arXiv:2601.03328v1 [cs.MA] 6 Jan 2026

大语言模型赋能的多智能体系统：新兴设计模式与范式的实证评估及见解

Harri Renney
Kaze Technologies Kaze Consulting 巴斯，BA1 2HN，英国 harri@kaze-consulting.com

Maxim N Nethercott Kaze Technologies Kaze Consulting 巴斯，BA1 2HN，英国 max@kaze-consulting.com

Nathan Renney西英格兰大学 布里斯托尔，英国 nathan.renney@uwe.ac.uk

Peter Hayes
Kaze Technologies Kaze Consulting 巴斯，BA1 2HN，英国 peter@kaze-consulting.com

2026年1月8日

摘要

本文对大语言模型（LLM）赋能的多智能体系统（MAS）新兴设计模式与范式相关文献进行了系统梳理，并评估其在不同领域中的实用价值。我们界定了关键架构组件，包括智能体编排、通信机制和控制流策略，并展示这些组件如何助力快速开发模块化、领域自适应解决方案。我们在受控的容器化试点中，对三个真实案例研究进行了测试，涉及电信安全、国家遗产资产管理以及公用事业客户服务自动化。初步实证结果表明，在这些案例研究中，原型可在两周内交付，可供试点的解决方案则可在一个月内完成；这说明，与传统方法相比，此类方案能够降低开发开销并提升用户可访问性。然而，研究结果也进一步印证了文献中所记载的局限性，包括大语言模型行为存在差异，导致从原型迈向生产成熟度的过程面临挑战。最后，我们概述了提升多智能体系统架构的可靠性、可扩展性和治理水平所需的关键研究方向，以及进一步成熟多智能体系统设计模式、缓解其固有挑战所需开展的工作。

1 引言

将问题求解分散到多个人工智能程序中，是当代人工智能（AI）领域的一个研究方向，起源于 20 世纪 70 年代末 VR Lesser [1]和 Hewitt C. [2]的研究。研究人员探索了分布式问题求解，即多个人工智能类程序协同解决复杂任务，而这些任务在当时规模过大，单个单体系统难以应对。这些概念催生了多智能体系统（MAS）这一现代术语，并使其正式确立 [3, 4]。随着 Transformer [5], 大语言模型（LLM） [6], 等关键赋能技术的结合近期兴起，以及对大量算力的使用 [7], ，过去仅停留在概念层面的多智能体设计和多智能体系统如今得以借助大语言模型进行实际研究[8]。

自 Google 发布《Attention is All You Need》以来， [5], 现代语言模型一直逐渐采用*Transformer* 深度学习架构，并取得了显著的生成式结果 [9]。随着模型参数规模扩大，逐词预测机制带来了令人印象深刻的涌现能力。这些能力包括解决某些算术计算 [10], 、创意写作 [11] 以及软件代码生成 [12]。诸如

GPT [13] 和 PaLM [14] 被称为大语言模型，而事实证明，某些大语言模型能够通过职业考试，例如美国医师执照考试 [15] 和美国法律执业资格考试 [16], ，同时还能在写作 [17, 18]和代码生成 [19]中令人信服地不被察觉。

大语言模型在当代人工智能研究和产业中的重要性不言而喻，领先的跨国公司纷纷投入巨资开发大语言模型。单个大语言模型的开发成本据估计在100万美元至1亿美元之间 [20], ；自2023年以来，已有至少86个重大版本发布（图1）。这一趋势反映出模型创新和资本支出的空前加速，进一步凸显了采用可扩展且系统化的设计范式以支持可持续部署的必要性。

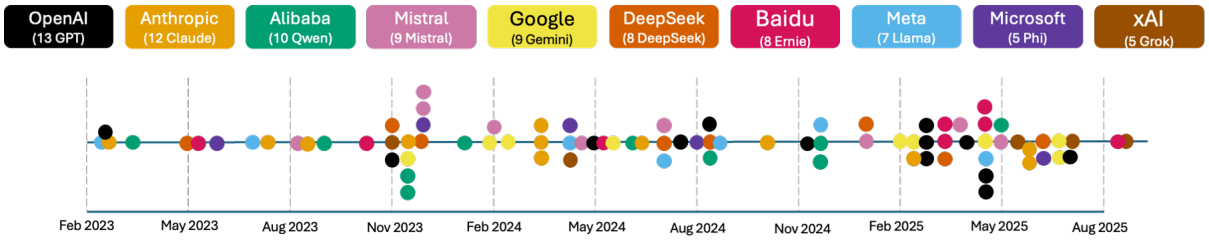


图1：时间线展示了自2023年以来，十家领先人工智能公司累计发布的大语言模型数量[21]。

以现代大语言模型作为核心推理引擎，可以构建专业人工智能代理 [22]。通过精心设计的提示词、获取最新领域数据并配备必要工具，智能体可以针对特定任务或领域进行定制。随后，智能体将针对目标任务高度专业化，从而提高效能，同时缩短执行时间并降低计算成本 [23, 24, 25]。

通过将多个专业智能体组成一个网络，并让它们能够将流程的下一部分移交给其他专业智能体，可以构建多智能体系统解决方案。其效率源于多智能体系统固有的劳动分工：将复杂任务拆分为多个较小的任务，并分别分配给不同的智能体 [26]。正如本文所提出的，正是这种灵活性使多智能体系统适用于解决公用事业、电信业等多个领域的问题。

本文在多智能体系统研究既有基础上，阐述了大语言模型赋能的多智能体系统相关的新兴设计模式，并致力于推动其在相关社群中的应用走向规范化。我们通过涵盖多个领域的一系列案例研究对这一方法进行评估，并根据研究结果与观察，阐明其优势和局限。在此基础上，我们确定了推动这一新兴范式进一步成熟和稳定、迈向可投入生产的技术所需取得进展的关键领域。

1.1 论文结构

我们对这一领域展开研究，并提供现实世界实现中的形式化描述和结果，以更好地理解基于大语言模型的多智能体系统方法的效用及其注意事项。为此，本文其余部分安排如下：

- 第2节回顾了有关大语言模型赋能的多智能体系统的最新学术、行业和开源文献，并总结本文如何通过提出形式化的设计模式，并在真实案例研究中检验这一方法，为该领域作出贡献。
- 第3节阐明了采用基于大语言模型的多智能体系统解决方案的动机，以应对组织面临的关键数据挑战。
- 第4节介绍了我们对一种常见多智能体系统设计范式的形式化，说明如何依据可重复使用的设计模式配置专业智能体及网络架构，从而解决数据检索以及半自动化、人在回路中的流水线等问题类别。
- 第5节记录了这一方法在三个真实案例研究中的应用，并总结开发人员、终端用户和高级企业管理人员的体验与观察。
- 第6节讨论研究结果，指出所提出设计模式的优势与局限，并探讨其对多智能体系统开发的更广泛影响。
- 最后，第7节总结了本文的关键见解，并探讨这一不断发展的领域未来研究方向。

2 文献综述

大语言模型架构的快速发展及其不可预测的涌现行为表明，这项技术仍处于初步发展阶段 [27]。由于人们尚未充分理解大语言模型如何展现涌现能力 [28]，且对可能导致政府监管的伦理问题 [29], 感到担忧，因此，如何将大语言模型有效应用于智能体网络仍在探索之中，也正逢其时。

一种能够提升大语言模型推理能力的基础技术是思维链（CoT）提示 [30]。该方法引导模型先经过一系列中间推理步骤，再给出最终答案，从而提高其在需要逻辑推理的任务中的准确性。思维链在复杂问题求解方面尤其有效，还能以可解释的方式呈现模型的推理过程，揭示模型如何得出结论，以及错误可能出现在哪里。思维链采用顺序推理，而一种名为思维树（ToT）的扩展方法则引入了分支推理路径，在复杂度较高的任务中带来了可衡量的改进 [31]。值得注意的是，思维树推理会调用多个智能体来探索不同的推理路径，这代表了一种初步的动态多智能体协调形式；本文将在后文对此概念进行更详细的探讨。

除了提示工程和多智能体调用之外，工具集成也已成为将通用大语言模型专门化为特定任务智能体的一项关键技术。一个典型例子是 Lewis 等人于 2020年 提出的检索增强生成（RAG） [32], ，它使大语言模型能够访问并推理其训练语料库中未包含的外部数据集。通过为动态、特定领域或专有数据源建立索引，检索增强生成使模型能够生成信息充分且基于上下文的输出，因此成为知识密集型应用的行业标准方案 [33]。正如一位检索增强生成的先驱研究者所指出的 [34]:

> “La言模型约占整个系统/解决方案的 20%，其周围还包含更多工程 i-nee环节。”

这强调了设计系统的必要性，而不是依赖构建孤立的模型。同样，其他专用智能体也需要接口，以便与各种工具交互，例如 SQL 数据库。这进一步推动了多智能体系统（MAS）的发展：多个由大语言模型驱动的专用智能体协作解决复杂、异构的任务。

2.1 学术文献

随着专用智能体日益普及，研究也越来越多地探索如何在多智能体系统（MAS）中连接和协调这些智能体，以解决复杂、目标明确的特定领域问题。近期文献提出了多种面向特定应用的多智能体系统设计。例如，Okonkwo 和 Onobhayedo [35] 研究了用于软件开发需求获取的多智能体系统，展示了由大语言模型驱动的智能体如何协助 eliciting and validating 规格说明。同样，Lin 等人 [36] 提出了一种用于代码生成的多智能体系统框架，其中智能体在开发生命周期的不同阶段担任领域专家，并在一个人机协作环境中与工程师互动。他们的研究结果表明，智能体在承担工程职责和促进协作工作流方面具有良好的应用前景。除软件工程之外，Kearney 的 *Bots of the SOC* 研究 [37] 评估了多智能体系统在安全运营中心（SoC）中的集成情况，并使用 Boss of the SOC数据集 [38]对不同的智能体配置进行基准测试。结果表明，测试中最有效的多智能体系统配置达到了与初级网络安全分析师相当的表现，凸显了多智能体系统在高风险领域增强人类专业能力的潜力。

尽管文献中的结果颇具前景，多智能体系统的实现仍面临显著挑战。Pan 等人 [39] 指出，随着智能体网络规模扩大，协调复杂性可能带来大量额外开销，降低效率和响应能力。这可能导致多智能体系统解决方案出现偏差，原因包括智能体的局部优化与全局目标相冲突、使用大语言模型所具有的随机性，以及错误传播——一个智能体的错误推理可能在系统中层层扩散。因此，要取得成效，多智能体系统方法需要采用结构化设计模式和范式，以缓解多智能体系统固有的挑战，包括协调失败，并提升可靠性。此外，随着多智能体系统架构以大语言模型为基础，还需考虑可持续性和伦理问题，以应对基于大语言模型的系统所固有的新兴挑战 [40, 41, 42]。在某些情况下，原型可能让人认为可以暂缓重视已核实的问责、偏见和新的利用途径等问题；但对这些问题加以考虑并妥善处理至关重要 [43]。因此，随着我们对这一领域的认识不断加深，持续关注相关进展十分重要，尤其是审查、透明度、知识产权和剽窃等目前较少探讨的伦理考量。

除了聚焦于特定领域的多智能体系统设计的研究之外，更具雄心的前瞻性倡议也正在涌现。这些努力探讨人工智能智能体如何实现大规模协作，并有望发展为无处不在的工具，取代包括互联网某些方面在内的现有技术。一个值得关注的例子是麻省理工学院的 NANDA 项目 [44, 45], ，该项目提出了一个去中心化的人工智能智能体互联网框架，旨在支持分布式架构中数十亿个专用智能体之间的协作。本文立足于范围狭窄的多智能体系统实现与有关

全局智能体自主性的愿景概念之间，致力于将新兴设计模式形式化，从而为各种特定领域问题提供切实可行的多智能体系统解决方案。

2.2 开源与产业倡议

从学术文献之外的动态来看，开源社区正积极推进框架和架构的发展，以支持大语言模型赋能的多智能体系统的开发。LangChain 框架为多智能体大语言模型编程提供了大量支持 [46]。其中包括 LangChain表达式语言 [47], ，这是一种由 LangChain 框架解析的领域特定语言，可用于编排智能体“链”，使其相互传递输入和输出，并主要支持顺序排列。LangGraph 项目 [48] 扩展了 LangChain 表达式语言，以管理和编排多个智能体的分支网络，推动多智能体系统开发。

大型行业供应商正日益与社区驱动的框架保持一致，积极将多智能体方法整合到其产品中。显著的例子包括微软的 AutoGen [49] 和 Copilot [50], ，以及亚马逊的 Bedrock 智能体 [51]。随着组织和开源项目不断发展，互操作性挑战愈发突出。对此，Anthropic 推出了[1] 模型上下文协议（MCP），这是一项开放标准，旨在使大语言模型能够与外部工具、数据源和服务无缝连接并交互 [52]。
大多数领先的云计算供应商和智能体人工智能供应商都在竞相开发类似的工具和支持，并在各自的专有环境中提供这些服务；这些服务要么基于开放标准和倡议，要么深受其影响。截至撰写本文时，微软的智能体人工智能开发工具仍处于 Azure AI Foundry [53], 的测试阶段，而 OpenAI 则提供自定义的「*GPT*」[54], 供用户定制智能体，随后将其集成到更广泛的协议和环境中。

2.3 研究空白

我们的综述揭示了学术文献中两大主流方向之间的脱节：**(i)** 在狭窄情境下评估高度专门化的大语言模型赋能多智能体系统设计；以及**(ii)** 提出全球化、去中心化智能体生态系统的愿景框架。相比之下，业界正迅速将发展重点汇聚到务实的多智能体系统开发上，并借助先进工具和开放标准，帮助组织大规模应对特定领域的挑战，同时缓解多智能体系统所带来的固有挑战。
这种分歧凸显了将新兴设计模式形式化的必要性，这些模式是行业驱动的解决方案的基础。尽管此类模式在实践中日益得到采用，但在学术讨论中仍未得到充分探讨。本文通过记录一种常见的多智能体系统设计范式，并在三个案例研究中通过实证测试评估其效用，来弥补这一空白。我们的研究结果揭示了这种方法的优势与局限，并指出了对齐和可扩展性等复杂问题，而传统架构往往会避开这些问题。

3 推动组织采用大语言模型赋能的多智能体系统设计模式

组织在有效管理其数据资产方面面临诸多挑战 [55, 56]。尤其是，许多组织积累了海量数据 [57], ，却仍难以有效组织、治理和解读这些数据，以便为决策提供有意义的洞见并支持自动化 [58, 59], 。根据 Lewkowicz J. 的说法，只有 16% 的组织被归类为数据驱动型 [60]。本节将探讨组织面临的三个核心数据挑战，而多智能体系统有望应对这些挑战：异构数据集、非结构化数据集和领域特定数据上下文。

3.1 异构数据

随着组织规模扩大、复杂性增加，它们往往会遇到与数据碎片化和信息孤岛系统相关的重大挑战 [61]。对于金融 [62] 和政府 [63], 等领域的大型组织，数据通常由多个部门、地点和平台生成并存储，而每个部门、地点和平台都可能采用不同的数据标准、格式和模式。久而久之，这种缺乏管理的去中心化会导致数据不一致和不兼容，使数据集成、治理和跨职能分析愈发困难。静态数据管道或模式映射工具等传统解决方案，往往难以应对这些分布式数据环境动态且异构的特性，尤其是在事后应用时 [64]。

大语言模型赋能的多智能体系统为克服这一挑战提供了一种颇具前景的替代方案。通过使用能够实时解读、对齐和转换异构数据模式的专业人工智能代理，多智能体系统可以动态

[1]而且自移交给 Agentic AI Foundation 后，该项目由 Linu x 基础模型

整合来自多个此前相互隔离的数据源的信息。这些智能体能够自主识别数据集之间的关系，解决模式不匹配问题，并协调数据结构，从而实现统一访问和分析。这种适应性使基于智能体的系统能够充当智能中介，促进在多样化、分布式且不断演变的数据格局中进行更高效的导航，而这一过程通常会耗费大量人力和时间。

3.2 非结构化数据

如果数据在源头就具有结构且组织良好，那么便可以轻松地对其进行管理、查询和分析，从而获得可靠的洞见。例如，传感器输出通常遵循预定义的模式 [65], ，生成格式一致的记录；而存储在关系数据库中的事务数据则遵循既定的数据模型和验证规则 [66]。这类结构化数据集非常适合采用传统分析和自动化技术[67]。

然而，组织日益面临大量非结构化或半结构化数据，据估计，这些数据可能占企业信息的高达 90% [68]。这些数据集缺乏一致的模式或格式 [69]，包括访谈记录、电子邮件、报告和自由文本等，其特点是含义模糊、依赖上下文且语言变化多样 [70]。这些特性使数据整合和解读变得极具挑战性，通常需要借助先进的自然语言处理（NLP）和语义推理技术来提取有意义的结构 [71, 72]。

基于大语言模型的智能体通过对非结构化数据集执行复杂的自然语言处理和语义推理，为应对这些挑战提供了强大能力 [73]。当这些智能体在多智能体系统中进行编排时，能够无缝处理结构化和非结构化数据源，通过整合的单一信息环境（SIE）实现信息的实时导航、查询与理解 [74, 8]。

3.3 特定领域问题

在各个行业中，组织通常面临相似类别的挑战，但每个领域的具体背景、约束条件和需求会带来细微差异，因此需要量身定制的解决方案 [75]。例如，为医疗保健 [76], 、国防 [77], 或金融 [78] 构建的系统，可能都需要安全数据检索或分析，但它们在数据语义、监管义务和解释逻辑方面存在显著差异。开发和维护此类定制系统，传统上需要专业的软件工程 expertise 和能够使技术解决方案与特定领域需求相匹配的人员，从而形成可能限制可扩展性和敏捷性的依赖关系 [79]。

大语言模型赋能的多智能体系统提供了自适应人工智能，将其与上下文资源和工具链连接后，便可快速配置以满足特定领域需求。通过为专业智能体配置与领域相关的知识、本体和推理能力，多智能体系统能够快速适应新的应用场景，而无需进行大规模再训练或重新开发。这些智能体可以解读特定领域数据 [80], 、应用上下文理解 [81], 并生成基于充分信息的输出，从而有效弥合通用人工智能能力与领域专业化应用之间的差距。因此，多智能体系统能够减少对人工干预来解决定制化问题的依赖 [82],，使专业人员专注于更高层次的分析，同时保持一个灵活且可复用的框架，以应对多样化的特定领域挑战。

4 一种新兴范式

本节立足于组织面临的关键挑战，介绍本文所阐述的新兴多智能体系统范式的基本要素。我们从专用自主智能体的最新概念化形式入手，这类智能体通常称为 ReAct 智能体，并进一步探讨如何将其整合进协作网络。这些网络构成了更广泛系统的基础，旨在解决复杂的特定领域问题。

4.1 ReAct 智能体

2022年，单个智能体在思维链推理循环中运行并执行决策任务这一概念，已正式纳入 ReAct 智能体的定义中 [83]。ReAct 智能体包含以下核心组件：

- **工具：** 用于执行特定任务的函数，例如查询 Google 搜索 API、访问 SQL 数据库、通过 Python 解释器执行代码 [84],或进行计算。
- **推理引擎：** 为系统提供动力的大型预训练模型。由于具备先进的推理能力，因此优先选择最先进的大语言模型。

- **智能体编排：** 负责管理大语言模型与其工具之间交互的整体系统。
- **记忆：** 用于跟踪过去的推理和输入，以便为当前决策提供信息的机制。短期记忆通常保存在提示上下文中，而长期记忆则存储在外部（例如向量数据库中），并通过语义相似度进行检索，为持续进行的任务提供相关上下文。

按照图2所示的工作流循环，此类智能体通常通过以下步骤运行：

1. **查询处理：** 系统处理来自其他实体（例如用户或另一智能体）的输入查询。 2. **工具使用：** 智能体选择适当的工具（如有必要），准备其输入，执行该工具，并获取输出。 3. **信息处理：** 智能体解读工具的输入和输出，生成观察结果，并确定下一步行动。 4. **综合与响应：** 利用积累的信息，智能体判断其是否拥有足够的上下文来返回响应，或是否需要重复该过程（返回步骤1），直至根据思维链推理形成连贯的答案。

有了这一对能够进行递归推理和动作执行的专门化 ReAct智能体的定义，我们便可以开始思考如何将此类智能体组织为更广泛的多智能体系统的一部分。

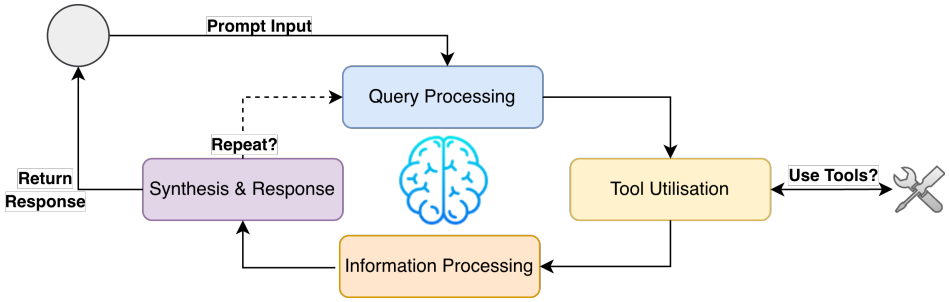


图2：ReAct智能体的工作流循环，展示关键阶段中反复进行的推理与动作执行，并通过思维链推理实现递归推理。

4.2 多智能体系统（多智能体系统）

虽然针对专门化任务进行定制的单个智能体可能非常有效，但通过添加过多可用工具来扩大其范围，往往会引入复杂性并降低性能。实证证据表明，当工具包扩展到超过 8–12 个工具时，智能体的性能通常会因上下文窗口过载和认知干扰而下降 [86, 87]。这正是多智能体系统中将能力委派给专业智能体，而不是交由单个负担过重的通用模型处理的依据。

借助多智能体系统，可以将能力分配给彼此通信并共享推理过程的专业智能体。这种方法既能保持单个智能体的有效性，又能使系统处理更加复杂、多方面的问题。由此形成的多智能体系统具有以下几个关键优势：**（i）模块化：** 独立的智能体可简化开发、测试和维护；**（ii）专业化：** 专业智能体可以专注于特定领域，从而提高准确性和效率；**（iii）控制：** 每个智能体都可以进行明确配置和管理，从而实现更精细的控制，改善与系统目标的一致性；**（iv）经济性：** 任务仅分配给相关智能体，因此不需要参与的智能体可以保持非活动状态。这种模块化激活方式降低了计算开销和运营成本。此外，还可以将智能体蒸馏为更小、更高效的版本，并针对其专门化任务进行优化 [88]。

定义通信机制是构建多智能体系统的关键步骤。基于第4.1节介绍的专业 ReAct 智能体概念，表1涵盖了本文后续将反复提及的多智能体系统架构关键组件，包括控制流策略、交互方式、历史共享策略和网络配置，以有效协调智能体的行为。图3展示了这些组件在抽象的单一信息环境（SIE）配置中的情况。在此示例中，一名战略决策者以人在回路上的方式与系统交互，并通过协调器智能体请求报告。协调器采用动态控制流，在运行时确定应通过带有历史共享的智能体交接来调用哪些专业数据检索智能体。一名

方面	描述
控制流	**显式：** 通过图边预定义的智能体交互序列。 **动态：** 大语言模型在运行时决定流程。
交互方式	**交接：** 将提示词传递给新的智能体。 **工具流：** 叶节点调用工具；中间节点管理交接。
历史共享	**完整推理轨迹：** 智能体共享一份带标签的日志，其中记录了所有智能体操作、通信和推理步骤，并将其作为交接提示词的一部分。 **仅最终结果：** 输入与结果之间的内部步骤不会在智能体之间交接时交换。
网络配置	**监督者：** 由监督代理协调的叶节点智能体。 **群体：** 一种没有任何层级的去中心化结构，其中智能体根据专业化情况动态地相互交接任务。 **层级式：** 一种分层架构，将智能体组织在多个监督层级之下，以实现可扩展性和结构化控制。 **单一信息环境（SIE）：** 一种以数据为中心的设计，其中智能体专精于各自独特的数据集，由协调器将查询路由至适当的智能体。
人机交互	**人在回路：** 批准/拒绝、审查工具调用、中断。 **人在监督回路：** 仅进行监督。

表1：用于定义多智能体系统架构的关键组件常见定义汇总。

专业智能体采用显式工具流来获取数据，而另一名则在显式的人在回路控制流程下进行数据采集。本文余下部分将使用这种图示语法，以简洁地呈现多智能体系统的网络配置。

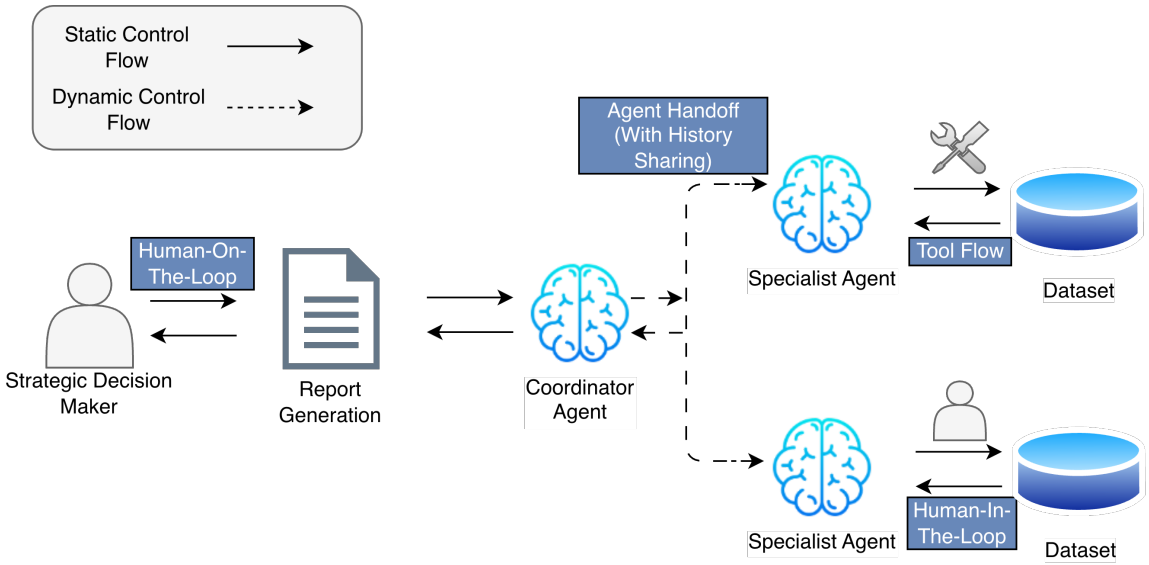


图3：配置为单一信息环境（SIE）的多智能体系统的抽象表示。该图展示了动态控制流、智能体交接策略，以及针对协同数据检索和决策的人在环监督。

5 病例系列

本节将利用多智能体系统模式和大语言模型作为每个智能体的核心推理引擎这一新兴范式，应用于表2所概述的三项概念验证和试点研究，以应对现实世界的挑战

这些挑战涉及多个行业，包括电信、政府国防、国家遗产和公用事业，展现了多智能体系统在多元且高风险领域中的通用性与可扩展性。

ID	领域	多智能体系统架构	评估指标
CS1	电信安全	SIE	利益相关者反馈
CS2	国家遗产领域	SIE	利益相关者反馈与每项查询的开放式评审
CS3	公用事业行业	层级式	用户验收测试、李克特量表评分、分类标注

表2：本研究涵盖的案例研究汇总表。

除上述示例外，该方法还正在扩展至政府国防部门内部的智能化安全数据迁移，并将在未来工作中作为其中一部分进行评估。

5.1 电信安全—安全运营中心智能体

在此案例研究中，一家英国大型电信运营商的安全部门希望增强其安全运营中心中的智能化工具和数据支持。该机构现有的网络威胁情报处理方式高度依赖人工，需要数十名分析师管理海量数据 [89]。随着全球威胁态势呈指数级增长且日益复杂，这种方式正变得越来越难以持续，无法跟上其发展速度 [90]。作为补充背景，仅占安全运营中心数据源一小部分的公开披露漏洞数量，就已从2016年的几千个激增至每年超过46,000个 2025[2]。此外，在估计每天在线生成的4亿太字节数据中 [91]，还必须收集、筛选和分析开源情报（OSINT）。依靠传统的人工分析方式进行管理，远远超出了人力所能承受的范围 [92]。

让这一挑战雪上加霜的是，网络安全领域的威胁分类体系不一致、数据源彼此割裂，且存在明显的西方中心偏见 [93]。数据过载、分析碎片化和情报缺口交织在一起，形成了网络防御中的关键瓶颈。具有前瞻性的组织正在探索如何利用大语言模型驱动专用智能体，在安全运营中心环境中自动检索数据并生成洞见。

本研究探讨了多智能体系统架构如何通过自动执行数据分析和交叉关联等关键任务，为安全运营中心分析师提供支持。图4展示了该原型，其实现了 SIE，使结构化安全运营中心数据集与非结构化开源情报源能够无缝集成。为提升易用性，该方案整合了对话式聊天机器人界面，使分析师能够直观地实时查询和浏览复杂的数据源。

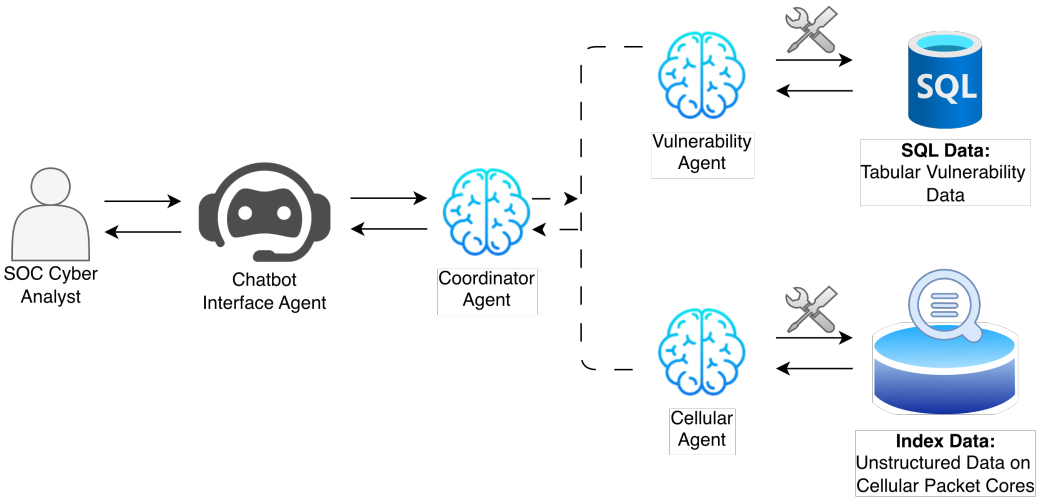


图 4：在电信安全运营中心案例研究中部署的多智能体系统架构。该设计集成了用于威胁情报检索与关联分析的专用智能体，由中央监督智能体协调，并提供供分析人员交互的对话界面。

[2] https://www.cvedetails.com/browse-by-date .php

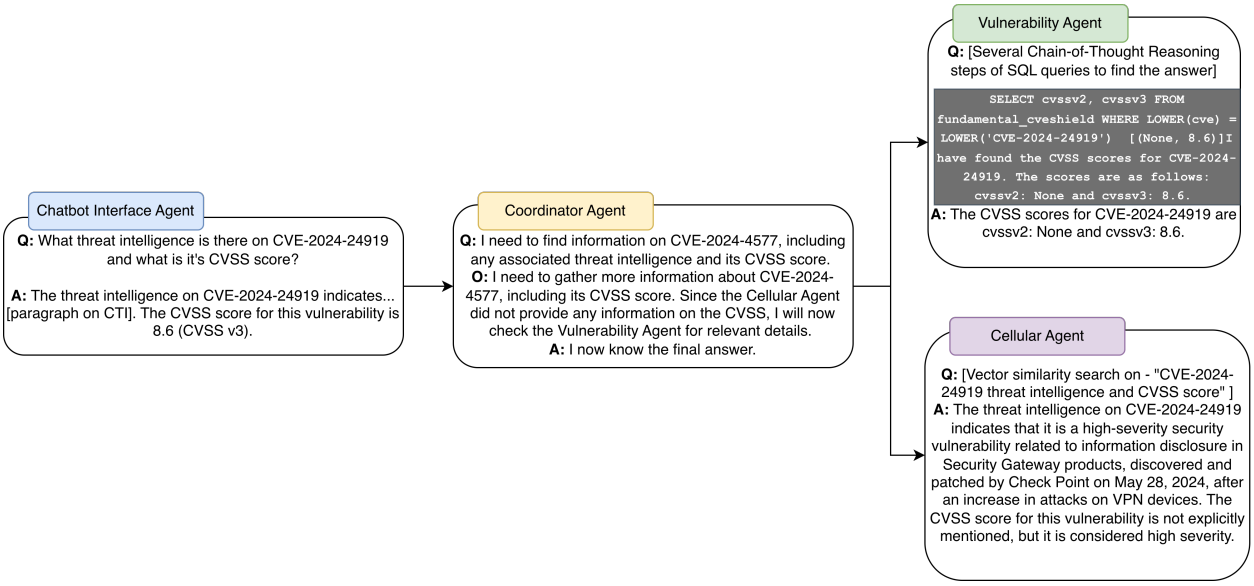


图5：电信安全运营中心案例研究中多智能体系统推理阶段示例。该示例展示了结构化数据源与非结构化数据源的无缝集成，支持对分析师查询提供高效且内容丰富的响应。

图5展示了电信安全运营中心案例研究中记录的推理阶段示例。在此示例中，用户通过聊天机器人接口智能体发起查询，要求获取某个特定通用漏洞披露及其相关 CVSS评分的详细信息。协调器智能体将任务分配给两个专用智能体：蜂窝智能体执行向量相似性搜索，以提取相关威胁情报；漏洞智能体则运用思维链推理执行 SQL查询，以检索 CVSS评分。这一多智能体工作流展示了多智能体系统范式整合异构数据源的能力：将结构化漏洞数据库与非结构化威胁报告相结合，同时保持安全运营中心运营所需的模块化与适应性。此外，协调器智能体能够识别查询是否只需使用单一数据源，并据此分配任务，从而优化资源利用率，减少不必要的计算开销。

为确保符合电信安全政策，多智能体系统解决方案以可移植的Docker容器形式部署，从而实现安全的本地部署。该概念验证已与关键利益相关者进行测试，并在可用性和潜在影响方面获得了高度积极的反馈。分析师指出，该系统能够通过自动化异构数据源之间的数据导航与关联，显著减轻工作负担。

在演示以及随后与首席信息安全官（CISO）的讨论之后，他们计划进一步研究这一方法，以增强现有的安全运营中心分析师工具。该反馈表明，在网络空间复杂性日益增加的情况下，多智能体系统作为扩展安全运营中心运营的方法具有可行性。这既凸显了其为分析师带来的运营优势，也彰显了其对推动数字化转型、迈向数据中心化安全运营中心模型的高级领导层所具备的战略潜力。

5.2 国家资产登记册 - 数据清理与检索

本案例研究聚焦于一家大型英国国家组织，该组织在众多站点管理着大量资产和库存清单。随着时间推移，各站点逐渐形成了彼此孤立的数据集，各自采用独特的数据采集方法和结构规范。这种分散状况导致数据标准化程度低，使资产清单管理和检索高度不一致，员工也难以访问。因此，每个站点的数据集都需要采用不同的解读方式，增加了整合工作的复杂性。

虽然已规划一项长期举措，旨在标准化数据存储和模式设计，但仍需要一种过渡方案，以便在英国所有站点无缝访问和查询资产信息。为此，团队依据本文概述的设计范式开发了一个多智能体系统概念验证。该方案采用了SIE多智能体系统架构，重点在于弥合结构化数据集与非结构化数据集之间的不一致。

通过利益相关者发现会议和业务需求研讨会，确定了图 6 **(a)** 所示的 SIE多智能体系统架构。该架构采用由专用智能体组成的协调框架，首先由协调器智能体

动态地将提示词交由适当的数据检索专家处理，这些专家经过训练，并配备了数据检索工具。为最大限度地方便非技术人员使用，该界面被设计为自然语言聊天机器人，只需极少培训即可使用，并支持直观交互。

这项平台无关的设计部署在该组织的 Microsoft Azure 云环境中，并利用原生智能体服务来确保可扩展性和合规性。为进行验证，概念验证由十名高级职员测试了一个月，并收集开放式定性反馈，同时记录每次使用该解决方案时的意见。通过基于词典的匹配进行情感分析 [94]，将回复归类为正面和负面两类，如图 6（**b**）所示。总体而言，反馈中 61% 略偏正面；反馈中的详细意见表明，可以通过调整迅速改进该方案。利益相关者认可了概念验证的潜力，并要求开展后续工作以扩展该解决方案。此外，相关人员还讨论了将内部工具发展为面向客户的聊天机器人，以提供有关其国家资产的全面洞察，从而提升用户体验。

这项概念验证表明，SIE多智能体系统架构有望整合彼此分散的数据集，而无需立即进行模式标准化。对话式界面降低了非技术用户的使用门槛，而云端部署则确保了可扩展性和合规性。然而，考虑到开发仅用了一个月，结果表明仍需提升一致性和可靠性。尽管存在这些局限，利益相关者对将该解决方案扩展至面向客户的应用表现出浓厚兴趣，这凸显了经过进一步测试后，该方案有望在组织内产生更广泛的影响。

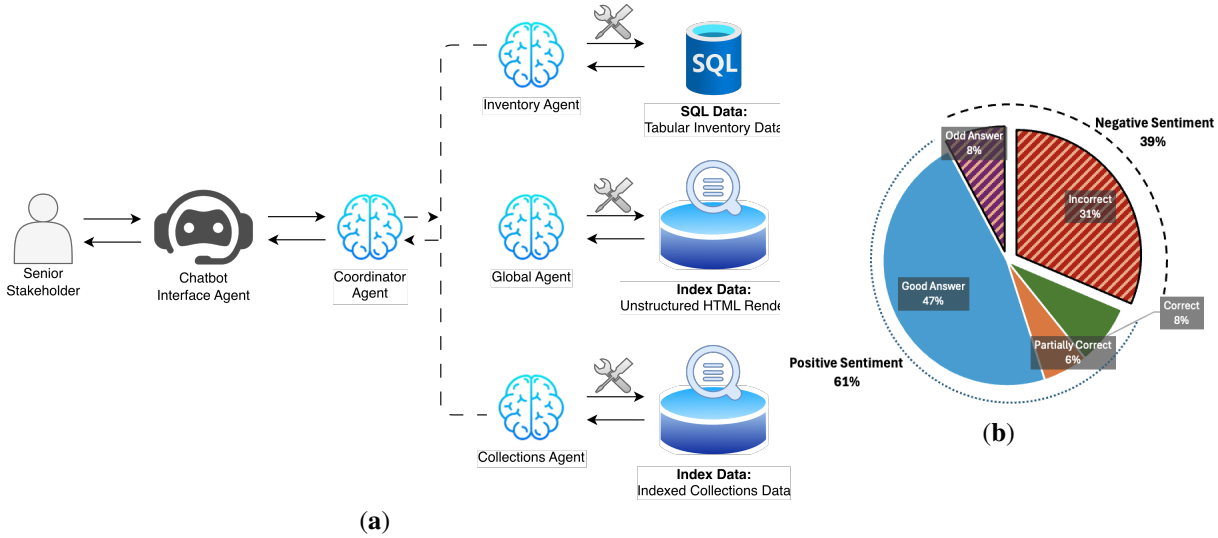


图 6：(a) 国家资产登记册案例研究中的多智能体系统架构，展示了用于跨站点数据检索和数据清洗的动态智能体编排。(b) 利益相关者反馈的情感分析，将反馈分为正面和负面回应，表明总体评价积极，但仍有明显的改进空间。

5.3 客户服务 - 自动化查询与投诉回复

本案例研究考察了一家英国公用事业公司，该公司希望提高客户服务运营的效率和一致性，尤其关注自动发送首次回复（FTR）电子邮件。该组织此前曾委托两家外部承包商应对这一挑战；然而，两者都未能提供切实可行且可扩展的解决方案。因此，本研究探讨了多智能体系统方法，以评估有针对性的自动化能否在保留必要人工监督的同时，带来可衡量的绩效提升。

通过探索性会议、对现有架构的分析以及与利益相关者的磋商，我们发现电子邮件分流、知识检索和回复起草方面存在关键的自动化机会。在迭代螺旋式开发过程中，原有设计经过了调整 [95]。最终形成的多智能体系统架构（图7）整合了知识库文章（KBA）中的领域专用背景知识，以及客户关系管理（CRM）系统中的最新客户记录。专用智能体负责从收件邮件中提取信息、检索并综合相关的KBA和CRM背景信息，以及生成符合预定义模板的回复草稿。对于涉及风险的决策和质量保证，系统仍嵌入了人在回路检查点，尤其是在用户完善阶段，以便将经FTR完善的银级邮件转变为可供发送的金级邮件。

这一配置构成了一种领域专用自动化策略，其灵活性超过了传统的脚本式或纯粹基于规则的流水线。

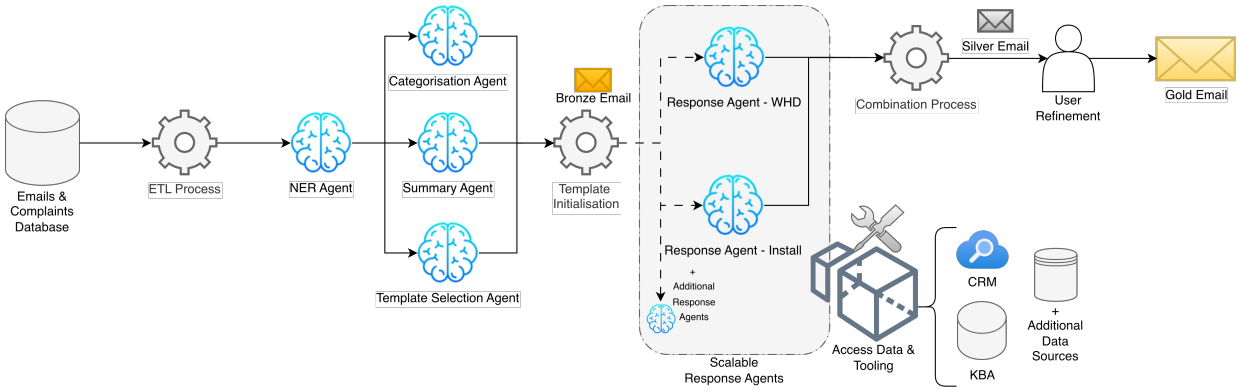


图7：用于客户服务自动化的端到端多智能体系统流水线，整合了电子邮件分流、上下文知识检索和回复起草。人在回路检查点确保自动化工作流符合合规性和质量保证要求。

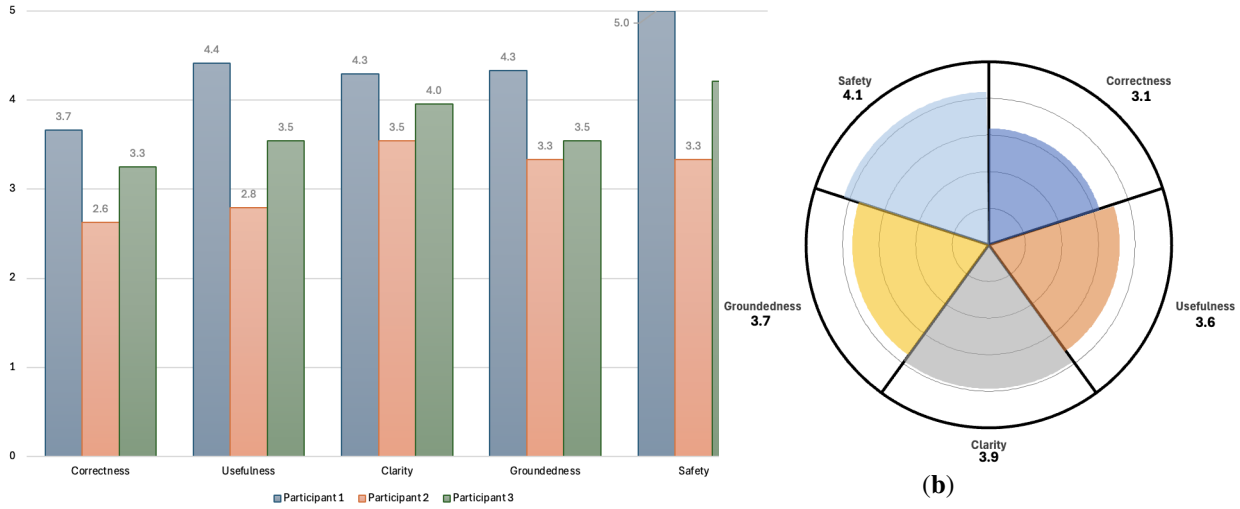
该解决方案采用平台无关的设计，在 Microsoft Azure 上部署，利用 Azure 的智能体服务，并托管于 Microsoft Fabric 生态系统中。与 Power BI 集成后，可实现运营监控和业务分析。在这一环境中，多智能体系统每分钟约生成五封 FTR 电子邮件，每封电子邮件的估算运营成本为 ~£0.05；通过分布式并行执行，还可实现水平可扩展性。相比之下，根据企业估算，完全人工的基线每分钟约生成三封 FTR 电子邮件，每封电子邮件的成本则高得多，为 ~£0.33，这表明吞吐量和成本效益均有望提升。

从工程角度来看，多智能体系统范式加快了初始功能的交付。作为对比，项目首席开发人员报告称，传统的正则表达式（regex）分类基线需要 ~4.5 小时才能生成首批可测试输出，而功能相当的多智能体系统专用智能体不到一小时便生成了类似的首批结果，体现了开发速度和可扩展性的提升。

一项试点用户验收测试（UAT）由三位参与者完成，他们评估了 24 封真实客户电子邮件。图8（**a**）中记录的参与者使用五个李克特量表维度对 FTR 的系统输出进行评分：正确性、实用性、清晰度、依据充分性和安全性（1 = 差； 5 = 优）[3]。评估考察了两项任务：（i）对收到的电子邮件进行分类；（ii）根据组织模板生成 FTR。

汇总所有参与者的判断后，电子邮件分类的准确率达到 100%。对于 FTR 生成邮件的质量，各维度的平均得分（图8（**b**））均超过 3/5，其中清晰度和安全性的平均得分为 ~4/5。尽管观察到参与者间差异（例如，安全性评分介于 3.3 至 5.0 之间），但整体表现优于人工基线的起草时间，且展现出良好的质量指标。

[3]感兴趣的读者可在此查阅完整详情和数据：https://osf.io/4dzmv/overview



(**a**) (**b**)

图8： (a) 用户验收测试中每位参与者的评估结果，展示了正确性、实用性、清晰度、依据充分性和安全性五个维度的李克特量表评分。(b) 相同结果按参与者汇总后的平均值。

这项试点研究表明，多智能体系统架构能够显著提升客户服务工作流的运营效率和响应一致性，在提高吞吐量、降低单位成本的同时，加快开发周期。尽管评估范围有限，且响应质量存在一定差异，但利益相关者有意扩大系统规模并将其拓展至首次联系解决，这凸显了该系统作为一种可扩展、适应性强的企业客户互动方案所具有的潜力。未来工作需要优先开展更大规模的试验，严格通过 A/B测试与人工基准进行对比，并针对性地优化，以减少安全性和清晰度指标方面的差异。

6 讨论

本文所呈现的一系列案例研究，为探讨采用以大语言模型作为智能体推理引擎的多智能体系统架构所带来的实际影响提供了契机。讨论借鉴了电信安全、国家资产管理和客户服务自动化三个不同领域的见解，考察了这一新兴范式的优势、局限性和未来发展方向。以下小节将探讨所有案例研究中涌现出的三个关键主题。

6.1 快速原型开发

这一系列案例研究表明，多智能体系统架构能够显著加快原型开发，使功能性解决方案可在数周而非数月内完成。例如，在案例研究3（客户服务自动化）中，此前两家承包商经过数月开发，仍未能交付任何可行的解决方案。相比之下，采用多智能体系统方法后，原型和用户验收测试在一个月内便已完成。

多智能体系统的平台无关特性进一步推动了这一加速进程，使其能够部署于本地部署容器和云生态系统中，而无需进行重大基础设施变更，从而有效弥合互操作性差距。然而，这种速度优势也带来了关键的权衡：尽管早期开发得以提速，但转入生产环境仍需进行大量调优，以解决对齐问题，并应对大语言模型固有的额外计算成本，例如输出结果的可变性和合规限制。这些挑战可能抵消最初节省的时间，凸显了未来研究评估大规模多智能体系统完整生命周期成本、可靠性和性能基准的必要性。

6.2 领域特定适应性与效率

多智能体系统架构的一项关键优势在于能够适应不同领域，尤其是在结合大语言模型推理，并通过检索增强生成和工具集成丰富上下文时。与僵化的基于规则的工作流不同，

多智能体系统支持专用智能体的动态编排，使系统能够契合领域特定语义、合规要求和运营约束。

案例研究清楚展现了这种灵活性：例如，安全运营中心原型实现了对异构威胁情报来源的自动交叉关联，这项工作过去通常需要大量人工分析；而客户服务解决方案则整合了客户关系管理和知识库数据，生成基于具体情境的答复，而这些知识通常需要专家学习才能掌握。

除适应性外，多智能体系统还能通过减少对大型开发团队的依赖并加快创新周期来提升效率。这些益处不止体现在速度上，还体现为多智能体系统无需彻底重新设计，便能扩展至不同问题空间的能力，使这一范式成为定制化高风险应用可重复使用的基础。

直接后果是对组织产生颠覆性影响，正如新兴企业人工智能研究所指出的那样[96]。快速适应特定领域的能力可能重塑劳动力结构，或会减少对某些专业岗位的需求，并促使人们重新评估组织战略。

6.3 人工监督：一项持续性要求

尽管观察到自动化带来的效益，所有案例研究都再次证实，必须有人参与其中或对其进行监督，以确保问责、合规性和结合情境的判断。正如 Brown 所强调的 [97],“领导力的未来在于互补 [人工智能]，而非取而代之。”多智能体系统架构能够自动执行常规任务并提供可执行的洞见，但无法复制人工监督所固有的细致决策能力和伦理考量。实践中，这体现为客户服务概念验证中的监督检查点，以及安全运营中心和资产管理解决方案中的战略决策者角色。这些发现进一步印证了这一观点：在组织工作流程中，多智能体系统应被定位为增强型技术，而非替代型技术。

6.4 主要局限

案例系列凸显了多智能体系统范式的若干优势，例如能够在初期快速完成开发生命周期。然而，开发人员、用户的观察以及利益相关者反馈也揭示了关键局限。即使借助检索增强生成和其他工具，利用特定领域的上下文来辅助，大语言模型推理仍存在固有风险，包括幻觉、基础错误和可解释性问题，这些问题可能会在整个多智能体系统中扩散。案例研究2和案例研究3的结果清楚地表明了这一点，其中可靠性和正确性的测量结果显示仍有改进空间。要构建可扩展的稳健设计模式和护栏，使解决方案从初期快速开发阶段进一步推进，并将原型转入生产/发布阶段，还需要投入更多工作。这些问题在网络安全等高风险领域或高度受监管行业中尤为突出，进一步凸显了稳健验证流程和人在回路监督的必要性。

最后，尽管多智能体系统架构支持平台无关的灵活部署，但仍受计算资源要求和依赖项管理的限制。基础设施有限或数据驻留政策严格的组织可能会面临集成障碍，尤其是在异构环境中进行扩展时。

7 结论

本研究系统总结了大语言模型赋能的多智能体系统的新兴设计模式，并通过三个真实案例研究评估了这些模式在不同领域的实际效用。结果表明，多智能体系统架构能够显著加快原型开发、降低开发开销，并为复杂且特定于领域的挑战提供适应性强的解决方案。通过发挥模块化、专业化和动态编排的优势，多智能体系统提供了一种可复用的范式，能够弥合僵化的基于规则的工作流与定制化工程方法之间的差距。

研究结果也进一步印证了长期存在的局限性。大语言模型行为的可变性、幻觉风险以及可解释性方面的挑战，仍是实现生产成熟度的关键障碍，在高风险或受监管环境中尤为如此。此外，尽管多智能体系统架构在可扩展性和互操作性方面展现出巨大潜力，但也带来了对计算资源和治理框架的依赖，组织必须对此加以应对。

未来研究将着重开展迭代式用户研究，以严格评估和完善这一方法，并据此开发满足严格要求的增强型设计特性。这些工作将优先加强验证流程，并实施稳健的护栏 [98] ，以降低可靠性和安全性风险。

数据与材料的可用性：支持本研究发现的数据可通过开放科学框架公开获取：https://osf.io/4dzmv/overview。

伦理审批：本研究已获得 Kaze Consulting 审查委员会的伦理审批，所有研究方案均按照公司准则执行。所有收集的数据均已匿名化并安全存储，符合公司政策和数据保护法规的要求，以确保参与者信息的保密性和安全性。

利益冲突： 作者声明，就本研究而言不存在需要报告的利益冲突。 y.

参考文献

[1] Victor R. Lesser 和 Daniel D. Corkill。人工智能技术在协作式分布处理中的应用。载于 第六届国际人工智能联合会议论文集——第*1*卷，IJCAI'79，第537–540页，美国加利福尼亚州旧金山，1979年。Morgan Kaufmann Publishers Inc.[2] Carl Hewitt。将控制结构视为消息传递模式。人工智能，8(3):323–364，1977年。[3] Hosny Ahmed Abbas、Samir Ibrahim Shaheen 和 Mohammed Hussein Amin。多智能体系统的组织：概述。*arXiv* 预印本 *arXiv:1506.09032*，2015年。[4] Ali Dorri、Salil S Kanhere 和 Raja Jurdak。多智能体系统：综述。《*IEEE*开放获取期刊》，6:28573–28593，2018年。[5] Ashish Vaswani、Noam Shazeer、Niki Parmar、Jakob Uszkoreit、Llion Jones、Aidan N Gomez、Łukasz Kaiser 和 Illia Polosukhin。Attention is All You Need。神经信息处理系统进展，第30卷，2017年。[6] Humza Naveed、Asad Ullah Khan、Shi Qiu、Muhammad Saqib、Saeed Anwar、Muhammad Usman、Naveed Akhtar、Nick Barnes 和 Ajmal Mian。大语言模型综合概述。*ACMTransactionsonIntelligent Systems and Technology*，16(5):1–72，2025年。[7] Girish Sastry、Lennart Heim、Haydn Belfield、Markus Anderljung、Miles Brundage、Julian Hazell、Cullen O'keefe、Gillian K Hadfield、Richard Ngo、Konstantin Pilz 等。计算能力与人工智能治理。*arXiv* 预印本 *arXiv:2402.08797*，2024年。[8] Harri Renney、Max Nethercott、Olivia Williams、Jayden Evetts 和 James Lang。重塑数据格局：一种用于数据接口的多智能体范式。载于 *2025*年第八届数据科学与机器学习应用国际会议（*CDMA*），第114–119页。IEEE，2025年。[9] John Ndia Charles Munyao。基于 Transformer 模型的自然语言处理：元分析。*Journal on Artificial Intelligence*，7(1):329–346，2025年。[10] Wei Zhang、Chaoqun Wan、Yonggang Zhang、Yiu-ming Cheung、Xinmei Tian、Xu Shen 和 Jieping Ye。解读并改进大语言模型的算术计算能力。载于 第四十一届国际机器学习大会。[11] Carlos Gómez-Rodríguez 和 Paul Williams。模型联盟：对大语言模型创意写作能力的综合评估。*arXiv* 预印本 *arXiv:2310.08433*，2023年。[12] Sarah Fakhoury、Aaditya Naik、Georgios Sakkas、Saikat Chakraborty 和 Shuvendu K Lahiri。基于大语言模型的测试驱动交互式代码生成：用户研究与实证评估。*arXiv* 预印本 *arXiv:2404.10100*，2024年。[13] Josh Achiam、Steven Adler、Sandhini Agarwal、Lama Ahmad、Ilge Akkaya、Florencia Leoni Aleman、Diogo Almeida、Janko Altenschmidt、Sam Altman、Shyamal Anadkat 等。GPT-4 技术报告。*arXiv* 预印本 *arXiv:2303.08774*，2023年。[14] Aakanksha Chowdhery、Sharan Narang、Jacob Devlin、Maarten Bosma、Gaurav Mishra、Adam Roberts、Paul Barham、Hyung Won Chung、Charles Sutton、Sebastian Gehrmann 等。PaLM：借助路径扩展语言建模。*Journal of Machine Learning Research*，24(240):1–113，2023年。[15] Dana Brin、Vera Sorin、Eli Konen、Girish Nadkarni、Benjamin S Glicksberg 和 Eyal Klang。大语言模型在美国医师执照考试中的表现：系统综述。*MedRxiv*，第2023–09页，2023年。[16] Daniel Martin Katz、Michael James Bommarito、Shang Gao 和 Pablo Arredondo。GPT-4 通过律师资格考试。*Philosophical Transactions of theRoyal SocietyA*，382(2270):20230254，2024年。[17] Junchao Wu、Shu Yang、Runzhe Zhan、Yulin Yuan、Lidia Sam Chao 和 Derek Fai Wong。大语言模型生成文本检测综述：必要性、方法与未来方向。*ComputationalLinguistics*，51(1):275–338，2025年。

[18] Lilia-Eliana Popescu-Apreutesei、Mihai-Sorin Iosupescu、Sabina Cristiana Necula 和 Vasile-Daniel P˘av˘aloaia。在先进语言模型兴起之际维护学术诚信：评估双向长短期记忆网络结合 GloVe 嵌入对人工智能生成的科学摘要的检测能力。*Computers,Materials & Continua*，84(2)，2025年。[19] Zhenyu Xu 和 Victor S. Sheng。利用大语言模型的困惑度检测人工智能生成的代码作业。载于 第三十八届人工智能促进协会人工智能大会、第三十六届人工智能创新应用大会暨第十四届人工智能教育进展研讨会论文集，AAAI'24/IAAI'24/EAAI'24。AAAI出版社，2024年。[20] Ari Chanen。我从彭博社自建大语言模型的经验中学到的内容。网址：https://www.linkedin.com/pulse/what-i-learned-from-bloombergs-experience-building-own-chanen-phd/

，

2023年。[21] Le Luyen 和 Marie-Hélène Abel。《大语言模型预测先备技能的效果如何？与专家定义概念的零样本比较》，2025年7月。[22] Valentina Alto。构建大语言模型驱动的应用：使用大语言模型创建智能应用和智能体。Packt Publishing Ltd，2024年。[23] Haochun Wang、Sendong Zhao、Zewen Qiang、Nuwa Xi、Bing Qin 和 Ting Liu。超越直接诊断：基于大语言模型的多专科智能体会诊用于自动诊断。*arXiv*预印本 *arXiv:2401.16107*，2024年。[24] Anna Kalyuzhnaya、Sergey Mityagin、Elizaveta Lutsenko、Andrey Getmanov、Yaroslav Aksenkin、Kamil Fatkhiev、Kirill Fedorin、Nikolay O Nikitin、Natalia Chichkova、Vladimir Vorona 等。用于智慧城市管理的大语言模型智能体：通过多智能体人工智能系统增强决策支持。*Smart Cities*（*2624-6511*），8(1)，2025年。[25] Yan Zhang、Ahmad Mohammad Saber、Amr Youssef 和 Deepa Kundur。Grid-agent：用于电网控制的大语言模型驱动多智能体系统。*arXiv*预印本 *arXiv:2508.05702*，2025年。[26] Hamed Rezaee 和 Farzaneh Abdollahi。高阶多智能体系统上的平均一致性。*IEEE*自动控制汇刊，60(11)：3047–3052，2015年。[27] Leonardo Berti、Flavio Giorgi 和 Gjergji Kasneci。大语言模型中的涌现能力：综述。*arXiv*预印本 *arXiv:2503.05788*，2025年。[28] Chandan Singh、Jeevana Priya Inala、Michel Galley、Rich Caruana 和 Jianfeng Gao。重新思考大语言模型时代的可解释性。*arXiv*预印本 *arXiv:2402.01761*，2024年。[29] Bertalan Meskó 和 Eric J Topol。大语言模型（或生成式人工智能）在医疗保健领域加强监管监督的必要性。*NPJ Digital Medicine*，6(1)：120，2023年。[30] Jason Wei、Xuezhi Wang、Dale Schuurmans、Maarten Bosma、Fei Xia、Ed Chi、Quoc V Le、Denny Zhou 等。思维链提示激发大语言模型中的推理能力。神经信息处理系统进展，35：24824–24837，2022年。[31] Shunyu Yao、Dian Yu、Jeffrey Zhao、Izhak Shafran、Tom Griffiths、Yuan Cao 和 Karthik Narasimhan。思维树：使用大语言模型进行审慎的问题求解。神经信息处理系统进展，36，2024年。[32] Patrick Lewis、Ethan Perez、Aleksandra Piktus、Fabio Petroni、Vladimir Karpukhin、Naman Goyal、Heinrich Küttler、Mike Lewis、Wen-tau Yih、Tim Rocktäschel 等。面向知识密集型自然语言处理任务的检索增强生成。神经信息处理系统进展，33：9459–9474，2020年。[33] Agada Joseph Oche、Ademola Glory Folashade、Tirthankar Ghosal 和 Arpan Biswas。关键检索增强生成（RAG）系统的系统综述：进展、空白与未来方向。*arXiv*预印本 *arXiv:2507.18910*，2025年。[34] Douwe Kiela。生产环境中的检索增强生成智能体：我们学到的10条经验——RAG创作者 Douwe Kiela，2025年。最后访问日期：2025年11月13日。[35] Charles Igah Afam Okonkwo、Pius Onobhayedo。将人工智能技术应用于传统软件开发生命周期流程的需求工程阶段。*Journal on Artificial Intelligence*，6(1)：379–401，2024年。[36] Feng Lin、Dong Jae Kim 等。基于大语言模型的代码生成遇上软件开发流程。*arXiv*预印本 *arXiv:2403.15852*，2024年。[37] Michael Kearney。安全运营中心的机器人。网址：https://www.youtube.com/watch?v=WLP5eEqmbxQ，2024年8月。[38] Splunk GitHub。botsv3。网址：https://github.com/splunk/botsv3，2020年2月。

[39] Melissa Z Pan、Mert Cemri、Lakshya A Agrawal、Shuyi Yang、Bhavya Chopra、Rishabh Tiwari、Kurt Keutzer、Aditya Parameswaran、Kannan Ramchandran、Dan Klein 等。多智能体系统为何会失败？载于*ICLR 2025*语言模型与应用信任构建研讨会，2025年。[40] Yi Ding 和 Tianyao Shi。可持续的大语言模型服务：环境影响、挑战与机遇：特邀论文。载于*2024*年第*15*届*IEEE*国际绿色与可持续计算会议（*IGSC*），第37–38页，2024年11月。ISSN：2993-2084。[41] Pamela S. Hinds 和 Amy Bedinger Miller。我们的话语与人工智能的话语：问责属于我们。*Cancer Care Research Online*，3(2)：e041，2023年4月。[42] Shivani Kapania、Ruiyi Wang、Toby Jia-Jun Li、Tianshi Li 和 Hong Shen。“我将大语言模型归类为生产力工具”：考察大语言模型在人机交互研究实践中的使用伦理。《*ACM*人机交互会议论文集》，9(2)：CSCW102:1–CSCW102:26，2025年5月。[43] Junfeng Jiao、Saleh Afroogh、Yiming Xu 和 Connor Phillips。探索大语言模型伦理：进展、挑战与未来方向。《人工智能与伦理》，5(6)：5795–5819，2025年12月。[44] 麻省理工学院。Nanda：人工智能智能体互联网。网址：https://nanda.media.mit.edu。[45] Ramesh Raskar、Pradyumna Chari、John Zinky、Mahesh Lambe、Jared James Grogan、Sichao Wang、Rajesh Ranjan、Rekha Singhal、Shailja Gupta、Robert Lincourt 等。超越域名系统：通过Nanda索引和经验证的智能体事实解锁人工智能智能体互联网。*arXiv*预印本 *arXiv:2507.14263*，2025年。[46] Oguzhan Topsakal 和 Tahir Cetin Akinci。利用LangChain创建大语言模型应用：快速开发大语言模型应用的入门指南。载于应用工程与自然科学国际会议，第1卷，第1050–1056页，2023年。[47]Tom Darmon。释放LangChain表达式语言（LCEL）的力量：从概念验证到生产环境。网址：
h
t
t
ps://
www.artefact.com/blog/unleashing-the-power-of-langchain-expression-language-lcel-from-proof-of-concept-to-pro
duction/,
1 2024年。[48] Cheonsu Jeong。基于图的智能体高级检索增强生成系统实现方法研究。*arXiv* 预印本 *arXiv:2407.19994*，2024年。[49] Qingyun Wu、Gagan Bansal、Jieyu Zhang、Yiran Wu、Shaokun Zhang、Erkang Zhu、Beibin Li、Li Jiang、Xiaoyun Zhang 和 Chi Wang。AutoGen：通过多智能体对话框架支持新一代大语言模型应用。*arXiv* 预印本 *arXiv:2308.08155*，2023年。[50] Adeel Khan。Microsoft Copilot Studio。载于《为管理者介绍 *Microsoft Copilot*：借助生成式人工智能助手提升团队生产力与创造力》，第621–694页。施普林格，2024年。[51] 亚马逊。Amazon Bedrock智能体。网址：https://aws.amazon.com/bedrock/agents。[52] Xinyi Hou、Yanjie Zhao、Shenao Wang 和 Haoyu Wang。模型上下文协议（MCP）：现状、安全威胁与未来研究方向。*arXiv* 预印本 *arXiv:2503.23278*，2025年。[53] 微软。人工智能应用与智能体工厂。网址：https://ai.azure.com。[54] Tyna Eloundou、Sam Manning、Pamela Mishkin 和 Daniel Rock。GPT即GPT：大语言模型对劳动力市场的潜在影响。《科学》，384(6702):1306–1308，2024年。[55] Supriya Sarker、Mohammad Shamsul Arefin、Md Kowsher、Touhid Bhuiyan、Pranab Kumar Dhar 和 Oh-Jin Kwon。工业大数据综述：挑战与机遇。《*IEEE*开放获取期刊》，11:744–769，2022年。[56] Carlos A Escobar、Megan E McGovern 和 Ruben Morales-Menendez。质量4.0：制造业大数据挑战综述。《智能制造期刊》，32(8):2319–2334，2021年。[57] Carrie Pallardy。对于组织而言，数据多到什么程度才会妨碍价值挖掘？，2024年。最后访问日期：2025年11月13日。[58] Ruben Ugarte。《数据幻象：企业为何未能真正利用数据》。Business Expert Press，2021年。[59] Sellbery。为什么多数企业仍在为有效利用数据而苦苦挣扎，2025年。最后访问日期：2025年11月13日。[60] Jakub Lewkowicz。尽管多数企业都关注数据，但真正实现“数据驱动”的仅约16%，2024年。最后访问日期：2025年11月13日。[61] Andrew Carruthers。打破数据孤岛。载于《构建 *Snowflake* 数据云：实现数据变现与民主化》，第29–50页。施普林格，2022年。

[62] Ricky Johnny。通过金融机构的治理框架解决数据孤岛问题。2023年9月。[63] Piers Kelly。政府遗留系统：如何打破数据孤岛并推动创新。网址：https://blog.govnet.co.uk/technology/legacy-systems-in-government-how-to-break-data-silos-and-innovate，2025年。[64] Nick Bakis、Ghassan Aouad 和 Mike Kagioglou。迈向分布式产品数据共享环境——迄今进展与未来挑战。《*Automation in Construction*》，16(5):586–595，2007年。[65] Ted Dunning 和 Ellen Friedman。时序数据库。《存储和访问数据的新方法》，2015年。[66] Chris J Date。《*SQL* 标准指南》。Addison-Wesley Longman Publishing Co., Inc.，1989年。[67] IBM。结构化数据与非结构化数据的主要区别是什么？网址：https://www.ibm.com/ think/topics/structured-vs-unstructured-data，2025年。[68] H Muscolino、A Machado、J Rydning 和 D Vesset。尚未挖掘的价值：每位高管都需要了解的非结构化数据，2023年。[69] Luke Tredinnick 和 Claire Laybats。管理非结构化信息，2024年。[70] William H Inmon 和 Anthony Nesavich。《挖掘非结构化数据：将非结构化数据和文本分析整合到商业智能中》。Pearson Education，2007年。[71] Farhad Soleimanian Gharehchopogh 和 Zeinab Abbasi Khalifelu。非结构化数据的分析与评估：文本挖掘与自然语言处理。在*2011*年第五届信息与通信技术应用国际会议（*AICT*）上发表，第1–4页。IEEE，2011年。[72] Irene Li、Jessica Pan、Jeremy Goldwasser、Neha Verma、Wai Pan Wong、Muhammed Yavuz Nuzumlalı、Benjamin Rosand、Yixin Li、Matthew Zhang、David Chang 等。面向电子健康记录中非结构化数据的神经自然语言处理：综述。《*Computer Science Review*》，46:100511，2022年。[73] Qiyan Deng、Jianhui Li、Chengliang Chai、Jinqi Liu、Junzhi She、Kaisen Jin、Zhaoze Sun、Yuhao Deng、Jia Yuan、Ye Yuan 等。使用大语言模型分析非结构化数据：全面的基准测试。*arXiv* 预印本 *arXiv:2510.27119*，2025年。[74] Ying Li、Zhen Tan 和 Weidong Xiao。通过多任务学习优化实现统一信息抽取的大语言模型。在亚太万维网会议（*APWeb*）与 *Web*时代信息管理会议（*WAIM*）联合举办的 *Web*与大数据国际会议上发表，第17–29页。施普林格，2024年。[75] Parastoo Mohagheghi 和 Øystein Haugen。评估领域特定建模解决方案。在概念建模国际会议上发表，第212–221页。施普林格，2010年。[76] S Arunprasath 和 Suresh Annamalai。改善医疗保健中的以患者为中心的数据检索与网络安全：面向安全未来的隐私保护解决方案。《*Multimedia Tools and Applications*》，83(27):70289–70319，2024年。[77] Rathnam Yuvatha、J Laxmi Narayana 和 V Gouthami。去中心化、抗中断国防数据网络中的安全数据检索与恢复系统。[78] Syed Tatheer Kazmi、Rohma Fatima Qayyum。英国金融业的数据法规。网址：https: // securiti.ai/data-regulations-in-the-uk-financial-sector/，2025年。[79] Marjan Mernik、Jan Heering 和 Anthony M Sloane。何时以及如何开发领域特定语言。《*ACM*计算调查》（*CSUR*），37(4):316–344，2005年。[80] Shiva Aryal、Tuyen Do、Bisesh Heyojoo、Sandeep Chataut、Bichar Dip Shrestha Gurung、Venkataramana Gad-hamshetty 和 Etienne Gnimpieba。利用多人工智能智能体实现跨领域知识发现。*arXiv* 预印本 *arXiv:2404.08511*，2024年。[81] Hung Du、Srikanth Thudumu、Rajesh Vasa 和 Kon Mouzakis。上下文感知多智能体系统综述：技术、挑战与未来方向。*arXiv* 预印本 *arXiv:2402.01968*，2024年。[82] Alexia Cambon、Brent Hecht、Ben Edelman、Donald Ngwe、Sonia Jaffe、Amy Heger、Mihaela Vorvoreanu、Sida Peng、Jake Hofman、Alex Farach 等。早期基于大语言模型的工具很可能显著提升企业信息工作者的生产力。微软研究院。*MSR-TR-2023*，43，2023年。[83] Shunyu Yao、Jeffrey Zhao、Dian Yu、Nan Du、Izhak Shafran、Karthik Narasimhan 和 Yuan Cao。ReAct：让语言模型中的推理与行动协同。*arXiv* 预印本 *arXiv:2210.03629*，2022年。[84] Python软件基金会。使用 Python 解释器。网址：https://docs.python.org/3/tutorial/ interpreter.html，2025年。[85] Mohamed Amine Ferrag、Norbert Tihanyi 和 Merouane Debbah。从大语言模型推理到自主人工智能智能体：全面综述。*arXiv* 预印本 *arXiv:2504.19678*，2025年。

[86]Will Fu-Hinthorn。多智能体架构的基准测试。网址：https://blog.langchain.com/benchmarking-multi-agent-architectures/，2025年。[87]PromptForward Team。MCP 过载：为什么你的大语言模型智能体不需要 20 个工具。网址：https:// promptforward.dev/blog/mcp-overload，2025年。[88] Bohao Yang、Chen Tang、Kun Zhao、Chenghao Xiao 和 Chenghua Lin。有效蒸馏大语言模型的基于表格的推理能力。载于*2024*年计算语言学、语言资源与评估联合国际会议（*LREC-COLING 2024*）论文集，第 5538–5550 页，2024年。[89] Chris Crowley。安全运营中心的通用最佳实践：2019年安全运营中心调查结果，2019年。[90] Kamal Zidan、Abu Alam、Jordan Allison 和 Ali Al-sherbaz。评估安全运营中心面临的挑战。载于未来信息与通信大会，第 256–271 页。施普林格，2024年。[91] Matt Loy。每天会产生多少数据。网址：https://www.techbusinessnews.com.au/blog/402-74-million-terrabytes-of-data-is-created-every-day/，2025年。[92] Harold D Stolovitch 和 Erica J Keeps。人类绩效技术手册：原则、实践与潜力。约翰·威立父子出版公司，2006年。[93] Fabio Cristiano、Xymena Kurowska、Tim Stevens、Louise Marie Hurel、Noran Shafik Fouad、Myriam Dunn Cavelty、Dennis Broeders、Tobias Liebetrau 和 James Shires。网络安全与知识生产的政治：迈向反思性实践。《网络政策杂志》，8(3)：331–364，2023年。[94] Jennifer Contreras、Melvin Ballera、Ace Lagman 和 Jennalyn Raviz。结合模式匹配应用与正则表达式自动机的基于词典的情感分析。2019年3月。[95] Risna Sari、Anggi Muhammad Rifa'i、Muhammad Salimy Ahsan、Mohammad Rezza Pahlevi 和 M Ilham Arief。螺旋式开发模型的系统性文献综述：主题、趋势与应用领域。《国际研究与应用技术杂志》（*INJURATECH*），2(2)：154–171，2022年。[96] Vasile-Daniel P˘av˘aloaia 和 Sabina-Cristiana Necula。人工智能作为颠覆性技术——系统性文献综述。《电子学》，12(5)：1102，2023年。[97] Alan Brown 教授。人工智能对领导力过去、现在和未来的影响——第一部分。网址：https: //www.oxford-group.com/insights/the-impact-of-ai-on-leadership/，2025年。[98] Eleena Sarah Mathew。提升大语言模型的安全性：提示注入攻击与防御措施综合综述。*Journal on Artificial Intelligence*，7(1)：347–363，2025年。