

硅基“车圈欢姐”原型更期望人机共生

► 本报记者 李洋



受访者供图

在南京天沃红旗体验中心, AI车圈总经理“车圈欢姐”正在为用户答疑解惑。

“车子出了事故,请问定损和做漆的费用要怎么算?”“车子没电了,请问可以安排上门救援吗?”面对用户提出的一系列问题,南京天沃红旗体验中心不久前上线的 AI车圈总经理“车圈欢姐”,总能迅速给出专业解答。

无独有偶。4月1日,武汉理工大学继 2023 年率先探索并发布国内首个 AI 校长助理后,再度推出 AI 校长助理 2.0 版本,并同步推出包括 AI 人事助手、AI 科研助手、AI 宣传助手等在内的“AI+教育”智能体矩阵。4月25日,饿了么推出 AI“小饿”,蓝骑士们有了智能 AI 助手。

凭借高效、智能、便捷的特性, AI 助手正逐渐成为人们日常生活与专业领域中不可或缺的伙伴,推动着各行业的智能化变革。

AI 赋能 服务模式变革

“车圈欢姐”的硅基分身由南京硅基智能科技有限公司以南京天沃红旗体验中心总经理高欢为原型打造, 1:1 复刻真人的形象与声音, 并通过大模型学习了红旗品牌相关的知识库, 可与用户进行实时交互。

而现实生活中, 高欢有着 12 年汽车 4S 管理经验, 从基层员工成长为 4S 店的总经理, 在内训师、人事和客服等岗位上工作过, 从销售冠军到全国销售技能大赛十五强, 从江苏省优秀销售总监到全国优秀总经理。

“我总在深夜幻想: 若有平行时空的另一个我, 该多好。如今, 我在云端复刻了十几年的职场基因库——这个硅基分身献给并肩工作的同事、信任的客户, 以及每个在暗夜赶路的职场

人。”南京天沃红旗体验中心总经理高欢在接受记者采访时说。

不仅是汽车圈, 当下 AI 技术正以前所未有的速度渗透各个行业, 催生出一系列令人瞩目的创新应用。

作为国内首个基于大模型技术打造的骑手端智能体, 饿了么推出的 AI“小饿”凭借自然语言处理、多模态交互及实时数据分析能力, 全面覆盖骑手配送场景。只需一句“小饿小饿”的呼唤, 骑手就能通过语音完成接单、确认到店等操作, 不仅减少了手动点击步骤, 还提升了操作效率。同时, “小饿”能实时分析骑手位置、订单状态及环境数据, 主动推送权益提醒、天气预警、路线及封路提示等信息, 基于历史数据和订单热力图, 为骑手提供接单策略优化建议, 有效降低配送风险, 助力骑手提升收入。

“您好, 我是门头沟区检察院 AI 法律助手‘门小检’, 请问有什么劳动纠纷问题需要咨询?” 在北京市门头沟区东辛房街道党群服务中心变身科技秀场, 大屏上跃动的“智检速答” AI 助手不仅能秒回欠薪追讨、工伤认定等高频问题, 还能根据咨询内容

智能推送维权指引。

从外卖配送、汽车销售服务到法律咨询服务再到校园管理, AI 助手的身影无处不在。

AI 虽强 短板仍存

帮助客户从如何选购一辆适合自己的汽车, 到如何使用车辆全部功能, 再到车辆出现故障处理, 与市面上传统直播带货数字人相比, AI 车圈总经理“车圈欢姐”有着无可比拟的优势。高欢说: “其他数字人提供的多是通识性回答, 而我们的‘车圈欢姐’扎根汽车领域特别是红旗品牌, 由此客户问的问题, 它能给出更深度、更专业的解答, 不像网上搜索到的信息那么碎片化。此外, 它也是我们员工的‘移动知识库’, 销售顾问如果想了解车型参数, 直接问它就行。”

尽管 AI 助手在各行业展现出诸多优势, 但要完全替代人工客服, 仍面临诸多挑战。

高欢认为, AI 助手尽管部分地具备情绪识别功能, 但在面对复杂情感时, 其回应往往显得生硬、机械, 难以真正与客户产生情感共鸣, 容易导致客户体验下降。

“人工客服有着不可替代的灵活性, 能敏锐感知客户情绪, 如, 客户问了一个知识库没覆盖的问题, 人工客服就能灵活应对, 还能根据客户语气语调调整沟通方式, 这是目前 AI 做不到

的。”高欢表示。

人机协作 未来所向

AI 助手的出现是行业发展的必然趋势。然而, 短期内 AI 助手完全替代人工客服并不现实。

业内人士认为, 在未来的服务领域中, 人机协作将成为主流模式, 为人们带来更加优质、高效的服务体验。当用户的问题超出 AI 助手的处理能力范围时, 智能系统可以自动将问题转接给人工客服。人工客服在处理问题的过程中, 还可以将新问题和处理经验反馈给 AI 助手, 帮助其不断学习和优化, 提升服务能力。通过这种人机协作模式, 不仅可以提高服务效率, 减少客户等待时间, 还能提升服务质量, 增强客户满意度。

谈及引入“车圈欢姐”的初衷, 高欢直言与行业现状紧密相关: “现在行业越来越‘卷’, 经营成本不断上涨, 我们想通过 AI 数字人的方式助力门店降本增效。”她期望通过智能服务与人工服务的协同, 实现服务团队的高效运转。

此外, 作为红旗品牌经销商, 南京天沃红旗与硅基智能的合作也承载着服务创新的使命。“很多人对红旗经销商及品牌的印象还停留在过去, 我们希望通过拥抱人工智能, 传递品牌服务与时俱进的形象。”高欢说。

当 AI 攻防战在云端打响

► 本报记者 李争粉

当旅行者将拍摄的雪山星空同步到云相册时, 当智能家居摄像头通过云端向千里外的手机传输画面时, 在数据流动的每一毫秒, 或发生或暗藏着一场攻防战。

攻击者用 AI 生成足以乱真的钓鱼邮件, 利用大模型漏洞窃取医疗数据; 防守者则训练 AI 成为“鉴谎师”, 给算法穿上“防弹衣”——这场发生在数字世界的“猫鼠游戏”, 正因云安全技术的革新, 悄然改写胜负天平。

“黑客利用 AI 批量生成钓鱼邮件, 我们就用 AI 识别并防御其带来的风险。”天融信科技集团副总裁李玮近日接受采访时, 向记者展示了一封几近完美的伪造邮件: 措辞严谨的采购需求、格式规范的合作附件, 甚至发件人邮箱前缀都与某三甲医院的真实合作方仅差一个字符。但在天融信的“天问大模型+钓鱼识别小模型”双引擎下, 智能系统仅用 2 秒钟即拆解出邮件中的多重破绽, 拦截含木马的

“医疗设备采购清单”, 避免了电子病历数据泄露。

“现在云上的应用都在做智能化改造, 对云环境不仅要考虑云上的安全风险, 同时也需要考虑大模型引入所带来的新安全风险。”李玮说。

据了解, 目前, 天融信基于自主研发的“天问大模型”安全中枢, 构建了“大模型研判+小模型检测”智能架构, 成功实现了威胁检测能力跃升、策略响应效率质变、安全运营成本降低等多项技术难题的破解。例如钓鱼邮件识别准确率提升至 96%, 较传统规则引擎效率提升 5 倍; AI 驱动的微隔离策略生成, 将云环境安全策略配置时间从 8 小时缩短至 15 分钟, 策略验证周期压缩 70%; 通过自动化威胁处置闭环, 企业安全运营人力成本减少 60%, 威胁平均响应时间降至 2 分钟。

技术突破正在转化为守护数字世界的坚实盾牌。

“天融信智算一体机内生安全防护系统, 可集成容器安全、API 防护等 8 类安全能力, 实现大模型从数据集清洗到推理服务的全链路防护; 大模型安全防护网关能够有效应对提示词注入、模型滥用等风险, 覆盖站点安全、API 调用安全及合规管理等场景, 项目中累计拦截提示词注入攻击 5 万+次, 防护 API 调用超 100 万次。”李玮介绍道。

目前, 天融信云安全产品和解决方案已深入政府部门、医疗、能源等八大领域, 为 1500 余家政企客户筑起安全防线, 在数字经济高速公路上架起 AI 哨岗。

“当黑客按下回车键时, 我们的 AI 已经预演了多种可能的攻防路径, 并自动生成防御方案。”李玮用比喻揭示了一个事实: 在云端安全的新纪元, 人类与 AI 共同编写的算法正成为数字文明最坚固的基座, 守护每一位公民的“云上生活”。

本报讯 4月27日, 北京人工智能产业生态创新发布会在北京经济技术开发区(以下简称“北京经开区”)通明湖会展中心举行。

发布会上, 北京市经济和信息化局发布《北京市关于支持信息软件企业加强人工智能应用服务能力行动方案(2025年)》, 提出 MaaS(出行即服务)企业、在京集聚发展、支持通用智能体发展、实施软件企业智能技改工程等 8 条支持措施。

北京经开区发布《关于加快建设全域人工智能之城的实施方案(2025)》, 紧扣北京经开区全域人工智能之城发展蓝图, 采取“一模一案、一业一策”推进机制, 布局基础能力支撑、核心产业集群、数据汇聚流通等五大方面 30 项具体行动计划, 并将提供总计不低于 10 亿元专项政策资金。

在聚焦创新策源生态共建环节, 北京经开区“产业人工智能赋能中心”正式发布。该中心依托北京人工智能数据训练基地基础能力, 围绕行业模型落地的核心流程, 提供“数算模用”一站式服务, 打造“算力广场、数据商城、模型超市、调优工厂”四大服务平台。

在 AI 开源开放生态共创环节, 北京经开区开源人工智能社区“模力方舟”发布, 将为全球开发者提供异构算力、模型托管、应用开发等全生命周期服务。与此同时, 国内最大研发效能平台、最大开源代码托管平台 Gitee 正式落地北京经开区, 并同步启动国际开源人工智能创新大赛, 支持开源项目培育转化。

刘琴

北京举行人工智能产业生态创新发布会