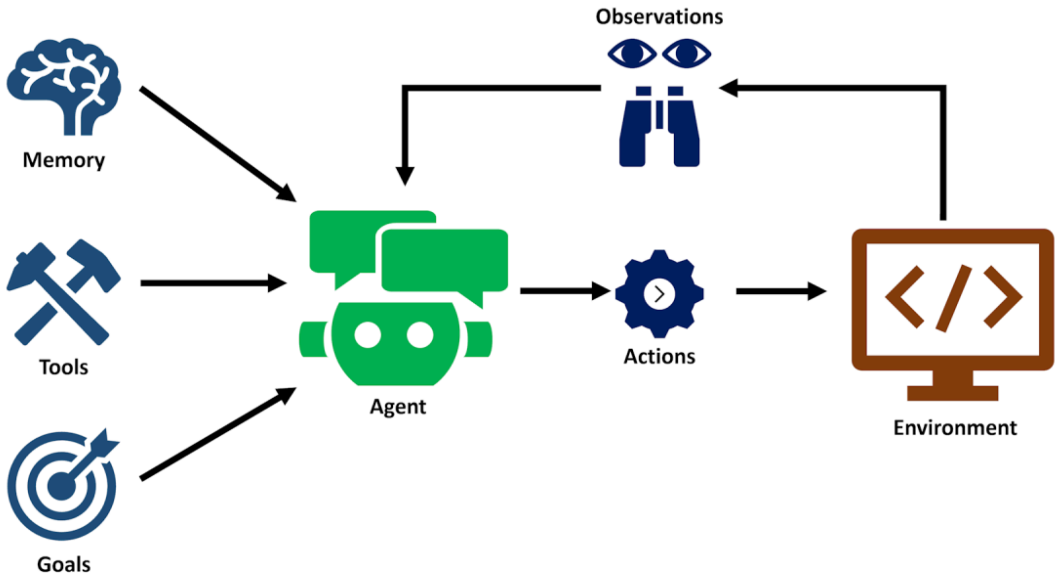
Agentic AI



What is an AI Agent?

An AI agent is an autonomous entity, often powered by a Large Language Model (LLM) serving as its "brain," that can perform complex, multi-step actions without explicit step-by-step human direction.

Key characteristics of an AI agent include:

- **Autonomy:** It can make decisions and take actions independently to reach its goal.
- **Goal-Oriented:** It pursues a predefined objective.
- **Perception:** It collects data from its environment (via sensors, APIs, user inputs, etc.).
- **Reasoning/Planning:** It breaks down complex goals into smaller steps, evaluates potential actions, and chooses the best course of action.
- **Action/Execution:** It performs the planned steps, often by using **tools**.
- **Memory and Learning:** It can remember past interactions and use that information to adapt and improve its performance over time.

What is Memory for an AI Agent?

Memory is a critical component that allows an AI agent to retain context, knowledge, and past experiences to inform future decisions and actions. Without memory, an agent would treat every interaction as if it were the first.

Type of Memory	Description	Function
Short-Term Memory (STM)	Information retained for immediate, ongoing use within a single session or task.	Maintains the context of the current conversation or task steps (like a chatbot remembering the immediate back-and-forth).
Long-Term Memory (LTM)	Information persistently stored for extended periods, across different sessions or tasks.	Allows for learning and personalization, enabling the agent to recall specific events, facts, and procedures over time.

Long-Term Memory can be further refined:

- **Episodic Memory:** Stores specific past events, interactions, or sequences of actions.
- **Semantic Memory:** Stores general knowledge, facts, concepts, and rules (a knowledge base).
- **Procedural Memory:** Stores learned skills, procedures, and "how-to" knowledge for automating tasks

What are its tools?

Tools (or Functions) are external functions, APIs, or software systems that an AI agent can call upon to interact with the real world or a digital environment, extending its capabilities beyond simple language generation.

The LLM acts as the reasoning engine to decide *when* and *how* to use the available tools to achieve its goal.

Common types of tools include:

- **Data Retrieval Tools:** Searching the web, querying databases, reading documents (PDFs, spreadsheets).
- **Action/Interaction Tools:** Sending emails, updating a CRM record, calling an external API to book a flight, or controlling hardware (in the case of a robot).

- **Code Interpreter Tools:** Executing code (like Python) for complex calculations, data analysis, or dynamic processing.
- **Orchestration Tools:** Allowing one AI agent to call or coordinate the actions of other agents.

What is Agentic AI?

Agentic AI is a term that describes the broader advanced form of artificial intelligence focused on **autonomous decision-making and action**. It is the paradigm or architecture built around the concepts of agency.

- **Relationship to AI Agents:** AI agents are the **building blocks** or autonomous entities that form the foundation of an Agentic AI system.
- **Focus:** Agentic AI focuses on the orchestration and coordinated use of one or more AI agents to handle complex, multi-step workflows with minimal human oversight, working towards high-level goals.
- **Goal:** To create proactive, adaptive systems that can "think" (reason, plan, reflect) and "do" (execute actions via tools) in a human-like, goal-driven manner.