银行“下注”DeepSeek大模型 数据隐私和幻觉问题待解

蛇年春节前后,DeepSeek公司推出旗下包括V3大模型、R1大模型等一系列大语言模型,较市面上已有的大模型,其训练成本更低,引起了“狂卷”大模型的银行机构的注意。记者发现,邮储银行、北京银行、重庆银行、江苏银行、苏商银行、重庆农商行等多家银行机构近期纷纷完成了DeepSeek的本地化部署。

业内人士表示,当下银行业对大模型的应用主要是为了建立内部使用的助手,以提高员工的办公效率。在银行业竞相接入大模型的当下,将有更多银行机构探索与DeepSeek公司合作,接入V3大模型、R1大模型等一系列大模型。对于银行来说,在接入最新大模型提高效率的同时,还要注意数据安全、信息泄露、文本幻觉等风险。

图片来源:视觉中国

银行探索多场景应用

从智能风控、个性化服务、网点运营,再到多种远程服务,银行与DeepSeek的合作正向多场景应用拓展。

邮储银行2月8日透露,通过本地部署的方式,旗下“邮智”大模型集成了DeepSeek-V3模型及轻量级的DeepSeek-R1推理模型。邮储银行率先将DeepSeek大模型应用于“小邮助手”,实现了以下创新突破:一是新增逻辑推理功能,显著提升精准服务效能;二是通过深度分析功能,能够更精准地识别用户需求,进而提供个性化、场景化的服务方案;三是凭借高效的推理性能,大幅加快响应速度和任务处理效率。

借助DeepSeek的技术能力,邮储银行布局多金融场景特色化服务,例如,在远程银行服务领域,通过引入多步骤推理优化能力,进一步强化手机银行的陪伴式数字员工功能,同时对坐席助手和智能陪练系统进行优化升级,从而显著提升客服的专业性与工作效率。

“我行与华为紧密合作,成功引入并部署了DeepSeek系列大模型。目前,该模型已在AIB平台的京行研究、京行智库、客服助手、京客图谱等多个核心业务场景中开展试点应用,显著提升了基于知识驱动的大模型服务质量和效率。”北京银行人士表示。

江苏银行在其数字金融官微发布公告称,该行已应用DeepSeek大语言模型。公告提到,依托“智慧小苏”大语言模型服务平台,该行本地化部署微调DeepSeek-VL2多模态模型、轻量DeepSeek-R1推理模型,分别运用于智能合同质检和自动化估值对账场景。

江苏银行人士表示,通过应用R1推理模型,结合邮件网关解析处理能力,实现邮件分类、产品匹配、交易录入、估值表解析对账全链路自动化处理,识别成功率达90%以上,目前已初步实现业务集中运营,按照平均手工操作水平测算,每天可节约9.68小时工作量。

重庆农村商业银行则宣布在其企业微信上线基于DeepSeek模型的智能助手应用“AI小渝”,未来将应用在智能风控、场景金融、数据决策等场景中,实现构建分钟级响应的智能客服系统,结合知识库实现个性化财富管理建议等。

苏商银行人士向记者透露,该行凭借对DeepSeek系列模型技术的深度整合,打造了“数据算法、算力、场景”四轮驱动的智能决策系统。目前,该系统已在信贷风控、反欺诈监测等20多个业务场景中落地应用,尽调报告生成效率提升40%。

有望缩小“技术鸿沟”

近年来,银行为自研金融大模型投入了巨大资源,而中小银行则无法跟上大型银行接入大模型的步伐,其中的“技术鸿沟”越拉越大。业内人士认为,凭借DeepSeek较低的算力需求和训练成本,能为中小银行带来机会,有助于缩小与大型银行的技术差距。

DeepSeek的大模型技术具备强大的推理能力、高效的计算性能,推理成本又比较低,很适合在特定场景下实现高频调用和落地应用,为中小银行在人工智能领域的应用和发展提供了有力支持。”某城商行人士对记者表示。

根据浙商证券发布的研报,DeepSeek-V3大模型整个训练过程用了不到280万GPU(图形处理器)小时,相比之下,美国互联网巨头Meta发布的Llama3-405B的训练时长是3080万GPU小时。从训练成本来看,DeepSeek-V3约为557.6万美元,而OpenAI为聊天机器人ChatGPT发布的语言模型GPT-4的训练成本则达到数亿美元。

较低的训练成本为中小银行跨越“技术鸿沟”带来机会。上海金融与发展实验室主任、首席专家曾刚指出,DeepSeek为中小银行提供了一种高性价比的解决方案。首先,中小银行能够根据自身业务需求,灵活调整DeepSeek模型的参数和功能。其次,DeepSeek具备开箱即用的模型能力,中小银行无需投入大量资源进行技术研发,即可快速部署并应用大模型。最后,中小银行可以直接利用DeepSeek的成熟技术,快速上线智能风控、合同校验、客户洞察等功能,显著缩短从技术引入到实际应用的周期。

“未来,预计将有更多持牌金融机构加入AI升级的浪潮,通过提升传统金融业务的质效,进一步保障金融安全和用户资金账户的安全。”素喜智研高级研究员苏筱芮指出,DeepSeek模型具备多元化的应用能力,不仅在逻辑推理和自然语言处理方面表现出色,还能够实现高性价比的部署。人工智能大模型在智能营销、智能风控等多个细分场景中展现出广阔的应用前景。

不过,目前银行仍处于探索DeepSeek大模型技术应用的初期阶段。据记者了解,银行业对大模型的应用主要集中在内部场景,比如智能代码编写、内部AI办公、智能客服等中台运营管理,以此来提升员工工作效率,但并未涉及账户交易等核心业务的应用。

此外,虽然DeepSeek能够在一定程度上帮助中小银行缩小与大型银行在大模型应用方面的差距,但大型银行在资源投入、生态构建以及数据积累等方面的优势仍然十分突出。

数据风险、“幻觉”挑战

大模型技术提升银行工作效率的同时,可能带来的风险也不容忽视。最受关注的便是数据隐私与安全问题。“大模型的应用意味着要处理大量个人和企业的数据,增加了信息泄露的风险,客户的信息泄露后可能会被非法获取用于诈骗活动等,导致银行声誉受损。”有银行业人士对记者表示。

记者注意到,DeepSeek的隐私政策中包含电子邮件地址、电话号码、击键模式等个人隐私数据收集。近日,DeepSeek的ClickHouse数据库因配置错误而暴露,导致敏感信息泄露。该数据库暴露了超过100万条记录,涵盖聊天记录、API密钥、操作日志等高度敏感的信息,并且由于未配置身份验证机制,这些数据任何人都可以随意访问。随后,DeepSeek遭意大利个人数据保护局询问,并从应用商店下架。

上海段和段律师事务所高亚平律师认为,各国的监管机构正在加强对大模型数据处理活动的监督,但确保管理体系能够有效应对合规要求并非易事,在数据处理的完整生命周期中,AI算法、爬虫技术的使用,使得合规的技术目标变得难以捉摸,给大模型数据治理带来新的挑战。

“幻觉”问题是另一大挑战。记者注意到,目前已有使用者发现DeepSeek存在一本正经地“胡说八道”的情况。例如,在生成学术论文材料时,DeepSeek会生成不存在的材料,或指向无关的论文。业内人士对记者表示,大模型目前面临的“幻觉”问题,其主要根源在于训练数据的污染。

清华大学计算机科学与技术系教授孙茂松认为,尽管生成式人工智能在生成流畅文本方面表现优异,但由于缺乏真正的理解能力,在数据匮乏或信息不明确的情况下,可能会生成不准确甚至虚假的内容。“幻觉”在高精度任务中可能会带来严重的限制。

上述金融业人士表示,在金融领域,由于对数据精度的要求极高,同时需要确保模型的可解释性以及严格的风险控制,金融机构在应用大模型时往往表现得较为谨慎。

在北京大学智能学院教授王立威看来,大模型的“幻觉”现象是一种内在特性。当前的大模型主要通过从海量数据中学习来构建其能力,本质是一种基于统计的方法。由于这种方法是基于统计规律而非逻辑推理,因此无法保证输出结果100%准确。

“为解决这一问题,一方面需要从软件工程的角度出发,优化算法,提升数据质量,从而提高大模型的精度;另一方面,也需要通过制定行业规范和法律法规,对大模型技术加以约束和引导,使其能够更加安全、可靠地服务于经济社会的发展。”某国有大行金融科技业务部人士建议。 (一财)