾矩。技术发展的历程,也应是政策法规不断完善的过程。

持续织密安全防护网,既要为发展划定红线,也要为创新留足空间。从发布《生成式人工智能服务管理暂行办法》,实行包容审慎和分类分级监管;到公布《互联网信息服务深度合成管理规定》,要求给相关 AI 内容“进行显著标识”;再到印发《人工智能生成合成内容标识办法》,推进从生成到传播全链条治理……近年来,以网络安全法、数据安全法等为依据,AI 领域的政策文件不断出台,推动人工智能治理沿着法治轨道向前迈进。始终跟随技术前进的步伐动态完善政策法规,方能实现促进发展和依法管理的有机统一。

企业是推动人工智能发展的重要力量,也是直面用户的第一道安全防线,必须担负起主体责任。人工智能技术日新月异,但无论形势如何变化,情况如何复杂,“技术向善”应始终是企业追求的原则。从生成式人工智能为例,腾讯宣布,对违规“AI 洗稿”发文行为的主体进行限制和清理;抖音明确,对不当利用 AI 生成虚拟人物的内容严格处罚;今日头条披露,2024 年处理低质 AI 内容超 93 万条。企业“立规矩、明边界”,既有效防范了风险,也促进了生成式人工智能健康发展。企业增强责任感,不断拧紧“安全阀”、系紧“安全带”,确保技术进步服务于人、造福于人,才能在激烈市场竞争中赢得信任和支持。

发展的问题要靠发展来解决。以技术对技术,以技术管技术,才能真正筑牢安全的底线。针对 AI 造假,合合信息推出新型检测技术,可捕捉图像篡改过程中留下的细微痕迹,慧眼辨伪;面向网络诈骗,浙江一团队开发“电子标识”,嵌入的音视频若被用于 AI 加工,就会触发“引信”,破坏生成后的内容;奇富科技研发智能风控系统,2024 年发布 AI 反诈提醒 13.8 万次,劝阻潜在被骗者超 2.9 万人。善用“技防”,以技术之盾抵御技术之矛,“通过魔法打败魔法”,安全防护会更及时,更智能、更高效。

在规范中释放活力,在创新中筑牢防线,这是保障人民群众合法权益的必需,也是推动我国人工智能健康有序发展的必然。

王可心:于钢轨之上 见证时代奔腾

(上接 A1 版)300 多个日日夜夜,手绘图纸近百张,数千次整机调试,多少次因为切割碳纤维,粉屑沾到皮肤上又疼又痒,多少次在隧道内爬高走低,身上磕得青一块紫一块……直至 2022 年 8 月,随着爬行试验取得突破,第 1 代“铁航”混凝土质量检测机器人终于研制成功,王可心与团队相拥而泣。如今,“铁航”混凝土质量检测机器人已升级至第 8 代,突破了隧道环向检测的技术瓶颈,经鉴定总体达到了国际领先水平。当“铁航”系列产品亮相亚欧博览会时,很多外国同行惊叹:“中国基建正在重新定义行业标准!”

然而,王可心并未止步于此。2025 年,第一台钢拱架智能生产流水线在宁夏正式交付。钢拱架是一种由型钢制成的拱形结构,被广泛应用于隧道、桥梁、煤矿及地下工程等领域。然而传统钢拱架生产主要依赖人工操作和半自动化设备,存在生产效率低、质量不稳定、成本高等诸多问题。

“刚开始我们联系了相关厂家,希望能作出改进,但调整后的设备与我们的现场需求总是不能很好地契合,而且加工费、改装费动辄都要上百万元。”王可心说,“正好我们也在做科研产品,不如自己研发一款。”

当时国内制作相关生产流水线的企业有十几家,为了摸清情况,王可心把这些企业都跑了一遍。回来以后,他迅速成立调研攻关小组,并深入一线了解工人们的需求。“现在的设备有哪些用得顺手的地方”“生产出的碳钢管材兼容度怎么样”……每个细节,王可心都仔细询问。正是有了前期详细的调研,2 个月后续的研发顺利进行。

2025 年 5 月,钢拱架智能生产流水线一经投产,就带来了显著效益,单班作业人员从 6-8 人减至 1-2 人,智能生产流水线可以昼夜无休运转,人工成本降低 80%,废品率趋近于零。

时间的长河奔涌向前,奋斗的脚步永不停歇。这些年,王可心潜心钻研,一项项科技成果在他手中诞生。问及一路走来最大的感悟是什么,他爽朗一笑,说:“我始终认为只要在自己的岗位上踏实肯干、坚持到底,所有的付出终会有所收获。”

从普通技术员到科技分公司的掌舵人,王可心始终怀着这样的坚定信念做事。繁忙的工作之余,他每天总要留出 1-2 小时用于学习,出差皮箱里 2/3 的地方都是专业书籍。通过坚持学习,他考取了注册土木(岩土)工程师、结构工程师等含含金量的职业证书。

新时代为每个人提供了无比广阔的人生舞台。王可心用实际行动告诉大家:只要有坚定的理想信念、不懈的奋斗精神,坚持把每一件小事做好,终会实现自己的梦想,成就不平凡的业绩。

拧紧新技术发展的『安全阀』

■ 常普