

Architecting agentic apps

Building a standardized ecosystem for next-generation
AI tools



Synopsis

This whitepaper delves into the rapidly evolving landscape of agentic apps, a new breed of applications designed to operate autonomously, leveraging AI and machine learning to perform complex tasks with minimal human intervention. As these applications become more prevalent, a standardized ecosystem of tools, protocols and data models becomes increasingly critical. This whitepaper addresses the challenges associated with the fragmented nature of the current agentic apps ecosystem and proposes solutions to enhance their effectiveness and interoperability.

Agentic apps, which include components like Large Language Models (LLMs), memory systems, goal definition mechanisms and advanced planning processes, represent a significant shift in how digital tasks are executed. However, without standardized tools and protocols, the potential of these apps remains underutilized. This whitepaper explores the importance of establishing a common framework for tool configuration, a unified data model and standardized communication protocols. By creating a common runtime environment and ensuring interoperability within the agentic apps ecosystem and beyond, we can unlock the full potential of these applications, driving greater efficiency, innovation and value across industries.



In summary, this whitepaper provides a comprehensive overview of the challenges and opportunities in the Agentic apps ecosystem and offers practical solutions to ensure successful integration and widespread adoption. By focusing on the standardization of tools and protocols, we aim to pave the way for a more connected and effective digital landscape where agentic apps can truly thrive.

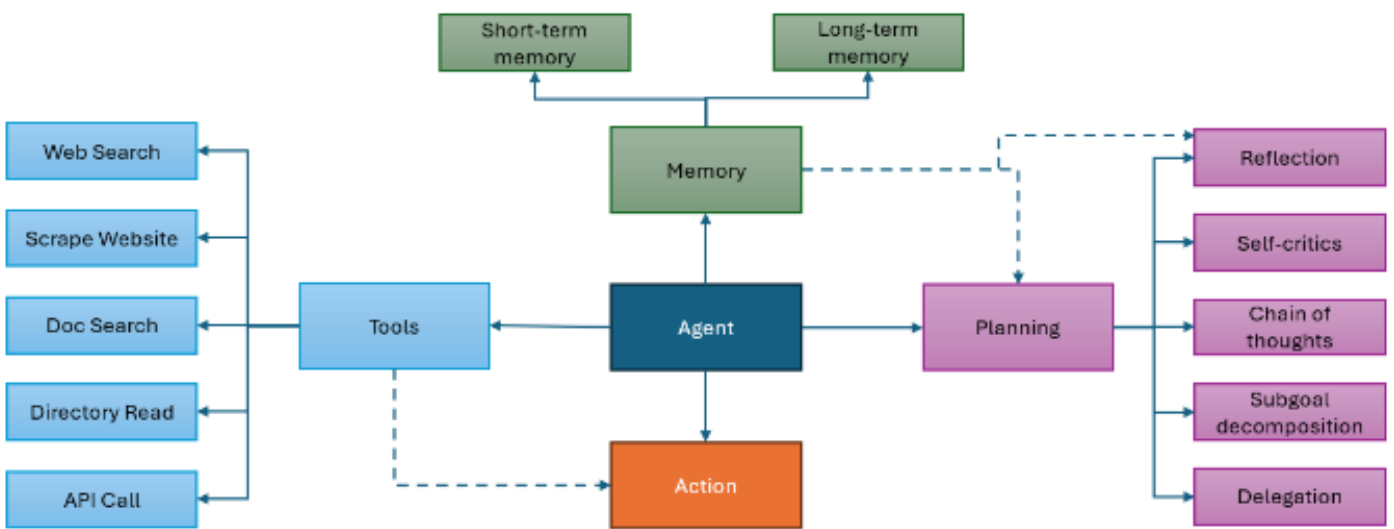
Understanding the agentic apps

The history of agentic apps can be traced back to the evolution of AI technologies that sought to automate repetitive and logic-driven tasks. Initially, these applications focused on executing predefined rules with limited flexibility. However, over the last few years, advancements in machine learning, large language models (LLMs) and AI tools have transformed agentic apps into more autonomous systems capable of learning from their environment, making decisions and performing complex tasks with minimal human intervention. This evolution marks a shift from rule-based systems to highly dynamic, self-adapting applications that are reshaping industries.

Agentic apps represent a new frontier in software design, where autonomous AI agents carry out complex tasks with minimal human intervention. These apps are designed to work alongside humans, augmenting their capabilities, automating routine processes and tackling challenges that would otherwise require significant cognitive effort. As we move towards an era where AI becomes increasingly embedded in everyday activities, agentic apps are poised to revolutionize work performance, driving productivity and innovation across industries.

Agentic apps offer organizations significant benefits by automating complex workflows, reducing operational costs and enhancing decision-making through real-time data insights.

Anatomy of the AI Agent



They enable businesses to improve efficiency, scale processes seamlessly and foster innovation by empowering AI-driven systems to operate with minimal human oversight, leading to faster and more accurate outcomes.

Critical components of agentic apps

1

Large language models (LLMs) are the core engines of agentic apps, enabling them to understand and generate human-like text. These models have been trained on vast amounts of data, allowing them to process and respond to complex queries, generate creative content and provide nuanced recommendations.

2

Memory. Agentic apps are equipped with memory systems that allow them to retain information over time, enabling them to learn from past interactions, maintain context and improve their performance through experience. This memory can be short-term (working memory) and long-term, influencing how the agent makes decisions and interacts with users.

3

Tools. Beyond processing language, agentic apps leverage various external tools to perform specialized tasks. These tools can range from simple APIs to complex software systems and they are crucial for enabling the app to interact with different digital environments, gather data, and execute commands.

4

Definition of goals. Goals are the driving force behind an agentic app's actions. Users can predefine these goals or dynamically generate them based on the agent's understanding of the task. Defining clear, actionable goals is essential for guiding the agent's behaviour and ensuring it aligns with the desired outcomes.

5

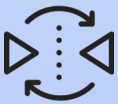
Backstory. A backstory provides context and continuity to an agentic app's actions. It encompasses the history of interactions, past decisions and the rationale behind previous actions. This allows the agent to maintain operations coherence and adapt strategies based on accumulated experience.

6

Task management. Agentic apps can manage multiple tasks simultaneously, prioritizing them based on importance, urgency and resource availability. This involves breaking down complex tasks into manageable sub-tasks, sequencing actions and allocating resources effectively.

7

Planning process



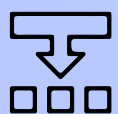
Reflection. Agentic apps regularly reflect on their performance, evaluating the success of their actions against set goals. This process allows them to identify areas of improvement and adjust their strategies accordingly.



Self-critique. Through self-critique, the agent assesses its decision-making process, learns from mistakes and refines its approach to problem-solving.



Chain of thoughts. This component enables the agent to maintain a coherent and logical flow of ideas, ensuring its actions are consistent and aligned with the overall goal.



Subgoal decomposition. Complex tasks are often broken down into smaller, more manageable subgoals. This decomposition allows the agent to tackle each aspect of a task systematically, improving efficiency and effectiveness.



Delegation. In multi-agent environments, agentic apps can delegate specific tasks to other agents, leveraging their specialized capabilities to achieve the overall goal more effectively.

Challenges in the agentic apps ecosystem

As we consider the challenges and opportunities facing the burgeoning agentic apps ecosystem, it is instructive to draw parallels with past technological advancements. Just as the rise of Enterprise Application Integration (EAI) in the 1990s brought about significant challenges in interoperability, security and standardization, we now face similar hurdles with agentic apps. The lessons learned from those earlier developments provide valuable insights into how we can navigate the complexities of this new era. By understanding and addressing these challenges, we can create a robust foundation for the successful integration and widespread adoption of agentic apps.

Challenges



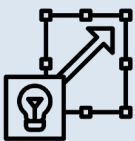
Interoperability issues

Fragmented tooling:

The current landscape of agentic apps is characterized by a lack of standardized tools, making seamless communication between agents and systems difficult. Integrating various agentic apps into existing digital ecosystems can be complex and inefficient without a common framework.

Compatibility barriers:

Different agentic apps may use distinct protocols, data formats and communication methods, making it challenging to achieve a cohesive multi-agent environment where tasks can be delegated and managed effectively.



Scalability and resource management

Computational demands:

As agentic apps become more sophisticated, they require significant computational resources to process complex tasks, manage memory and interact with multiple tools. This can limit their scalability, especially in resource-constrained environments.

Efficient resource allocation:

Managing and optimizing the use of resources, such as processing power and memory, across multiple agents is a challenge that needs to be addressed to ensure the efficient operation of agentic apps at scale.



Security, ethical and regulatory considerations

As agentic apps become more autonomous, the potential security risks and ethical implications grow increasingly significant. These apps often have access to sensitive data, decision-making power and the ability to interact with various systems, raising concerns about unauthorized access, data breaches and misuse of information. Ensuring robust security protocols, encryption and continuous monitoring are critical to safeguarding against these threats.

Beyond technical security, ethical considerations are equally important. AI-driven apps' decisions can have far-reaching consequences, from bias in decision-making to transparency in their actions. Organizations must ensure that these systems are designed to be fair, transparent and accountable, aligning with ethical guidelines and public trust.

Moreover, regulatory compliance is a pressing issue as governments and industry bodies begin to set frameworks for AI usage. Agentic apps must comply with data protection laws (such as GDPR) and sector-specific regulations, especially in industries like healthcare and finance, where data privacy and legal compliance are paramount. Establishing a balance between innovation, security, ethics and regulatory adherence is crucial for successfully deploying agentic apps in real-world scenarios.

Proposal: Building a standardized tool ecosystem for agentic apps

The future success of agentic apps hinges on creating a standardized tool ecosystem. As these AI-driven applications continue to gain traction, the need for a unified framework becomes paramount. Standardization is not just a technical necessity but a foundational requirement for ensuring that agentic apps can operate effectively and deliver their full potential.

The importance of standardization

Without standardization, the diverse tools and components of the agentic apps ecosystem will remain fragmented, leading to inefficiencies, compatibility issues and limited interoperability. Standardized tools are essential for ensuring that agentic apps can communicate seamlessly with each other and integrate smoothly into existing digital infrastructures. Without this cohesion, the autonomy and intelligence that make agentic apps powerful will be undermined by inconsistent performance and limited scalability.

A key aspect of enabling agentic apps to function effectively across diverse environments is developing a standardized tool framework. This framework should include the following elements:

Standardized framework for tools

Standardizing communication protocols:

Effective communication is the backbone of any distributed system and agentic apps are no exception. Standardizing communication protocols such as SOAP and REST ensures that these apps can exchange information reliably and securely. These protocols provide a consistent framework for data transmission, enabling agentic apps to interact with internal and external systems with minimal friction. By adopting standard protocols, we can enhance the entire ecosystem's scalability, security and performance.

Establishing a common data model:

A common data model enables consistent data exchange between agentic apps and their associated tools. This model defines the data's structure, format and semantics, ensuring that information can be accurately interpreted and processed across different ecosystem components.

By standardizing the data model, we can eliminate the discrepancies that often arise from disparate data formats, thereby improving the accuracy and efficiency of AI-driven tasks.

Interoperability with semantics:

Moving beyond basic data exchange, the proposal emphasizes the importance of semantic interoperability. This involves creating a common vocabulary and shared meanings, enabling agentic apps to understand and contextualize information across various domains. By incorporating semantic standards, agents can achieve a higher level of understanding and collaboration, reducing the risk of miscommunication and errors.

Configuring tools with a common manifest:

To streamline the deployment and operation of agentic apps, tools must be configured using a common manifest. This manifest serves as a blueprint, outlining how each tool should be set up and how it interacts with other components in the ecosystem. By adhering to a common configuration standard, developers can reduce complexity, minimize errors, and ensure that tools are deployed consistently across different environments. This approach enhances reliability and accelerates the development and scaling of agentic apps.

Creating a common runtime environment:

Finally, establishing a common runtime environment is essential for the seamless execution of agentic apps. This environment provides a standardized platform for harmonizing tools, protocols and data models. Creating a unified runtime ensures that agentic apps can be deployed and managed efficiently across different infrastructures, reducing operational overhead and enabling faster innovation.

Tool directory and certification

The proposal includes further creating a comprehensive tool directory to enhance agentic apps' reliability and security. This directory will serve as a centralized repository for tools vetted and certified for use by agentic apps.

Tool discovery and lookup:

The directory will allow agents to discover and look up tools based on their capabilities, compatibility and certification status. This ensures that agentic apps can easily access the tools they need to perform specific tasks while promoting trusted and reliable tools.

Certification process:

A rigorous certification process will be established to evaluate tools based on security, performance, interoperability and compliance with standards. Only tools that meet these criteria will be listed in the directory, providing users with confidence in the quality and safety of the tools they integrate into their agentic apps.

Security and auditability:

The directory will address security concerns by ensuring that only certified tools are used within the agentic apps ecosystem. This approach will minimize the risk of vulnerabilities and unauthorized access. Additionally, auditability features will be built into the framework, allowing for the tracking and logging of tool usage, ensuring transparency and enabling the identification of potential security breaches.

Facilitating ecosystem growth through collaboration and standardization

The proposal advocates for collaboration among industry stakeholders to develop and maintain these standards to accelerate the adoption and evolution of agentic apps. This collaborative approach will involve:

Industry Consortia and Working Groups:

Establishing consortia and working groups consisting of industry leaders, developers and

regulators to drive the creation and adoption of standards. These groups will play a key role in identifying best practices, addressing emerging challenges and ensuring that the standards remain relevant and effective as the ecosystem evolves.

Open standards and APIs:

Promoting the use of open standards and APIs will encourage innovation and allow the seamless integration of new tools and technologies into the agentic apps' ecosystem. This openness will foster competition, drive down costs and spur the development of cutting-edge tools that can further enhance the capabilities of Agentic apps.

Continuous improvement and feedback loops:

Finally, the proposal recommends establishing continuous improvement processes, where feedback from users and developers is actively sought and incorporated into the standards. This iterative approach will ensure that the framework remains responsive to the ecosystem's needs, allowing it to adapt to new challenges and opportunities.

While the proposal to build a standardized tool ecosystem for agentic apps offers numerous advantages—such as enhanced interoperability, security and scalability—it also presents certain limitations. One challenge is achieving consensus across diverse industries and technology providers, as different sectors may have unique requirements and standards that make uniform adoption difficult. Additionally, the rapid pace of AI advancements may outpace the development of standardized protocols, causing delays in implementation or creating gaps in functionality. There are also concerns about limiting innovation if strict standards hinder flexibility or create barriers for emerging tools and technologies outside the standardized framework. These limitations highlight the need for a balanced approach accommodating structure and innovation.

Promising initiatives

OpenAI's API ecosystem:

OpenAI has developed an API that allows developers to integrate advanced AI tools, including language models like GPT, into various applications. This initiative provides a standardized interface for accessing sophisticated AI capabilities, promoting interoperability and ease of use for businesses.

OpenAI and Microsoft's partnership for enterprise-grade AI:

Microsoft's integration of OpenAI models within the Azure platform offers a standardized, scalable solution for enterprises. The collaboration promotes a cohesive ecosystem for developing and deploying AI-driven applications, aligning with agentic apps' broader vision.

Hugging Face transformers and dataset libraries:

Hugging Face provides an open platform that standardizes access to various AI models and datasets. The platform's interoperability across different languages and models allows developers to build agentic apps using a consistent toolset. Their efforts to create a shared space for developers to access, fine-tune and deploy models can be a notable reference.

Google's TensorFlow Hub:

TensorFlow Hub is a library for reusable machine learning modules, promoting standardization and interoperability in AI development. This initiative allows developers to access a wide array of pre-trained models and integrate them seamlessly into their applications, which supports the standardization of tools for AI-driven applications like agentic apps.

Kubernetes and the Cloud Native Computing Foundation (CNCF):

Kubernetes has become a de facto standard for orchestrating containerized applications across different cloud environments. Its open-source nature and wide adoption have led to the

development of a standardized ecosystem for deploying and managing cloud-native applications, which can also be applied to agentic app architectures.

W3C (World Wide Web Consortium) for Web Standards:

The W3C has long been a leader in creating web standards, including APIs, protocols and formats that support interoperability. This effort is important as it provides a framework for agentic apps to communicate and operate across diverse platforms using standardized web protocols.

Data exchange standards in Healthcare (FHIR by HL7):

In the healthcare industry, FHIR (Fast Healthcare Interoperability Resources) by HL7 has emerged as a leading standard for exchanging healthcare data between systems. This standardization enables the seamless integration of agentic apps in healthcare environments, ensuring interoperability and consistency in data handling.

Financial services industry standards (ISO 20022):

The ISO 20022 standard is used for electronic data interchange between financial institutions. Many banks and payment systems worldwide have adopted this standardized messaging format, allowing agentic apps in the financial services sector to operate seamlessly within a consistent ecosystem.

These initiatives provide concrete examples of how standardization is being pursued across industries and technologies, supporting the development of cohesive ecosystems that foster innovation and interoperability.



Conclusion

The evolution of agentic apps represents a significant leap forward in the capabilities of AI-driven applications. However, to fully harness their potential, we must address the challenges associated with a fragmented ecosystem. This whitepaper has outlined the critical importance of building a standardized tool ecosystem to support agentic apps' effective deployment and operation.

Standardization is essential for ensuring interoperability, scalability and reliability. Without a unified framework, agentic apps risk being constrained by inconsistencies. We can create a robust foundation that allows these applications to thrive by focusing on standardizing tools, data models, communication protocols, and runtime environments.

Interoperability enables seamless integration, ensuring that agentic apps can operate efficiently regardless of the deployment environment. A common configuration manifest, standardized data models and consistent communication protocols will facilitate smoother operations.

In conclusion, the proposals in this whitepaper aim to create a unified and effective ecosystem of agentic apps. By embracing standardization, we can unlock new levels of digital productivity and innovation, positioning agentic apps as a transformative force in the digital landscape.

HCLTech | Supercharging
Progress™

hcltech.com