

智能体技术演进：场景分析、 关键技术与发展趋势

姜春宇, 韩晓璐, 王超伦

中国信息通信研究院, 北京 100191

摘要

当前, 基于大模型的智能体技术正经历爆发式演进, 其开发、协作与全生命周期管理已成为产业核心议题。结合行业实践, 提炼了典型应用场景, 深度解析了智能体开发和通信涉及的关键技术, 提出了一套完整的智能体研发及运营能力框架, 最后展望了智能体发展趋势。

关键词

智能体; 智能体应用; 智能体开发平台

中图分类号: TP311.13

文献标志码: A

doi:10.11959/j.issn.2096-0271.2026001

Evolution of agent technology: scenario analysis, key technologies and development trends

Jiang Chunyu, Han Xiaolu, Wang Chaolun

China Academy of Information and Communication Technology, Beijing 100191, China

Abstract

Currently, LLM-based agent technology is experiencing explosive evolution, and its development, collaboration, and full lifecycle management have become core issues in the industry. Based on industry practices, this article identifies typical application scenarios, conducts an in-depth analysis of the key technologies involved in agent development and communication, and proposes a comprehensive framework for the development and operation of agents. Finally, it explores the future development trends of agents.

Key words

AI agent, agent application, agent development platform

0 引言

智能体（agent）的概念来源于哲学，描述具有欲望、信念、意图和行动能力的实体。后来智能体概念被引入人工智能领域，用于表达能够感知周围环境、作出决策、开展行动的计算实体。其发展经历了5个阶段，即符号智能体、反应智能体、基于强化学习的智能体、具有迁移和元学习能力的智能体、基于大模型的智能体^[1]。在大模型爆发之前，智能体就在计算和仿真领域得到了广泛应用。

近年来，以 GPT4、DeepSeek R1、Llama 为代表的大语言模型（简称大模型）技术取得了较大进展，通用大模型具备泛化能力强、知识覆盖广泛且准确的特点，能够处理多模数据，具备语义理解和生成能力，在语言、内容生成、自动驾驶、气象预报、数学推理等多个方面取得重大突破。尽管大模型在数据处理、复杂模式理解、内容生成方面表现出色，但它们是“静态”的，既无法整合新的信息，也不具备直接与外部世界交互并执行具体任务的能力。而智能体则是能够在环境中自主运行，并根据环境变化作出决策的系统。在处理复杂任务时，智能体通常利用多种外部工具，特别是实时数据源来弥补大模型训练数据更新滞后问题^[2]。对比来看，大模型更像是“大脑”，提供知识处理能力；

智能体偏向于“身体”，协调各种资源来实现目标。二者结合使智能体具备较好的学习和迁移能力，同时增强了智能体的泛化能力。

本文对基于大模型的智能体概念进行了定义，梳理了其核心组成；对典型的智能体应用进行了总结和分析，梳理了智能体开发、通信方面最新技术发展情况，并提出了一套企业进行智能体开发、运营、管理的体系框架；最后展望了智能体的5个发展趋势。

1 智能体定义

1.1 智能体的定义和特点

基于大模型的智能体是能够感知环境、自主规划、进行决策和执行动作以实现目标的人工智能系统，具有自主性、交互性、适应性等基本特征。大模型（如 GPT-4、Llama 等）是智能体的核心，承担了智能体的大脑角色，为智能体提供了感知和行动能力^[1]。**表1**梳理了3个模块详细的功能和具体内容。

大模型是智能体的大脑，提供自然语言交互、知识存取、记忆管理、推理和泛化能力。大模型在自然语言交互方面表现较好，具备多轮对话和高质量内容生成的能力，但在意图理解方面还有一定的提升空间，尤其是面对模糊指令或隐含信息

表1 基于大模型的智能体核心模块

模块	功能	具体内容
大脑	承担记忆、信息处理与决策	由大模型构成,具备自然语言交互、知识存储与检索、记忆管理、推理、泛化学习能力
感知	获取和处理多模态的信息	能够输入文本、视觉、听觉等多种信息
行动	使用工具与环境进行交互	具有基本的文本输出和工具使用能力,具备具身行动能力

时,可以将隐含意义形式化为一个奖励函数,使大模型在新场景中选择符合用户偏好的选项^[3]。在知识存取方面,大模型存在知识过时、错误和生成内容“幻觉”等挑战。一方面,可以通过编辑大模型来修改模型内部存储的特定知识来解决过时和错误的知识问题;另一方面,可以通过检索增强生成(retrieval-augmented generation, RAG)等技术来避免“幻觉”问题。在记忆管理方面,基于大模型的智能体面临历史记忆长度受限和记忆提取困难等挑战,可以采用提高大模型的最大长度限制或者采用记忆摘要的方式来提升记忆的能力。

对于智能体来说,从环境中感知各类信息至关重要,感知能力能帮助智能体更好地理解环境、作出明智决策。大模型使智能体具备多模态感知能力,包括文本、视觉和听觉和其他输入形式。目前,大模型在文本处理方面表现较好,但在视觉和听觉方面还面临不少挑战。在视觉方面,一方面直接输入图-文对数据,能够帮助智能体直接理解图像中的含义;另一方面,将图像编码器与大模型结合,通过优化大模型的图像处理能力,可提升智能体的视觉感知能力^[4]。在音频处理方面,可以通过音频频谱图等形式优化大模型,并以大模型为控制中枢,调用其他工具来增强对音频信息的感知^[1]。

在智能体的构建中,行动模块接收来自“大脑”模块发送的动作序列,并执行相应的动作与环境互动,主要的行动能力有文本输出、外部工具的使用和具身行动。大模型赋予了智能体优秀的文本输出能力,而外部工具的使用能够补充大模型专业知识不足、透明度不够的劣势,具身行动使智能体可以直接与物理世界进行交互,扩大了智能体的行动空间。

1.2 智能体架构设计

基于大模型的智能体,其核心能力来自于大模型,除此外还应该具备3个核心能力:记忆能力、规划能力和行动能力^[5]。

规划能力在管理活动和促进明智决策方面发挥着关键作用,其核心能力分为任务分解和反馈驱动的迭代优化能力。它使智能体能够将复杂的任务分解为更小、更易于管理的子任务,并制定有效的实施策略,在实施过程中能够不断反思和改良,从而优化最终结果^[6]。任务分解能够将复杂的任务分解为更小、更易于管理的子任务,并制定有效的实施策略,主要的任务分解策略有单路径链式分解和多路径树状扩展^[7]。单路径模式主要有3类实现:第一类是零样本思维链方式,将任务拆解为一系列相互依赖的子任务,然后按顺序依次执行子任务,但存在灵活性不足的问题;第二类是动态规划方法,允许智能体接受环节反馈调整计划,根据当前状态生成下一个子任务,从而增加鲁棒性;第三类方法是采用多个思维链来提高规划过程的稳定性^[8]。多路径模式采用树状结构规划数据,在规划过程中允许多个可能推理路径的存在,并可以根据反馈回溯到之前的状态。反馈驱动的迭代优化是规划能力的重要组成部分,使智能体能够从反馈中学习并随着时间推移不断提升其性能。反馈来源多样,包括环境输入、人类指导、模型内省和多智能体协作等^[7]。

记忆可以被定义为用于获取、存储、保持信息,并在之后检索信息的过程,记忆能力对于信息的存储和检索至关重要,它使智能体的交互具备上下文感知能力^[5]。类似人类记忆,智能体记忆结构分为短期、长期两种。短期记忆保留智能体内部的对话历史和环境的反馈信息,用来支持上下文敏感的任务执行。长期记忆系统地存储

智能体中间推理过程，并将这些信息合成为未来可重用的工具，主要通过技能库、经验库、工具合成框架3种范式来实现^[7]。智能体与环境之间的交互是通过3个关键的记忆操作来实现的：记忆读取、记忆写入和记忆反思^[9]。当智能体感知到信息后，其中的关键信息会通过记忆写入操作存储在数据库中，有的智能体系统设计了记忆控制器来决定何时执行写入操作，有的完全由智能体自主完成^[10-11]。当智能体需要进行推理与决策时，记忆读取操作将从存储中提取相关信息，由于记忆信息庞杂，如何设计读取机制，依据相关性和任务导向提取有用信息成为关键。有的智能体体系通过SQL语句来读取记忆；有的利用向量库作为记忆池，通过获取与当前任务相似度最高的轨迹来提取信息^[12]。记忆反思主要模拟人类大脑的工作机制，对记忆信息进行不断的加工和抽象，生成更高层次的信息。有的智能体系统将对话内容处理并提炼为日常事件的高层次摘要，并不断评估优化知识，形成每日洞察；有的智能体能够根据环境反馈对自己的记忆进行优化^[13]。

行动能力负责将智能体的决策转化为具体结果。行动模块需要关注4个方面的内容：行动的目标、行动是如何产生的、有哪些可用的行动以及行动会产生哪些影响。智能体执行的行动通常可以分为使用

外部工具和利用大模型内部知识，外部工具主要有调用外部API、集成外部数据库或知识库、调用外部大模型等。

2 智能体应用

2024年第四季度到2025年初，智能体产业迎来快速发展，大型科技巨头和人工智能明星创业企业均布局智能体领域，推出多款功能强大的产品。科技巨头通过“智能体-开发平台-通信协议”来构建智能体生态。比如，谷歌近期发布Deep Search智能体，升级Astra、Mariner等多款智能体，开源多智能体协议A2A(agent to agent)。初创公司致力于研发显著提升生产效率的智能体应用，比如OpenAI的研究智能体Open Research、Cursor Lab的代码智能体Cursor、Monica的通用智能体Manus。

基于当前技术发展和行业实践，智能体可按照服务对象分为面向个人用户(2C)和面向企业用户(2B)两大类(见表2)，其核心差异在于服务场景的复杂度、技术深度及用户需求特性。

个人智能体主要面向个人用户，覆盖生活、娱乐、办公等高频场景，强调便捷性与个性化，其中通用智能体擅长完成跨

表2 面向个人用户智能体与面向企业用户智能体差异比较

对比项	个人用户智能体(2C)	企业端智能体(2B)
技术重点	自然语言交互、轻量化部署	领域模型微调、多工具集成
数据来源	用户行为数据、开放知识库	企业私有数据和知识库
价值目标	提升用户生活效率与体验	优化业务流程,提升办公效率和决策能力
典型应用方向	生活助手、知识管理、效率工具、娱乐与社交	数据分析、决策支持、流程自动化、客户服务、营销、客服
典型应用	Manus、Deep Research、Cursor	字节跳动Data Agent、协和医院Med Agent

领域多类任务，专用智能体聚焦垂直领域，解决特定的问题。以 OpenAI 的 Deep Research 为例，它是一个研究类的专用智能体，采用单智能体架构，能够在 5~30 min 内搜索、解读并整合海量在线信息，生成专业级的研究报告。Deep Research 基于优化版 o3 模型，通过端到端强化学习训练，使系统可以模拟人类研究者的决策过程，能够拆解任务，对执行过程进行动态调整，以及验证结论的可靠性^[14]。Deep Research 的方案实现有 3 个重要进步：一是动态自适应地迭代研究工作流程，能够在任务执行中不断优化自身策略；二是强化了上下文记忆能力和多模态信息处理能力，能够有效整合多种信息来源；三是全面的工具集成能力，能够生成高质量的报告^[15]。Manus 是由中国团队 Monica.im 于 2025 年 3 月推出的全球首款端到端执行型通用智能体，其具备从规划到执行全流程自主完成多种任务的能力，如旅行规划、市场研究、商业决策、金融分析等。Manus 采用了典型的多智能体体系架构，该架构由多个交互的智能体组成，每个智能体都有其独有的能力和目标，都能够感

知、学习环境、作出决策并行动。智能体间通过信息共享和任务分工机制来协同工作，以完成更复杂的任务^[16-18]。

企业端智能体聚焦企业降本增效与决策优化，需深度适配行业知识与业务流程，强调精准性与可扩展性。根据不同的行业，企业端智能体还可以根据行业属性进行细分，比如金融业、通信业、医疗业智能体。以金融行业为例，金融智能体主要分为生成、识别和推理三大方向，生成类智能体能够支撑金融机构实现营销内容自动化、交互式报告生成等目的，识别类智能体能够支撑风险信息识别、合规与反欺诈监测、信用评估等场景，推理类智能体支撑金融机构动态风险管理、智能体营销等场景。典型金融智能体应用见表 3。除了金融领域，智能体在医疗领域也有广阔的应用前景，医疗智能体可以应用于临床诊疗支持、患者服务与管理、医院运营管理、药物研发、医学教育五大方面。例如北京协和医院研发的“Med Agent”智能体，为临床医生智能推荐医学量表，实现数据自填充、量表自评估，同时支持参考文献一键追溯和医学量表自动更新。

表 3 典型金融智能体应用

智能体类型	智能体	功能描述
生成类	交互式报告生成	整合宏观经济数据、行业动态一键生成专家级市场分析报告,辅助分析师完成投资策略报告
	营销内容自动化	结合客户画像与产品数据库,动态生成适配不同场景的营销素材
	财务分析	提供财务分析报告智能生成、衍生指标智能计算、财务情况智能分析等能力
识别类	风险信息识别	解析用户银行流水,识别高频彩票消费、异常交易等风险信号,结合收入负债评估信贷风险
	合规与反欺诈监测	实现合同条款解析与反洗钱规则匹配,识别违规操作
	信用评估	通过征信报告解读生成 40 万维风险变量,显著降低小微企业信贷风险
推理类	动态风险管理	在信贷审批中穿透式分析企业财务数据与宏观经济关联性,预测违约概率
	智能营销	提供营销需求识别、产品组合建议、营销方案创作、营销回顾管理等能力

3 智能体关键技术与管理体

智能体的构建与管理需以开发平台为技术底座，以通信技术为协作纽带，以全生命周期管理为可持续保障，三者协同驱动智能体从实验室原型向产业级应用跨越。

3.1 智能体开发平台

智能体开发平台是支持构建、训练、部署和协同管理 AI 智能体的综合性工具环境。其核心定位在于降低智能体应用开发门槛，通过集成大模型、工具链、知识库和可视化界面，帮助开发者快速实现从需求分析到成果交付的全流程智能化。根据行业的需求，可以将智能体开发平台分为两类：通用性开发工具和企业级开发平台。

通用性开发工具主要面向个人用户，通过可视化界面、预置模板，降低开发门槛，帮助用户快速构建轻量级的智能体应用，典型的产品有 Dify 和字节跳动的 Coze^[19-20]。其核心能力如下：一是低代码或零代码的开发能力，支持拖曳式工作流编排和预置模板，如 Coze 的电商客服模板，用户可通过自然语言指令快速生成应用原型^[20]；二是多模态交互和多模型兼容能力，形成文本、图像、音视频的输入输出能力，支持各类大模型的灵活切换；三是快速部署能力，能够一键发布到微信等终端，并内置各类插件。

企业级开发平台是针对复杂业务场景的深度定制化平台，强调与企业现有系统（ERP、CRM、数据平台、大模型平台等）无缝集成，提供高安全性、可扩展性和全生命周期管理能力，典型的产品有字节跳动的 HiAgent、蚂蚁集团的 agentUniverse、

百度千帆的 AgentBuilder。企业级开发平台主要关注业务系统的深度集成、全栈的智能体开发和管理能力，以及完备的安全管控能力。

根据对业界技术平台的调研和抽象，本文提出了企业级智能体开发平台的技术框架，其可以用于智能体平台的选型、评测和能力研发（如图 1 所示）。技术框架定义了企业级智能体平台的核心能力要求，包括数据接入及管理、模型接入及管理、插件开发及管理、工作流设计及管理、智能体研发、智能体管理、智能体市场、安全管理八大能力域，详细分为 28 个子能力。

3.2 智能体通信技术

智能体通信指的是智能体在完成任务的过程中，通过标准化的协议框架，与其他多样化元素进行多模态信息交换和动态行为协调的行为，并将结果返回给用户。根据通信对象不同，智能体通信可以分为 3 种类型：用户-智能体交互、智能体-智能体通信以及智能体-环境通信。

用户-智能体交互指的是智能体接收用户的指令，并将执行结果反馈给用户的过程，典型的协议有学习解释型智能体通信协议（PEX agent communication protocol, PXP）、空间群体协议、智能体用户交互协议（agent user interaction protocol, AG-UI）^[21-22]。PXP 的目的是在数据分析任务中构建一个用户与智能体交互的系统，主要面向科学、医学等应用场景。空间群体协议是一种分布式计算模型，主要解决物理空间中多个随机移动的计算单元（如机器人）分布式定位的问题。AG-UI 基于客户端-服务器架构，实现了用户与智能体之间的交互通信。

智能体-智能体通信是指两个或多个智

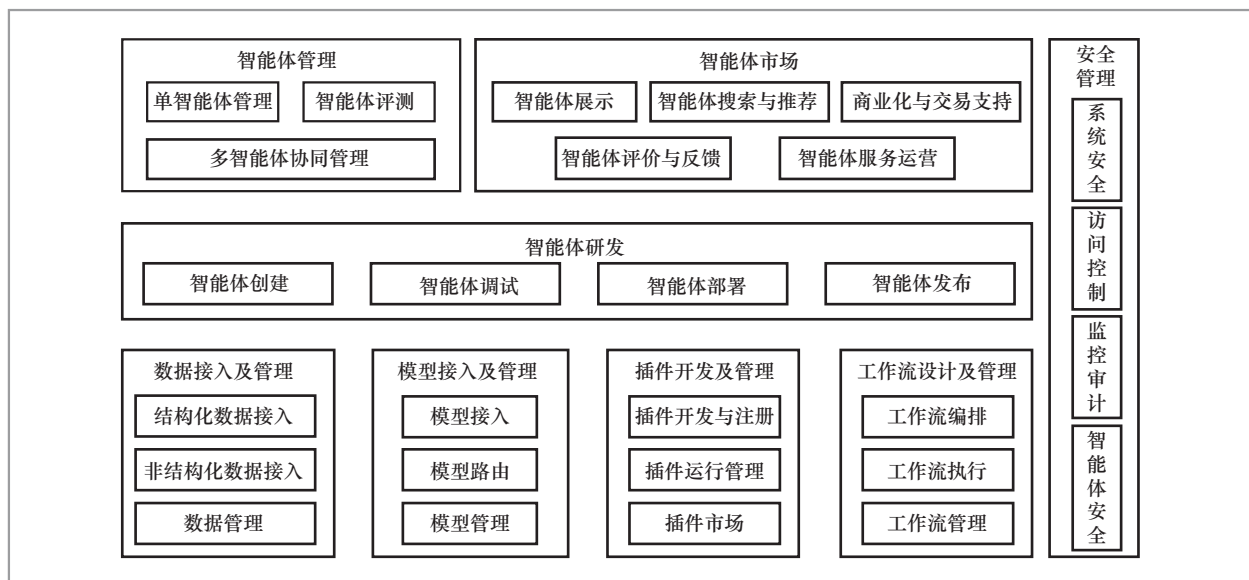


图1 企业级智能体开发平台技术框架

能体之间通过标准化协作协议进行协商、任务分解、子任务分配以及结果汇总，从而协同完成用户指定任务的过程^[22-23]。基于智能体发现机制的不同，目前的通信协议可以分为3类：客户端-服务器（CS-based）、对等网络（P2P-based）、混合型。客户端-服务器协议基于客户端-服务器架构的通信协议，依赖于集中式服务器来管理智能体的信息，典型的产品有ACP-IBM、ACP-AGNTCY。基于对等网络的通信协议通常使用全局标识符来支持智能体之间的搜索与发现，是一种去中心化的机制，其优势在于便捷的定位能力和全局搜索能力，典型的协议有智能体网络协议（agent network protocol, ANP）、Agora。混合型通信协议同时支持基于客户端-服务器和基于对等网络的智能体发现机制，基于不同场景能够切换策略，典型的产品有谷歌的A2A协议、语言模型操作系统（language model operating system, LMOS）协议。A2A协议由谷歌于2025年4月发布，其设计重点是实现不

同智能体之间的标准化通信，使它们能够跨平台、跨供应商和跨框架进行有效协作，解决了智能体之间能力发现、任务互操作和身份互信三大方面的问题^[24]。

智能体-环境通信指的是智能体通过一系列结构化的协议来调用外部工具、访问API并完成组合任务的行为，典型的智能体-环境协议有模型上下文协议（model context protocol, MCP）、函数调用（function calling）机制^[22]。MCP是Anthropic提出的一个开放标准，包含3个核心组件（主机、客户端和服务端），它制定了一套清晰的规则，指导模型和智能体查找、连接和使用外部工具，旨在解决智能体和外部工具连通性的问题^[25]。其中，主机负责客户端生命周期管理；客户端发现可用工具、生成结构化调用，并在任务执行过程中处理同步或异步响应；服务端是一个集中式的注册中心，主要负责维护工具的信息和工作流模板。总结来看，MCP有两个优点：首先，它是一个与模型无关的协议，不绑定任何大模型，能够兼

容市面上所有主流大模型，体现了一定的中立性和开放性；其次，它是标准化通信规范，开发者只需要按协议开发接口，即可被多个模型调用，实现“一次开发，全平台通用”的能力。

3.3 企业智能体开发运营体系

随着大模型能力的快速迭代、智能体开发框架的逐步完善，未来企业侧将产生海量专业智能体，并成为企业交互的核心入口，在智能体开发之外，它们的全生命周期管理将越发重要。然而智能体开发运营的理念刚刚开始，尚未形成体系化的方法，笔者参考软件领域 DevOps 体系，提出了 AgentOps 理念。AgentOps 是围绕智能体全生命周期（研发、交付、监控、运维、运营等环节）构建的系统性建设方法论，通过标准化流程、自动化工具链及跨职能协作机制，提升智能体开发效率、增强智能体运营稳定性、优化多智能体协同能力、促进智能体系统同业务场景的紧密耦合^[26]。AgentOps 核心关注 4 个方面的要点：一是研发的自动化，即构建敏捷、高效的智能体研发流水线，保证智能体快速的开发上线；二是行为的可观测性，即建立智能体全生命周期的可观测体系，及时发现智能体研发与运行过程的问题，快速解决问题；三是资源调度与编排，建设多智能体编排以及和外部系统间的协调能力，保障资源的有效利用；四是成本控制和效能度量，对各类智能体进行成本和效能的评价，减少无谓的支出。

4 结束语

2025 年被称为智能体元年，开年以来

Deep Research、Manus 等智能应用不断引领着智能体应用的创新，展现了良好的应用前景，让人们对智能体的落地充满了期待。同时智能体开发平台和通信协议在逐步完善，为智能体在个人市场和企业级市场广泛应用打好了基础。展望未来，智能体发展呈现五大趋势。第一，企业级专业智能体展现出巨大的发展潜力。为了充分利用这一潜力，企业不仅需要构建领域知识基础，还需要优化和梳理业务流程，并建立一套全面的智能体开发与运营体系。第二，大型模型能力的迭代升级成为推动智能体进化的核心驱动力。模型的进步能显著提升智能体的思考和规划能力，产业界需要致力于做好多模型适配工作，以确保不同应用场景下的最佳性能和适应性。第三，智能体生态系统的构建正逐渐成为行业发展的重要方向，特别是智能体通信协议成为业界关注的重点。目前，MCP 和 A2A 协议正在逐步演变为行业内的事实标准，这些协议的进步对于促进智能体间的高效协作至关重要。第四，相比单智能体，多智能体协作能更好地完成复杂任务，提升整体性能，多智能体推理框架和多智能体通信优化是业界关注的方向^[18,27]。第五，多模态大模型的发展提升了具身智能体的环境感知、长程任务规划、短程动作控制等能力，为实现具身智能带来新的曙光^[28]。

参考文献：

[1] Xi Z H, Chen W X, Guo X, et al. The rise and potential of large language model based agents: a survey[PP]. arXiv preprint, 2023, arXiv:2309.07864.

[2] 李述兴. 大语言模型驱动的智能体应用与挑战[J]. 科技视界, 2024(22): 67-70.

- Li S X. Application and challenge of agent driven by large language model[J]. Science & Technology Vision, 2024(22): 67–70.
- [3] Lin J, Fried D, Klein D, et al. Inferring rewards from language in context[C]//Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics. Stroudsburg: ACL, 2022: 8546–8560.
- [4] Lu J S, Clark C, Zellers R, et al. UNIFIED-IO: a unified model for vision, language, and multi-modal tasks [C]//Proceedings of the 11th International Conference on Learning Representations. [S.l.:s.n.], 2023.
- [5] Wang L, Ma C, Feng X Y, et al. A survey on large language model based autonomous agents[J]. Frontiers of Computer Science, 2024, 18(6): 186345.
- [6] Weng L. LLM powered autonomous agents[Z]. 2023.
- [7] Luo J Y, Zhang W Z, Yuan Y, et al. Large Language Model Agent: A Survey on Methodology, Applications and Challenges[PP]. arXiv preprint, 2025, arXiv: 2503.21460.
- [8] Wei J, Wang X, Schuurmans D, et al. Chain of thought prompting elicits reasoning in large language models[PP]. arXiv preprint, 2022, arXiv:2201.11903.
- [9] 胡伟, 姜晓夏, 邵洲天, 等. 大型语言模型智能体: 机制和应用的综述[J]. 指挥信息系统与技术, 2024, 15(6): 1–11.
- Hu W, Jiang X X, Shao Z T, et al. Large language model(LLM) agents: survey of mechanisms and applications [J]. Command Information System and Technology, 2024, 15(6): 1–11.
- [10] Packer C, Fang V, Patil S G, et al. MemGPT: Towards LLMs as Operating Systems[PP]. arXiv preprint, 2023, arXiv:2310.08560.
- [11] Wang B, Liang X N, Yang J, et al. SCM: enhancing large language model with self-controlled memory framework [PP]. arXiv preprint, 2023, arXiv: 2304.13343.
- [12] Zhang Z Y, Dai Q Y, Bo X H, et al. A survey on the memory mechanism of large language model based agents[J]. ACM Transactions on Information Systems, 2025: 3748302.
- [13] Zhong W J, Guo L H, Gao Q Q, et al. MemoryBank: enhancing large language models with long-term memory[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2024, 38(17): 19724–19731.
- [14] OpenAI. Introducing deep research[Z]. 2025.
- [15] Huang Y X, Chen Y H, Zhang H Z, et al. Deep research agents: a systematic examination and roadmap[PP]. arXiv preprint, 2025, arXiv:2506.18096.
- [16] MIT Technology Review. Everyone in AI is talking about Manus. We put it to the test[Z]. 2025.
- [17] Guo T C, Chen X Y, Wang Y Q, et al. Large language model based multi-agents: a survey of progress and challenges[C]//Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence. New York: ACM, 2024: 8048–8057.
- [18] Li X Y, Wang S, Zeng S Q, et al. A survey on LLM-based multi-agent systems: workflow, infrastructure, and challenges[J]. Vicinagearth, 2024, 1(1): 9.
- [19] Dify. Welcome to Dify[Z]. 2025.
- [20] Coze. Feature introduction[Z]. 2025.
- [21] Yang Y X, Chai H C, Song Y Y, et al. A survey of AI agent protocols[PP]. arXiv preprint, 2025, arXiv:2504.16736.
- [22] Kong D Z, Lin S, Xu Z H, et al. A survey of LLM-driven AI agent communi-

cation: protocols, security risks, and defense countermeasures[PP]. arXiv preprint, 2025, arXiv:2506.19676.

[23] Li G H, Hammoud H, Itani H, et al. CAMEL: communicative agents for “Mind” exploration of large language model society[C]//Proceedings of Neural Information Processing Systems 2023. [S.l.:s.n.], 2023.

[24] Anthropic. Introducing the model context protocol (MCP)[Z]. 2024.

[25] Google. A2A a new era of agent interoperability[Z]. 2025.

[26] Dong L M, Lu Q H, Zhu L M. AgentOps: enabling observability of LLM agents[PP]. arXiv preprint, 2024, arXiv: 2411.05285.

[27] 项凤涛, 罗俊仁, 谷学强, 等. 群视角下的多智能体强化学习方法综述[J]. 智能科学与技术学报, 2023, 5(3): 313-329.

Xiang F T, Luo J R, Gu X Q, et al. Survey on multi-agent reinforcement learning methods from the perspective of population[J]. Chinese Journal of Intelligent Science and Technology, 2023, 5(3): 313-329.

[28] 赵博涛, 亢祖衡, 瞿晓阳, 等. 基于多模态大模型的具身智能体研究进展与展望[J]. 大数据, 2025, 11(3): 108-138.

Zhao B T, Kang Z H, Qu X Y, et al. Review and emerging trends of embodied agent based on multimodal large language models[J]. Big Data Research, 2025, 11(3): 108-138.

作者简介



姜春宇（1987-），男，中国信息通信研究院高级工程师，大数据与智能化部主任，主要研究方向为大数据与人工智能技术、大模型、数据要素流通、数据资产管理、数据安全。参与起草多个国家文件，包括《促进国家大数据发展行动纲要》《大数据产业发展规划（2016—2020年）》。建立了国内首个大数据人工智能产品能力评测体系，制定了50多项数据标准规范，牵头编写《数据资产管理实践白皮书》《数据安全治理实践指南》《数据要素白皮书》《智能中台实践指南》等多本研究报告。



韩晓璐（1992-），女，中国信息通信研究院工程师，主要研究方向为数据智能、智能体、智能知识中台等。参与构建数据智能技术标准与评测体系，制定智能体平台、智能体研发运营一体化（AgentOps）、大模型智能数据分析、大模型智能知识管理等20余项数据智能标准规范，参与编写《数据智能白皮书（2024）》《人工智能时代知识中台发展报告（2024）》等多本研究报告。



王超伦（1990-），男，中国信息通信研究院中级工程师，主要研究方向为大数据与人工智能技术及行业应用。参与起草多个国家文件，包括《促进国家大数据发展行动纲要》《大数据产业发展规划（2016—2020年）》。参与编写了《检索增强生成技术要求》《智能体平台技术要求》《大模型应用开发平台技术要求》《大模型驱动的智能数据分析工具技术要求》《大模型一体机能力要求》《知识中台能力成熟度模型》《人工智能数据工程能力要求》《数据智能白皮书》等多项标准及研究报告，并开展相关评测工作。

收稿日期: 2025-07-28