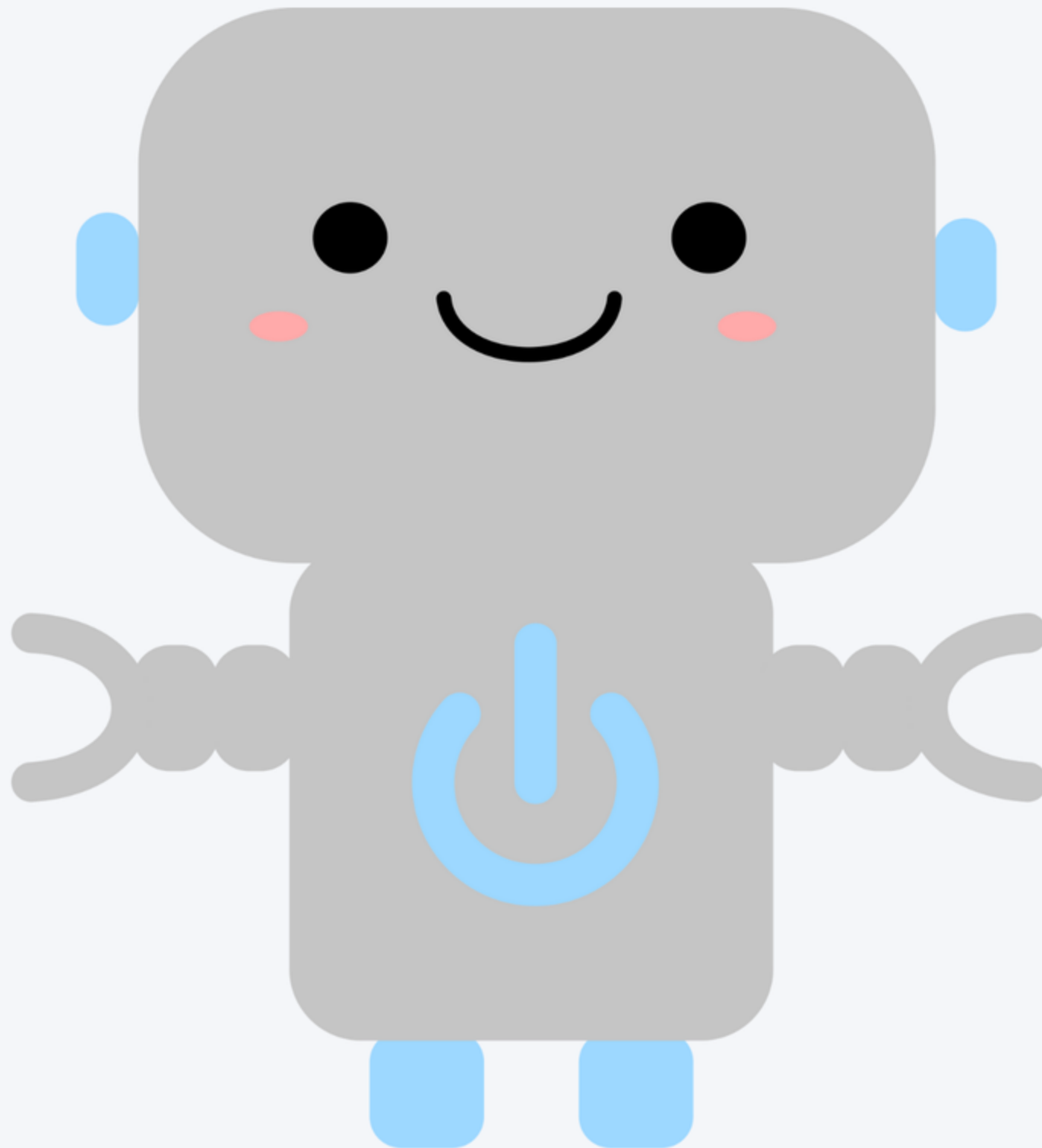


Tools and Tool Calling in Agentic AI



Shoaib Akthar
@datawithshoaib

Data Science | AI | ML | Python



What Are Tools in Agentic AI?

- Tools are external capabilities that an AI agent can use to perform tasks beyond generating text.
- Examples include web search, calculators, databases, APIs, code execution, and file systems.
- Tools allow an AI agent to interact with the outside world instead of only producing responses.
- An LLM can reason about a task, but tools give it the ability to retrieve information or perform actions.
- This transforms AI from a question-answering system into a task-performing system.



Why Do AI Agents Need Tools?

- LLMs have limitations: their knowledge may be outdated and they cannot directly access every external system.
- They may also struggle with precise calculations, large datasets, and real-time information.
- Tools solve these limitations by giving agents access to specialized capabilities.
- A financial agent can query market data, while a coding agent can execute code and inspect the output.
- The LLM provides the intelligence, while tools provide the capabilities.



What Is Tool Calling?

- Tool calling is the mechanism that allows an AI model to request the use of a specific tool.
- The model doesn't directly execute the tool; it generates a structured request describing what the application should do.
- The application receives the request, executes the tool, and sends the result back to the model.
- The model then uses the result to continue solving the task.
- The basic loop is: Think → Call Tool → Observe → Think Again → Act.



How Tool Calling Actually Works

- Developers first provide the AI model with available tools and their input schemas.
- The user gives the agent a task that may require one or more tools.
- The model decides whether a tool is necessary and selects the appropriate one.
- The application executes the tool using the arguments generated by the model.
- The tool's output is returned to the model, which uses it to produce the final response or make another tool call.



One Agent Can Use Multiple Tools

- Real-world tasks rarely require only one capability.
- An AI agent might use a web search tool to find information, a database tool to retrieve internal data, and a calculator to analyze the results.
- It can decide which tool to use based on what it needs at each step.
- Tools can also be called multiple times during a single task.
- Combining multiple tools allows agents to solve complex, multi-step workflows.



Tool Calling vs Function Calling

- Function calling is a common mechanism through which AI models interact with external functions.
- Tool calling is the broader concept of allowing a model to interact with different external capabilities.
- A function might retrieve customer information, while another tool could search the web or execute code.
- The terminology differs across AI frameworks and platforms.
- The underlying idea remains the same: the model decides what capability it needs and provides structured arguments to use it.



What Makes a Good Agent Tool?

- A good tool should have a clear purpose and a well-defined input/output structure.
- Tool descriptions should be specific enough for the model to understand when and how to use them.
- Inputs should be validated because the model can generate incorrect or unexpected arguments.
- Tools should return useful, structured results instead of unnecessary information.
- Good tools are designed around real tasks rather than simply exposing every possible API.



Tools Are the Hands of an AI Agent

- An LLM can reason, plan, and decide, but without tools its ability to interact with the real world is limited.
- Tools give agents access to data, computation, software systems, and real-world actions.
- Tool calling provides the connection between the model's reasoning and those external capabilities.
- As agents become more autonomous, the number and variety of tools they can safely use will continue to grow.
- The future of Agentic AI isn't just about smarter models; it's about smarter models connected to the right tools.





Shoaib Akthar

Data Scientist

I share things on Data & AI
follow if you wanna see more!