



From language to action: a review of large language models as autonomous agents and tool users

Sadia Sultana Chowdhury^{1,2,3} · Riasad Alvi^{2,4} · Subhey Sadi Rahman^{2,4} ·
Md Abdur Rahman^{2,4} · Mohaimenul Azam Khan Raiaan^{2,4,5} · Md Rafiqul Islam⁶ ·
Mukhtar Hussain⁸ · Sami Azam^{6,7}

Received: 25 August 2025 / Accepted: 14 December 2025 / Published online: 6 January 2026
© The Author(s) 2026

Abstract

The pursuit of human-level artificial intelligence (AI) has significantly advanced the development of autonomous agents and Large Language Models (LLMs). LLMs are now widely utilized as decision-making agents for their ability to interpret instructions, manage sequential tasks, and adapt through feedback. This review examines recent developments in employing LLMs as autonomous agents and tool users and comprises seven research questions. We only used the papers published between 2023 and 2025 in conferences of the A* and A-ranked and Q1 journals. A structured analysis of the LLM agents' architectural design principles, dividing their applications into single-agent and multi-agent systems, and strategies for integrating external tools is presented. In addition, the cognitive mechanisms of LLMs, including reasoning, planning, and memory, and the impact of prompting methods and fine-tuning procedures on agent performance are also investigated. Furthermore, we have evaluated current benchmarks and assessment protocols and provided an analysis of 68 publicly available datasets to assess the performance of LLM-based agents in various tasks. In conducting this review, we have identified critical findings on verifiable reasoning of LLMs, the capacity for self-improvement, and the personalization of LLM-based agents. Finally, we have discussed ten future research directions to overcome these gaps.

Keywords Large language models · Multi-agents · Reasoning · Evaluation · Generative AI

1 Introduction

Large language models (LLMs) have become central in artificial intelligence (AI) research due to their strong human-like ability to understand, generate, and reason in natural language (Kumar, 2024; Wang et al., 2025a). LLMs were used primarily as tools to serve as

Khan Raiaan and Sami Azam are equal supervision.

Extended author information available on the last page of the article

text generators or understanding modules within a larger application. However, further techniques such as few-shot prompting (Brown et al., 2020), chain-of-thought (CoT) prompting (Wei et al., 2022), and self-ask prompting (Press et al., 2023) demonstrated how the potential of LLMs could be improved through smart prompting and input pattern design. Beyond conventional natural language processing (NLP) tasks, LLMs are now serving as autonomous agents and intelligent tools. They are embedded into increasingly complex workflows where they perform planning, decision making, and tool interaction in various real-world applications, including research assistance (Schmidgall et al., 2025), software development (Qian et al., 2023), drug discoveries (Gottweis et al., 2025), multi-robot systems (Chen et al., 2025a), clinical support (Chen et al., 2025b), game simulation (Mao et al., 2023) and scientific simulations (Park et al., 2023).

LLMs as agents can observe their environment, make decisions, and take actions. Within this paradigm, single-agent LLM systems have demonstrated promising performance in decision-making tasks. Single-agent systems such as Reflexion (Shinn et al., 2023), Toolformer (Schick et al., 2023), and ReAct (Yao et al., 2023) showed how models can operate in decision loops that involve planning, memory, and tool use. However, they often struggle in dynamic environments that require simultaneous context tracking, external memory integration, and adaptive tool usage (Sun et al., 2025; Gao et al., 2025). To address these limitations, the concept of multi-agent LLM systems has gained increasing attention. In such systems, multiple LLMs interact as specialized agents, each with distinct roles or goals, collaborating to solve more complex tasks than a single agent can manage. Through structured communication, reflective reasoning, and explicit role assignments in simulated settings, multi-agent LLMs exhibit capabilities such as consensus building, uncertainty-aware planning, and autonomous tool interaction (Talebirad and Nadiri, 2023; Zhang et al., 2024a; Han et al., 2025). Examples such as MetaGPT (Hong et al., 2023), CAMEL (Li et al., 2023a), AgentBoard (Chang et al., 2024), AutoAct (Qiao et al., 2024a), and ProAgent (Zhang et al., 2024b) showcase how cooperative agents execute role-specific instructions and coordinate plans, while Generative Agents (Park et al., 2023) simulate human-like behaviors in interactive environments.

Moreover, LLMs as agents and tools now demonstrate massive potential in AI, and the demand to understand their evolving roles has intensified. Therefore, a systematic review of its recent advancement, a discussion of the remaining gaps, and a research direction for future advancements are essential to advance the field. With this focus, this survey provides a comprehensive and structured overview of current capabilities and system designs. We investigate the architectural foundations that enable agent-like behavior in LLMs, analyze how they interact with external tools, discuss the key limitations of current approaches, and highlight the remaining open challenges. Through this survey, our objective is to map the landscape of this emerging field and to offer a solid foundation for future research and development.

Our key contributions are summarized as follows.

- We conduct a comprehensive review of recent advancements in using LLMs as agents and tool users, with an explicit taxonomy that describes their architectures, frameworks, and interaction paradigms.
- We examine LLM reasoning, planning, and memory capabilities, and analyze how prompting, fine-tuning, and memory enhancement enhance agentic performance.

- We critically review current evaluation methods and benchmarks for LLM agents and tool users.
- We identify fundamental challenges, including alignment, reliability, and generalization, and outline promising research avenues to advance the robustness and intelligence of LLM agents.

The rest of the review is organized as follows. Section 2 presents related works, identifying gaps in existing surveys and situating our contribution. Section 3 outlines the methodology, including research questions, selection criteria, and search strategies. Section 4 explores the baseline LLMs used in agentic LLM systems. Section 5 focuses on tool integration in LLM workflows. Section 6 reviews the frameworks for constructing single-agent and multi-agent systems. Section 7 investigates the reasoning, planning, and memory capabilities of LLM agents. Section 8 discusses prompting, fine-tuning, and memory augmentation techniques that enhance agentic behavior. Section 9 evaluates current benchmarks and assessment methodologies. Section 10 provides a discussion. Section 11 outlines potential future research directions, and Sect. 12 concludes the review with a summary of the insights and contributions. Figure 1 illustrates the overall structure of the paper.

2 Related works

This section comprehensively analyzes the existing survey literature on LLMs as agents and tool users. The emergence of LLMs as autonomous agents and tool users has sparked interest in AI research. For example, Ferrag et al. (2025) provided a basic taxonomy of agents based on LLM, describing reasoning, planning, and tool use capabilities. Their survey cataloged over 60 benchmarks and systematically reviewed frameworks for agent behavior. Li (2025)

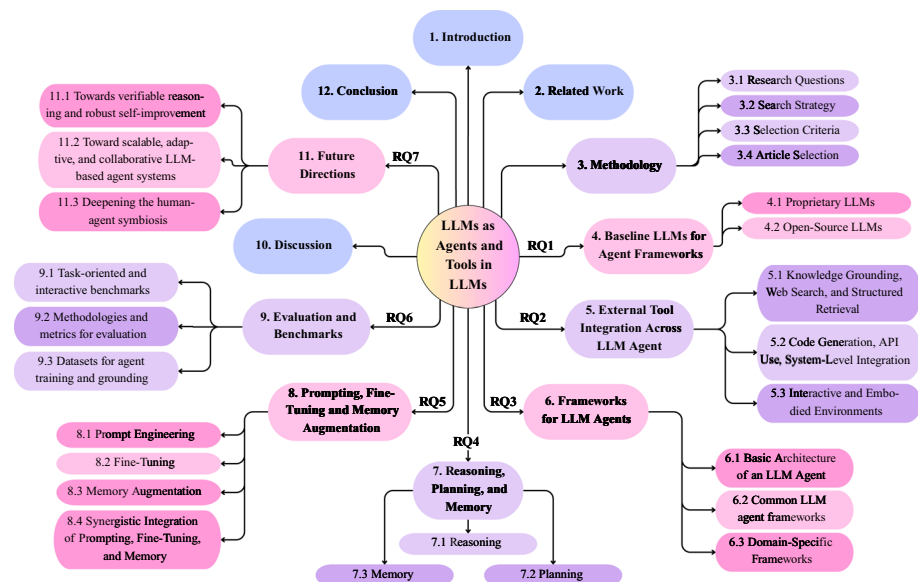


Fig. 1 An overview of the taxonomy used in this review

also offered an analysis of three agentic paradigms: tool use, retrieval-based planning, and feedback-driven learning. They categorized LLM agent roles, discussed the limitations of task-agnostic frameworks, and proposed directions for composable and generalizable agent development. Similarly, Xu et al. (2025a) focused on tool-augmented LLMs and outlined strategies for integrating external functionalities, including prompting, multimodal interaction, and agent coordination.

On the other hand, Xi et al. (2025) conceptualized LLM agents within a modular architecture 'brain, perception, and action' that includes reasoning, planning, and tool interaction. Wang et al. (2024a) organized a unified agent framework that integrates core modules such as reasoning, memory, planning, and action control. Their survey reviews capability acquisition strategies and discusses how LLM agents engage with external tools. Guo et al. (2024a) examined LLM-based multi-agent systems, classified popular architectures and communication strategies, tools integration, and evaluated agent interaction through benchmarks. Cheng et al. (2024a) analyzed the reasoning, planning, memory, and tool use mechanisms in single- and multi-agent environments. They explored architectural choices, prompting and fine-tuning techniques, and benchmark methodologies, while identifying limitations in adaptivity, robustness, and evaluation fidelity.

Although the existing surveys underscore significant progress in understanding LLM-based agents, particularly in tool use and architecture, they exhibit notable gaps in addressing the choice of baseline LLMs in multi-agent frameworks, the impact of prompting and fine-tuning, and a unified treatment of reasoning, memory, and evaluation. Addressing these limitations, our review systematically covers all key dimensions.

Table 1 presents a comparative analysis of seven prominent surveys against our review content, structured around the research questions (RQs): baseline LLMs used (RQ1), integration of external tools (RQ2), frameworks for building LLM agents (RQ3), reasoning, planning, and memory capabilities (RQ4), prompting and fine-tuning strategies (RQ5), evaluation and benchmarks (RQ6) and concerns and limitations (RQ7).

Existing studies often emphasize the discussion of integrating external tools across LLM agent workflows (i.e., RQ2); however, foundational dimensions, such as baseline LLM usage and the impact of prompting, fine-tuning, and memory enhancement, receive comparatively limited attention. In contrast, addressing all seven key areas, we propose our own taxonomy of agentic systems based on LLM, presented in Table 2. This taxonomy extends existing frameworks by organizing the field into core methodologies, agent capabilities, domain-specific applications, evaluation and safety aspects, and human-agent interaction. Our holistic approach distinguishes us as the most comprehensive to date, addressing the

Table 1 Comparative analysis of existing survey papers on LLM agents and tool use based on key research questions

Papers	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6	RQ7
Ferrag et al. (2025)	✗	✓	✓	✓	✗	✓	✓
Li (2025)	✗	✓	✓	✓	✗	✗	✓
Xu et al. (2025a)	✓	✓	✗	✓	✗	✓	✓
Xi et al. (2025)	✓	✓	✓	✓	✗	✗	✓
Wang et al. (2024a)	✗	✓	✓	✓	✗	✓	✓
Guo et al. (2024a)	✗	✓	✓	✗	✗	✓	✓
Cheng et al. (2024a)	✗	✓	✓	✓	✗	✓	✓
Ours	✓	✓	✓	✓	✓	✓	✓

Table 2 Taxonomy of LLM-based agentic systems

Category	References
1. Core Methodologies and Agent Architectures	
<i>1.1 Multi-Agent Systems & Collaboration Frameworks</i>	
1.1.1 General Collaborative Architectures	Ni and Buehler (2024); Cheng et al. (2024b); Klein et al. (2025); Jin et al. (2024)
1.1.2 Domain-Specific Collaborative Architectures	Lu et al. (2024); Kim et al. (2024)
1.1.3 Hierarchical & Role-Based Collaboration	Bai et al. (2025); Zhang et al. (2024c)
<i>1.2 Training & Learning Paradigms</i>	
1.2.1 Reinforcement & Self-Evolutionary Learning	Ma et al. (2024)
1.2.2 Offline & Self-Improvement Methods	Xi et al. (2025); Zhou et al. (2024)
1.2.3 Modular & Unified Training Architectures	Yin et al. (2024); Xu et al. (2024)
1.2.4 Bootstrapping from LLM Knowledge	Zhu and Simmons (2024); Jorgensen et al. (2024)
<i>1.3 Advanced Reasoning & Planning Mechanisms</i>	
1.3.1 Structured & Logical Reasoning	Abdaljalil et al. (2025)
1.3.2 Planning with World Knowledge	Qiao et al. (2024)
1.3.3 Contrastive Reasoning for Optimization	Wu et al. (2024)
2. Agent Capabilities and Enhancements	
<i>2.1 Tool & API Integration</i>	
2.1.1 Frameworks for Tool Mastery	Qin et al. (2024); Yuan et al. (2025)
2.1.2 Tool-Augmented Reasoning in Specific Domains	Wang et al. (2024b), (Goodell et al. (2025); Bran et al. (2024)
<i>2.2 Embodied Agents & Physical/Virtual Interaction</i>	
2.2.1 Vision-Language Navigation (VLN) & Grounding	Schumann et al. (2024); Zheng et al. (2024); Hong et al. (2024)
2.2.2 Robotics & Multi-Robot Task Planning	Zhang et al. (2024d); Kannan et al. (2024a)
2.2.3 Unified Multimodal Interaction	Wang et al. (2024c)
<i>2.3 Communication Mechanisms</i>	
2.3.1 Novel Communication Modalities	Kannan et al. (2024b)
2.3.2 Facilitating Agent Dialogue & Negotiation	Kannan et al. (2024c); Li et al. (2023a)
<i>2.4 Personalization & User Understanding</i>	
2.4.1 Implicit Intent Recognition	Qian et al. (2024)
2.4.2 Personalized Agent Behavior	Singh et al. (2024)
3. Domain-Specific Applications	
<i>3.1 Science & Engineering</i>	
3.1.1 Scientific Research & Discovery	Ni and Buehler (2024); Zhang et al. (2023); Ghafarollahi and Buehler (2024); Boiko et al. (2023)
3.1.2 Industrial & Infrastructure Management	Jin and Ma (2024); Xia et al. (2024); Xu et al. (2024)
3.1.3 Electronic Design Automation (EDA)	Wu et al. (2024a)
<i>3.2 Healthcare & Biomedicine</i>	
3.2.1 Clinical Decision Support & Diagnosis	Lu et al. (2024); Kim et al. (2024); Wang et al. (2025b); Ferber et al. (2025); Chen et al. (2025c)
3.2.2 Biomedical Data Analysis & Research	Huang et al. (2024); Liu et al. (2025a)
3.2.3 Patient & Provider Communication	Yang et al. (2024a); Jo et al. (2023); Abbasian et al. (2025); Barra et al. (2025)
3.2.4 Medical Data Generation & Calculation	Goodell et al. (2025)
<i>3.3 Software, Code & IT Operations</i>	

Table 2 (continued)

Category	References
3.3.1 Code Generation & Refinement	Bai et al. (2025)
3.3.2 Test Case Generation	Jorgensen et al. (2024)
3.3.3 Cloud Root Cause Analysis (RCA)	Wang et al. (2024b)
<i>3.4 Economics, Finance & Urban Planning</i>	
3.4.1 Macroeconomic & Market Simulation	Li et al. (2024a); Zhao et al. (2024a)
3.4.2 Urban Knowledge Graph Construction	Ning and Liu 2024)
<i>3.5 Interactive Systems & User Interfaces</i>	
3.5.1 Conversational Recommendation	Huang et al. (2025)
3.5.2 Natural User Interfaces (Gesture & Voice)	Yang et al. (2024a); Zeng et al. (2024)
4. Evaluation, Safety, and Alignment	
<i>4.1 Benchmarking & Evaluation Frameworks</i>	
4.1.1 General Agent Evaluation Platforms	Wijk et al. (2025); Chang et al. (2024)
4.1.2 Domain-Specific Benchmarks	Zhang et al. (2024e); Cheng and Chin 2024c)
<i>4.2 Safety, Security & Robustness</i>	
4.2.1 Security Threats & Backdoor Attacks	Yang et al. (2024b)
4.2.2 Privacy Preservation	Zhang et al. (2024f)
4.2.3 Resilience to Faulty Agents	tse Huang et al. (2025)
4.2.4 Safeguarding & Guardrail Mechanisms	Xiang et al. (2025)
<i>4.3 Alignment & Behavior Control</i>	
4.3.1 Value Alignment & Social Norms	Wang et al. (2024d); Pang et al. (2024)
4.3.2 Eliciting & Mitigating Undesirable Behaviors	Li et al. (2025a)
4.3.3 Automated Guideline Generation	Fu et al. (2024)
<i>4.4 Understanding Agent Limitations & Weaknesses</i>	
4.4.1 Probing for Failure Modes	George et al. (2024); Jo et al. (2023)
5. Human-Agent Interaction and Social Dynamics	
<i>5.1 Human-in-the-Loop & Collaboration</i>	
5.1.1 Synergistic Task Solving	Feng et al. (2024)
5.1.2 Integrating with Symbolic AI for Explainability	Frering et al. (2025)
<i>5.2 Simulating Human & Social Phenomena</i>	
5.2.1 Modeling Social Cognition & Prosocial Behavior	Li et al. (2023b); Zhang et al. (2024a); Liu et al. (2025b)
5.2.2 Simulating User Behavior & Economic Dynamics	Jin et al. (2024); Wang et al. (2025c); Behari et al. (2024)

foundational and emergent dimensions of agents and tools based on LLM, offering a unified perspective on their architectures, capabilities, and future directions.

3 Methodology

This study uses a clear and organized methodology to explore the evolving field of LLM agents. The analysis is guided by targeted RQs that aim to clarify the basic structures, capabilities, and environments of these agents. The literature selection process included a wide range of studies that focused on foundational structures, new methods, and practical implementation approaches. The selected works were organized to allow for a detailed look at new trends, system designs, and mechanisms that allow agent-like behaviors in LLMs.

3.1 Research questions (RQs)

The main goal of this review is to synthesize the current state of LLM-based agents by examining their basic principles and real-world applications. To achieve this, the following research questions were created:

RQ1: What core architectures and training mechanisms enable LLMs to exhibit agent-like behavior?

RQ2: How do LLMs interface with external tools, and what frameworks or paradigms govern this interaction?

RQ3: What are the key frameworks and systems for building single- or multi-agent ecosystems using LLMs?

RQ4: In what ways can LLM agents demonstrate reasoning, planning, memory, and self-reflection, and how do they compare with classical agents?

RQ5: How do prompting techniques, fine-tuning strategies, and memory augmentation impact the use and autonomy of tools in LLM agents?

RQ6: How is the performance of LLM agents evaluated, and what are the key benchmarks, metrics, and methodologies for measuring agent intelligence?

RQ7: What are the main challenges, limitations, and ethical concerns associated with the development and deployment of LLM-based agents?

These RQs are designed to offer a comprehensive multi-sided analysis of the field. RQ1 looks at the basic structures and training methods that help LLMs evolve from passive language models to active agents. RQ2 investigates how LLM agents interact with their environments, focusing on methods to integrate tools that guide their actions. RQ3 reviews the software frameworks and systems used in the creation and use of LLM agents, providing information on practical applications. RQ4 examines cognitive functions similar to those of LLM agents, such as reasoning, planning, and memory. RQ5 explores how optimization methods, including prompting, fine-tuning, and memory enhancement, affect agent independence and effectiveness. RQ6 addresses the critical area of evaluation, surveying the benchmarks and metrics used to validate agent capabilities and measure their effectiveness against established standards or human performance. In conclusion, RQ7 provides a critical perspective by investigating the inherent challenges, risks, and ethical considerations, such as reliability, security, and potential misuse, that accompany the rise of autonomous agents.

3.2 Search strategies

Search sources. The literature search focused on peer-reviewed publications from high-impact journals and conference proceedings in AI, machine learning, and natural language processing. The main sources included NeurIPS, ICML, ICLR, ACL, EMNLP, AAAI, EAAI, CVPR, ICCV, ACM, Nature Machine Intelligence, NPJ Digital Medicine, ACM Transactions, IEEE Transactions, and AI journals. These venues were selected for their reliable coverage of recent advances in LLMs and agent-based systems. The search looked for publications from 2023 to the present to capture the latest developments in this fast-moving field.

Search terms. A focused set of search terms was created to target the overlap of LLM and autonomous agents. These included: “Large Language Model agents,” “LLM-based agents,” “multi-agent LLM systems,” “tool-augmented LLMs,” “LLM planning and rea-

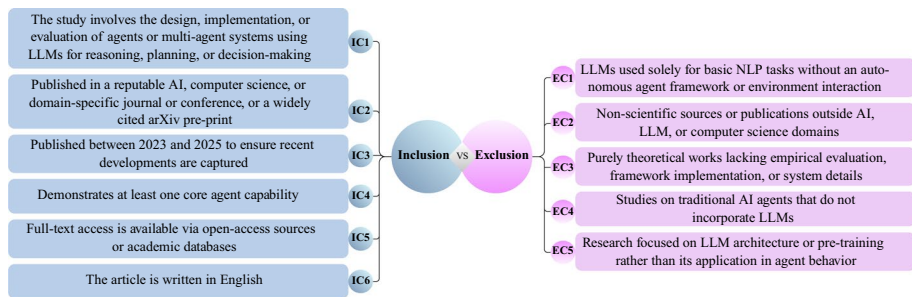


Fig. 2 Inclusion and exclusion criteria for article selection

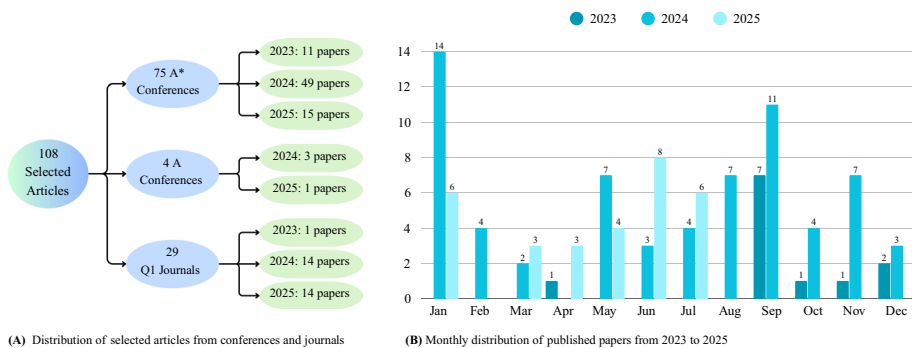


Fig. 3 (A) Flow diagram illustrating the distribution of selected articles across conferences and journals. (B) Bar chart showing the monthly publication trends from 2023 to 2025

soning,” “LLM self-reflection,” “autonomous LLM agents,” “communicative LLM agents,” “LLM agent frameworks,” “embodied LLM agents,” and “LLM tool integration.” The terms were gradually refined on the basis of keywords found in the literature and emerging trends in the literature.

3.3 Selection criteria

To compile the final list of articles for this review, we set up a strict checklist of inclusion and exclusion criteria. The key inclusion criteria and exclusion criteria are shown in Fig. 2.

3.4 Article selection

We systematically reviewed agentic LLM systems and the role of integrated tools within such systems. Articles were selected from A* and A-ranked conferences and leading Q1 journals. Figure 3 presents two complementary views of the publication distribution: (A) the distribution of selected articles between conferences and journals, and (B) the monthly distribution of published articles from 2023 to 2025. The review considered studies published between 2023 and 2025, with the majority appearing in 2024 and 2025. A total of 108 articles were included based on predefined inclusion (IC) and exclusion (EC) criteria. Among those, 75 were published in A* conferences, highlighting our concentration of high-impact

research. Furthermore, Table 3 summarizes the geographical distribution of the publications, indicating that China and the United States account for the majority of contributions.

3.5 Thematic scoring for article selection

A total of 108 papers were included in this review. To ensure a systematic and objective selection, each paper was evaluated using a structured thematic scoring framework, which quantified coverage across eight predefined dimensions:

- Focus on LLM Agentic Behavior
- Training Mechanisms for Autonomy
- Interaction with External Tools or Environments
- Frameworks for Single/Multi-Agent Systems
- Reasoning, Planning, Memory, or Self-Reflection
- Prompting, Fine-Tuning, or Memory Augmentation
- Evaluation Metrics and Benchmarks for Agentic Performance
- Challenges, Limitations, and Ethical Considerations

Each dimension was scored on a scale from 0, 1, or 2 per co-author, where (0) means "no", (1) means "partially", and (2) means "yes". The score for each question is a cumulative score of four co-authors, with a maximum score of 8 for each question (i.e., if co-author one gives 2, co-author two gives 1, co-author three gives 0, and co-author four gives 2, then the thematic score of this question is 5). Then the total score for each paper was computed as the sum across all eight dimensions, with a maximum possible score of 64. Papers with higher total scores were considered more comprehensive, while all included papers met a minimum inclusion threshold (total score ≥ 48).

The scoring was conducted independently by four co-authors with expertise in LLMs and autonomous systems. Any disagreements in scoring were resolved through discussion until consensus was reached, ensuring high reliability and reproducibility. This structured approach allows for transparent, objective synthesis of the literature, highlighting methodological trends, key contributions, and gaps in the study of LLMs as autonomous agents.

The complete thematic scoring for all 108 papers is provided as supplementary material in Table S1.¹

¹<https://github.com/mak-raiaan/LLMAgentsReview>.

Table 3 Geographical distribution of publications in agentic LLM research

Country	Number of papers	Country	Number of papers
China	46	Austria	1
USA	42	Korea	1
Germany	5	Denmark	1
UK	3	Ireland	1
Canada	3	Sweden	1
Singapore	2	Italy	1
Switzerland	1		

4 Baseline LLMs for agent frameworks

The architecture and functionality of an LLM agent are fundamentally related to its underlying language model (Cheng et al., 2024a; Chen et al., 2025b; Su et al., 2024). The selected foundational model ultimately determines the agent's attainable performance levels, associated costs, and flexibility for adaptation (Su et al., 2024; Guo et al., 2024a; Zhang et al., 2024g). Our findings from the reviewed literature reveal a distinct pattern of model adoption, characterized by the widespread use of proprietary models alongside an increasing use of competitive open source models (Li et al., 2025a; Jin and Ma, 2024; Ma et al., 2024; Zhang et al., 2024e; Li et al., 2025b). This section provides a structured overview of the LLMs employed across the reviewed papers, drawing attention to key trends in model selection, ranging from direct deployment to extensive fine-tuning.

4.1 Proprietary LLMs for agentic applications

Several contemporary studies on agents are heavily based on state-of-the-art proprietary models from leading AI research organizations (Bai et al., 2025; Cai et al., 2025). These models are frequently chosen for their advanced reasoning, strong instruction-following abilities, and robust integration with external tools, positioning them as a reliable benchmark for evaluating novel agentic architectures and methods (Zhang et al., 2024h; Wang et al., 2024d; Huang et al., 2025; Ruan et al., 2024; Zheng et al., 2024; Kannan et al., 2024c). Table 4 provides a comprehensive summary of the proprietary LLMs examined in this review.

Among the available language models, the Generative Pre-trained Transformer (GPT) family, most notably GPT-4 and its variants, remains the most widely adopted foundation for agent implementations (Li et al., 2025b). These models often serve as the core decision-making component or serve as reference baselines to assess the relative performance of novel techniques. For example, GPT models such as GPT-4 and GPT-3.5 provide a consistent point of comparison when evaluating the effectiveness of other open source LLMs (Li et al., 2025b; Jin and Ma, 2024; Zhang et al., 2024g; Pang et al., 2024; Ning and Liu, 2024; Chang et al., 2024; Ruan et al., 2024). In certain studies, GPT models have been integrated with other open-source counterparts to work collaboratively within multi-agent settings (Bai et al., 2025; Li et al., 2023b; Lu et al., 2024; Kim et al., 2024; Bo et al., 2024; Ghafarollahi and Buehler, 2024). In addition to being used to benchmark and integrate other models, GPT variants are frequently used as foundational models in several agent-based systems explored in studies (Bai et al., 2025; Jin and Ma, 2024; Ni and Buehler, 2024; Cheng et al., 2024b; Ma et al., 2024; Zhang et al., 2024h; Li et al., 2023b; Zhang et al., 2024g; Zhang et al., 2024a; Li et al., 2024a; Lu et al., 2024; Feng et al., 2024; George et al., 2024; Yuan et al., 2025; Zhu and Simmons, 2024; Kim et al., 2024; Cheng and Chin, 2024c; tse Huang et al., 2025; Xing et al., 2024; Jorgensen et al., 2024; Cuadra et al., 2024; Yang et al., 2024a; Zeng et al., 2024; Huang et al., 2025; Arumugam and Griffiths, 2025; Huang et al., 2023; Kannan et al., 2024c; Zhao et al., 2024a; Jin et al., 2024; Kannan et al., 2024b; Frering et al., 2025; Yang et al., 2024c; Song et al., 2023; Kannan et al., 2024c; Fu et al., 2024; Zhang et al., 2024f; Feldt et al., 2023; Wei et al., 2024; Xue et al., 2025; Ghafarollahi and Buehler, 2024; Huang et al., 2024; Boiko et al., 2023; Chen et al., 2025c; Bran et al., 2024; Ferber et al., 2025). Based on our analysis, we identified approximately 55 studies that employed GPT-4 or its variants

Table 4 Overview of proprietary LLMs for LLM agent research

Provider	Model variants	Primary applications	Key differences
OpenAI Li et al. (2025b); Jin and Ma (2024); Zhang et al. (2024g); Pang et al. (2024); Ning and Liu (2024); Chang et al. (2024); Ruan et al. (2024); Bai et al. (2025); Li et al. (2023b); Lu et al. (2024); Kim et al. (2024); Bo et al. (2024); Ghafarollahi and Buehler (2024); Ni and Buehler (2024); Cheng et al. (2024b); Ma et al. (2024); Zhang et al. (2024h); Zhang et al. (2024a); Li et al. (2024a); Feng et al. (2024); George et al. (2024); Yuan et al. (2025); Zhu and Simmons (2024); Cheng and Chin (2024c); tse Huang et al. (2025); Xing et al. (2024); Jorgensen et al. (2024); Cuadra et al. (2024); Yang et al. (2024a); Zeng et al. (2024); Huang et al. (2025); Arumugam and Griffiths (2025); Huang et al. (2023); Kannan et al. (2024c); Zhao et al. (2024a); Jin et al. (2024); Kannan et al. (2024b); Frering et al. (2025); Yang et al. (2024c); Song et al. (2023); Fu et al. (2024); Zhang et al. (2024f); Feldt et al. (2023); Wei et al. (2024); Xue et al. (2025); Huang et al. (2024); Boiko et al. (2023); Chen et al. (2025c); Bran et al. (2024); Ferber et al. (2025); Wang et al. (2023a); Zhang et al. (2023); Yang et al. (2024d); Wijk et al. (2025)	GPT-4, GPT-3.5, GPT-2, Text-DaVinci-003, Code-DaVinci-002, o1-preview, o1-mini	Core reasoning, planning, benchmark reference, multi-agent collaboration, embodied agents	multi-modal, tool-use/agents, advanced reasoning
Anthropic Zhang et al. (2024c); Chang et al. (2024); Kannan et al. (2024a); Zhang et al. (2024f); Wu et al. (2024); Liu et al. (2025b); Wijk et al. (2025); Cai et al. (2025); Li et al. (2025a); Zhang et al. (2024a); Ruan et al. (2024); Huang et al. (2023)	Claude 1, 2, 3 Opus, 3.5, 3.7 Sonnet, 3 Haiku	Benchmarking, time series learning, hallucination detection, R&D comparison, behavior elicitation	ultra-long context, safety-first alignment, strong instruction following
Google DeepMind Zhang et al. (2024f); Barra et al. (2025); Zhang et al. (2024e); Zhang et al. (2024g); Kim et al. (2024); Behari et al. (2024); George et al. (2024); Liu et al. (2025b); Zhang et al. (2024c); Muthusamy et al. (2023)	Gemini 1.0 Pro, Gemini 1.5 Pro, Gemini Pro, PaLM 2, FLAN-T5	Agent development, distraction reasoning, comparative evaluation, enterprise agent foundation	native multimodal, million-token context, Google-ecosystem integration
Others Liu et al. (2025b); Lampinen et al. (2023); Jo et al. (2023)	Mistral-medium-2312, Chinchilla-LM (70B), HyperCLOVA (82B)	Benchmark tasks, collaborative agents, large-scale agent frameworks	inference-efficient small models, data-efficient scaling

and around 23 studies that used GPT-3.5. Beyond GPT-4 and GPT-3.5, our review also identified the use of additional OpenAI models, including Code-DaVinci-002 (Wang et al., 2023a), Text-DaVinci-003 (Song et al., 2023; Wang et al., 2023a; Zhang et al., 2023; Yang et al., 2024d), and GPT-2 (Ma et al., 2024) as agents. Furthermore, Wijk et al. used the variant o1-preview (Wijk et al., 2025), and o1-mini appeared in the study by Arumugam and Griffiths (2025).

The Claude model family, developed by Anthropic, has emerged as a key player in the proprietary LLM domain and is often considered as a primary competitor to OpenAI models

(Zhang et al., 2024c; Chang et al., 2024; Kannan et al., 2024a; Zhang et al., 2024f). The Claude 3 lineup includes the Claude 3 Opus, the most advanced and capable model in the family, which has been used in several studies (Wu et al., 2024; Liu et al., 2025b). Claude 3.5 and 3.7 Sonnet, recognized for their improved speed and capability, have been used as agents in several tasks such as LLM behavior elicitation, time-series ML engineering, and comparing research and development (R&D) capabilities (Wijk et al., 2025; Cai et al., 2025; Li et al., 2025a). Earlier generation models, such as Claude-2, have been examined in multiple comparative evaluation studies (Zhang et al., 2024a; Ruan et al., 2024), and the research capabilities of agents powered by Claude-1 have been benchmarked (Huang et al., 2023). Moreover, GPT models excel in reasoning, instruction-following, and tool integration, making them highly versatile and widely adopted for general-purpose and multi-agent applications. However, Claude 3 models, especially Opus and 3.5/3.7 Sonnet, provide faster responses and stronger performance in R&D.

In LLM agent research, Google's proprietary models are frequently featured, particularly in frameworks involving multiple model evaluations. The Gemini series is the most prominent (Zhang et al., 2024f; Barra et al., 2025), with Gemini Pro emerging as the version most often used in agent development and evaluation (Zhang et al., 2024e; Zhang et al., 2024g; Kim et al., 2024; Behari et al., 2024). Gemini 1.5 Pro, known for its large context window, has been used in LLM-based agent reasoning under distraction tasks (George et al., 2024), and Gemini 1.0 Pro can be found in specific LLM agent benchmark studies (Liu et al., 2025b; Zhang et al., 2024c). The PaLM lineup is also represented, and PaLM 2 appears in the work of (Zhang et al., 2024c). Other significant models include FLAN-T5, which is noted as a foundational component for enterprise-level agents (Muthusamy et al., 2023). In addition to proprietary models from well-known tech companies, the Mistral medium-2312 (Liu et al., 2025b), Chinchilla-LM (70B) (Lampinen et al., 2023), and HyperCLOVA (82B) (Jo et al., 2023) models are also included in our review of LLM agents.

4.2 Open-sourced LLMs for agentic applications

The landscape of open-source LLMs used in agent research and development is rapidly diversifying, offering researchers and developers powerful alternatives to proprietary models (Huang et al., 2025; Xu et al., 2024). With models like Meta's LLaMA, Mistral, Google's Gemma, and the Qwen model from Alibaba gaining traction, open models now support a wide spectrum of capabilities, from code generation and dialogue to visual reasoning and collaborative decision making (Feng et al., 2024; Yuan et al., 2025; Schumann et al., 2024; Xing et al., 2024). An overview of all open source LLMs studied is presented in Table 5.

Meta's LLaMA suite of models is widely regarded as the default open source platform that supports contemporary research on LLM agents. The LLaMA 2 series (Zhang et al., 2024d; Zheng et al., 2024; Wu et al., 2024a; Xie et al., 2024; Ning and Liu, 2024), comprising models with 7B (Jin and Ma, 2024; Qin et al., 2024; Ma et al., 2024; Yin et al., 2024; Feng et al., 2024; Schumann et al., 2024; Huang et al., 2025; Pang et al., 2024; Yang et al., 2024b; Xu et al., 2024), 13B (Yin et al., 2024; Feng et al., 2024; Xing et al., 2024), and 70B (Xing et al., 2024; Xu et al., 2024; Xia et al., 2024) parameters, remains integral to the field, frequently used for zero-shot assessments via chat-tuned versions or as foundational checkpoints for lightweight LoRA alignment. With the advent of LLaMA 3 (Hemken et al., 2025; Ning and Liu, 2024; Singh et al., 2024; Liu et al., 2025a), this foundation has grown

Table 5 Overview of the open-source LLMs for LLM agent research

Model family	Model variants	Primary applications	Key differences
Meta LLaMA Zhang et al. (2024d); Zheng et al. (2024); Wu et al. (2024a); Xie et al. (2024); Ning and Liu (2024); Jin and Ma (2024); Qin et al. (2024); Ma et al. (2024); Yin et al. (2024); Feng et al. (2024); Schumann et al. (2024); Huang et al. (2025); Pang et al. (2024); Yang et al. (2024b); Xu et al. (2024); Xing et al. (2024); Xu et al. (2024); Xia et al. (2024); Hemken et al. (2025); Singh et al. (2024); Liu et al. (2025a); Yuan et al. (2025); Qiao et al. (2024); Chang et al. (2024); tse Huang et al. (2025); Goodell et al. (2025); Klein et al. (2025); Zhang et al. (2024g)	LLaMA 2 (7B, 13B, 70B), LLaMA 3 (8B, 70B), LLaMA–3.1 (11B), LLaMA–3.2 (90B), CodeL-LaMA (7B, 34B), ToolLLaMA-7B, COLLaMA-2	Zero-shot eval, LoRA fine-tuning, tool use, programming agents, collaborative agents	Open-weights, broad sizes, strong coding, huge ecosystem, multilingual, tool-use
Mistral AI Jin and Ma (2024); Zhang et al. (2024e); Qian et al. (2024); Wang et al. (2024d); Abdaljalil et al. (2025); Qiao et al. (2024); Zhai et al. (2024); Liu et al. (2025b)	Mistral-7B, Mixtral-8×7B	Efficient inference, strong generation quality, GPT–3.5 comparable coding	Inference-efficient, Mixture of Experts (MoE), fast throughput, long-context, strong coding
Google Gemma Zhou et al. (2024); Qiao et al. (2024); Tennant et al. (2025)	Gemma-7B, Gemma-2 (2B)	Retrieval-augmented planning, low-resource numerical agents	Lightweight, safety-tuned, efficient fine-tuning
Alibaba Qwen Li et al. (2025b); Zhou et al. (2024)	Qwen-max, Qwen 2.5 (72B)	Star-Agents, SMAC reinforcement	Chinese-English, long-context, tool-use & enterprise features, multimodal
DeepSeek AI Li et al. (2025b); Wang et al. (2025b); Abdaljalil et al. (2025)	DeepSeek-r1-70B, DeepSeek-7B, DeepSeek V2.5	Open-source agent models	Reasoning-focused, math/code strength, cost-efficient, RL-style alignment, long-context
Vicuna/WizardLM Zhang et al. (2024e); Pang et al. (2024); Wang et al. (2024b); Ruan et al. (2024); Xie et al. (2024); Liu et al. (2024a); de Almeida et al. (2025); Xia et al. (2024)	Vicuna-13B, Wizard-Vicuna-30B, WizardLM-70B	Conversational agents, high-capacity chat models	Instruction-tuned chat, easy fine-tune
Zhipu AI Zhou et al. (2024)	GLM-4, ChatGLM3	General chat and task execution	Chinese-first bilingual, tool-use & agents, long-context, enterprise stack
Microsoft Li et al. (2025b)	Phi-2, Phi–3.5 Mini	Compact inference agents	Ultra-small, on-device ready, textbook-style data curation, inference-efficient
OpenChat/Baichuan Ruan et al. (2024)	OpenChat–3.5, Baichuan-13B	Dialogue-optimized agents	Conversational alignment, Chinese-English, open-weights
LongChat Bo et al. (2024)	LongChat-7B	Long-context critic agents	Extra-long context, memory retention, position scaling tricks

Table 5 (continued)

Model family	Model variants	Primary applications	Key differences
Multimodal Zhai et al. (2024); Wang et al. (2024c); Hong et al. (2024)	LLaVA-7B, LLaVA-v1.6-mistral-7B, CogVLM-17B	Vision-language agents, GUI-based interactions	Vision-language, image grounding, visual question-answering & captioning, perceptual reasoning
Generative/Visual Zheng et al. (2024)	CLIP, Stable Diffusion XL, VQ-GAN	Image generation, visual embedding for agents	Image generation, latent diffusion, visual embeddings

significantly: its 8B (Singh et al., 2024; Yuan et al., 2025; Qiao et al., 2024; Chang et al., 2024) and 70B (Yuan et al., 2025; tse Huang et al., 2025; Goodell et al., 2025) instruction-tuned models are now integral to planning, tool-use, and multi-agent benchmarks. Additional advancements include the 'LLaMA-3-8B-instruct-8k' for longer input contexts, as well as newer model checkpoints such as LLaMA-3.1 (11B) (Klein et al., 2025) and LLaMA-3.2 (90B) (Klein et al., 2025), which support more advanced reasoning. Additionally, several specialized extensions have emerged alongside the base models: CodeLLaMA 7B and 34B enable programming agents (Zhang et al., 2024g); ToolLLaMA-7B facilitates the generation of structured tool calls (Yuan et al., 2025); and COLLaMA-2 (Zhang et al., 2024d) is designed for collaborative behaviors in AI embodied systems. These derivatives are integrated as either immutable inference modules prompted externally or as adaptable architectures through adapter-based tuning.

The models developed by Mistral AI offer a highly efficient line of alternatives, optimized for strong performance at relatively moderate computational cost. The dense Mistral-7B model is frequently preferred (Jin and Ma, 2024; Zhang et al., 2024e; Qian et al., 2024; Wang et al., 2024d; Abdaljalil et al., 2025; Qiao et al., 2024; Zhai et al., 2024) over LLaMA-2-7B, delivering better generation quality. On the other hand, the Mixtral-8×7B (Zhang et al., 2024e; Liu et al., 2025b) model, also known as open-mixtral-8×7B, utilizes a sparse expert architecture to achieve performance similar to GPT-3.5 in coding and planning tasks, while still benefiting from light inference.

The Gemma model family from Google represents a valuable addition to the open source LLM space (Zhou et al., 2024), the 7B version is already being integrated into retrieval-augmented planning architectures (Qiao et al., 2024). Furthermore, the Gemma-2 (2B) model tuned according to the instruction is utilized in studies (Tennant et al., 2025) involving numerical agents operating in low-resource or constraint environments.

A wider collection of open-source models contributes further diversity to the landscape of agent baselines. Alibaba's Qwen line (Qwen-max and the 72B parameter Qwen 2.5) competes strongly in Star Agents and SMAC reinforcement tasks (Li et al., 2025b; Zhou et al., 2024); DeepSeek AI's DeepSeek-r1-70B, DeepSeek-7B, and DeepSeek V2.5 achieve a top-tier score among open source models (Li et al., 2025b; Wang et al., 2025b; Abdaljalil et al., 2025). Conversation-centric agents often adopt Vicuna-13B or the larger Wizard-Vicuna-Uncensored 30B (Zhang et al., 2024e; Pang et al., 2024; Wang et al., 2024b; Ruan et al., 2024; Xie et al., 2024; Liu et al., 2024a; de Almeida et al., 2025), while the instruction-tuned WizardLM 70B serves as a high-capacity but fully open chat baseline (Xia et al., 2024). GLM-4 and ChatGLM3 (Zhipu AI), Microsoft's compact Phi-2 and Phi-3.5 Mini, the OpenChat-3.5 chat model optimized for dialogue, Baichuan's 13B chat model, and the

LongChat-7B enhanced by long context, the latter fine-tuned as a reflective critic in collaborative frameworks (Zhou et al., 2024; Li et al., 2025b; Abdaljalil et al., 2025; Bo et al., 2024; Zhang et al., 2024c).

This domain is further enriched by multimodal and architectural developments. Vision language assistants such as LLaVA-7B and the more recent LLaVA-v1.6-mistral-7B combine a CLIP-style image encoder with a chat-based LLM, allowing agent capabilities in embodied environments and GUI-based interfaces (Zhai et al., 2024; Wang et al., 2024c). CogVLM-17B expands this functionality with enhanced visual reasoning and understanding capacity (Hong et al., 2024). In the realms of perception and generative synthesis tasks, agents commonly use OpenAI CLIP, Stable Diffusion XL for high-resolution image generation, and VQ-GAN to produce latent image tokenization (Zheng et al., 2024). These components are often combined with the LLaMA-2 models in interactive applications. These model ecosystems establish the foundational open source landscape on which LLM agent research is currently based.

A critical comparison of proprietary versus open-source models reveals divergent evolutionary trajectories in LLM agent research. Although proprietary models such as GPT-4 and Claude demonstrate superior performance on complex reasoning benchmarks, their widespread deployment involves notable trade-offs. First, the cost of inference remains prohibitively high for large-scale or real-time applications. Second, the closed-source nature of GPT models restricts model transparency and limits fine-tuning flexibility compared to open-source alternatives. Furthermore, reliance on cloud-based APIs raises privacy and security concerns for sensitive domains such as healthcare and finance, where data cannot be externally shared. Recent studies also indicate that domain-specific tasks often require task-adaptive fine-tuning to achieve competitive accuracy. In this regard, open-source models such as Mistral-7B, DeepSeek-V2.5, and LLaMA-2-70B, when fine-tuned effectively, can achieve between 60% and 95% of GPT-4 and other models' performance while being significantly more cost-efficient (Wang et al., 2024d; Qian et al., 2024; Wang et al., 2025b; Qin et al., 2024). As a result, hybrid model architectures are increasingly adopted, where proprietary models are used as a high-level supervisor for data generation or validation, while smaller open-source models manage routine inference and domain-specific downstream tasks.

5 External tool integration across LLM agent workflows

The transformation of an LLM into an autonomous agent fundamentally relies on its capacity to engage with external systems and sources beyond the operational reach of its pre-trained data (Jin and Ma, 2024; Kannan et al., 2024b; Chen et al., 2025b; Jin et al., 2024; Ramos et al., 2025). It is facilitated through an increasingly rich ecosystem of external tools, APIs, and software frameworks (Cheng et al., 2024b; Qin et al., 2024). Far from being optional add-ons, the integration of these tools serves as foundational components that empower agents to access real-time information, perform complex operations, and the ability to interact with environments ranging from software platforms to physical systems (Li et al., 2025b; Jin and Ma, 2024; Ni and Buehler, 2024; Bran et al., 2024). A summary of the tools covered in various studies is presented in Table 6. Our review of existing studies

Table 6 Overview of the tools usage across LLM agents' capabilities

Domain	Single-agent	Multi-agent	(Single + Multi)	Key differences
Interactive and Embodied Environments Zhu and Simmons (2024); Frering et al. (2025); Zheng et al. (2024); Wang et al. (2023a); Jorgensen et al. (2024); Shinn et al. (2023); Li et al. (2025b); Zhang et al. (2024b); Jin et al. (2024)	MineDojo (Minecraft), MarioAI, ALFWorld	SMAC, Overcooked-AI, DeCoAgent (Smart Contracts)	AI2THOR, ROS 2, Gazebo, Clearpath Husky	Open-source stacks; simulation & robotics; embodied/multimodal interaction; native multi-agent tasks; RL & perception-action loops
Code Generation, API Use, and System-Level Integration Cheng et al. (2024b); Zhang et al. (2024g); Ni and Buehler (2024); Lu et al. (2024); Ghafarollahi and Buehler (2024); Chen et al. (2025c); Qian et al. (2024); Ramos et al. (2025); Qin et al. (2024); Wu et al. (2024a); Cuadra et al. (2024)	Code Interpreters, Copilot, Excel, Power BI, Jupyter AI, Chapyter, CoML, RDKit, Scikit-learn, ChatEDA (OpenROAD), Speechly	AutoGen	RapidAPI	Open-source & proprietary; code execution; API orchestration; system/engineering integration
Knowledge Grounding, Web Search, and Structured Retrieval Cheng et al. (2024b); Qian et al. (2024); Yin et al. (2024); Cheng and Chin (2024c); Lu et al. (2024); Feng et al. (2024); Yuan et al. (2025); Kim et al. (2024); Bran et al. (2024)	—	—	Bing Search API, Google Search, DuckDuckGo, Wikipedia API, PubMed, UMLS, ESI Handbook, FinBERT, MedRAG, ChemCrow (RoboRXN)	Open-source & proprietary mix; textual/structured retrieval; domain-specialized; RAG-ready

identifies several distinct patterns in tool utilization, from basic retrieval tasks to the management of sophisticated multi-agent systems.

5.1 Usage of tools across knowledge grounding, web search, and structured retrieval

One of the fundamental applications of tools is to mitigate the limitations of an LLM's fixed internal knowledge. These tools enable agents to retrieve real-time data and access domain-specific specialized knowledge repositories (Lu et al., 2024; Kim et al., 2024; Wang et al., 2025b; Kannan et al., 2024b; Ferber et al., 2025).

The integration of web search APIs is the most common and standard strategy for equipping agents with real-time data retrieval capabilities and overcoming the limitations of LLM knowledge. Studies frequently use tools such as the Bing Search API, Google Search, and DuckDuckGo to extend agents' access to up-to-date online content (Cheng et al., 2024b; Qian et al., 2024; Yin et al., 2024; Cheng and Chin, 2024c).

In addition, these tools are often paired with structured external knowledge sources. In particular, agents operate in domain-specific settings. For example, biomedical agents are linked to PubMed and UMLS knowledge bases, one also found using the Emergency Severity Index (ESI) handbook (Lu et al., 2024) for access to specialized medical information, FinBERT to classify sentiment of financial texts, while the Wikipedia Web API is a widely used source for general encyclopedic information (Feng et al., 2024; Yin et al., 2024; Lu et al., 2024; Cheng and Chin, 2024c; Yuan et al., 2025).

Frameworks such as MedRAG apply a retrieval augmented generation (RAG) approach explicitly to ensure that medical agents provide responses that are factually grounded in validated clinical knowledge (Kim et al., 2024). Bran et al. (2024) introduced ChemCrow to overcome the limitations of LLM in chemistry, which leverages GPT-4, RoboRXN, and 18 expert tools to autonomously plan and execute intricate chemical tasks in organic synthesis, drug discovery, and materials design (Bran et al., 2024).

5.2 Usage of tools across code generation, API use, and system-level integration

The generation and execution of code serves as a key mechanism of agentic behavior, empowering agents to perform sophisticated calculations, handle complex data operations, and engage with various software environments.

A widely used tool in agentic systems is the diverse types of Code Interpreter developed in a number of studies (Cheng et al., 2024b; Zhang et al., 2024g). This is particularly relevant for data science agents, which are evaluated for their integration with platforms and tools such as Excel, Copilot, Power BI, Jupyter AI, Chapyter, and CoML (Zhang et al., 2024g). Some studies also incorporate AutoGen, a framework designed to build agentic AI systems through multi-agent interactions and improved LLM inference capabilities (Ni and Buehler, 2024; Lu et al., 2024; Ghafarollahi and Buehler, 2024; Chen et al., 2025c). These agents often produce code to interact with file systems (Qian et al., 2024), command-line utilities (Qian et al., 2024), and domain-specific libraries, such as RDKit for chemical informatics (Ramos et al., 2025) and Scikit-learn for machine learning. Qin et al. found that using ChatGPT's function calling mechanism, LLMs can interact with 16,464 RESTful APIs sourced from RapidAPI by utilizing a neural API retriever and structured API documentation (Qin et al., 2024).

In the EDA sector, the ChatEDA agent demonstrates this capability through its Python wrapper-based interaction with the OpenROAD platform (Wu et al., 2024a). Cuadra et al., in their study, used Speechly to support the speech-to-text task for the purpose of entering health data (Cuadra et al., 2024).

5.3 Usage of tools across interactive and embodied environments

To investigate complex and interactive behaviors, agents are often employed in simulated or real-world environments. They function as tools that offer detailed, state-dependent feedback in response to agent interactions. Zhu and Simmons (2024) employed AI2THOR, a simulation platform that supports realistic 3D environments with physical interactions and dynamic visual states, for the purpose of assessing embodied agents within household environments.

In human-robot interaction, Frering et al. (2025) utilized ROS 2 and the Gazebo simulator with a model like the Clearpath Husky. Interactive environments used in agentic research include virtual platforms like game worlds such as Minecraft (via MineDojo) (Zheng et al., 2024; Wang et al., 2023a), the MarioAI platform (Jorgensen et al., 2024), and text-based simulations such as ALFWorld (Shinn et al., 2023). In multi-agent contexts, popular benchmarks include the StarCraft Multi-Agent Challenge (SMAC) and the collaborative game Overcooked-AI (Li et al., 2025b; Zhang et al., 2024b). An especially innovative example can be seen in the DeCoAgent framework, where LLM agents autonomously coordinate with the help of smart contracts, overcoming limitations of static, closed multi-agent environments (Jin et al., 2024).

6 Frameworks for building LLM agents

LLMs align closely with the core properties of agents in AI, making them strong candidates for agent foundations. First, they demonstrate autonomy by performing tasks without granular instructions, adapting responses to input, and generating creative content independently (Liu et al., 2024b; Wang et al., 2023b; Franceschelli and Musolesi, 2025). In terms of reactivity, LLMs can now handle multimodal inputs and interact with their environment using embodiment and tool integration, despite the latency caused by the textual reasoning stages (Schick et al., 2023; Qin et al., 2024; Driess et al., 2023; Kang et al., 2024). Their proactivity is seen in their ability to reason and plan when asked, including setting goals and decomposition of tasks in dynamic settings (Xi et al., 2025).

This section systematically reviews the frameworks developed for building LLM agents, highlighting their architectural designs, core capabilities, and operational domains. Categorizing existing solutions and analyzing their design principles provides a foundational lens for understanding how LLM agents are constructed and deployed in diverse scenarios.

6.1 Basic architecture of an LLM agent

Building LLM-based agents requires a systematic architectural design that enables LLMs to interact autonomously with their environment, recall relevant information, plan strategically, and execute appropriate actions. Unlike traditional question-answering models, these agents continuously perceive, reason, and adapt to various tasks. A widely adopted architecture for LLM agents primarily includes four core components: profile definition, memory, planning, and action execution, which together form a feedback-driven system in which memory shapes planning, actions modify memory, and update the agent's operational profile.

Profiling. The profiling module defines an agent's operational persona (e.g., developer, advisor, or task-specific role), conditioning its behavior and role policy through static profiles defined by experts or dynamic generative mechanisms (Hong et al., 2023; Dong et al., 2024). Static profiles encode domain knowledge and role-specific behaviors, while dynamic profiles simulate human-like variability by generating diverse agent personas through prompt engineering or parameter sampling (Wang et al., 2025c). These profiles may include demographic data, personality traits, and social relationships, significantly influencing downstream decisions in memory retrieval, planning strategies, and action selection.

Memory. Memory enables agents to maintain context across interactions through short-term (prompt-based) and long-term (externally stored) forms. Short-term memory supports in-the-moment reasoning by storing dialogue history and environmental signals, but is limited by LLM context windows (Wang et al., 2024a). Long-term memory captures reusable skills, patterns, or tools from past interactions. Memory formats vary from natural language, embeddings, databases (e.g., SQL), to structured lists, each chosen based on task requirements. Common operations include reading (prioritized by recency, relevance, and importance), writing (handling duplication and overflow), and reflection (summarizing past experiences into high-level insights).

Planning. Planning modules decompose complex tasks using strategies like CoT (Wei et al., 2022) and Tree-of-Thought (ToT) (Yao et al., 2023). Planning can occur with or without feedback. Feedback-free strategies often use stepwise prompting (e.g., CoT, ToT). Feedback-based iteration allows agents to dynamically adapt plans using signals from the environment, human input, or memory reflections.

Action execution. The action module translates plans into executable outputs. Actions may follow retrieved memories or precomputed plans. Furthermore, agents may engage in feedback loops in which the outcome of an action informs subsequent memory updates, plan revisions, or behavioral adaptations and can impact both the environment and the agent itself (Luo et al., 2025). Moreover, this module is crucial for grounding the agent in real or simulated environments.

Together, these components enable LLMs to function as autonomous agents, reasoning, remembering, planning, and acting in open-ended and evolving tasks. This modular architecture is foundational to both single-agent and multi-agent systems discussed in Sect. 7.

6.1.1 Single-agent LLM system

Single-agent LLM frameworks are often superior in generalization, reasoning, and task execution without additional model training. A single agent LLM can be conceptualized using a five-core component (LOMAR) (Cheng et al., 2024a): LLM, Objective, Memory, Action, and Rethink. Figure 4 illustrates the LOMAR framework.

LLM is the core of an agent, which allows task planning and decision making based on current inputs, memory, and feedback (Liu et al., 2024c). In addition, a **objective** defines the target goal and guides how the agent breaks down complex tasks to formulate a strategy. **Memory** is a dynamic storehouse of past interactions and relevant contextual information,

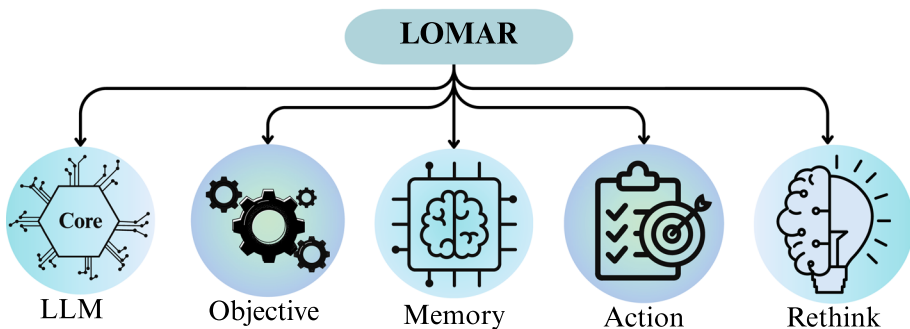


Fig. 4 An illustration of the LOMAR framework

enabling the agent to adapt its behavior thoughtfully (Wang et al., 2023c; Xu et al., 2025b). **Action** refers to the operational capabilities of the agent. It executes commands, interacts with tools, or communicates outputs (Schick et al., 2023); and **Rethink** facilitates reflective learning by evaluating previous actions and environmental feedback to inform future decisions (Yao et al., 2023).

These agents are designed to learn from continuous interactions and maintain coherent behavior over time through memory systems. Unlike multi-agent architectures that depend on collaborative dynamics, single-agent systems operate autonomously to complete tasks independently.

6.1.2 Multi-agent LLM systems

Multi-agent LLM systems are designed for coordinated collaboration, where multiple agents communicate, adapt, and solve problems together (Fig. 5). A description of how multiple agents observe, interact with, and adjust to different environments to work together toward shared objectives is given to highlight the foundation for effective multi-agent collaboration.

Agents-environment interaction. In a multi-agent LLM framework, individual agents operate within simulated, physical, or abstract environments based on their assigned roles. This layer allows agents to detect contextual changes, perform environment-specific actions, and adapt dynamically in response to feedback.

Communication structures. In this layer, three major paradigms are prevalent for agent communication, including *cooperative* (to work together toward shared goals), *debate* (to argue opposing views to reach consensus), and *competitive* (to pursue individual objectives). Communication can be centralized, decentralized, or shared memory-based, where agents publish and subscribe to a shared message pool.

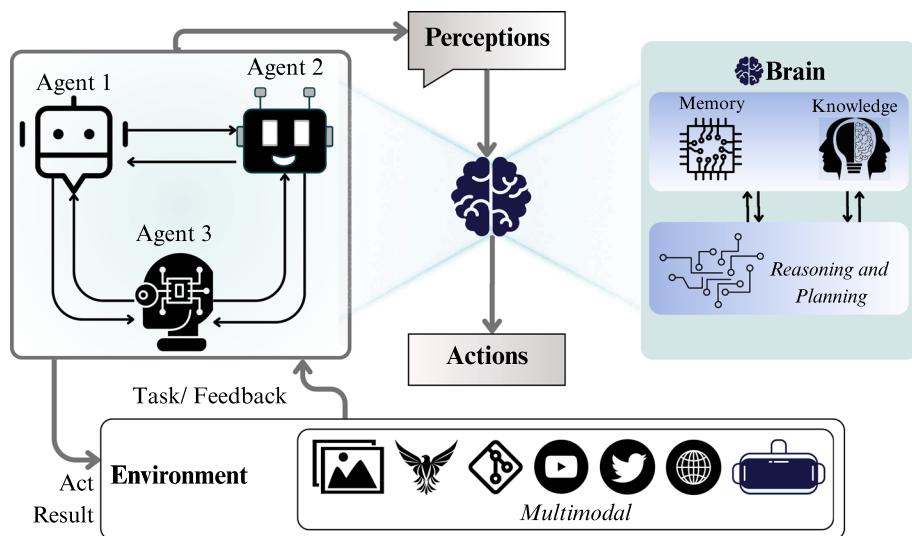


Fig. 5 A general overview of a multi-agent LLM system. Here, three agents operate within a multimodal environment where they act, generate results, and exchange feedback. Each agent is equipped with internal modules (brain), including memory, reasoning, and planning, that guide its behavior. Through collaborative communication, agents perceive the environment, coordinate strategies, and ultimately take action

Adaptive learning through feedback. Agents learn and adapt based on the feedback of the environment and interactions with other agents and humans. They can refine agent behavior by adjusting their strategies in response to dialogues or integrating human corrections, enabling flexible learning across dynamic scenarios.

Dynamic agent role. Multi-agent LLM frameworks support real-time agent generation or profile updates. This includes generating new agents with targeted roles or modifying goals in mid-task. However, as agent populations grow, maintaining coordination becomes increasingly vital for overall system performance.

6.2 Common LLM agent frameworks

Several frameworks have been adopted to implement LLM agents, facilitating reasoning, decision making, memory management, and action execution in single-agent and multi-agent contexts. Figure 6 presents a categorized overview of these frameworks based on their application in single-agent or multi-agent systems.

Among these, ReAct and Reflexion are the prominently utilized frameworks within single-agent LLM architectures. The selection between ReAct and Reflexion in LLM agents depends on the nature of the task. ReAct, by interleaving structured reasoning with action, such as planning or tool use, facilitates effective and context-aware execution. In contrast, Reflexion enables agents to retrospectively evaluate their prior outputs, learn from feedback, and refine subsequent decisions. Integrating both mechanisms allows for a balance between immediate operational efficiency and iterative self-improvement in complex tasks. AutoGen and CAMEL are widely employed in multi-agent environments. AutoGen is designed for building customizable, complex workflows that emphasize structured role coordination and task orchestration. CAMEL, on the other hand, focuses on autonomous role-playing and goal-driven collaboration, making it especially suited for dialogue-intensive or simulation-based environments. Furthermore, LangChain is also recognized as a versatile framework, applied across single-agent and even in multi-agent paradigms. While it offers a flexible,

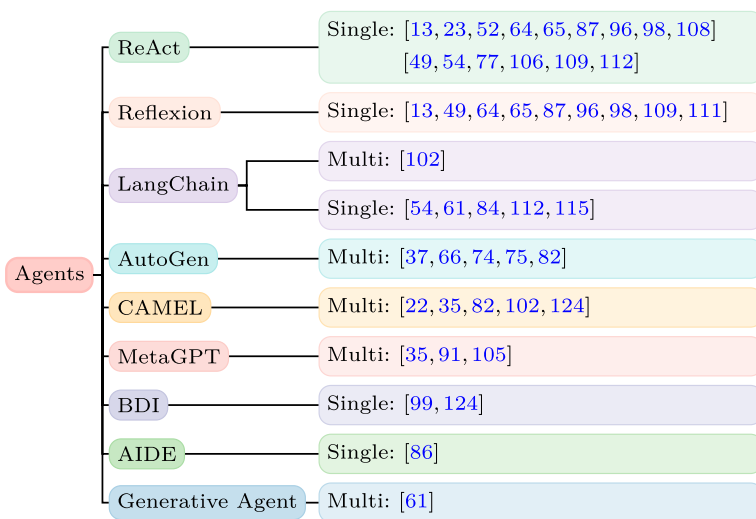


Fig. 6 Common LLM agent frameworks used in single- and multi-agent LLMs

modular infrastructure for LLM applications, its relatively unopinionated design can limit its applicability for certain tasks, as it places the responsibility for key architectural decisions largely on developers.

6.3 Domain-specific frameworks

Existing research on LLM-based agents is classified according to domain-specific applications, with each domain further divided into single-agent and multi-agent architectures. We have organized the review into nine specialized domains and comprehensively analyzed the relevant works within each.

6.3.1 Single-agent LLM systems' application domain

Single-agent LLM-based systems have been demonstrating remarkable performance across various application domains. These systems benefit from centralized decision making, lower communication overhead, and seamless knowledge integration, making them especially suitable for scalable and autonomous deployment. This section synthesizes evidence from recent works to highlight the breadth and depth of capabilities exhibited by single-agent LLM systems across multiple domains.

Healthcare. LLM agents in healthcare have shown promise in tasks ranging from personalized consultation to domain-specific scientific analysis. Conversational agents provide personalized health advice and support elderly care through natural interfaces (Yang et al., 2024a; Abbasian et al., 2025). Others optimize public health policies using reinforcement learning (RL) (Behari et al., 2024) or operate in real-world clinical settings (Jo et al., 2023). More specialized agents help with cancer protein analysis and biomedical research tasks (Liu et al., 2025a), underscoring the ability of single agent systems to operate in high-stakes and knowledge-intensive settings.

Software engineering. It is one of the major areas where single-agent LLM systems offer substantial automation and support. They improve code generation (Bai et al., 2025), perform automated software testing (Feldt et al., 2023), and diagnose complex failures in cloud systems through the use of integrated tools (Wang et al., 2024b). These agents operate autonomously in mobile and distributed environments, even as the limitations in edge cases are explored (Xing et al., 2024), showcasing their adaptability and evolving maturity.

Scientific research. LLMs are increasingly being positioned as autonomous scientific researchers. Agents can benchmark themselves against human researchers in AI tasks (Wijk et al., 2025), conduct chemistry experiments autonomously (Boiko et al., 2023), or aid in semiconductor and biological sequence analysis (Zhang et al., 2024i; de Almeida et al., 2025). These systems highlight how single-agent architectures enable sustained domain-specific scientific inquiry without constant human intervention (Huang et al., 2023).

Robotics. In robotics, single-agent LLM systems are cognitive controllers capable of grounded reasoning and planning. Integrating BDI architectures (Frering et al., 2025), visual grounding (Zheng et al., 2024; Frering et al., 2025), and few-shot learning for robot task planning (Song et al., 2023), these agents demonstrate their ability to translate high-level instructions into actions in physical or simulated environments. Embodied LLM agents are further empowered by cognitive initialization and explainability features (Zhu and Simmons, 2024), pushing forward the boundary of autonomous, language-guided robotics.

Recommendation system. Conversational LLM agents are deployed in recommendation systems to improve personalization and interaction. Agents simulate realistic user behavior for testing (Wang et al., 2025c) and provide interactive recommendation dialogues (Huang et al., 2025), capturing evolving user intent with minimal supervision.

Urban systems. In urban systems, LLM agents contribute to intelligent infrastructure management. They optimize mixed vehicle parking strategies (Jin and Ma, 2024), generate comprehensive urban knowledge graphs (Ning and Liu, 2024), and facilitate vision- and language-based street navigation (Schumann et al., 2024). These use cases highlight the scalability of single-agent systems in real-world multimodal environments.

General-purpose systems. A growing body of work seeks to develop general-purpose agent frameworks that empower LLMs with reasoning, planning, and tool use capabilities (Qin et al., 2024; Zhang et al., 2024h; Qian et al., 2024; Yuan et al., 2025; Xu et al., 2024). These systems support multitask environments (Zhang et al., 2024e), enhance collaboration with humans (Feng et al., 2024), and enable long-horizon planning through world knowledge and instruction tuning (Qiao et al., 2024; Fu et al., 2024). Several benchmarks have been proposed to assess performance in data science (Zhang et al., 2024g), safety (Ruan et al., 2024), and reasoning tasks (Abdaljalil et al., 2025; Liu et al., 2024c), while architectures address self-improvement (Pang et al., 2024) and causal reasoning (Lampinen et al., 2023). RL paradigms adapted to LLM further boost agent autonomy (Zhang et al., 2023; Shinn et al., 2023; Pang et al., 2024).

Beyond standard domains, single-agent LLM systems have also been adapted for specialized applications and use cases such as hand gesture understanding (Zeng et al., 2024) and time-series engineering challenges (Cai et al., 2025). These illustrate how adaptable the agentic paradigm is to domain constraints and modality fusion.

Security and privacy. Given their growing autonomy, security and privacy are critical concerns for LLM agents. Many studies have discovered backdoor vulnerabilities (Yang et al., 2024b), privacy risks during tool use (Zhang et al., 2024f), and the challenge of enforcing confidentiality and intentional alignment (Hemken et al., 2025; Khan et al., 2025).

These efforts highlight the need for principled design and evaluation in real-world deployments. Agents have to act ethically and socially responsibly. Work in the domain of social intelligence and ethics ensures that LLM agents adhere to the principles of moral reasoning and avoid harmful behaviors (Tennant et al., 2025), demonstrating the growing maturity in aligning LLM actions with human values.

6.3.2 Multi-agent LLM systems' application domain

The evolution from single-agent to multi-agent LLM systems represents a paradigmatic shift toward distributed intelligence architectures that include collaboration, specialization, and coordination to address complex real-world challenges. Multi-agent frameworks represent a significant evolution in AI capabilities, enabling complex problem-solving through collaboration, specialization, and coordination. This shift has expanded new frontiers in diverse domains where collective intelligence offers advantages in robustness, scalability, and adaptability (Cheng et al., 2024b; Ma et al., 2024; Zhang et al., 2024b; tse Huang et al., 2025; Klein et al., 2025).

Healthcare. It is among the most impactful domains that benefit from multi-agent LLM-based systems. These systems improve diagnostic accuracy through expert role assignment

and collaborative reasoning (Kim et al., 2024; Chen et al., 2025c; Ferber et al., 2025) and enhance electronic health record (EHR) processing through coordinated agent interaction (Wang et al., 2025b). Applications also include triage decision support (Lu et al., 2024), scenario-based medical training (Barra et al., 2025), and co-dialogue agents for clinical support (Chen et al., 2025c). Such systems enable distributed medical reasoning, integrating diverse knowledge modalities while improving interpretability and human-AI alignment.

Software engineering and scientific discovery. Multi-agent systems are also capable of optimizing complex workflows in the engineering domain. Agents collaboratively design hardware systems (Wu et al., 2024a), co-develop AI pipelines (Xue et al., 2025), and solve engineering problems through shared knowledge and dynamic role allocation (Ni and Buehler, 2024). In computational biology and chemistry, agents combine domain-specific tools with LLM reasoning for protein discovery (Ghafarirollahi and Buehler, 2024), molecular analysis (Huang et al., 2024), and automated lab planning (Bran et al., 2024), highlighting the benefits of combining symbolic, statistical, and simulation-based reasoning between agents.

Social intelligence and cognitive modeling. Agentic models offer testing environments to simulate human-like collaboration. Multi-agent frameworks explore cognitive process (Li et al., 2023a), trust dynamics (Xie et al., 2024), prosocial behavior (Liu et al., 2025b), and social psychology-informed coordination (Zhang et al., 2024a). Several works introduce benchmarking frameworks to assess social intelligence and collaborative behaviors in multi-agent LLM systems (Wang et al., 2024d; Chang et al., 2024). Others focus on reflective collaboration, where agents monitor and revise their strategies (Bo et al., 2024), or compete for performance gains (Zhao et al., 2024a). These advances contribute to the development of agents that exhibit nuanced social behaviors and adaptive communication (Wang et al., 2024d; Pang et al., 2024).

Robotics and embodied AI. Multi-agent LLMs coordinate robotic units in both virtual and physical environments. Agents collaboratively plan multi-robot tasks (Kannan et al., 2024a), generate adaptive driving simulations (Wei et al., 2024), and train embodied agents using parallel text world simulations (Yang et al., 2024d). Expanding on these capabilities, LLM-based multi-agent systems like CoELA demonstrate how language interfaces can enable decentralized planning, communication, and cooperation in complex embodied environments (Zhang et al., 2024d).

General-purpose multi-agent frameworks. The frameworks include co-evolutionary agent training (Ma et al., 2024), platforms for the discovery of emergent behavior (Cheng et al., 2024b), decentralized collaboration via blockchain (Jin et al., 2024), and robust systems designed to tolerate partial agent failure (tse Huang et al., 2025). These systems manage long-context tasks through sequential delegation (Zhang et al., 2024c), self-optimization of training data (Zhou et al., 2024), and proactive collaborative behavior (Zhang et al., 2024b). Other frameworks address reflective improvement (Bo et al., 2024), analytical decision-making (Cheng and Chin, 2024c), and social self-improvement through simulated interaction (Pang et al., 2024), forming the backbone for more domain-specific deployments.

Urban planning and telecommunications. Domains such as urban planning and communication are among the few unexplored domains that have also adopted a multi-agent LLM system. Coordinated agents manage large-scale network infrastructures (Xu et al., 2024) and satellite communication systems using expert mixtures (Kannan et al., 2024b), demonstrating scalability in mission-critical and real-time environments. Moreover, the

multi-agent approach improves specialization and fault tolerance (tse Huang et al., 2025), promotes cumulative problem solving (Klein et al., 2025), and allows systems that better reflect human collaborative dynamics (Zhang et al., 2024a; Xie et al., 2024). As these systems advance in capability and complexity, they are set to transform the way intelligent agents engage in various research domains and real-world applications.

7 Reasoning, planning, and memory of LLM agents

This section reviews the core cognitive functions: reasoning, planning, and memory, within agents based on LLM. We compare how these capabilities are designed and utilized across single-agent and multi-agent systems, highlighting common strategies and architectural distinctions. An overview of the reasoning, planning, and memory techniques employed in LLM-based agents in single-agent, multi-agent, and widely used categories is summarized in Table S2 of the Supplementary Material.

7.1 Reasoning in LLM-based agents

7.1.1 Application-specific reasoning techniques

Application-specific reasoning techniques address the limitations of standard approaches in specialized contexts by incorporating domain-specific knowledge, such as scientific logic, API tool usage, or multi-agent interaction dynamics.

Single-agent reasoning techniques. A range of reasoning strategies has been designed for single-agent settings where an agent acts, plans, and self-assesses autonomously. TOOLLLM (Qin et al., 2024) employed depth-first search-based decision trees to navigate over 16,000 real-world APIs, highlighting the strength of search-based reasoning in tool-rich environments. This reasoning technique outperforms ReACT by approximately 81% in average pass rate. This result suggests that the primary bottleneck in LLM agent reasoning lies less in algorithmic complexity and more in the model's capacity for coherent long-horizon planning. EASYTOOL (Yuan et al., 2025) advanced task decomposition by breaking high-level goals into modular sub-problems to improve step-wise execution. It significantly enhances LLM performance by providing concise, structured tool instructions. Compared to methods like ReAct and CoT prompting, it achieves higher success rates with fewer errors, demonstrating superior reasoning and tool-utilization capabilities. MATRIX (Pang et al., 2024) introduced simulation-based self-critique for introspective evaluation. ToolEmu (Ruan et al., 2024) introduced risk-prompted reasoning, implemented based on the ReAct framework, which allows GPT-4 to assess the risks of tool execution within a sandboxed setup. It allows systematic risk analysis of LLM agents and expands evaluation capability across various tools and testing configurations. Formal frameworks such as Theorem-of-Thought (ToTh) (Abdaljalil et al., 2025) decompose reasoning into abductive, deductive, and inductive subagents coordinated through belief propagation and NLI-based edge scoring. Compared to widely utilized techniques like CoT, CoT-Decoding, and Self-Consistency, ToTh achieved up to 29% higher accuracy on symbolic tasks and consistently strong performance across complex symbolic and numerical reasoning benchmarks.

Cognitive realism is further explored in CogMir (Liu et al., 2025b), which uses social context prompts to emulate cognitive biases, and moral regret mechanisms (Tennant et al., 2025) introduce ethically aware reasoning processes. Domain-specific adaptations include SHAP-based interpretability for semiconductor prediction (Kannan et al., 2024c), beneficial hallucination-driven hypothesis testing in software debugging (Feldt et al., 2023), and perplexity-informed confidence estimation for DNA sequence interpretation in ChatNT (Bran et al., 2024).

Collectively, these single-agent innovations demonstrate how LLMs can reason, evaluate, and adapt in isolation, often tackling complex tasks that demand high degrees of autonomy, safety, and explainability.

Multi-agent reasoning techniques. Several frameworks demonstrate specialized reasoning innovations tailored to multi-agent settings, showcasing how LLM agents collectively coordinate, communicate, and reason in complex environments.

For example, Prompt-Structured Strategic Reasoning (Li et al., 2025b) was introduced for multi-agent RL, enabling agents to collaborate in cooperative games effectively. AGENTVERSE (Cheng et al., 2024b) supports collaborative reasoning of multiple agents through structured logical representations such as logic grid puzzles and Modular Grounded Symbolic Modules. It addresses issues such as erroneous feedback and incomplete task coverage. In experiments, GPT-4 agent groups consistently achieve stronger performance than single-agent and CoT approaches across various reasoning tasks. Modeling belief states is essential in dynamic and partially observable domains; a Theory-of-Mind (ToM) inspired belief module (Li et al., 2023b) was developed to enhance coordination in multi-agent text-based games.

Similarly, Thread Memory (Jin and Ma, 2024) enables contextual reasoning in urban simulations involving mixed fleets of autonomous and human-driven agents. These innovations increasingly emphasize social, communicative, and contextual reasoning mechanisms that empower LLM agents to function as coherent participants in distributed, multi-agent ecosystems.

7.1.2 Widely-used reasoning techniques

Existing reasoning methods, such as CoT, ReAct, Self-Reflection, and Self-Critique, are crucial to enabling LLMs to perform complex cognitive tasks. These techniques support step-by-step problem solving, adaptive decision-making, and collaborative reasoning, contributing to their widespread adoption and effectiveness in improving LLM reasoning capabilities. CoT prompting (Bai et al., 2025; Li et al., 2023b; Yin et al., 2024; Zhu and Simmons, 2024; Zhang et al., 2024b; Ruan et al., 2024; Abdaljalil et al., 2025; Liu et al., 2025b; Wu et al., 2024a; Kannan et al., 2024b; Hong et al., 2024; Yang et al., 2024c; Zhai et al., 2024; Wang et al., 2024c; Xu et al., 2024; Xue et al., 2025; Liu et al., 2025a) is one of the most prominent approaches. It decomposes complex problems into intermediate logical steps, demonstrating success across the code generation, healthcare, and robotics domains.

Another notable technique, ReAct (Shinn et al., 2023; Xing et al., 2024; Feng et al., 2024; Zhang et al., 2024h; Zhang et al., 2024e) integrates reasoning with real-time task-specific actions, allowing agents to adapt dynamically to environmental feedback. This feature is particularly beneficial in interactive and decision-intensive settings. Furthermore, the Self-Reflection and Self-Critique mechanisms (Zhang et al., 2024e; Zhang et al., 2024a;

Liu et al., 2025b; Zhang et al., 2024d; Kannan et al., 2024b; Yang et al., 2024c; Wang et al., 2023a; Shinn et al., 2023; Behari et al., 2024; Zhai et al., 2024; Qu et al., 2024; Bo et al., 2024; Ning and Liu, 2024; Barra et al., 2025; Bran et al., 2024) are robust and widely used for their ability to empower agents to assess their outputs, identify errors, and improve subsequent reasoning through iterative metacognitive processes. Self-consistency methods (Kim et al., 2024; Wang et al., 2024b) improve reliability by generating multiple reasoning trajectories and selecting the most coherent response. This process, with variants such as Trajectory Level Self-Consistency, further improves the accuracy of planning.

In addition, collaborative approaches such as Multi-Agent Collaborative Reasoning (Zhang et al., 2024a; Lu et al., 2024; Ghafarollahi and Buehler, 2024; Chen et al., 2025c) allow interactions between multiple agents to debate and refine conclusions. Lastly, ensemble and consensus strategies, including ensemble refinement and temperature-based ensembles (Kim et al., 2024), improve decision making by aggregating multiple model perspectives and combining in-context learning (Ma et al., 2024; Fu et al., 2024) for better adaptability and knowledge transfer.

Comparatively, CoT exhibits strong performance in structured, stepwise reasoning but is less effective for interactive or dynamic tasks. Conversely, ReAct augments adaptability through the integration of reasoning and action, although it is associated with increased implementation complexity. Self-reflection facilitates iterative optimization of outputs but remains contingent upon adequate contextual information. Accordingly, the selection of an appropriate reasoning methodology requires rigorous consideration of task attributes, interaction requirements, and computational constraints.

7.2 Planning in LLM-based agents

7.2.1 Application-specific planning techniques

By integrating customized strategies, agents can better handle complex scenarios that general planning approaches might not optimally solve. We have categorized the existing planning methods into multi-agent and single-agent strategies.

Single-agent planning techniques. Single-agent frameworks emphasize self-sufficient decision making and autonomous planning that support independent agent functionality. Examples include TIMEARENA (Zhang et al., 2024e), which employs heuristic planning through temporal task decomposition to simulate realistic and time-sensitive environments. By addressing the critical issue of coordinating overlapping tasks with limited resources, it enables the evaluation and improvement of language agents' multitasking and temporal reasoning capabilities. ReHAC (Feng et al., 2024) applies multistep planning grounded in Markov Decision Processes (MDP), allowing agents to navigate human task allocations using formal probabilistic frameworks. Unlike traditional rule-based or prompt-driven planning models, it comprises RL to generalize across different tasks, datasets, and collaboration paradigms, reducing reliance on extensive human input or domain expertise. Cognitive agents using task stack planning (Zhu and Simmons, 2024) achieve structured goal decomposition, particularly useful in household or task-intensive domains.

Single-shot planning (Cai et al., 2025) generates a complete plan in a single step, ideal for time-constrained decision-making contexts. The World Knowledge Model (Qiao et al., 2024) introduces guided planning informed by persistent task knowledge, reducing the

dependency on blind exploration by encoding task-specific insights. Lastly, RAFA (Liu et al., 2024a) separates reasoning about future actions from current behavior through multi-step trajectory generation, enabling proactive planning in sequential decision-making tasks.

Multi-agent planning techniques. Several studies have proposed multi-agent planning strategies to address the complexities of coordination, delegation, and collaboration between distributed agents. For example, ProAgent (Zhang et al., 2024b) enabled modular planning supported by validation mechanisms to facilitate robust collaboration. This approach outperforms traditional learning-based agents, particularly in zero-shot coordination scenarios where such agents typically struggle. Then, in the recommendation system domain, a plan-first execution paradigm (Huang et al., 2025) was adopted to improve the reliability of action through comprehensive pre-action planning. DeCoAgent (Jin et al., 2024) utilized the decomposition of tasks based on prompts, based on a few shots, to enable decentralized agents to collaborate autonomously through smart contracts, offering a scalable framework for coordination.

Adaptive planning also appears in causal strategy learning systems like (Lampinen et al., 2023). This implements a two-phase structure, experimentation followed by exploitation, to allow agents to dynamically adjust strategies over time. AGENTBOARD (Chang et al., 2024) introduces a progress rate metric to monitor sub-goal completion across agents, thus supporting continuous evaluation in collaborative settings. It gives a clearer insight into agent capabilities compared to conventional success-rate benchmarks. Star Agents (Zhou et al., 2024) adopt an evolutionary strategy planning to enhance data optimization through agent evolution. Structured workflows are demonstrated in UrbanKGent (Ning and Liu, 2024), where fixed pipeline planning ensures deterministic construction of knowledge graphs in a multi-agent environment. SMART-LLM (Kannan et al., 2024a) tackles multi-robot coordination through coalition formation planning, dynamically forming agent teams to achieve shared objectives. Human-in-the-loop workflow planning in healthcare simulations (Barra et al., 2025) enables structured scenario designs, combining multiple agents under expert-defined protocols for controlled execution.

7.2.2 Widely-used planning techniques

Planning methods are vital for agents to perform effectively across diverse tasks, with several robust techniques widely used due to their versatility across domains. Multistep planning enables agents to sequence actions over extended horizons, adapting dynamically based on intermediate outcomes and environmental feedback (Feng et al., 2024; Cai et al., 2025; Kannan et al., 2024a; Liu et al., 2024a). Task decomposition planning breaks down complex goals into manageable subtasks, facilitating efficient resource allocation and parallel execution (Wei et al., 2024; Jin et al., 2024; Yuan et al., 2025; Zhang et al., 2024e). Its main advantage is the reduction of overall problem complexity, but performance can degrade when subtasks are highly interdependent, requiring careful sequential coordination to ensure correct execution. ReAct-based planning integrates reasoning with action, allowing agents to adjust plans in real time according to environmental feedback (Zhang et al., 2024h; Zhang et al., 2024e; Singh et al., 2024). While it can improve adaptability, its effectiveness varies with task complexity and depends heavily on accurate environment modeling. Reflexion planning incorporates feedback loops and self-correction mechanisms, helping agents learn from errors and improve future performance (Zhang et al., 2024e; Singh et al., 2024; Feng

et al., 2024). Re-planning and dynamic adaptation techniques enable agents to revise strategies responsively when initial plans fail or conditions change unexpectedly (Song et al., 2023; Wang et al., 2023a), which can improve robustness in uncertain environments, though frequent replanning may introduce computational overhead. Furthermore, plan generation and evaluation approaches improve overall planning quality by creating and assessing multiple candidate plans prior to execution (Wang et al., 2024d; Huang et al., 2023).

7.3 Memory mechanisms in LLM agents

7.3.1 Application-specific memory techniques

Single-agent memory techniques. Single-agent LLM systems emphasize memory techniques that optimize resource management, contextual awareness, and episodic continuity within individual agent frameworks. For example, RE-Bench, proposed by Wijk et al., tracks background memory during training (Wijk et al., 2025), and RCAgent's OBSK manages the structured context (Wang et al., 2024b). Healthcare dialogue benefits from memory buffers (Cuadra et al., 2024), while VLN-Imagine augments vision transformer memory with generated images (Perincherry et al., 2025).

Temporal memory tools include prompt context tracking in ToolEmu (Ruan et al., 2024) and compressed Research Logs in MAgentBench (Huang et al., 2023). Formal Reasoning Graphs (Abdaljalil et al., 2025) and STEVE-EYE's episodic re-prompting (Zheng et al., 2024) support transparency and continuity. Specialized memory includes moral alignment prompts (Tennant et al., 2025), extended histories in AGENTBENCH (Liu et al., 2024c), and integration of external screenshots and latent weights in CogAgent (Hong et al., 2024).

Additional methods involve rolling logs for robots (Frering et al., 2025), previous tool output in context (Yang et al., 2024c), negotiated ontologies to prevent repetition (Kannan et al., 2024c), and concatenated dialogue contexts for interactive planning (Wang et al., 2023a). These techniques improve adaptability and long-term task performance in single-agent systems.

Multi-agent memory techniques. Application-specific memory techniques in multi-agent LLM systems have been developed to address the complexities of collaborative and distributed environments, employing advanced retrieval and dynamic management strategies tailored to these settings.

The recent K and relevant K retrieval strategies of ProAgent (Zhang et al., 2024b) and ColaCare's retrieval-augmented generation module (Wang et al., 2025b) exemplify efficient memory access. Domain-specialized structures include satellite network knowledge bases segmented into sub-blocks (Kannan et al., 2024b). Dynamic memory approaches involve refeeding prior dialogue turns for attitude shifts (Liu et al., 2025b), discounted back-tracking for state revival (Klein et al., 2025), and running textual memory in MATRIX (Pang et al., 2024). Long-term persistent storage for agent states and blockchain collaboration is implemented in DeCoAgent (Jin et al., 2024), while CompeteAI maintains daybook and comment histories to analyze strategies over time (Zhao et al., 2024a).

These systems emphasize coordinated memory for inter-agent planning and sustained reasoning. Moreover, these approaches demonstrate the critical importance of memory architectures that support inter-agent coordination, long-term strategic planning, and specialized domain reasoning in multi-agent LLM systems.

7.3.2 Widely-used memory techniques

Various memory techniques have been proposed to support LLM agents in different operational contexts, each addressing specific information retention and recall requirements. Context window memory is one of the most commonly used methods (Zhang et al., 2023; Pang et al., 2024; Wang et al., 2024c; Qu et al., 2024; Ning and Liu, 2024; Xie et al., 2024; Kannan et al., 2024a; Song et al., 2023; Jo et al., 2023; Boiko et al., 2023; Goodell et al., 2025). Using the internal mechanisms of the transformer, it retains recent inputs and preserves local coherence throughout the prompt. This approach enables agents to maintain consistency during short interactions without relying on external systems. In contrast, conversational and dialogue history stores complete sequences of past interactions to support context-aware responses and maintain continuity over extended sessions (Wang et al., 2024d; Li et al., 2023a; Jo et al., 2023; Wei et al., 2024; Ghafarollahi and Buehler, 2024; Barra et al., 2025; Chen et al., 2025c).

More complex memory implementations include Reflexion-style memory systems, which integrate recent context with structured representations of prior outcomes, allowing agents to update behavior based on previous successes and failures (Singh et al., 2024; Feng et al., 2024; Shinn et al., 2023; Bo et al., 2024). Furthermore, RAG methods connect agents to external knowledge sources during inference, enabling access to factual information (Wang et al., 2025b; Jin et al., 2024; Barra et al., 2025; Goodell et al., 2025). The components of the working memory and the scratchpad temporarily hold intermediate reasoning steps and enable sequential problem solving (Abdaljalil et al., 2025; Cai et al., 2025). In parallel, long-term episodic memory models iteratively capture and organize agent experiences, supporting generalization of past situations and improving task adaptation (Zhang et al., 2023; Yang et al., 2024d). Specific systems apply short-term memory optimization techniques for immediate reactivity tasks to focus on rapid access to updated data while minimizing overhead (Bo et al., 2024; Jo et al., 2023; Xu et al., 2024; Huang et al., 2024). Several systems implement hybrid memory mechanisms, including models that merge local prompt-based memory with persistent indexed documents (Boiko et al., 2023). These designs reflect ongoing efforts to construct memory architectures that support immediate responsiveness and long-term behavioral consistency.

Different memory mechanisms vary in effectiveness according to the task and the context of the agent. Context window memory suits short-term, reactive tasks, while conversational and episodic memory support extended interactions and continuity. Retrieval-augmented and hybrid systems improve access to external knowledge, enhancing reasoning in complex domains. In multi-agent settings, structured and dynamic memory enable coordinated planning. In general, memory designs are most effective when aligned with specific operational demands.

8 Impact of prompting, fine-tuning, and memory augmentation

Although foundational LLMs have extensive general knowledge and strong reasoning skills, they are not automatically independent agents. Turning these general models into specialized, goal-driven agents that can see, plan, and act well requires a variety of advanced techniques (Jin et al., 2024; Lu et al., 2024; Feng et al., 2024). The performance, reliability, and

independence of LLM-based agents are highly dependent on three key areas of improvement: prompting, fine-tuning, and memory enhancement. These methods help developers shape the agent's behavior, give it expertise in specific areas, and prepare it for complex long-term tasks (Ghafarollahi and Buehler, 2024; Huang et al., 2024; Abbasian et al., 2025).

8.1 Prompt engineering: a non-parametric approach to dynamic control and role delegation

Prompt engineering has become a key method for directing the behavior of LLM-based agents (Barra et al., 2025; Li et al., 2025a; George et al., 2024). Unlike parametric approaches like fine-tuning, which change a model's weights, prompt engineering works during inference time. It offers a simple way to define tasks, assign roles, and control agent behavior dynamically without needing a lot of computing power. This method takes advantage of the natural instruction-following and in-context learning abilities of LLMs to manage complex tasks (Abdaljalil et al., 2025). This includes everything from individual agent reasoning to complex teamwork among multiple agents (Kim et al., 2024). The flexibility of prompting makes it the primary way to set goals, integrate tools, and simulate complex social interactions. At the single-agent level, prompt engineering plays a key role in defining an agent's operational settings and reasoning style. For instance, Reflexion (Shinn et al., 2023) demonstrates how prompts enable self-reflection without weight updates, achieving performance improvements through feedback-guided adjustments. This type of self-correction, guided by prompts, also works well in dynamic situations. (Behari et al., 2024) used a Decision-Language Model (DLM) to understand natural language policy goals, suggest reward functions as code, and adjust them based on the results of simulations. However, the effectiveness of this control can be limited by context length and complexity. George et al. (2024) notes that agents may struggle to use important information when faced with long histories and distracting "red herring" facts, even with CoT prompting. Moreover, prompting is the main way to enable agents to use external tools, which enhances their abilities beyond their existing knowledge. EASYTOOL (Yuan et al., 2025) converts extensive tool documentation into clear, simple instructions. This helps LLMs choose and perform the correct functions and has been successfully applied in specialized fields. Besides, ChemCrow (Bran et al., 2024) combines 18 expert-designed chemistry tools that an LLM agent learns to use through well-designed prompts to independently plan and carry out complex syntheses. In the medical field, Goodell et al. (2025) show that giving agents task-specific calculation tools like OpenMedCalc via prompting greatly reduces math errors. These domain-specific designs, ChemCrow and OpenMedCalc, yield higher precision in their respective fields yet require substantial expert knowledge. Therefore, selecting a prompt-tool strategy depends on whether adaptability or domain performance is prioritized. This concept extends to multimodal contexts, where Yang et al. (2024c) apply prompts in LLM-Grounder to break down language queries and manage visual grounding tools. Meanwhile, Song et al. (2023) connect agent plans in LLM-Planner by updating prompts with lists of visually perceived objects. Prompt engineering ranges from controlling individual agents to managing entire "societies" of agents. Here, system-level prompts set roles, responsibilities, and communication protocols. Ni and Buehler (2024) show this with the MechAgents framework, which creates teams of agents with roles such as planner, coder, and critic to solve mechanics problems. Cheng et al. (2024b) propose AGENTVERSE to create expert roles and task instructions

in a zero-shot manner. To manage long-context tasks, Zhang et al. (2024c) introduce the Chain-of-Agents (CoA) framework, where a manager agent combines contributions from multiple worker agents, each handling a part of the document. Likewise, Klein et al. (2025) suggest the FLEET OF AGENTS (FOA) framework, which uses a particle filtering method where many agents explore a search space, guided by prompts to improve the cost-quality balance. This approach has proven very effective in simulating complex social and economic systems that resemble human behavior. Zhang et al. (2024a) build LLM agent societies with distinct traits and thinking patterns using only prompts. These societies display behaviors such as conformity and consensus. Zhao et al. (2024a) employ prompts in CompeteAI to create a virtual town filled with competing restaurant agents to examine market dynamics. Liu et al. (2025b) present the CogMir framework, which uses prompts to encode social variables and induce prosocial irrationality, showing that LLM agents can repeatedly mimic human cognitive biases. This multi-agent, prompt-driven method has strong applications in specific fields. In clinical triage, Lu et al. (2024) use TRIAGEAGENT to simulate a multi-disciplinary team. Chen et al. (2025c) apply a similar method, MAC, for diagnosing rare diseases. In scientific discovery, Ghafarollahi and Buehler (2024) organize agents in ProtAgents to design new proteins together. Barra et al. (2025) create a workflow to automate the production of healthcare simulation scenarios. While prompt engineering is a strong non-parametric tool, it also works well with parametric fine-tuning. Prompting often serves as a way to create high-quality, structured datasets for training smaller, specialized agents. For example, Qin et al. (2024) use ChatGPT in their ToolLLM framework to generate a large dataset of instructions and API call solutions. This dataset is then used to fine-tune LLaMA into the effective ToolLLaMA. Similarly, Qian et al. (2024) develop Mistral-Interact by fine-tuning Mistral-7B on a set of user dialogues created by prompting GPT-4. Pang et al. (2024) use the MATRIX framework to generate alignment data for fine-tuning. This method, as Wu et al. (2024a) point out, allows the skills of large, proprietary models to be distilled into smaller, open-source agents. On the other hand, fine-tuning can help agents better follow complex prompts or perform specific skills. Yin et al. (2024) demonstrate that fine-tuning agents with the LUMOS framework on unified, high-quality annotations improves their planning and grounding abilities. Wang et al. (2024d) fine-tune a 7B model in SOTOPIA- π using data from prompted social interactions. This makes it match the social intelligence of a much larger GPT-4-based agent. This technique proves particularly useful in embodied AI. Yang et al. (2024d) show that an LLM expert, enhanced through reflective prompting, can generate distillation data to fine-tune a Vision-Language Model (VLM), teaching it to navigate and interact with a visual world. This shows that while prompting offers dynamic, real-time control, fine-tuning can embed more robust and specialized abilities into agents.

8.2 Fine-tuning: embedding domain expertise and core behavioral traits

While prompt engineering allows for quick control during inference, fine-tuning offers an additional method to embed specialized knowledge and important traits into an agent's design (Kim et al., 2024; Zheng et al., 2024; Klein et al., 2025). This process updates the model's weights using curated datasets. It is essential for developing smaller, more efficient agents that can imitate the abilities of larger models or for teaching complex skills that are difficult to achieve through prompting alone (Lu et al., 2024). Fine-tuning is the main way

to adapt to new fields, gain skills, and improve the basic reasoning and interaction abilities of agents based on LLMs (Zhang et al., 2024d; Wu et al., 2024a; Zhang et al., 2023). A common practice in developing agents is using fine-tuning for knowledge distillation. In this method, the advanced reasoning of a large, skilled model generates high-quality training data for a smaller, open-source model (Lu et al., 2024). This makes powerful capabilities more accessible. For example, Qin et al. (2024) pioneered this with ToolLLaMA by fine-tuning LLaMA on a vast dataset of tool-use instructions and solutions from ChatGPT. This led to a highly capable open-source tool-using agent. Qian et al. (2024) created Mistral-Interact by fine-tuning Mistral-7B on user dialogues simulated by GPT-4. It focuses on enhancing user-agent interaction, proactively clarifying vague instructions, and refining user intentions before task execution. Pang et al. (2024) applied the MATRIX framework to produce social simulation data for alignment fine-tuning. This method also works for specialized fields, as shown by Wu et al. (2024a) with ChatEDA, where a fine-tuned model, AutoMage, outperformed GPT-4 in electronic design automation tasks. The process is often iterative. Frameworks like Star-Agents from Zhou et al. (2024) use multi-agent systems to automatically generate, evaluate, and refine instruction data to improve the fine-tuning process itself. Beyond simple knowledge transfer, fine-tuning is essential for developing the complex behavioral and cognitive skills that define an agent's main abilities. This includes social intelligence, where Wang et al. (2024d) used data from guided social interactions to fine-tune SOTOPIA- π . This approach enabled a 7B model to achieve social goal completion similar to that of a larger GPT-4 agent. Fine-tuning can also improve self-awareness skills. Qu et al. (2024) created RISE, an iterative fine-tuning process that helps agents to think about their own actions and fix their mistakes, which is difficult to accomplish through prompting alone. Similarly, Bo et al. (2024) fine-tuned a shared "reflector" agent within their COPPER framework to enhance collaboration among multiple agents. This method works particularly well for embodied agents, as fine-tuning connects abstract reasoning with physical action. Zhai et al. (2024) used RL to fine-tune VLMs, improving their decision-making in goal-oriented tasks. Yang et al. (2024d) employed an LLM expert to create distillation data to fine-tune a VLM called EMMA, teaching it to understand and interact with a visual environment. Fine-tuning is also crucial for transforming general models into specialized experts that can function in complex, real-world settings. In the realm of embodied AI, Schumann et al. (2024) demonstrated that while prompting VELMA had some success, fine-tuning on navigation examples resulted in a 25% relative improvement in task completion. Hong et al. (2024) fine-tuned CogAgent on GUI-grounding data, greatly enhancing its ability to navigate and manage computer interfaces. This specialization is vital in the fields of science and medicine. Liu et al. (2025a) fine-tuned DrBioRight 2.0 on a large cancer proteomics dataset to develop an expert bioinformatics chatbot. In addition, de Almeida et al. (2025) fine-tuned ChatNT to create a multimodal agent with a deep understanding of DNA, RNA, and protein sequences. However, embedding expertise comes with risks; Yang et al. (2024b) showed that the fine-tuning process itself can be an avenue for backdoor attacks, where tainted data might train an agent to carry out harmful actions secretly. Ultimately, fine-tuning and prompting work together in a complementary way. Good prompting often serves as a foundation for creating the high-quality data needed for effective fine-tuning. On the other hand, fine-tuning can help agents respond better to complex prompts and improve their planning. Yin et al. (2024) illustrate this with the LUMOS framework, demonstrating that fine-tuning on unified, high-quality annotations enhances both planning and grounding

skills. This interaction facilitates the development of strong, specialized, and efficient agents where parametric training builds basic skills and non-parametric prompting guides their active use during inference.

Moreover, fine-tuning introduces risks, including model overfitting, amplification of biases present in the training data, and susceptibility to malicious data injection. While fine-tuning can achieve higher task-specific performance, it requires careful dataset curation, extensive computational resources, and rigorous validation. In contrast, prompt engineering offers flexibility and safety, but generally cannot reach the same depth of expertise.

8.3 Memory augmentation: enabling grounded reasoning and experiential learning

While prompting gives immediate instructions for an agent, memory augmentation extends agents beyond context limits (Lu et al., 2024; Jin et al., 2024) by changing them from simple instruction-followers into adaptable systems (Jin and Ma, 2024). Memory can be divided into two main types: retrieval of external knowledge (RAG) and accumulation of internal dynamic experience that supports learning and self-correction. RAG grounds agent reasoning in verifiable information. It helps reduce mistakes and improve reliability. For example, in clinical settings, frameworks like TRIAGEAGENT (Lu et al., 2024) and ColaCare (Wang et al., 2025b) use RAG to give agents access to medical handbooks and guidelines. This ensures their decisions are based on solid evidence. This method works well in specialized technical areas; (Barra et al., 2025) employs RAG to offer established simulation guidelines for scenario design. Xia et al. (2024) use it to access technical datasheets for creating digital twin models. However, the effectiveness of RAG can depend on the model. Xia et al. mention a “cheat-sheet effect,” where it greatly improves performance in weaker LLMs compared to stronger ones. This suggests that the value of external memory depends on the agent’s inherent reasoning capabilities. The external memory can also be dynamic, as shown in frameworks like DeCoAgent (Jin et al., 2024). Here, a JSON memory module pulls current on-chain data, preventing unnecessary blockchain scans. Beyond retrieving static facts, memory is vital for experiential and reflective learning. One important framework in this area is Reflexion (Shinn et al., 2023) that stores verbal reflections in episodic buffers. This helps guide future attempts. This process of self-correction has been shown to be effective in many applications, from improving public health policies in simulations (Behari et al., 2024) to generating high-quality distillation data for training other models (Yang et al., 2024d). However, compared to an episodic system like Reflexion, RAG is more reliable for factual grounding but less effective for long-term adaptation. The concept has evolved into more organized, long-lasting memory systems. REMEMBERER (Zhang et al., 2023) updates an agent’s long-term experience memory through RL. AVATAR (Wu et al., 2024) maintains a “Memory Bank” to store high-performing action sequences and instructions. Similarly, Star-Agents (Zhou et al., 2024) uses an “Instruction Memory Bank” to continuously improve data generation strategies. Memory also helps agents stay grounded in their immediate, dynamic environment, especially in interactive settings. This is often done by updating the agent’s prompt with real-time perceptual information. For example, Song et al. (2023) keep plans grounded in LLM-Planner by constantly updating the prompt with a list of visually perceived objects. Yang et al. (2024c) use prompts to coordinate visual grounding tools. This grounding includes more abstract representations of the state as well. Li et al.

(2023b) show that giving agents an explicit belief state representation greatly enhances planning and reduces errors in Theory of Mind tasks. In multi-agent systems, memory can be distributed. The CoA framework from Zhang et al. (2024c) passes a "Communication Unit" in sequence between agents, allowing each to build on the previous work. A more complex version is CoELA (Zhang et al., 2024d), which resembles human thinking with distinct semantic, episodic, and procedural memory modules to support long-term cooperation. Despite its advantages, memory enhancement is not perfect and faces significant challenges. The main limitation lies in how well the agent can manage long and complex memory streams. George et al. (2024) points out that even with CoT prompting, agents can struggle to use crucial information from lengthy histories filled with distracting facts. Additionally, some memory strategies can backfire in specific situations. Zhang et al. (2024e) discovered that a Reflexion-style memory system led to worse performance in complex multitasking scenarios. Sometimes, simpler approaches like a "sliding window" memory can be a more effective, if less advanced, solution (Chang et al., 2024). Ultimately, how well memory is implemented is what distinguishes an agent as a reactive tool versus a cognitive entity capable of learning, adapting, and maintaining coherent long-term behavior.

8.4 The synergistic integration of prompting, fine-tuning, and memory

The development of capable LLM-based agents relies on the interaction of prompting, fine-tuning, and memory augmentation (Ni and Buehler, 2024; Cheng et al., 2024b; Zhang et al., 2024e). The combined use of these three elements is crucial for increasing agent autonomy, from single-agent reasoning to complex multi-agent collaboration (Kim et al., 2024; Ni and Buehler, 2024; Ghafarollahi and Buehler, 2024). At its core, prompt engineering is the main method for guiding agent behavior. However, relying solely on prompting can be fragile. Performance drops significantly when agents deal with long contexts filled with distracting "red herring" facts, even with CoT prompting. While prompting provides dynamic control, fine-tuning offers a method for permanently embedding specialized knowledge and complex skills in an agent. This is essential for creating agents that are trained by instructions and are inherently capable in specific domains. One of the most effective combinations occurs when prompting serves as a tool for generating data, creating high-quality datasets for refining smaller, more efficient agents. This model allows the reasoning abilities of large proprietary models to be distilled into open-source alternatives. A clear example is the ToolLLM framework (Qin et al., 2024), which uses ChatGPT to produce a vast dataset of instructions and API call solutions to fine-tune LLaMA into the highly effective ToolLLaMA. A similar method is used by Qian et al. (2024) to develop Mistral-Interact by fine-tuning on user dialogues generated by prompting GPT-4. Pang et al. (2024) also use the MATRIX framework to create alignment data. This bidirectional relationship extends further: fine-tuning can enhance an agent's ability to follow complex prompts and execute domain-specific instructions more reliably. Yin et al. (2024) demonstrate this with the LUMOS framework, showing that fine-tuning on unified, high-quality annotations improves both planning and grounding abilities when combined with structured prompting strategies.

Memory augmentation bridges prompting and fine-tuning mechanisms by providing the contextual foundation necessary for effective prompting and the experiential data required for targeted fine-tuning. RAG-based systems like TRIAGEAGENT (Lu et al., 2024) and ColaCare (Wang et al., 2025b) use external memory to ground prompts in factual medical

knowledge, mitigating hallucinations during inference. Conversely, episodic memory systems like Reflexion (Shinn et al., 2023) accumulate task-specific experience in the form of episodic verbal reflections, which are used in subsequent prompts to improve both immediate reasoning and performance. The most advanced agents successfully combine all three components. In these systems, fine-tuning develops core skills, prompting guides inference-time reasoning and tool use, while memory offers dynamic context and knowledge. The CoELA framework (Zhang et al., 2024d) fine-tunes CoLLAMA using data collected by agents and applies structured prompts alongside a multi-part memory system (semantic, episodic, procedural) to enable complex collaboration. OmniJARVIS (Wang et al., 2024c) demonstrates this integration by fine-tuning a VLA model on unified tokens that represent instructions, memories, and actions. These tokens are coordinated by prompts for open-world tasks. These systems illustrate that, while each mechanism is effective independently, their combination is essential for developing truly autonomous, capable, and reliable LLM-based agents.

9 Evaluation benchmarks and datasets

The rapid growth of LLM agents has required a change in how we evaluate them. Early methods that depended on static NLP benchmarks do not effectively capture the interactive, goal-driven, and often multi-step nature of these systems. The literature shows a clear shift towards more dynamic, specific, and analytical evaluation methods (Zhang et al., 2024e; Wijk et al., 2025; Wang et al., 2024d).

To give a clear overview of this progress, this section looks at the evaluation landscape through three connected lenses. First, it reviews the specialized benchmarks and interactive environments designed to test the abilities of agents in realistic situations (Chang et al., 2024; Lu et al., 2024). Next, it examines the various methods and metrics developed to judge performance beyond simple accuracy, including factors like efficiency, quality, and behavioral strength (Chang et al., 2024). Finally, the section highlights the important role of the datasets used to train and ground these agents since they provide the basis for agentic behavior.

9.1 Task-oriented and interactive benchmarks

Evaluating the capabilities of LLM-based agents requires a shift from static language metrics to dynamic benchmarks that focus on task performance and interactivity in complex environments. A notable trend is the creation of simulated environments where agents must engage in multi-step reasoning and actions. For example, TIME-ARENA (Zhang et al., 2024e) introduced a text-based simulation that includes time-based dynamics and constraints, challenging agents with multitasking scenarios in cooking, household tasks, and lab work. Advancing this complexity, AndroidArena (Xing et al., 2024) offers a general-purpose operating system environment to assess agents on intricate tasks that need cooperation between applications and compliance with user constraints. In a more specific area, RE-Bench provides demanding, open-ended machine learning research tasks, allowing for a direct comparison between AI agents and human experts. Environments like Overcooked-AI, ALFRED, and WebShop are established settings for testing zero-shot coordination,

instruction following, and web navigation, respectively (Zhang et al., 2024b; Song et al., 2023; Klein et al., 2025).

An important part of agent functionality is their ability to interact with and manipulate external tools and APIs. ToolLLM introduced ToolBench, which is a detailed instruction-tuning dataset with over 16,000 real-world APIs, along with an automatic evaluator called ToolEval to assess pass rates and solution quality (Qin et al., 2024). Frameworks like EASYTOOL aim to improve agent performance on these benchmarks by converting extensive tool documentation into brief, clear instructions (Yuan et al., 2025). The assessment of tool use also includes specialized scientific fields. For instance, ChemCrow and Coscientist are agent systems evaluated on their ability to plan and carry out complex chemical syntheses using expert-designed chemistry tools (Bran et al., 2024; Boiko et al., 2023). In industrial applications, RCAgent showcases a tool-enhanced agent for cloud root cause analysis, evaluated using proprietary system log data (Wang et al., 2024b).

Beyond executing tasks, researchers are creating benchmarks to evaluate more subtle human-like and social behaviors. The IN3 benchmark focuses on assessing an agent's capacity to understand user intentions by prompting them to ask clarifying questions (Qian et al., 2024). To examine the limits of agent reasoning, the OEDD corpus presents scenarios where agents must make sense of various experiences while ignoring misleading information (George et al., 2024). Assessing collaborative and social intelligence is another critical area. SOTOPIA- π features an interactive learning approach along with an evaluation suite, SOTOPIA-EVAL, which employs both human and LLM-based assessments on aspects like goal completion and believability (Wang et al., 2024d). Additionally, frameworks have been developed to create "societies" of LLM agents to observe collaborative behaviors on tasks from the MMLU, MATH, and Chess datasets. The ability for agents to mimic human behavior is tested in frameworks that use Trust Games to compare agent decisions with recognized human patterns.

Several meta-evaluation frameworks have been created to consolidate and analyze agent performance across various tasks. AgentBoard (Chang et al., 2024) offers an evaluation board that includes nine different multi-turn, partially observable tasks from areas like embodied AI, gaming, and web navigation. It provides a detailed metric to track progress, offering deeper insights beyond basic success rates. In the medical field, new benchmarks are emerging to ensure clinical safety and effectiveness. TRIAGE AGENT (Lu et al., 2024) released the first public benchmark for clinical triage, using metrics like discordance and undertriage rates against human expert performance. Other studies assess agents in their ability to execute clinical calculations using established medical calculators or make complex oncology decisions based on multimodal patient data (Goodell et al., 2025; Ferber et al., 2025). These interactive benchmarks are essential for fostering the growth of more capable, reliable, and aligned LLM agents.

9.2 Methodologies and metrics for evaluation

The evaluation of LLM-based agents is quickly changing from basic accuracy checks to more complex methods that look at task performance, reasoning quality, and interaction dynamics (Wang et al., 2024d; Li et al., 2023b; Chang et al., 2024). A key approach continues to focus on task-oriented performance metrics, where we measure an agent's success by its ability to reach specific goals (Lu et al., 2024; Qin et al., 2024).

This is often assessed through accuracy or success rates on established benchmarks for coding, like HumanEval, math reasoning datasets such as GSM8K and MATH, and embodied AI tasks in settings such as ALFRED and Overcooked-AI (Cheng et al., 2024b; Ma et al., 2024; Song et al., 2023; Zhang et al., 2024b). In addition to these general benchmarks, evaluations are frequently customized for specific fields, using metrics like discordance and undertriage rates in clinical triage, the emergence of macroeconomic laws in economic simulations, and improvements in material properties for scientific discovery (Goodell et al., 2025; Ferber et al., 2025; Li et al., 2024a).

For tasks where success is more subjective or quality has shades of meaning, researchers are turning to human experts and "LLM-as-a-Judge" frameworks. This approach is essential for evaluating things like the quality of travel plans, the realism and empathy of synthetic medical dialogues, and the solution quality for complex tool-use instructions. Metrics in this area often involve comparative judgments, such as win/tie/lose rates against baseline models or preference rates where evaluators choose the better of two outputs. Frameworks like SOTOPIA-EVAL use both human and LLM-based judgments across various dimensions, including believability and relationship development, to evaluate social intelligence (Wang et al., 2024d).

Evaluating multi-agent systems brings in metrics that capture the complexities of teamwork, social dynamics, and system-level properties (Ni and Buehler, 2024; Wang et al., 2024d). Performance is often measured by team scores, completion times, and comparisons between collaborative groups and solo agents (Zhang et al., 2024e; Cheng et al., 2024b). Methods also explore emerging social behaviors, such as conformity and reaching consensus in agent societies, or the ability to simulate human trust behaviors in economic games (Zhang et al., 2024a; Li et al., 2024a). The resilience of these systems is another major concern, with some evaluations measuring how performance degrades when faulty or malicious agents join the collaborative process (tse Huang et al., 2025).

In addition to these outcomes, a growing number of studies focus on the efficiency and internal reasoning processes of agents. Metrics like token consumption, tool invocation efficiency, and the balance between cost and quality are used to evaluate how resourceful agent solutions are (Yuan et al., 2025; Klein et al., 2025). At the same time, new methods are being developed to investigate the quality of an agent's reasoning. This includes detailed detection of different types of errors in math problems, assessing ToM accuracy in cooperative games, and evaluating the logical coherence of reasoning sequences using formal graphs (Li et al., 2023b; Jo et al., 2023). This attention to internal processes is vital for creating more reliable and interpretable agents.

To create a standard evaluation across different tasks, several meta-evaluation frameworks have been proposed. AgentBoard (Chang et al., 2024) provides a comprehensive evaluation platform that combines nine unique multiturn tasks and introduces a detailed progress rate metric for deeper insight beyond simple success rates. Likewise, specialized evaluators like ToolEval (Qin et al., 2024) have been created to specifically assess tool-use capabilities, measuring metrics like pass rates and solution quality across thousands of real-world APIs. These initiatives indicate a maturation in the field, moving toward more comprehensive and insightful assessment tools that can help develop more capable and aligned agents.

9.3 Datasets for agent training and grounding

The development of effective LLM agents heavily depends on the availability of diverse, high-quality datasets for training and grounding in specific areas. These datasets are rapidly changing, moving away from traditional static text collections to dynamic, interactive, and domain-specific resources. This shift helps agents acquire complex skills and emphasizes grounding their abilities in real-world tasks, tools, and social contexts. Table 7 presents an overview of sixty-eight publicly available datasets employed to train, evaluate, or benchmark LLMs in agent modeling, organized by task type and citation.

A key strategy involves using and adapting existing public benchmarks to build core reasoning and instruction-following skills. Datasets like those for mathematics (GSM8K, MATH), question-answering (HotPotQA, StrategyQA), and coding (HumanEval) are commonly used for fine-tuning models and serve as a baseline for assessing logical and problem-solving abilities (Shinn et al., 2023; Yin et al., 2024; tse Huang et al., 2025). Instruction-tuning datasets, such as Alpaca, are used to improve the overall capabilities of models before tailoring them for specific agent tasks (Zhou et al., 2024). To promote broader agent learning, there are ongoing efforts to collect large-scale, unified annotations based on various reasoning frameworks across these complex interactive tasks. A notable trend involves employing agents to automate the enhancement and diversification of these instructional datasets, creating a constant cycle to improve data quality.

A major development in agent training is creating datasets and simulated environments designed for tool use and interaction in complex digital spaces. ToolBench provides an extensive instruction-tuning dataset with over 16,000 real-world APIs, allowing models to learn to execute advanced instructions and adapt to new tools (Yang et al., 2024b). For grounding in interactive settings, benchmarks like WebShop and ALFRED serve as established bases for training and testing web navigation and embodied instruction-following, respectively (Klein et al., 2025; Song et al., 2023). More intricate environments, such as AndroidArena (Xing et al., 2024), assess agents on complex tasks that require cooperation between applications, while TIME-ARENA (Zhang et al., 2024e) introduces time dynamics and multitasking challenges in simulated household and lab scenarios. AgentBoard (Chang et al., 2024) combines nine distinct multi-turn, partially observable tasks from areas like embodied AI, gaming, and web navigation into one evaluation framework.

To ground agents in specialized, high-stakes fields, researchers are curating and generating domain-specific datasets. In the medical sector, this includes datasets derived from clinical triage manuals (TRIAGE AGENT), public EHR data such as MIMIC-IV, patient engagement logs, and extensive cancer proteomics resources such as TCGA and CCLE (Lu et al., 2024; Wang et al., 2025b; Liu et al., 2025a). In science and engineering, agents are trained on tailored datasets drawn from scientific literature for research in organic semiconductors and chemistry or data generated from physics-based simulations for mechanics problems (Boiko et al., 2023; Ni and Buehler, 2024). Similarly, specialized collections are being built for urban planning using public data from cities like San Francisco, for finance using public datasets like MovieLens and Amazon-Beauty to simulate user behavior, and for electronics design automation by generating custom code-instruction pairs (Jin and Ma, 2024; Wang et al., 2025c; Huang et al., 2025).

A growing area of research focuses on datasets meant to enhance more nuanced social and collaborative intelligence. The SOTOPIA- π dataset supports the interactive learning of

Table 7 Details of the sixty-eight publicly available datasets analyzed in this study, including their limitations and type

Dataset	Dataset type	Limitations	Dataset	Dataset type	Limitations
HumanEval Chen et al. (2021)	Code Generation	Limited Task Diversity	MBPP Austin et al. (2021)	Code generation	Limited Concept Coverage
LeetCodeDataset Xia et al. (2025)	Code Generation	Narrow Problem Coverage	CoNaLa Yin et al. (2018)	Code generation	Single Answer Bias
RepoBench-P Liu et al. (2023)	Code Completion	Limited Language Diversity	Evol-CodeAlpaca Luo et al. (2023)	Code instruction	Limited Domain Coverage
InterCode Yang et al. (2023)	Interactive Coding	Limited Language Coverage	GSM8K Cobbe et al. (2021)	Math reasoning	Limited Problem Variety
MGSM Shi et al. (2022)	Math Reasoning	Limited Problemset Coverage	Math-Shepherd Wang et al. (2023d)	Math reasoning	Narrow Problem Scope
MultiArith Multiarith dataset (2023)	Math Reasoning	Limited Problem Complexity	MATH Saxton et al. (2019)	Math reasoning	Lacks Algorithmic Reasoning Problems
TabMWP Lu et al. (2023)	Math Word Problem	Limited Problem Diversity	MoST Codeca and Härrä (2018)	Multi-step reasoning	Inherent Annotation Noise
STaRK Wu et al. (2024)	Reasoning	Limited Human-Query Variety	BridgeData Walke et al. (2023)	Reasoning	Limited Task Diversity
Aci-bench Yim et al. (2023)	Agent Interaction	Synthetic Data Reliance	HotpotQA Yang et al. (2018)	Multi-hop QA	Limited Domain Coverage
MuSiQue Trivedi et al. (2022)	Multi-hop QA	Restricted Question Diversity	StrategyQA Geva et al. (2021)	Multi-step QA	Limited Factual Diversity
ArxivQA Li et al. (2024b)	Scientific QA	Limited Disciplinary Diversity	QASPER Dasigi et al. (2021)	Scientific QA	Limited Domain Coverage
NarrativeQA Kočíský et al. (2018)	Long-form QA	Limited Training Data	FEVER Thorne et al. (2018)	Fact verification	Limited Evidence Scope
QMSum Zhong et al. (2021)	Query Summarization	Limited Domain Coverage	WikiHow Koupaee and Wang (2018)	Summarization	Limited Abstraction
GovReport Huang et al. (2021)	Summarization	Limited Domain Representation	BookSum Kryściński et al. (2021)	Long summarization	Limited Coverage Of Diverse Genres
Stanford Alpaca Taori et al. (2023)	Instruction Tuning	Limited Contextual Variation	OpenAssistant Köpf et al. (2023)	Instruction tuning	Limited Domain Coverage
OpenOrca Lian et al. (2023)	Instruction Tuning	Limited Domain Coverage	WildChat Zhao et al. (2024b)	Instruction tuning	Limited Real-World Diversity
IN3 Qian et al. (2024)	Instruction Tuning	Limited Task Diversity	FineWeb Penedo et al. (2024)	Pre-training corpus	Limited Content Diversity
RefinedWeb Penedo et al. (2023)	Pre-training Corpus	Contains Residual Noise	RedPajama Weber et al. (2024)	Web text	Benchmark Contamination Risk
LLMSecEval Tony et al. (2023)	Code Security	Limited CWE Coverage	PKU-SafeRLHF Ji et al. (2024)	Safety	Limited Scale And Harm Granularity

Table 7 (continued)

Dataset	Dataset type	Limitations	Dataset	Dataset type	Limitations
HarmfulQA Bhardwaj and Poria (2023)	Safety	Synthetic Prompt Bias	HH-RLHF Bai et al. (2022)	Alignment	Limited Generalization Scope
BeaverTails Ji et al. (2023)	Alignment	Narrow Harm Category	LLM Attacks Zou et al. (2023)	Adversarial	Limited Attack Diversity
R2R Anderson et al. (2018)	Embodied AI	Limited Context Diversity	REVERIE Qi et al. (2020)	Embodied AI	Sparse Object Annotations
Touchdown Chen et al. (2019)	Embodied AI	Narrow Urban Context	ALFRED Shridhar et al. (2020)	Instruction	Limited Environment Diversity
ALFWorld Shridhar et al. (2021)	Instruction	Limited Task Variety	TravelPlanner Xie et al. (2024)	Planning	Low Real-World Complexity
BlocksWorld Valmeekam et al. (2023)	Planning	Lacks Real-World Variability	HaGRID Kapitanov et al. (2024)	Gesture recognition	Lacks Dynamic Gestures
EgoGesture Zhang et al. (2018)	Gesture Recognition	Limited Gesture Diversity	CogScene Jeong et al. (2022)	3D scene understanding	Lacks Scenario Diversity
WIDER FACE Yang et al. (2016)	Face Detection	Demographic Bias	CelebA Liu et al. (2015)	Face attributes	Limited Attribute Diversity
CDSL Ritore et al. (2024)	Clinical Data	Lacks Temporal Coverage	CCLE Ghandi et al. (2019)	Genomics	Limited Tissue Representation
APARENT2 de Almeida et al. (2025)	Genomics	Limited Task Complexity	Saluki Agarwal and Kelley (2022)	Genomics	Limited Domain Coverage
SKEMPI Jankauskaitė et al. (2019)	Protein Binding Affinity	Lacks Structural Diversity	PubMed National Library of Medicine (2023)	Scientific abstracts	Possesses Inconsistent Indexing
GAIA Mialon et al. (2023)	General AI Assistant	Lacks Language Diversity	BIG-bench Srivastava et al. (2023)	General evaluation	Limited Task Diversity
MMLU Hendrycks et al. (2021)	General Evaluation	Data Contains Cultural Bias	CAMEL Li et al. (2023a)	Multi-agent convo	Limited Temporal Coverage
SOTOPIA-PI Wang et al. (2024d)	Social Simulation	Limited Safety Dimensions	ToolBench Guo et al. (2024)	Tool use	Exhibits Tool Specific Bias
Mind2Web Deng et al. (2023)	Web Agent	Evaluation Bias And Limited Scope	RoboNet Dasari et al. (2019)	Trajectory	Limited Task Modalities

social skills through imitation and RL based on filtered social interaction data (Wang et al., 2024d). Other approaches create "societies" of LLM agents to explore emergent collaborative behaviors using established benchmarks like MMLU and MATH (Zhang et al., 2024a). To assess an agent's ability to recognize implicit human needs, the IN3 benchmark tests proactive clarification skills, while the OEDD corpus presents scenarios where agents must apply different experiential information without being misled by distractions (Qian et al., 2024; George et al., 2024). These varied and increasingly sophisticated datasets are essential for developing agents that excel in tasks and are grounded, reliable, and socially aware.

Benchmarks and datasets play a crucial role in evaluating LLM-based agents by directly testing key capabilities such as reasoning, planning, tool use, collaboration, and generalization. For reasoning, the GSM8K dataset evaluates mathematical problem-solving. The CORY framework (Ma et al., 2024) improves policy optimality by reducing distribution collapse, showing strong deductive reasoning. Similarly, HumanEval and MBPP (Bai et al., 2025) test code generation.

In terms of planning, ALFRED (Song et al., 2023) assesses agents' few-shot performance. LLM-Planner's few-shot performance reveals grounding challenges. Similarly, TIME-ARENA (Zhang et al., 2024e) examines time-aware multitasking in cooking and lab tasks and highlights LLMs' difficulties with temporal dependencies.

AGENTVERSE (Cheng et al., 2024b) evaluates text understanding and coding, showing emerging cooperative behaviors. SOTOPIA- π (Wang et al., 2024d) uses MMLU to achieve social goal completion, matching GPT-4, which emphasizes social intelligence. Tool use is assessed through ToolBench (Qin et al., 2024), which tests API handling with strong zero-shot generalization. RE-Bench (Wijk et al., 2025) shows that LLMs outperform human experts in time-constrained R&D tasks, indicating effective decision-making.

Multimodal grounding is evaluated through VQAv2 and Text-VQA. CogAgent (Hong et al., 2024) excels in GUI navigation, which evaluates agents' visual-language integration. By directly examining the strengths of LLM, these benchmarks also uncover limitations, such as long-term focus issues (Zhang et al., 2024c) and social biases (Liu et al., 2025b). Although datasets in LLM-based autonomous agent research have significantly advanced areas such as reinforcement learning, code generation, healthcare, and urban planning, they still present major limitations that hinder generalization and real-world applicability. Many existing datasets are built within simulated or synthetic environments, including ALFRED (Song et al., 2023), Overcooked AI (Zhang et al., 2024b), and Sociodojo (Cheng and Chin, 2024c). These settings often fail to capture the inherent noise, unpredictability, and multimodal complexity of real environments, leading to overfitting and poor performance (Xing et al., 2024; Zhang et al., 2024d; Qiao et al., 2024). Robotics and navigation datasets, for instance Street View (Schumann et al., 2024) and AndroidArena (Xing et al., 2024) often lack diversity in user behavior, scene variation, and environmental dynamics, resulting in biased models with limited robustness (Singh et al., 2024; Yang et al., 2024c). Standard benchmarks, including HumanEval, MBPP, GSM8K, MATH, and WebShop, remain task-specific with limited cross-domain and multilingual coverage (Shinn et al., 2023; Bai et al., 2025; Ma et al., 2024; Li et al., 2024c).

Existing benchmarks and datasets inadequately measure agentic reasoning by testing performance in simplified, static environments that fail to reflect real-world complexity. They often prioritize subjective, language-level evaluation over assessing an agent's objective, action-level impact on achieving goals (Li et al., 2025a). This reliance on metrics like final success rate offers few insights into the actual reasoning process (Chang et al., 2024) and neglects crucial challenges like navigating dynamic action spaces (Xing et al., 2024). Furthermore, these benchmarks often overlook critical real-world constraints, such as temporal dynamics, which are essential for assessing an agent's ability to plan and multitask efficiently (Zhang et al., 2024e).

10 Discussion

Our review explored the rapid use of LLMs as agents and tools for complex autonomous tasks. This study presents a comprehensive examination of existing LLM-based frameworks and discusses cognitive and operational components critical to agentic intelligence. By analyzing a broad spectrum of prior work, we identified how these systems are architected, the capabilities that underpin their autonomy, and the current limitations constraining their scalability. We categorized the most widely adopted methods and their implementation within single-agent and multi-agent systems across various application domains. In general, this review offers a coherent foundation for understanding the developmental trajectory of LLM agents and tools to guide future advancements in this rapidly evolving field.

Baseline LLMs. Recent studies addressing (*RQ1*) reveal that GPT-4 is currently the dominant foundational model, cited in fifty-five studies, followed by GPT-3.5 in 23 studies, establishing it as a performance benchmark despite cost and access restrictions. GPT variants fulfill three roles: first, as gold-standard ablation references; second, as multi-agent collaborators with open models; and third, as primary reasoning modules within agent stacks.

In addition to OpenAI models, Anthropic's Claude 3 series is a prominent proprietary alternative (Zhang et al., 2024c; Chang et al., 2024; Kannan et al., 2024a; Zhang et al., 2024f). Google's Gemini excels at very-long-context reasoning for document-scale planning. Meanwhile, the open-source ecosystem is rapidly advancing, reducing the performance gap. Models such as LLaMA-2/3 (Zhang et al., 2024d; Zheng et al., 2024; Wu et al., 2024a; Xie et al., 2024; Ning and Liu, 2024), Mistral (Jin and Ma, 2024; Zhang et al., 2024e; Qian et al., 2024; Wang et al., 2024d; Abdaljalil et al., 2025; Qiao et al., 2024; Zhai et al., 2024), Gemini (Zhang et al., 2024f; Barra et al., 2025), Qwen, DeepSeek, Vicuna, WizardLM, and GLM-4 are increasingly adopted for coding, planning, and dialogue. Specialized derivatives like CodeLLaMA and ToolLLaMA demonstrate, task-specific pre-training can produce domain expertise without complete retraining. For constrained environments, Phi-2, Phi-3.5 Mini (Li et al., 2025b), Gemini-2B, and Mistral-7B, are more efficient. Lastly, multimodality through CLIP, Stable Diffusion XL, and VQ-GAN enables LLM agents beyond text to vision and interface automation.

External tool integration in LLMs. We found that integrating external tools (*RQ2*) is a primary driver of LLM autonomy. LLMs paired with rich computational resources, web APIs, knowledge graphs, code execution, RESTful service libraries (Qin et al., 2024), and high-fidelity simulators elevate agent capability. Real-time data retrieval from domain-specific sources strengthens RAG accuracy while speech recognition tools, such as Speechly, enable real-world interaction. Furthermore, environments such as AI2-THOR, ALFWorld, and SMAC, connected through platforms like ROS 2 and Gazebo, demonstrate that LLMs can perceive state, reason, and act in dynamic and interactive settings (Wang et al., 2023a; Shinn et al., 2023; Li et al., 2025b; Zhou et al., 2024; Frering et al., 2025). Collectively, these patterns strongly suggest that external tool access is an essential foundational mechanism for accessing up-to-date knowledge, enabling perception, action, and reasoning in modern LLM agents.

Frameworks for LLM agents. Our analysis of LLM agent frameworks (*RQ3*) reveals single-agent scenario is dominated by ReAct and Reflection, prioritizing streamlined reasoning-action integration and iterative self-improvement. ReAct's thought-action sequences enable dynamic task adaptation, while Reflexion refines performance through memory-

based learning and feedback (Shinn et al., 2023). These frameworks excel at tasks that require adaptability, minimal infrastructure, and self-guided correction.

Multi-agent implementations favor frameworks such as AutoGen and CAMEL, effective for interaction, role differentiation, and collective planning (Wu et al., 2024b). AutoGen's conversation programming supports asynchronous, modular communication workflows. CAMEL's role-conditioned framework enables agents to solve tasks collaboratively through structured, multi-turn dialogues. These capabilities are critical for multistep reasoning, distributed system design, or collaborative creativity, where agents operate semi-independently while maintaining group objectives. LangChain is compatible in single and multi-agent setups with chain reasoning steps, memory access, and tool use (Huang et al., 2023; Klein et al., 2025). MetaGPT (Hong et al., 2023) integrates software engineering conventions among less prevalent frameworks, while AIDE (Wijk et al., 2025) and BDI (Frering et al., 2025) focus on interpretability and logical behaviors to enhance explainability and work in rule-constrained domains.

The trend is shifting from instruction-bound architectures to adaptive, role-aware, and coordination-driven systems. The widespread use of ReAct, Reflexion, LangChain, and AutoGen indicates a convergence on reasoning, memory integration, and collaborative execution as core capacities.

Reasoning, planning, and memory. Integration of reasoning, planning and memory mechanisms (RQ4) shaped the development of LLM-agents. During analysis, we found single-agent frameworks like TOOLLLM (Qin et al., 2024), EASYTOOL (Yuan et al., 2025), and ToTh (Abdaljalil et al., 2025) emphasize autonomy, safety, and introspective capability. In contrast, multi-agent frameworks like AGENTVERSE (Cheng et al., 2024b), Thread Memory (Jin and Ma, 2024), and ToM (Li et al., 2023b) prioritize coordination, belief modeling, and contextual reasoning. AGENTVERSE implements collaborative reasoning using structured symbolic modules; Thread Memory preserves context in multi-turn dialogue and interaction; ToM enhances coordination by modeling belief states in multi-agent settings. CoT, ReAct, and Self-Reflection appear in both. CoT is effective in code generation and robotics (Bai et al., 2025; Li et al., 2023b), where ReAct (Zhang et al., 2024e; Singh et al., 2024) and Reflexion (Zhang et al., 2024e; Feng et al., 2024) integrate feedback-aware reasoning, contributing to real-time adaptability and iterative self-improvement.

Single agent planning strategies, such as ReHAC (Feng et al., 2024) and RAFA (Liu et al., 2024a), emphasize proactive multistep forecasting and heuristic goal decomposition. Multi-agent systems such as DeCoAgent (Jin et al., 2024) and SMART-LLM (Kannan et al., 2024a) address coordination through prompt-based decomposition and coalition formation, respectively. In particular, adaptive and evolution-based planning in Star-Agents (Zhou et al., 2024) and UrbanKGent (Ning and Liu, 2024) reflect increasing interest in long-horizon self-organizing workflows.

We observe a clear divide between localized and distributed memory. Single-agent models optimize within episode retention using episodic reprompting (Zheng et al., 2024), compressed logs (Huang et al., 2023), or symbolic graphs (Abdaljalil et al., 2025), supporting isolated task continuity. Multi-agent models like ProAgent (Zhang et al., 2024b) provide shared task memory and thread-level history, while MATRIX (Pang et al., 2024) generates diverse interaction data as a multi-agent simulation environment, rather than managing shared memory. Context windows (Zhang et al., 2023; Pang et al., 2024) and dialogue history (Wang et al., 2024d; Li et al., 2023a) underpin both categories, while hybrid memory

systems (Boiko et al., 2023; Gao et al., 2024) signal convergence toward unified architectures that bridge short/long-term retention.

Prompting, fine-tuning, and memory augmentation. Our findings showed that agent autonomy is enabled by prompt engineering, fine-tuning, and memory augmentation (RQ5). Prompt engineering, a non-parametric technique, allows flexible, inference-time control over agent behavior, as seen in MechAgents (Ni and Buehler, 2024) and AGENTVERSE (Cheng et al., 2024b), which used structured prompts to simulate complex interactions such as expert collaboration, role play, trust modeling, and cognitive biases. However, in special domains where prompting is insufficient, fine-tuning is employed as a parametric approach to internalize domain expertise and task-specific skills, as seen in ToolLLM (Qin et al., 2024) for tool use specialization, RISE for self-correction abilities, and SOTOPIA- π (Wang et al., 2024d) for modeling social intelligence. Likewise, memory augmentation through external RAG and internal episodic memory is essential to ground agents in real-world contexts and support long-term reasoning. For example, TRIAGEAGENT (Lu et al., 2024) utilizes medical knowledge retrieval to mitigate hallucination, while Reflexion (Shinn et al., 2023) enables agents to adapt based on accumulated experience. Therefore, the architectural and behavioral autonomy of modern LLM agents is largely scaffolded by design choices rather than innate model capabilities.

Evaluation and benchmarks. Our analysis indicated that evaluating LLM-based agents (RQ6) requires a methodological change, from static NLP benchmarks to dynamic process-oriented evaluations. We also found that a robust evaluation framework should incorporate final outputs and the full agentic process. For example, AGENTBOARD (Chang et al., 2024) introduces "progress rate" metrics that capture incremental task completion across intermediate steps. Similarly, RE-Bench (Wijk et al., 2025) aligns agent performance with human expert benchmarks on complex research problems, reinforcing the importance of human-level baselines in agent evaluation.

In addition to this, controlled simulations reveal handling unreliable or adversarial collaborators (tse Huang et al., 2025), highlighting resilience as a critical component of agent intelligence. Domain-specific evaluations also emerged as essential for assessing practicality. For example, ChemCrow (Bran et al., 2024) benchmarks autonomous chemical synthesis against metrics grounded in scientific outputs, while tool-integrated agents in healthcare significantly reduce clinical calculation errors (Goodell et al., 2025).

Our analysis points to the growing recognition of failure analysis and safety evaluations as a key to agent benchmarking. Adversarial testing techniques are being developed to expose vulnerabilities, including backdoor attacks (Yang et al., 2024b), while new approaches such as PrivacyAsst (Zhang et al., 2024f) aim to maintain data confidentiality and trustworthiness during agent deployment. The evaluation state for LLM agents is rapidly evolving towards more comprehensive, interactive, and context-aware approaches. These emerging strategies emphasize whether an agent can succeed and how it reasons, interacts, adapts, and safeguards users along the way.

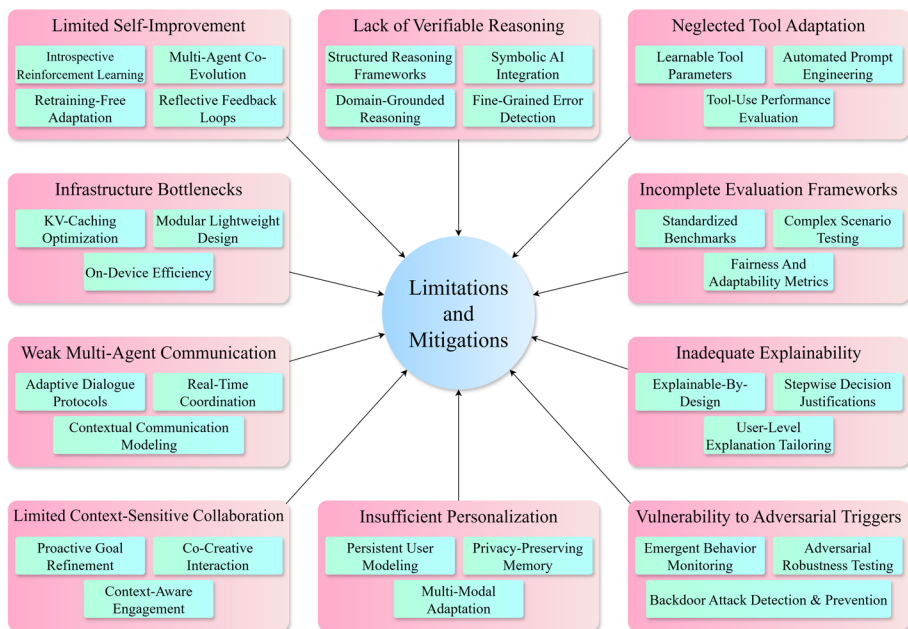


Fig. 7 Limitations in the current landscape of LLM-based agents and corresponding mitigation strategies

11 Future directions

LLM-based agents demonstrate significant potential to automate complex tasks, yet their current limitations (see Fig. 7) highlight the need for systemic research. To build agents that are reliable, adaptive, and ethically aligned, challenges such as unverifiable reasoning, limited contextual collaboration, vulnerability to adversarial attacks, and inadequate personalization must be addressed.

In this section, we outline the key areas where future work and critical research is needed (RQ7). Table S3, in the Supplementary Material, provides an organized summary of the existing research gaps and potential research pathways discussed in this section.

11.1 Towards verifiable reasoning and robust self-improvement

Although current agents based on LLMs show impressive abilities, their reasoning processes frequently remain unclear, and their capacity to learn from failure is limited. This lack of clarity and inflexibility limits their usage. Future work should develop agents with clear, verifiable reasoning methods and strong, efficient self-improvement cycles.

One major trend in improving reasoning is shifting from unstructured, free-form "CoT" to more organized and logically sound frameworks. Some methods ensure logical consistency from the start. For example, the ToTh model's reasoning is a multi-agent collaboration that simulates abductive, deductive, and inductive inference, assembling outputs into a formal reasoning graph, validating for coherence (Abdaljalil et al., 2025). In future works, a similar approach could assist in detecting financial fraud or security breaches by producing a reasoning graph that will provide a transparent, stepwise logic trail that authorities

can trace and validate. MechAgents (Ni and Buehler, 2024) utilizes a team of agents for complex engineering challenges and self-correcting physics-based simulation code. This verifies the reasoning of the agent against established scientific models. Building on this strategy, future work may explore the potential drug-drug interactions by modeling their combined molecular effects. Combining LLMs with traditional symbolic AI approaches, such as Belief-Desire-Intention agents, enables verifiable decision-making and improves safety (Frering et al., 2025). An essential aspect of verifiability is identifying and addressing flaws in the reasoning process. FG-PRM research (Li et al., 2024c) reliably tackles this by creating a classification of errors in mathematical reasoning and training a reward model to identify and penalize these errors.

Alongside verifiable reasoning is the goal of strong self-improvement, where agents learn from experience without needing retraining. Through strategies like Reflexion, agents can reflect on their performance and learn from mistakes, using verbal RL, creating a memory of these reflections that guides future attempts (Shinn et al., 2023). Studies such as RISE employ recursive introspection to fine-tune models through an ongoing process of self-correction, to improve their output over time (Xi et al., 2025). Subsequent work could apply these strategies to develop an agent for biomedical image segmentation that self-improves iteratively, minimizes reliance on continuous large-scale human annotation, and adapts to patient-specific image differences. Multi-agent dynamics also serves as a robust method for promoting self-improvement. In the CORY framework, a model is split into pioneer and observer agents that co-evolve through a cooperative RL process. This improves resilience and avoids policy failures common in traditional RL fine-tuning (Ma et al., 2024). Other frameworks, such as COPPER (Bo et al., 2024), feature a special reflector agent that provides tailored, constructive feedback to other agents, improving teamwork through a systematic self-improvement loop. Some studies, such as AgentOptimizer (Zhang et al., 2024h), suggest treating agent tools as learnable parameters, enabling task adaptation through tool improvement. Likewise, AVATAR (Wu et al., 2024) automates the optimization of prompts for tool use by employing a comparator module to reason over both positive and negative examples. Integrating structured reasoning, introspective learning, and adaptive capabilities is driving LLM agents toward more reliability, transparency, and continual improvement.

11.2 Towards scalable, adaptive, and collaborative LLM-based agent systems

Future research should enhance LLM agents' scalability, adaptability, and real-time operational capacity, for deployment in multimodal and domain-specific environments (Wang et al., 2025b; Yang et al., 2024a; Zeng et al., 2024; Wang et al., 2025c). Beyond internal agent reasoning and learning mechanisms, future work should address infrastructure constraints, memory usage, and latency, while enabling efficient inference through architectural techniques such as KV caching and optimized decoders (Jin and Ma, 2024; Zeng et al., 2024). These improvements are vital for low-resource or time-sensitive scenarios, such as on-device processing or streaming interaction.

Another key priority lies in enhancing multi-agent collaboration and the development of perceptually aware communication. The absence of adaptive communication protocols and contextual modeling in frameworks such as AGENTVERSE (Cheng et al., 2024b) limits their ability in dynamic multi-agent environments (Wijk et al., 2025). Future agent systems should adopt human-inspired, socially grounded dialogue strategies to enhance collabora-

tion capability, contextual awareness and intent inference among agents (Kim et al., 2024). Such improvements will enable the deployment of lightweight agents on edge hardware for traffic systems, warehouses, and drones, facilitating inter-agent communication and collaboration.

Furthermore, as the range of agent applications expands, extending to gesture-based interfaces, EHR prediction, collaborative games, continuous learning, coevolutionary training, and prompt refinement methods become essential (Wang et al., 2025b). Simultaneously, development of negotiation-heavy simulations like Lewis-style coordination games or Diplomacy can facilitate deeper understanding of agent reasoning under critical settings (Wijk et al., 2025; Wang et al., 2024d).

Likewise, ensuring robustness and interpretability remains a primary concern. Beyond introspective reasoning and verification, transparent evaluation pipelines are needed to track agent behavior over time, particularly under unpredictability and emergence. The acceleration of open-source advancements, led by models such as LLaMA-2-70B, provides an accessible, scalable, reproducible foundation, enabling researchers to collectively develop safe, effective, socially aligned agentic systems (Li et al., 2025a; Yin et al., 2024).

11.3 Deepening the human-agent symbiosis: personalization, proactivity, and trust

Future research should enhance autonomy, alignment, and practical deployability of LLM-based agents, for complex, dynamic, open-ended, and high-stakes environments. Increased operational freedom produces emergent effects, from strategic cooperative gains to unsafe shortcut-seeking actions. Addressing this duality requires robust alignment strategies to mitigate adverse behaviors while preserving constructive autonomy to operate efficiently and effectively.

Simultaneously, the strategic focus is shifting toward human-centered augmentation, emphasizing collaboration, reliability, and personalization. Realizing this calls for advances in intent recognition and co-creative interaction, where agents can engage in context-sensitive conversations that anticipate user needs and refine task goals interactively, an approach illustrated by studies like "Tell Me More" (Qian et al., 2024) and ReHAC (Feng et al., 2024).

Long-term personalization represents a critical research frontier in which future agents should build persistent, evolving user models over time while addressing memory and privacy, as stated in studies like PrivacyAsst (Zhang et al., 2024f). Achieving such personalization requires integrating multimodal capabilities while aligning interface modalities to user-specific preferences. Recently, personalized LLM-based agents have introduced complex ethical and societal risks, anthropomorphism, and over-trust. Their humanlike interactions create deception and encourage vulnerable populations, such as children or the elderly, to disclose sensitive information (Peter et al., 2025). Since LLM-based agents lack moral agency, attributing accountability is conceptually flawed (Meier, 2025). Beyond interface risks, agent architectures suffer from jailbreaking (Shen et al., 2024), and environmental signal-triggered backdoor attacks (Yang et al., 2024b). Jailbreaking refers to deliberate overriding of built-in safety measures of LLMs (Ouyang et al., 2022), and since agents need to handle multi-round dialogues and multiple sources of information, they become more prone to jailbreaking attacks. Effective human-agent collaboration requires both resilient

safeguard frameworks against vulnerabilities and transparent, explainable reasoning (Fring et al., 2025).

Continuous model optimization across collaborative decoding, lightweight modular execution strategies, and efficient caching mechanisms drives real-world scalability and enables a new class of agents that go beyond technical proficiency to ethically aligned, emotionally aware, privacy-conscious, and deeply integrated in complex workflows.

12 Conclusion

In this article, we present a comprehensive overview of LLM-based agents and the integration of tools within these systems. We examined how prompt engineering, fine-tuning, memory enhancement, and tool use contribute to the building of LLM agents by addressing seven focused research questions. We observed that single-agent systems prioritize autonomy and introspective decision making. However, multi-agent systems focus on coordination, role distribution, and collaborative planning. Crucially, this distinction becomes domain sensitive, with multi-agent configurations demonstrating pronounced advantages in areas requiring social intelligence, cooperative problem solving, and high-stakes decision support, such as healthcare, scientific research, and complex engineering tasks. Integrating external tools, real-time data sources, and multimodal systems has become essential to enable LLM agents to perform tasks beyond the limitations of pre-trained models. In parallel, the evaluation of these agents is changing from static accuracy-based benchmarks to dynamic process-oriented methods that account for reasoning quality, adaptability, and task completion in real-world settings.

We have also examined critical limitations and safety concerns as LLM agents are deployed in sensitive environments. These include risks related to security, performance limitations, adaptability in dynamic or personalized settings, and challenges in trust, explainability, and agent co-evolution. Addressing these challenges will ensure reliability, trust, and efficiency in future applications.

In our view, future work should focus on two critical goals: making agent reasoning transparent and verifiable and developing reliable methods for self-improvement without compromising safety. These capabilities are critical in high-risk environments, where errors can have serious consequences. Ensuring that LLM agents are trustworthy, resilient, and aligned with domain-specific requirements will be central to their responsible deployment across disciplines.

Author contributions Conceptualization: S.S.C., R.A., S.S.R., M.A.K.R.; Methodology: S.S.C., R.A., S.S.R.; Resources & Literature Review: S.S.C., R.A., S.S.R.; Writing – Original Draft: S.S.C., R.A., S.S.R., M.A.R., M.A.K.R.; Validation: S.A., M.A.K.R., M.A.R.; Formal Analysis: S.S.C., S.A., M.A.K.R., M.A.R.; Writing – Review & Finalization: M.A.K.R., S.A.; Project Supervision: M.A.K.R., S.A.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions. No external funding is available for this research.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no Conflict of interest.

Ethical approval Not applicable.

Consent to participate Not applicable.

Informed consent Not applicable.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abbasian M, Azimi I, Rahmani AM, Jain R (2025) Conversational health agents: a personalized large language model-powered agent framework. *JAMIA Open* 8(4):ooaf067
- Abdaljalil S, Kurban H, Qaraqe K, Serpedin E (2025) Theorem-of-thought: a multi-agent framework for abductive, deductive, and inductive reasoning in language models. In: *Proceedings of the 3rd workshop on towards knowledgeable foundation models (KnowFM)*. Association for Computational Linguistics, Vienna, Austria, pp 111–119
- Agarwal V, Kelley D (2022) Saluki: Predicting mrna half-life from mrna sequence. Data set, Zenodo, [Online]. Available: <https://doi.org/10.5281/zenodo.6326409>
- Anderson P, Wu Q, Teney D, Bruce J, Johnson M et al (2018) Vision-and-language navigation: Interpreting visually-grounded navigation instructions in real environments. In *Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR)*
- Arumugam D, Griffiths TL (2025) Toward efficient exploration by large language model agents. In: *The exploration in AI today workshop at ICML 2025*
- Austin J, Odena A, Nye M, Bosma M, Michalewski H et al (2021) Program synthesis with large language models. *arXiv preprint arXiv:2108.07732*
- Bai Y, Jones A, Ndousse K, Askell A, Chen A et al (2022) Training a helpful and harmless assistant with reinforcement learning from human feedback. *arXiv preprint arXiv:2204.05862*
- Bai X, Huang S, Wei C, Wang R (2025) Collaboration between intelligent agents and large language models: a novel approach for enhancing code generation capability. *Expert Syst Appl* 269:126357
- Barra FL, Rodella G, Costa A, Scalogna A, Carenzo L et al (2025) From prompt to platform: an agentic ai workflow for healthcare simulation scenario design. *Adv Simul* 10(1):29
- Behari N, Zhang E, Zhao Y, Taneja A, Nagaraj D, Tambe M (2024) A decision-language model (dlm) for dynamic restless multi-armed bandit tasks in public health. *Adv Neural Inf Process Syst* 37:3964–4002
- Bhardwaj R, Poria S (2023) Red-teaming large language models using chain of utterances for safety-alignment. *arXiv preprint arXiv:2308.09662*
- Bo X, Zhang Z, Dai Q, Feng X, Wang L et al (2024) Reflective multi-agent collaboration based on large language models. *Adv Neural Inf Process Syst* 37:138595–138631
- Boiko DA, MacKnight R, Kline B, Gomes G (2023) Autonomous chemical research with large language models. *Nature* 624(7992):570–578
- Bran AM, Cox S, Schilter O, Baldassari C, White AD, Schwaller P (2024) Augmenting large language models with chemistry tools. *Nat Mach Intell* 6(5):525–535
- Brown T, Mann B, Ryder N, Subbiah M, Kaplan JD et al (2020) Language models are few-shot learners. *Adv Neural Inf Process Syst* 33:1877–1901

- Cai Y, Li X, Goswami M, Wiliński M, Welter G, Dubrawski A (2025) LLM agents struggle at time series machine learning engineering. In: 1st ICML Workshop on foundation models for structured data
- Chang M, Zhang J, Zhu Z, Yang C, Yang Y, Jin Y, Lan Z, Kong L, He J (2024) Agentboard: An analytical evaluation board of multi-turn llm agents. *Adv Neural Inf Process Syst* 37:74325–74362
- Chen H, Suhr A, Misra D, Snively N, Artzi Y (2019) Touchdown: Natural language navigation and spatial reasoning in visual street environments. In: *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp 12 538–12 547
- Chen M, Tworek J, Jun H, Yuan Q et al (2021) Evaluating large language models trained on code. *arXiv preprint* [arXiv:2107.03374](https://arxiv.org/abs/2107.03374)
- Chen W, Su Y, Zuo J, Yang C, Yuan C et al (2024) Agentverse: Facilitating multi-agent collaboration and exploring emergent behaviors in agents
- Chen X, Xiang J, Lu S, Liu Y, He M, Shi D (2025a) Evaluating large language models and agents in health-care: key challenges in clinical applications. *Intell Med* 5(2):151–163
- Chen X, Yi H, You M, Liu W, Wang L et al (2025b) Enhancing diagnostic capability with multi-agents conversational large language models. *NPJ Digital Med* 8(1):159
- Chen J, Yu C, Zhou X, Xu T, Mu Y, et al (2025c) Emos: Embodiment-aware heterogeneous multi-robot operating system with llm agents. *arXiv preprint* [arXiv:2410.22662v2](https://arxiv.org/abs/2410.22662v2)
- Cheng J, Chin P (2024) Sociodojo: Building lifelong analytical agents with real-world text and time series. In: *The twelfth international conference on learning representations*
- Cheng Y, Zhang C, Zhang Z, Meng X, Hong S, et al (2024) Exploring large language model based intelligent agents: definitions, methods, and prospects. *arXiv preprint* [arXiv:2401.03428](https://arxiv.org/abs/2401.03428)
- Cobbe K, Kosaraju V, Bavarian M, Chen M, Jun H et al (2021) Training verifiers to solve math word problems. *arXiv preprint* [arXiv:2110.14168](https://arxiv.org/abs/2110.14168)
- Codeca L, Härrä J (2018) Monaco sumo traffic (most) scenario: a 3d mobility scenario for cooperative its. *EPiC Ser Eng* 2:43–55
- Cuadra A, Breuch J, Estrada S, Ihim D, Hung I et al (2024) Digital forms for all: A holistic multimodal large language model agent for health data entry. In: *Proceedings of the ACM on interactive mobile wearable and ubiquitous technologies* 8(2):1–39
- Dasari S, Ebert F, Tian S, Nair S, Bucher B et al (2019) Robonet: Large-scale multi-robot learning. *arXiv preprint* [arXiv:1910.11215](https://arxiv.org/abs/1910.11215)
- Dasigi P, Lo K, Beltagy I, Cohan A, Smith NA, Gardner M (2021) A dataset of information-seeking questions and answers anchored in research papers. In: *Proceedings of the 2021 conference of the North American chapter of the association for computational linguistics (NAACL)*
- de Almeida BP, Richard G, Dalla-Torre H, Blum C, Hexemer L et al (2025) A multimodal conversational agent for dna, rna and protein tasks. *Nat Mach Intell*, pp 1–14
- Deng X, Gu Y, Zheng B, Chen S, Stevens S et al (2023) Mind2web: Towards a generalist agent for the web. *Adv Neural Inf Process Syst* 36:28091–28114
- Dong Y, Jiang X, Jin Z, Li G (2024) Self-collaboration code generation via chatgpt. *ACM Trans Softw Eng Methodol* 33(7):1–38
- Driess D, Xia F, Sajjadi MSM, Lynch C, Chowdhery A et al (2023) Palm-e: An embodied multimodal language model. *arXiv preprint* [arXiv:2303.03378](https://arxiv.org/abs/2303.03378)
- Feldt R, Kang S, Yoon J, Yoo S (2023) Towards autonomous testing agents via conversational large language models. In: *2023 38th IEEE/ACM international conference on automated software engineering (ASE)*. IEEE, pp 1688–1693
- Feng X, Chen Z-Y, Qin Y, Lin Y, Chen X et al (2024) Large language model-based human-agent collaboration for complex task solving. In: *Findings of the association for computational linguistics: EMNLP. Assoc Comput Linguist* 2024:1336–1357
- Ferber D, El Nahhas OS, Wölflein G, Wiest IC, Clusmann J et al (2025) Development and validation of an autonomous artificial intelligence agent for clinical decision-making in oncology. *Nat Cancer*, pp 1–13
- Ferrag MA, Tihanyi N, Debbah M (2025) From llm reasoning to autonomous ai agents: a comprehensive review. *arXiv preprint* [arXiv:2504.19678](https://arxiv.org/abs/2504.19678)
- Franceschelli G, Musolesi M (2025) On the creativity of large language models. *AI Soc* 40(5):3785–3795
- Frering L, Steinbauer-Wagner G, Holzinger A (2025) Integrating belief-desire-intention agents with large language models for reliable human-robot interaction and explainable artificial intelligence. *Eng Appl Artif Intell* 141:109771
- Fu Y, Kim D-K, Kim J, Sohn S, Logeswaran L et al (2024) Autoguide: Automated generation and selection of context-aware guidelines for large language model agents. *Adv Neural Inf Process Syst* 37:119919–119948
- Gao C, Lan X, Li N, Yuan Y, Ding J et al (2024) Large language models empowered agent-based modeling and simulation: a survey and perspectives. *Human Soc Sci Commun* 11(1):1–24

- Gao J, Zhang Y, Chen Y, Dong Y, Chen Y et al (2025) Agent-in-the-loop to distill expert knowledge into artificial intelligence models: a survey. *Artif Intell Rev* 58(9):266
- George S, Sypherd C, Cashman D (2024) Probing the capacity of language model agents to operationalize disparate experiential context despite distraction. In: Findings of the association for computational linguistics: EMNLP 2024. Miami, Florida, USA: Association for Computational Linguistics, pp 15 447–15 459
- Geva M, Khashabi D, Segal E, Khot T, Roth D, Berant J (2021) Did Aristotle Use a Laptop? A question answering benchmark with implicit reasoning strategies. In: Transactions of the association for computational linguistics (TACL)
- Ghafarirollahi A, Buehler MJ (2024) Protagents: protein discovery via large language model multi-agent collaborations combining physics and machine learning. *Digital Discovery* 3(7):1389–1409
- Ghandi M, Huang FW, Jané-Valbuena J, Kryukov GV, Golub TR et al (2019) Next-generation characterization of the cancer cell line encyclopedia. *Nature* 569:503–508
- Goodell AJ, Chu SN, Rouholiman D, Chu LF (2025) Large language model agents can use tools to perform clinical calculations. *npj Digital Med* 8(1):163
- Gottweis J, Weng WH, Daryin A, Tu T, Palepu A et al (2025) Towards an ai co-scientist. *arXiv preprint arXiv:2502.18864*
- Guo Z, Cheng S, Wang H, Liang S, Qin Y et al (2024a) Stabletoolbench: Towards stable large-scale benchmarking on tool learning of large language models. *arXiv preprint arXiv:2403.07714*
- Guo T, Chen X, Wang Y, Chang R, Pei S et al (2024b) Large language model based multi-agents: a survey of progress and challenges. *arXiv preprint arXiv:2402.01680*
- Han S, Zhang Q, Yao Y, Jin W, Xu Z (2025) Llm multi-agent systems: Challenges and open problems. *arXiv preprint arXiv:2402.03578v2*
- Hemken N, Koneru S, Jacob F, Hartenstein H, Niehues J (2025) Can a large language model keep my secrets? a study on LLM-controlled agents. In: Proceedings of the 63rd annual meeting of the association for computational linguistics (Volume 4: Student Research Workshop). Association for Computational Linguistics, pp 746–759
- Hendrycks D, Burns C, Basart S, Zou A, Mazeika M et al (2021) Measuring massive multitask language understanding. In: Proceedings of the international conference on learning representations (ICLR)
- Hong S, Zhuge M, Chen J, Zheng X, Cheng Y et al (2023) Metagpt: Meta programming for a multi-agent collaborative framework. In: The twelfth international conference on learning representations
- Hong W, Wang W, Lv Q, Xu J, Yu W et al (2024) Cogagent: A visual language model for gui agents. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp 14281–14290
- Huang L, Cao S, Parulian N, Ji H, Wang L (2021) Efficient attentions for long document summarization. In: Proceedings of the 2021 conference of the North American chapter of the association for computational linguistics: human language technologies. Association for Computational Linguistics, pp 1419–1436
- Huang Q, Vora J, Liang P, Leskovec J (2023) Benchmarking large language models as ai research agents. In: NeurIPS 2023 foundation models for decision making workshop
- Huang H, Shi X, Lei H, Hu F, Cai Y (2024) Protchat: An ai multi-agent for automated protein analysis leveraging gpt-4 and protein language model. *J Chem Inf Model* 65(1):62–70
- Huang X, Lian J, Lei Y, Yao J, Lian D, Xie X (2025) Recommender ai agent: integrating large language models for interactive recommendations. *ACM Trans Inform Syst* 43(4):1–33
- Jankauskaitė J, Jiménez-García B, Dapkūnas J, Fernández-Recio J, Moal IH (2019) Skempi 2.0: an updated benchmark of changes in protein-protein binding energy, kinetics and thermodynamics upon mutation. *Bioinformatics* 35(3):462–469
- Jeong I-Y, Park J (2022) Cochlsene: Acquisition of acoustic scene data using crowdsourcing. In: Asia-pacific signal and information processing association annual summit and conference (APSIPA ASC). IEEE 2022:17–21
- Ji J, Liu M, Dai J, Pan X, Zhang C et al (2023) Beavertails: Towards improved safety alignment of llm via a human-preference dataset. *Adv Neural Inf Process Syst* 36:24678–24704
- Ji J, Hong D, Zhang B, Chen B, Dai J et al (2024) Pku-saferllm: Towards multi-level safety alignment for llms with human preference. *arXiv preprint arXiv:2406.15513*
- Jin Y, Ma J (2024) Large language model as parking planning agent in the context of mixed period of autonomous vehicles and human-driven vehicles. *Sustain Cities Soc* 117:105940
- Jin A, Ye Y, Lee B, Qiao Y (2024) Decoagent: Large language model empowered decentralized autonomous collaboration agents based on smart contracts. *IEEE Access*
- Jo E, Epstein DA, Jung H, Kim YH (2023) Understanding the benefits and challenges of deploying conversational ai leveraging large language models for public health intervention. In: Proceedings of the 2023 CHI conference on human factors in computing systems, pp 1–16

- Jorgensen S, Nadizar G, Pietropolli G, Manzoni L, Medvet E et al (2024) Large language model-based test case generation for gp agents. In: Proceedings of the genetic and evolutionary computation conference, pp 914–923
- Kang J, Laroche R, Yuan X, Trischler A, Liu X, Fu J (2024) Think before you act: Decision transformers with working memory. arXiv preprint [arXiv:2305.16338v3](https://arxiv.org/abs/2305.16338v3)
- Kannan SS, Venkatesh VL, Min BC (2024) Smart-llm: Smart multi-agent robot task planning using large language models. In: 2024 IEEE/RSJ international conference on intelligent robots and systems (IROS). IEEE, pp 12140–12147
- Kapitanov A, Kvanchiani K, xNagaev K, Kraynov R, Makhliarchuk A (2024) Hagrid – hand gesture recognition image dataset. In: Proceedings of the IEEE/CVF winter conference on applications of computer vision (WACV), pp 4572–4581
- Khan MA, Amani M, Das S, Ghosh B, Wu Q et al (2025) In agents we trust, but who do agents trust? latent source preferences steer LLM generations. In: ICML 2025 workshop on reliable and responsible foundation models
- Kim Y, Park C, Jeong H, Chan YS, Xu X et al (2024) Mdagents: An adaptive collaboration of llms for medical decision-making. *Adv Neural Inf Process Syst* 37:79410–79452
- Klein LH, Potamitis N, Aydin R, West R, Gulcehre C, Arora A (2025) Fleet of agents: coordinated problem solving with large language models. In: Forty-second international conference on machine learning
- Kočíšký T, Schwarz J, Blunsom P, Dyer C, Hermann KM, Melis G, Grefenstette E (2018) The NarrativeQA reading comprehension challenge. *Trans Assoc Comput Linguist* 6:317–328
- Köpf A, Kilcher Y, Von Rütte D, Anagnostidis S, Tam ZR et al (2023) Openassistant conversations-democratizing large language model alignment. *Adv Neural Inf Process Syst* 36:47669–47681
- Koupaee M, Wang WY (2018) Wikihow: A large scale text summarization dataset. arXiv preprint [arXiv:1810.09305](https://arxiv.org/abs/1810.09305)
- Kryściński W, Rajani N, Agarwal D, Xiong C, Radev D (2021) Booksum: A collection of datasets for long-form narrative summarization. arXiv preprint [arXiv:2105.08209](https://arxiv.org/abs/2105.08209)
- Kumar P (2024) Large language models (llms): survey, technical frameworks, and future challenges. *Artif Intell Rev* 57(10):260
- Lampinen A, Chan S, Dasgupta I, Nam A, Wang J (2023) Passive learning of active causal strategies in agents and language models. *Adv Neural Inf Process Syst* 36:1283–1297
- Li X (2025) A review of prominent paradigms for llm-based agents: tool use, planning (including rag), and feedback learning. In: Proceedings of the 31st international conference on computational linguistics, pp 9760–9779
- Li H, Chong Y, Stepputtis S, Campbell J, Hughes D et al (2023a) Theory of mind for multi-agent collaboration via large language models. In: Proceedings of the 2023 conference on empirical methods in natural language processing. Association for Computational Linguistics, pp 180–192
- Li G, Hammoud H, Itani H, Khizbullin D, Ghanem B (2023b) Camel: Communicative agents for “mind” exploration of large language model society. *Adv Neural Inf Process Syst* 36:51991–52008
- Li N, Gao C, Li M, Li Y, Liao Q (2024a) EconAgent: Large language model-empowered agents for simulating macroeconomic activities. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 15523–15536
- Li R, Luo Z, Du X (2024b) Fg-prm: Fine-grained hallucination detection and mitigation in language model mathematical reasoning. arXiv preprint [arXiv:2410.06304](https://arxiv.org/abs/2410.06304)
- Li L, Wang Y, Xu R, Wang P, Feng X et al (2024c) Multimodal ArXiv: A dataset for improving scientific comprehension of large vision-language models. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 14 369–14 387
- Li XL, Chowdhury N, Johnson DD, Hashimoto T, Liang P, et al (2025a) Eliciting language model behaviors with investigator agents. In: Forty-second international conference on machine learning
- Li Z, Zhang R, Wang Z, Xie Z, Song Y (2025b) Llm-guided decision-making toolkit for multi-agent reinforcement learning. *Neurocomputing* 638:130105
- Lian W, Goodson B, Pentland E, Cook A, Vong C (2023) Teknium, Openorca: An open dataset of gpt augmented flan reasoning traces. *HuggingFace repository*, [Online]. Available: <https://huggingface.co/datasets/Open-Orca/OpenOrca>
- Liu Z, Luo P, Wang X, Tang X (2015) Deep learning face attributes in the wild. In: Proceedings of international conference on computer vision (ICCV). pp 3730–3738
- Liu T, Xu C, McAuley J (2023) Repobench: Benchmarking repository-level code auto-completion systems. arXiv preprint [arXiv:2306.03091](https://arxiv.org/abs/2306.03091)

- Liu Z, Hu H, Zhang S, Guo H, Ke S, et al (2024a) Reason for future, act for now: a principled architecture for autonomous LLM agents. In: Proceedings of the 41st international conference on machine learning, ser. Proceedings of Machine Learning Research, vol. 235. PMLR, pp 31 186–31 261
- Liu R, Yang R, Jia C, Zhang G, Yang D, Vosoughi S (2024b) Training socially aligned language models on simulated social interactions. In: The twelfth international conference on learning representations
- Liu X, Yu H, Zhang H, Xu Y, Lei X et al (2024c) Agentbench: Evaluating LLMs as agents. In: The twelfth international conference on learning representations
- Liu W, Li J, Tang Y, Zhao Y, Liu C et al (2025a) Drbioright 2.0: an llm-powered bioinformatics chatbot for large-scale cancer functional proteomics analysis. *Nat Commun* 16(1):2256
- Liu X, ZHANG J, Shang H, Guo S, Chengxu Y, Zhu Q (2025b) Exploring prosocial irrationality for LLM agents: a social cognition view. In: The thirteenth international conference on learning representations
- Lu P, Qiu L, Chang KW, Wu YN, Zhu SC et al (2023) Dynamic prompt learning via policy gradient for semi-structured mathematical reasoning. In: International conference on learning representations (ICLR)
- Lu M, Ho B, Ren D, Wang X (2024) Triageagent: Towards better multi-agents collaborations for large language model-based clinical triage. Findings of the association for computational linguistics EMNLP 2024:5747–5764
- Luo Z, Xu C, Zhao P, Sun Q, Geng X et al (2023) Wizardcoder: Empowering code large language models with evol-instruct. *arXiv preprint arXiv:2306.08568*
- Luo J, Zhang W, Yuan Y, Zhao Y, Yang J et al (2025) Large language model agent: a survey on methodology, applications and challenges. *arXiv preprint arXiv:2503.21460*
- Ma H, Hu T, Pu Z, Boyin L, Ai X et al (2024) Coevolving with the other you: fine-tuning LLM with sequential cooperative multi-agent reinforcement learning. *Adv Neural Inf Process Syst* 37:15497–15525
- Mao S, Cai Y, Xia Y, Wu W, Wang X et al (2023) Alympics: Llm agents meet game theory – exploring strategic decision-making with ai agents. *arXiv preprint arXiv:2311.03220*
- Meier R (2025) Balancing minds and data: the privacy dilemma of llms and anthropomorphism in llms. *J Soc Comput* 6(3):173–183
- Mialon G, Fourrier C, Wolf T, LeCun Y, Scialom T (2023) Gaia: a benchmark for general ai assistants. In: The twelfth international conference on learning representations
- “Multiarithmetic dataset,” *Kaggle dataset*, 2023, accessed: 2025-08-22. [Online]. Available: <https://www.kaggle.com/datasets/dschettler8845/multiarithmetic-dataset>
- Muthusamy V, Rizk Y, Kate K, Venkateswaran P et al (2023) Towards large language model-based personal agents in the enterprise: current trends and open problems. Findings of the association for computational linguistics EMNLP 2023:6909–6921
- Ni B, Buehler MJ (2024) Mechagents: Large language model multi-agent collaborations can solve mechanics problems, generate new data, and integrate knowledge. *Extreme Mech Lett* 67:102131
- Ning Y, Liu H (2024) Urbankgent: A unified large language model agent framework for urban knowledge graph construction. *Adv Neural Inf Process Syst* 37:123 127–123 154
- Ouyang L, Wu J, Jiang X, Almeida D, Wainwright C et al (2022) Training language models to follow instructions with human feedback. *Adv Neural Inf Process Syst* 35:27730–27744
- Pang J-C, Yang S-H, Li K, Zhang J, Chen X-H et al (2024a) Kalm: Knowledgeable agents by offline reinforcement learning from large language model rollouts. *Adv Neural Inf Process Syst* 37:126620–126652
- Pang X, Tang S, Ye R, Xiong Y, Zhang B et al (2024b) Self-alignment of large language models via monologues-based social scene simulation. In: Proceedings of the 41st international conference on machine learning, ser. Proceedings of Machine Learning Research, vol. 235. PMLR, pp 39 416–39 447
- Park JS, O’Brien J, Cai CJ, Morris MR, Liang P, Bernstein MS (2023) Generative agents: Interactive simulators of human behavior. In: Proceedings of the 36th annual acm symposium on user interface software and technology, pp 1–22
- Penedo G, Malartic Q, Hesslow D, Cococarur R, Cappelli A et al (2023) The refinedweb dataset for falcon llm: outperforming curated corpora with web data, and web data only. *arXiv preprint arXiv:2306.01116*
- Penedo G, Kydlíček H, allal LB, Lozhkov A, Mitchell M et al (2024) The fineweb datasets: Decanting the web for the finest text data at scale. In: The thirty-eight conference on neural information processing systems datasets and benchmarks track
- Perincherry A, Krantz J, Lee S (2025) Do visual imaginations improve vision-and-language navigation agents?. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 3846–3855
- Peter S, Riener K, West JD (2025) The benefits and dangers of anthropomorphic conversational agents. *Proc Natl Acad Sci USA* 122(22):e2415898122
- Press O, Zhang M, Min S, Schmidt L, Smith N, Lewis M (2023) Measuring and narrowing the compositionality gap in language models. In: Findings of the association for computational linguistics: EMNLP. Association for Computational Linguistics 2023:5687–5711

- Qian C, Liu W, Liu H, Chen N, Dang Y et al (2023) Chatdev: Communicative agents for software development. arXiv preprint [arXiv:2307.07924v5](https://arxiv.org/abs/2307.07924v5)
- Qian C, He B, Zhuang Z, Deng J, Qin Y et al (2024) Tell me more! towards implicit user intention understanding of language model driven agents. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 1088–1113
- Qiao S, Fang R, Zhang N, Zhu Y, Chen X et al (2024a) Agent planning with world knowledge model. *Adv Neural Inf Process Syst* 37:114843–114871
- Qiao S, Zhang N, Fang R, Luo Y, Zhou W et al (2024b) Autoact: Automatic agent learning from scratch for qa via self-planning
- Qin Y, Hu S, Lin Y, Chen W, Ding N et al (2024a) Tool learning with foundation models. *ACM Comput Surv* 57(4):1–40
- Qin Y, Liang S, Ye Y, Zhu K, Yan L et al (2024b) ToolLLM: Facilitating large language models to master 16000+ real-world APIs. In: The twelfth international conference on learning representations
- Qi Y, Wu Q, Anderson P, Liu M, Shen C, van den Hengel A (2020) Reverie: Remote embodied visual referring expression in real indoor environments. arXiv preprint [arXiv:1904.10151v2](https://arxiv.org/abs/1904.10151v2), vol. 2
- Qu Y, Zhang T, Garg N, Kumar A (2024) Recursive introspection: teaching language model agents how to self-improve. *Adv Neural Inf Process Syst* 37:55249–55285
- Ramos MC, Collison CJ, White AD (2025) A review of large language models and autonomous agents in chemistry. *Chem Sci*
- Ritore A, Oprescu AM, Estirado Bronchalo A, Armengol de la Hoz MA (2024) Covid data for shared learning (cdsl): a comprehensive, multimodal covid-19 dataset from hm hospitales (version 1.0.0). *PhysioNet*
- Ruan Y, Dong H, Wang A, Pitis S, Zhou Y et al (2024) Identifying the risks of LM agents with an LM-emulated sandbox. In: The twelfth international conference on learning representations
- Saxton, Grefenstette, Hill, and Kohli, Analysing mathematical reasoning abilities of neural models. [arXiv:1904.01557](https://arxiv.org/abs/1904.01557), 2019
- Schick T, Dwivedi-Yu J, Dessi R, Raileanu R, Lomeli M et al (2023) Toolformer: Language models can teach themselves to use tools. *Adv Neural Inf Process Syst* 36:68539–68551
- Schmidgall S, Su Y, Wang Z, Sun X, Wu J et al (2025) Agent laboratory: Using llm agents as research assistants. arXiv preprint [arXiv:2501.04227](https://arxiv.org/abs/2501.04227)
- Schumann R, Zhu W, Feng W, Fu T-J, Riezler S, Wang WY (2024) Velma: Verbalization embodiment of llm agents for vision and language navigation in street view. *Proc AAAI Conf Artif Intell* 38(17):18924–18933
- Shen X, Chen Z, Backes M, Shen Y, Zhang Y (2024) "Do anything now": characterizing and evaluating in-the-wild jailbreak prompts on large language models. In: Proceedings of the 2024 on ACM SIGSAC conference on computer and communications security, pp 1671–1685
- Shinn N, Cassano F, Gopinath A, Narasimhan K, Yao S (2023) Reflexion: Language agents with verbal reinforcement learning. *Adv Neural Inf Process Syst* 36:8634–8652
- Shi F, Suzgun M, Freitag M, Wang X, Srivats S et al (2022) Language models are multilingual chain-of-thought reasoners. arXiv preprint [arXiv:2210.03057](https://arxiv.org/abs/2210.03057)
- Shridhar M, Thomason J, Gordon D, Bisk Y, Han W et al (2020) ALFRED: A benchmark for interpreting grounded instructions for everyday tasks. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp 10 740–10 749
- Shridhar M, Yuan X, Côté MA, Bisk Y, Trischler A, Hausknecht M (2021) ALFWorld: aligning text and embodied environments for interactive learning. In: Proceedings of the international conference on learning representations (ICLR)
- Singh H, Verma N, Wang Y, Bharadwaj M, Fashandi H et al (2024) Personal large language model agents: a case study on tailored travel planning. In: Proceedings of the 2024 conference on empirical methods in natural language processing: industry track, pp 486–514
- Song CH, Wu J, Washington C, Sadler BM, Chao WL, Su Y (2023) Llm-planner: Few-shot grounded planning for embodied agents with large language models. In: Proceedings of the IEEE/CVF international conference on computer vision, pp 2998–3009
- Srivastava A, Rastogi A, Rao A, Shueb AAM, Abid A et al (2023) Beyond the imitation game: quantifying and extrapolating the capabilities of language models. *Trans Mach Learn Res*
- Sun C, Huang S, Pompili D (2025) Llm-based multi-agent decision-making: challenges and future directions. *IEEE Robot Automat Lett* 10(6):5681–5688
- Su Y, Yang D, Yao S, Yu T (2024) Language agents: foundations, prospects, and risks. In: Proceedings of the 2024 conference on empirical methods in natural language processing: tutorial abstracts. Miami, Florida, USA: Association for Computational Linguistics, pp 17–24
- Talebirad Y, Nadiri A (2023) Multi-agent collaboration: Harnessing the power of intelligent llm agents. arXiv preprint [arXiv:2306.03314](https://arxiv.org/abs/2306.03314)

- Taori R, Gulrajani I, Zhang T, Dubois Y, Li X, Guestrin C, Liang P, Hashimoto TB (2023) Stanford alpaca: An instruction-following llama model. https://github.com/tatsu-lab/stanford_alpaca
- Tennant E, Hailes S, Musolesi M (2025) Moral alignment for LLM agents. In: The thirteenth international conference on learning representations
- Thorne J, Vlachos A, Christodoulopoulos C, Mittal A (2018) FEVER: a large-scale dataset for fact extraction and VERification. In: NAACL-HLT
- Tony C, Mutas M, Diaz Ferreyra N, Scandariato R (2023) Llmseceval: A dataset of natural language prompts for security evaluations. In: 2023 IEEE/ACM 20th international conference on mining software repositories (MSR)
- Trivedi H, Balasubramanian N, Khot T, Sabharwal A (2022) Musique: Multihop questions via single-hop question composition. *Trans Assoc Comput Linguist* 10:539–554
- Tse Huang J, Zhou J, Jin T, Zhou X, Chen Z et al (2025) On the resilience of LLM-based multi-agent collaboration with faulty agents. In: Forty-second international conference on machine learning
- U.S. National Library of Medicine, Pubmed baseline repository. https://www.nlm.nih.gov/databases/download/pubmed_medline.html, 2023, courtesy of the National Library of Medicine
- Valmeekam K, Marquez M, Olmo A, Sreedharan S, Kambhampati S (2023) Planbench: An extensible benchmark for evaluating large language models on planning and reasoning about change. *Adv Neural Inf Process Syst* 36:38975–38987
- Walke HR, Black K, Zhao TZ, Vuong Q, Zheng C et al (2023) Bridgedata v2: A dataset for robot learning at scale. In: Conference on robot learning. PMLR, pp 1723–1736
- Wang Z, Cai S, Chen G, Liu A, Ma X et al (2023a) Describe, explain, plan and select: interactive planning with large language models enables open-world multi-task agents. In: Proceedings of the 37th international conference on neural information processing systems, ser. NIPS '23. Red Hook, NY, USA: Curran Associates Inc
- Wang P, Li L, Shao Z, Xu R, Dai D et al (2023b) Math-shepherd: Verify and reinforce llms step-by-step without human annotations. arXiv preprint [arXiv:2312.08935v3](https://arxiv.org/abs/2312.08935v3)
- Wang G, Xie Y, Jiang Y, Mandlkar A, Xiao C et al (2023c) Voyager: An open-ended embodied agent with large language models. arXiv preprint [arXiv:2305.16291](https://arxiv.org/abs/2305.16291)
- Wang Z, Zhang G, Yang K, Shi N, Zhou W et al (2023d) Interactive natural language processing. arXiv preprint [arXiv:2305.13246](https://arxiv.org/abs/2305.13246)
- Wang Z, Cai S, Mu Z, Lin H, Zhang C et al (2024a) Omnijarvis: Unified vision-language-action tokenization enables open-world instruction following agents. *Adv Neural Inf Process Syst* 37:73278–73308
- Wang L, Ma C, Feng X et al (2024b) A survey on large language model based autonomous agents. *Front Comp Sci* 18:186345
- Wang Z, Liu Z, Zhang Y, Zhong A, Wang J et al (2024c) Ragent: Cloud root cause analysis by autonomous agents with tool-augmented large language models. In: Proceedings of the 33rd ACM international conference on information and knowledge management, pp 4966–497
- Wang R, Yu H, Zhang W, Qi Z, Sap M et al (2024d) SOTOPIA- π : Interactive learning of socially intelligent language agents. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 12912–12940
- Wang X, Jiang H, Yu Y, Yu J, Lin Y et al (2025a) Building intelligence identification system via large language model watermarking: a survey and beyond. *Artif Intell Rev* 58(8):249
- Wang L, Zhang J, Yang H, Chen Z-Y, Tang J et al (2025b) User behavior simulation with large language model-based agents. *ACM Trans Inform Syst* 43(2):1–37
- Wang Z, Zhu Y, Zhao H, Zheng X, Sui D et al (2025c) Colacare: Enhancing electronic health record modeling through large language model-driven multi-agent collaboration. *Proc ACM Web Conf* 2025:2250–2261
- Weber M, Fu DY, Anthony Q, Oren Y, Adams S et al (2024) Redpajama: an open dataset for training large language models. *NeurIPS Datasets and Benchmarks Track*
- Wei J, Wang X, Schuurmans D, Bosma M, Ichter B et al (2022) Chain-of-thought prompting elicits reasoning in large language models. In: Proceedings of the 36th international conference on neural information processing systems, ser. NIPS '22. Red Hook, NY, USA: Curran Associates Inc
- Wei Y, Wang Z, Lu Y, Xu C, Liu C et al (2024) Editable scene simulation for autonomous driving via collaborative llm-agents. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp 15077–15087
- Wijk H, Lin T, Becker J, Jawhar S, Parikh N et al (2025) RE-bench: Evaluating frontier AI r & d capabilities of language model agents against human experts. In: Forty-second international conference on machine learning
- Wu H, He Z, Zhang X, Yao X, Zheng S et al (2024a) Chatada: A large language model powered autonomous agent for eda. *IEEE Trans Comput Aided Des Integr Circ Syst* 43(10):3184–3197
- Wu S, Zhao S, Huang Q, Huang K, Yasunaga M et al (2024b) Avatar: Optimizing llm agents for tool usage via contrastive reasoning. *Adv Neural Inf Process Syst* 37:25981–26010

- Wu Q, Bansal G, Zhang J, Wu Y, Li B et al (2024c) Autogen: Enabling next-gen LLM applications via multi-agent conversations. In: First conference on language modeling
- Wu S, Zhao S, Yasunaga M, Huang K, Cao K et al (2024d) Stark: Benchmarking llm retrieval on textual and relational knowledge bases. In: NeurIPS datasets and benchmarks track
- Xi Z, Chen W, Guo X et al (2025) The rise and potential of large language model based agents: a survey. *Sci China Inf Sci* 68:121101
- Xia Y, Xiao Z, Jazdi N, Weyrich M (2024) Generation of asset administration shell with large language model agents: toward semantic interoperability in digital twins in the context of industry 4.0. *IEEE Access* 12:84863–84877
- Xia Y, Shen W, Wang Y, Liu JK, Sun H et al (2025) Leetcodedataset: A temporal dataset for robust evaluation and efficient training of code llms. *arXiv preprint arXiv:2504.14655*
- Xiang Z, Zheng L, Li Y, Hong J, Li Q et al (2025) Guardagent: safeguard LLM agents via knowledge-enabled reasoning. In: ICMML 2025 workshop on computer use agents
- Xie C, Chen C, Jia F, Ye Z, Lai S et al (2024a) Can large language model agents simulate human trust behavior? *Adv Neural Inf Process Syst* 37:15674–15729
- Xie J, Zhang K, Chen J, Zhu T, Lou R et al (2024b) Travelplanner: A benchmark for real-world planning with language agents. *arXiv preprint arXiv:2402.01622*
- Xing M, Zhang R, Xue H, Chen Q, Yang F, Xiao Z (2024) Understanding the weakness of large language model agents within a complex android environment. In: Proceedings of the 30th ACM SIGKDD conference on knowledge discovery and data mining, pp 6061–6072
- Xue X, Lu Z, Huang D, Wang Z, Ouyang W, Bai L (2025) Comfybench: Benchmarking llm-based agents in comfyui for autonomously designing collaborative ai systems. In: Proceedings of the computer vision and pattern recognition conference, pp 24 614–24 624
- Xu M, Niyato D, Kang J, Xiong Z, Mao S et al (2024a) When large language model agents meet 6g networks: perception, grounding, and alignment. *IEEE Wirel Commun*
- Xu Y, Su H, Xing C, Mi B, Liu Q et al (2024b) Lemur: Harmonizing natural language and code for language agents. In: The twelfth international conference on learning representations
- Xu W, Huang C, Gao S et al (2025a) Llm-based agents for tool learning: a survey. *Data Sci Eng*, pp 1–31
- Xu W, Mei K, Gao H, Tan J, Liang Z, Zhang Y (2025b) A-mem: Agentic memory for llm agents. *arXiv preprint arXiv:2502.12110*
- Yang S, Luo P, Loy CC, Tang X (2016) Wider face: a face detection benchmark. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 5525–5533
- Yang Z, Qi P, Zhang S, Bengio Y, Cohen W et al (2018) HotpotQA: A dataset for diverse, explainable multi-hop question answering. In: Proceedings of the 2018 conference on empirical methods in natural language processing. Association for Computational Linguistics, pp 2369–2380
- Yang J, Prabhakar A, Narasimhan K, Yao S (2023) Intercode: Standardizing and benchmarking interactive coding with execution feedback. *Adv Neural Inf Process Syst* 36:23826–23854
- Yang W, Bi X, Lin Y, Chen S, Zhou J, Sun X (2024a) Watch out for your agents! investigating backdoor threats to llm-based agents. *Adv Neural Inf Process Syst* 37:100938–100964
- Yang J, Chen X, Qian S, Madaan N, Iyengar M et al (2024b) Llm-grounder: Open-vocabulary 3d visual grounding with large language model as an agent. In: 2024 IEEE international conference on robotics and automation (ICRA). IEEE, pp 7694–7701
- Yang Z, Xu X, Yao B, Rogers E, Zhang S et al (2024c) Talk2care: An llm-based voice assistant for communication between healthcare providers and older adults. In: Proceedings of the ACM on interactive mobile wearable and ubiquitous technologies 8(2):1–35
- Yang Y, Zhou T, Li K, Tao D, Li L et al (2024d) Embodied multi-modal agent trained by an llm from a parallel textworld. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp 26 275–26 285
- Yao S, Yu D, Zhao J, Shafraan I, Griffiths T et al (2023a) Tree of thoughts: deliberate problem solving with large language models. *Adv Neural Inf Process Syst* 36:11809–11822
- Yao S, Zhao J, Yu D, Du N, Shafraan I et al (2023b) React: Synergizing reasoning and acting in language models. In: International conference on learning representations (ICLR)
- Yim WW, Fu Y, Ben Abacha A, Snider N, Lin T, Yetisgen M (2023) aci-bench-corpus.zip. Figshare. Dataset, [Online]. Available: <https://doi.org/10.6084/m9.figshare.22494601.v1>
- Yin P, Deng B, Chen E, Vasilescu B, Neubig G (2018) Learning to mine aligned code and natural language pairs from stack overflow. In: IEEE/ACM 15th international conference on mining software repositories (MSR). IEEE 2018:476–486
- Yin D, Brahman F, Ravichander A, Chandu K, Chang KW et al (2024) Agent lumos: Unified and modular training for open-source language agents. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 12380–12403

- Yuan S, Song K, Chen J, Tan X, Shen Y et al (2025) EASYTOOL: enhancing LLM-based agents with concise tool instruction. In: Proceedings of the 2025 conference of the nations of the Americas chapter of the association for computational linguistics: human language technologies (Volume 1: Long Papers). Association for Computational Linguistics, pp 951–972
- Zeng X, Wang X, Zhang T, Yu C, Zhao S, Chen Y (2024) Gesturegpt: Toward zero-shot free-form hand gesture understanding with large language model agents. In: Proceedings of the ACM on human-computer interaction 8(ISS):462–499
- Zhai S, Bai H, Lin Z, Pan J, Tong P et al (2024) Fine-tuning large vision-language models as decision-making agents via reinforcement learning. *Adv Neural Inf Process Syst* 37:110935–110971
- Zhang Y, Cao C, Cheng J, Lu H (2018) Egogesture: A new dataset and benchmark for egocentric hand gesture recognition. *IEEE Trans Multimedia* 20(5):1038–1050
- Zhang D, Chen L, Zhang S, Xu H, Zhao Z, Yu K (2023) Large language models are semi-parametric reinforcement learning agents. *Adv Neural Inf Process Syst* 36:78227–78239
- Zhang Q, Hu Y, Yan J, Zhang H, Xie X et al (2024a) Large-language-model-based ai agent for organic semiconductor device research. *Adv Mater* 36(32):2405163
- Zhang Y, Sun R, Chen Y, Pfister T, Zhang R, Arik S (2024b) Chain of agents: large language models collaborating on long-context tasks. *Adv Neural Inf Process Syst* 37:132208–132237
- Zhang X, Xu H, Ba Z, Wang Z, Hong Y et al (2024c) Privacyasst: Safeguarding user privacy in tool-using large language model agents. *IEEE Trans Depend Secure Comput* 21(6):5242–5258
- Zhang C, Yang K, Hu S, Wang Z, Li G et al (2024d) Proagent: building proactive cooperative agents with large language models. *Proceedings AAAI Conf Artif Intell* 38(16):17591–17599
- Zhang S, Dong Y, Zhang Y, Payne TR, Zhang J (2024e) Large language model assisted multi-agent dialogue for ontology alignment. In: Proceedings of the 23rd international conference on autonomous agents and multiagent systems, pp 2594–2596
- Zhang R, Du H, Liu Y, Niyato D, Kang J et al (2024f) Generative ai agents with large language model for satellite networks via a mixture of experts transmission. *IEEE J Selected Areas Commun*
- Zhang H, Du W, Shan J, Zhou Q, Du Y et al (2024g) Building cooperative embodied agents modularly with large language models. In: The Twelfth international conference on learning representations
- Zhang Y, Jiang Q, Xingyu Han X, Chen N, Yang Y, Ren K (2024h) Benchmarking data science agents. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 5677–5700
- Zhang J, Xu X, Zhang N, Liu R, Hooi B, Deng S (2024i) Exploring collaboration mechanisms for LLM agents: a social psychology view. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 14 544–14 607
- Zhang Y, Yuan S, Hu C, Richardson K, Xiao Y, Chen J (2024j) TimeArena: Shaping efficient multitasking language agents in a time-aware simulation. In: Proceedings of the 62nd annual meeting of the association for computational linguistics (Volume 1: Long Papers). Association for Computational Linguistics, pp 3894–3916
- Zhang S, Zhang J, Liu J, Song L, Wang C et al (2024k) Offline training of language model agents with functions as learnable weights. In: Proceedings of the 41st international conference on machine learning, ser. Proceedings of Machine Learning Research, vol. 235. PMLR, 21–27, pp 60315–60335
- Zhao W, Ren X, Hessel J, Cardie C, Choi Y, Deng Y (2024a) Wildchat: 1m chatGPT interaction logs in the wild. In: the twelfth international conference on learning representations
- Zhao Q, Wang J, Zhang Y, Jin Y, Zhu K, et al (2024b) CompeteAI: Understanding the competition dynamics of large language model-based agents. In: Proceedings of the 41st international conference on machine learning, ser. Proceedings of Machine Learning Research, vol. 235. PMLR, pp 61 092–61 107
- Zheng S, jiazheng liu, Feng Y, Lu Z (2024) Steve-eye: Equipping LLM-based embodied agents with visual perception in open worlds. In: The Twelfth international conference on learning representations
- Zhong M, Yin D, Yu T, Zaidi A, Mutuma M et al (2021) QMSum: a new benchmark for query-based multi-domain meeting summarization. In: North American association for computational linguistics (NAACL)
- Zhou H, Tang Y, Qin H, Yang Y, Jin R et al (2024) Star-agents: Automatic data optimization with llm agents for instruction tuning. *Adv Neural Inf Process Syst* 37:4575–4597
- Zhu F, Simmons R (2024) Bootstrapping cognitive agents with a large language model. *Proc AAAI Conf Artif Intell* 38(1):655–663
- Zou A, Wang Z, Carlini N, Nasr M, Kolter JZ, Fredrikson M (2023) Universal and transferable adversarial attacks on aligned language models. *arXiv preprint [arXiv:2307.15043](https://arxiv.org/abs/2307.15043)*

Authors and Affiliations

**Sadia Sultana Chowd^{1,2,3} · Riasad Alvi^{2,4} · Subhey Sadi Rahman^{2,4} ·
Md Abdur Rahman^{2,4} · Mohaimenul Azam Khan Raiaan^{2,4,5} · Md Rafiqul Islam⁶ ·
Mukhtar Hussain⁸ · Sami Azam^{6,7}**

✉ Mohaimenul Azam Khan Raiaan
mraiaan191228@bscse.uiu.ac.bd

✉ Sami Azam
sami.azam@cdu.edu.au

¹ Department of Computer Science and Engineering, Daffodil International University,
1341 Dhaka, Bangladesh

² Applied Artificial Intelligence and Intelligent Systems (AAIINS) Laboratory, 1217 Dhaka,
Bangladesh

³ Department of Software Systems & Cybersecurity, Monash University, 3800 Melbourne,
Australia

⁴ Department of Computer Science and Engineering, United International University,
1212 Dhaka, Bangladesh

⁵ Department of Data Science and Artificial Intelligence, Monash University, 3800, Melbourne,
Australia

⁶ Faculty of Science and Technology, Charles Darwin University, Casuarina, NT 0909, Australia

⁷ Energy and Resources Institute, Charles Darwin University, 0909 NT, Australia

⁸ Faculty of Science and Technology, Charles Darwin University, 2000 Sydney, Australia