AI: From Foundation to Frontier

A strategic overview of the modern AI landscape, its tools, and its potential.

Our Agenda, and a Critical First Step

The Journey

1. **The Landscape**
   Defining Our Terms

2. **The Cambrian Explosion**
   The Rise of Capable AI

3. **Mastering the Tools**
   From Theory to Practice

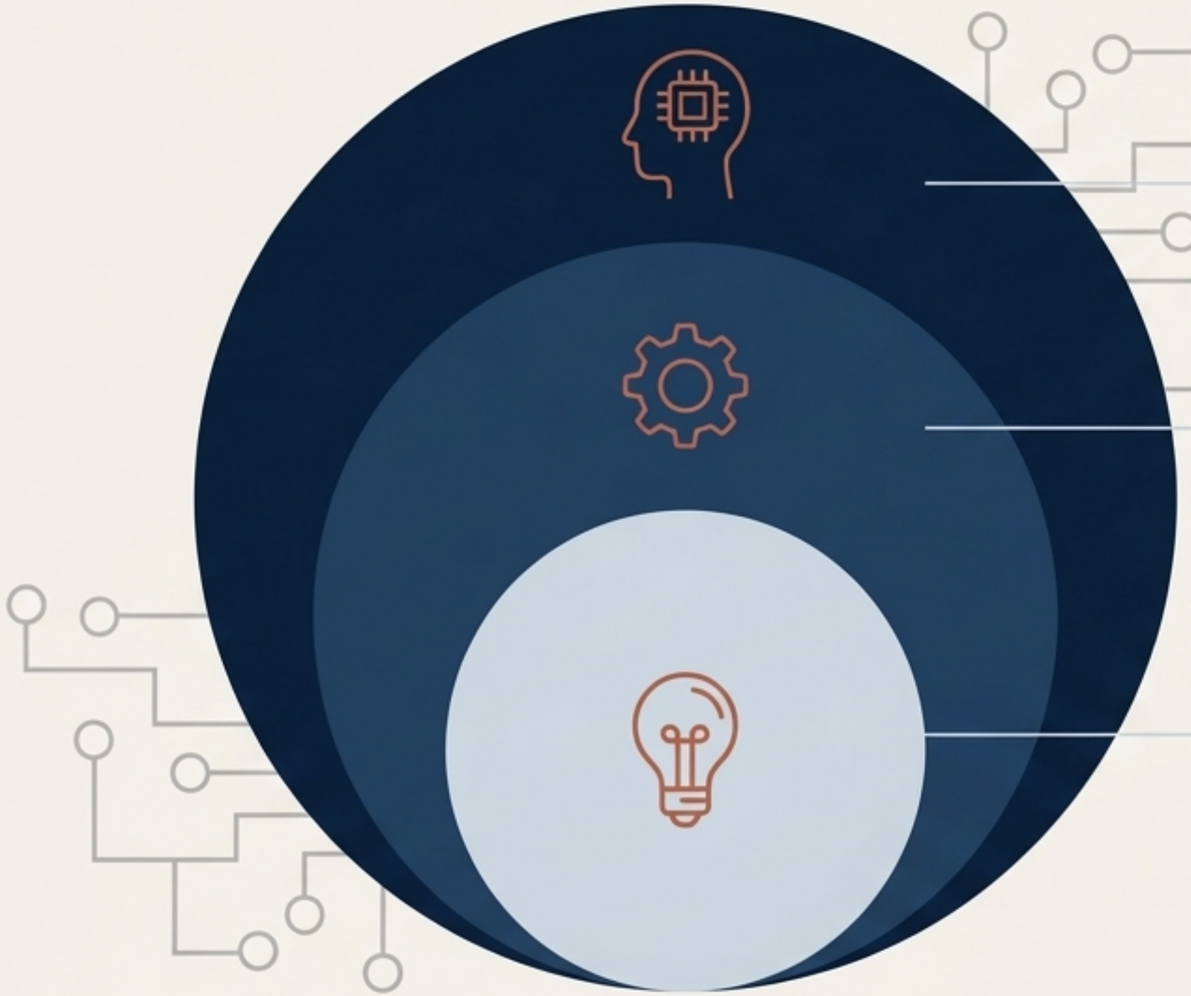
4. **The New Horizon**
   Impact & Outlook

Email Guidelines for Data Privacy

- ✓ Do not use personal or finance-linked email IDs when testing or evaluating AI tools.
- ✓ Create a separate, dedicated email account specifically for learning, testing, and development purposes.

This practice safeguards sensitive information and ensures a clean separation between personal data and experimental workflows.

The Landscape: Defining the Core Concepts



Artificial Intelligence (AI)

The broad concept of machines that can think, learn, and make decisions like humans. They perform tasks similar to human intelligence, such as pattern recognition and image analysis.

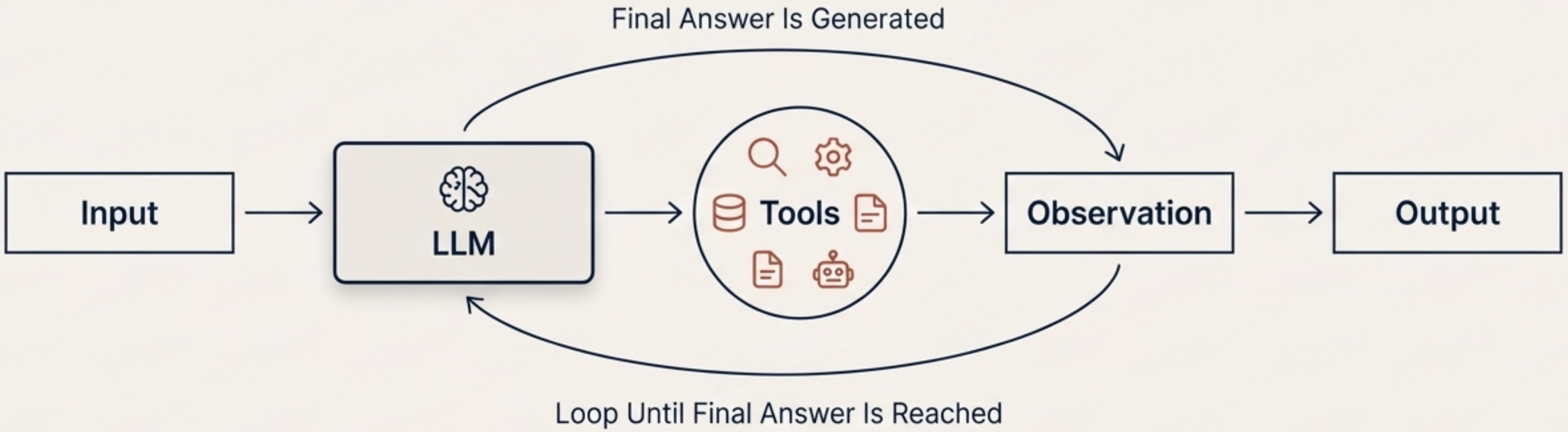
Machine Learning (ML)

A sub-domain of AI. It teaches computers to learn patterns from data and make predictions.

Deep Learning (DL)

A sub-domain of ML. It uses neural networks to learn from vast amounts of unstructured data like images and audio.

The Engine of Modern AI: The Large Language Model (LLM)



What is an LLM?

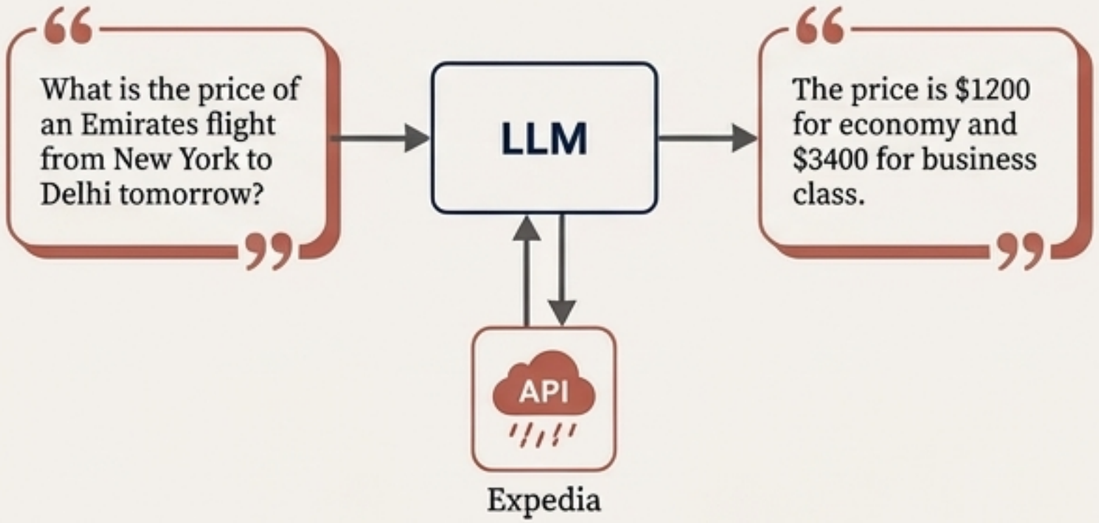
- An LLM is a type of artificial intelligence trained on vast amounts of text data to understand, process, and generate human-like text.
- It uses a transformer architecture to learn language patterns and context.
- **Scale in Perspective:** The raw dataset for ChatGPT-3 was 45TB, and the model has approximately 1.75 trillion parameters.

The Cambrian Explosion: A New Taxonomy of AI Systems

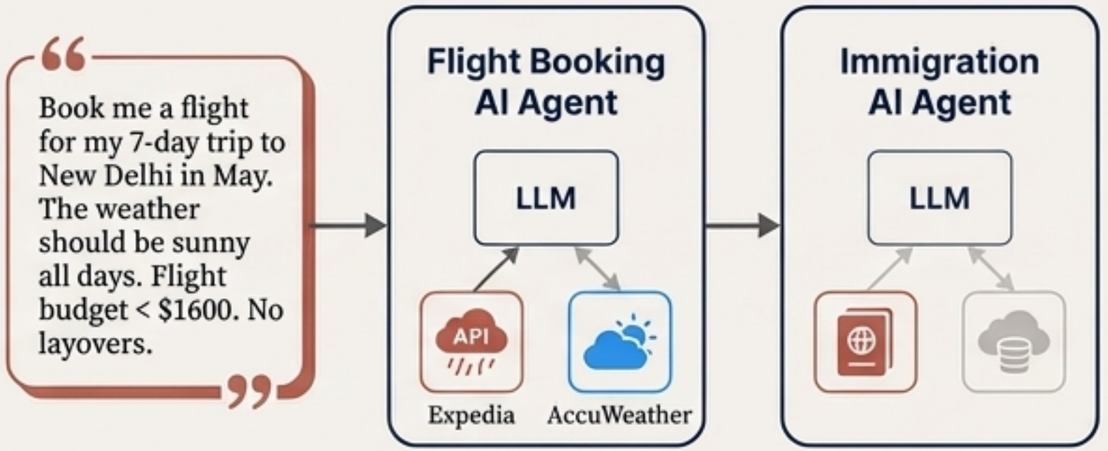
Characteristic	Generative AI (LLM Only)	AI Agent	Agentic AI
Task Capability	Answers based on pre-trained knowledge only (e.g., ChatGPT, Gemini).	Completes a task using tools, memory, and data APIs based on user input.	Handles multi-step problems with planning, co-ordination, and autonomy.
Tool Usage	No external tools.	Uses a specific set of tools to complete a single task.	Uses multiple tools and can call other AI agents to achieve a goal.
Decision Making	No decision-making ability.	Makes decisions to complete a defined task.	Plans, makes decisions, and operates autonomously.

From Simple Answers to Complex Actions: AI Agents at Work

Simple LLM Query

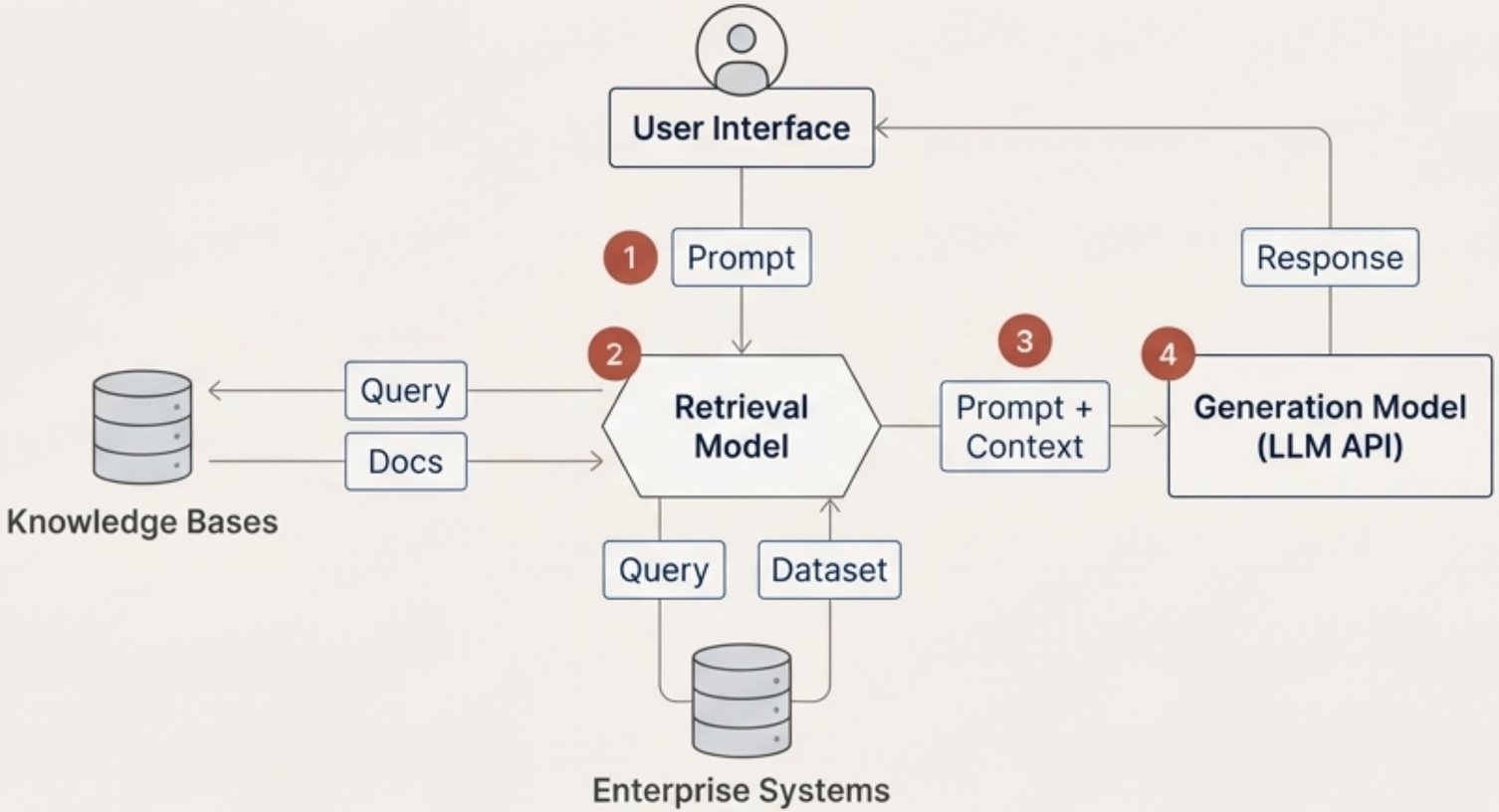


Complex AI Agent Task



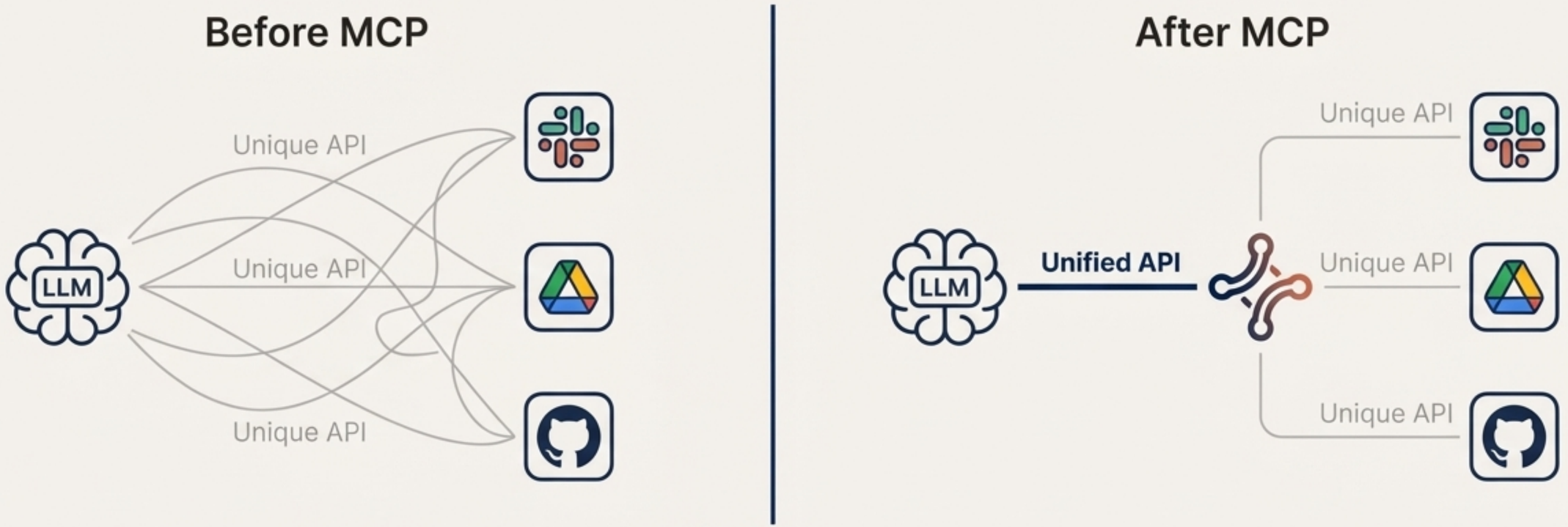
Agent Action: The agent synthesises constraints, queries multiple tools, and executes a multi-step booking process.

Grounding AI in Reality: Retrieval-Augmented Generation (RAG)



- RAG is an AI framework that improves LLM output by giving it access to external, private, or up-to-date knowledge bases ***before*** **generating a response.**
- It solves the problem of static knowledge and allows LLMs to use company-specific or real-time data.
- **Function:** Turns a simple text input into an improved, contextually-aware text output.

The Universal Connector: Model Context Protocol (MCP)

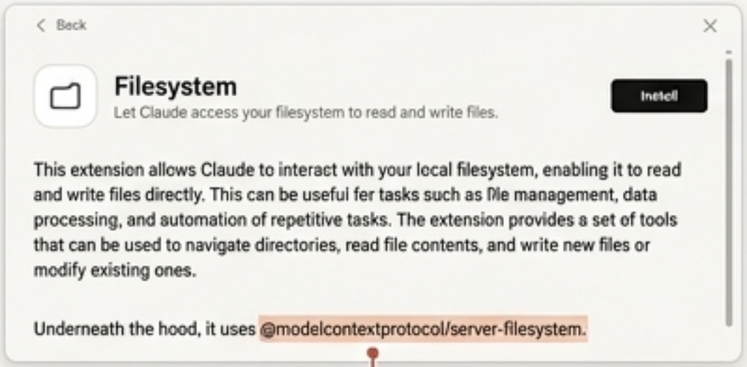


- MCP is an open-source framework that allows LLMs to interact with external data sources, APIs, applications, and databases in a secure and standardised way.
- While RAG focuses on retrieving data to enrich context, MCP provides the protocol for the AI to *act* on that context using tools.
- When combined, RAG and MCP create a powerful system for both knowledge retrieval and action.

Case Study: MCP in the Wild with Claude AI

1

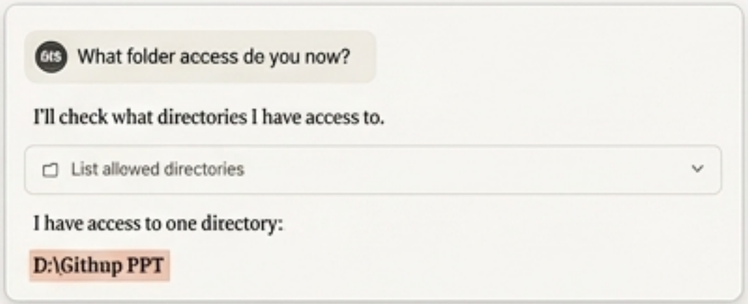
1. Installation



Underneath the hood, it uses @modelcontextprotocol/server-filesystem

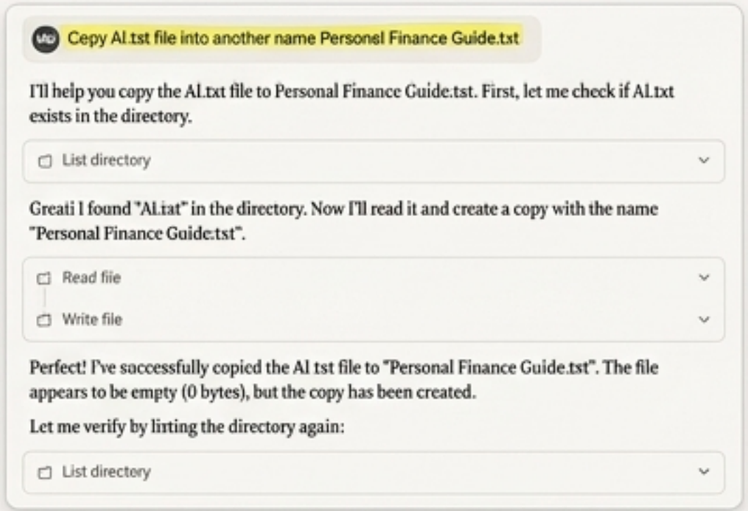
2

2. Permission Granted



3

3. Taking Action



This demonstrates an AI agent using a standardised protocol to securely read and write files on a local machine, a powerful example of agency.

The Art of the Ask: An Introduction to Prompt Engineering

The quality of the AI's output is directly proportional to the quality of your input.

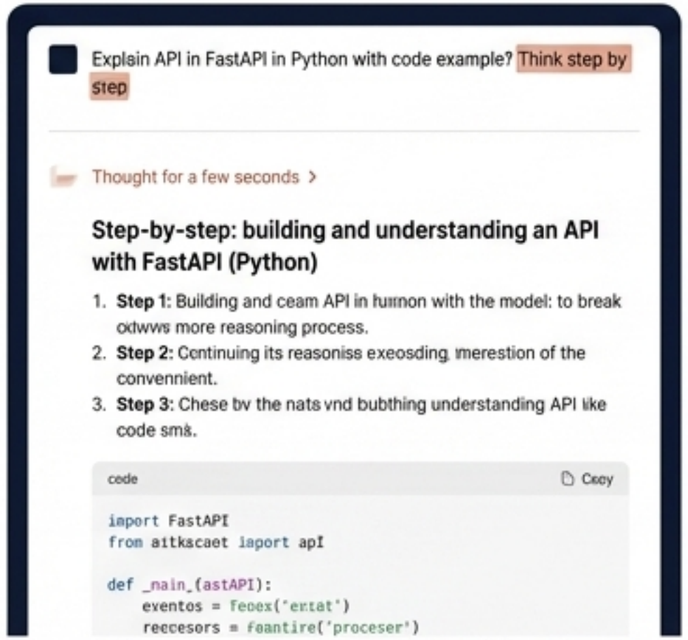
Anatomy of an Improved Prompt

- **Instructions**: The specific task you want the AI to perform. (e.g., "Explain...")
- **Context**: Background information that provides clarity and scope. (e.g., "...to a Junior cloud engineer...")
- **Input**: The data or question the AI should work with. (e.g., "...the concept of an "EC2 Setup"...")
- **Output**: The desired format for the response. (e.g., "...using a real-world analogy.")

Advanced Prompting Techniques for Superior Results

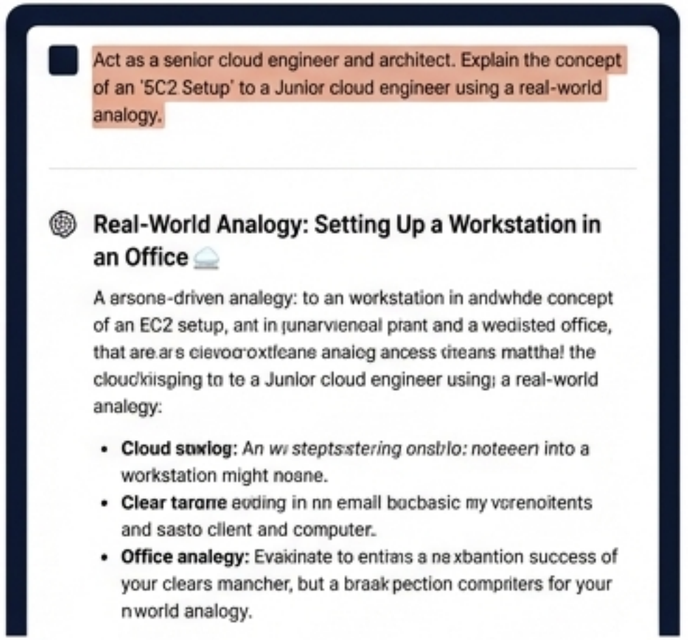
Chain of Thought

Adding “Think step-by-step” encourages the model to break down problems and show its reasoning, leading to more accurate results.



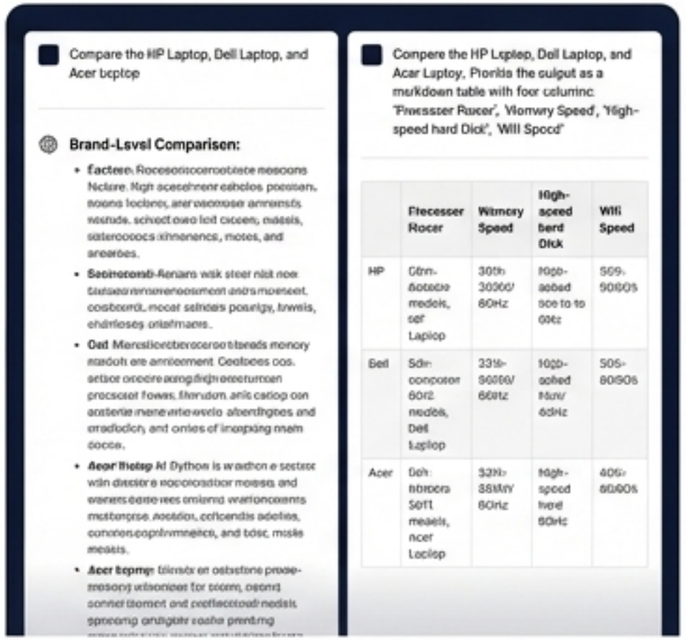
Role-Playing

Instructing the AI to ‘Act as a...’ primes it with a specific context, persona, and knowledge level, tailoring the tone and content of the response.



Structured Output

Explicitly defining the output format (e.g., markdown table, JSON, list) ensures the response is well-organised and ready for use.

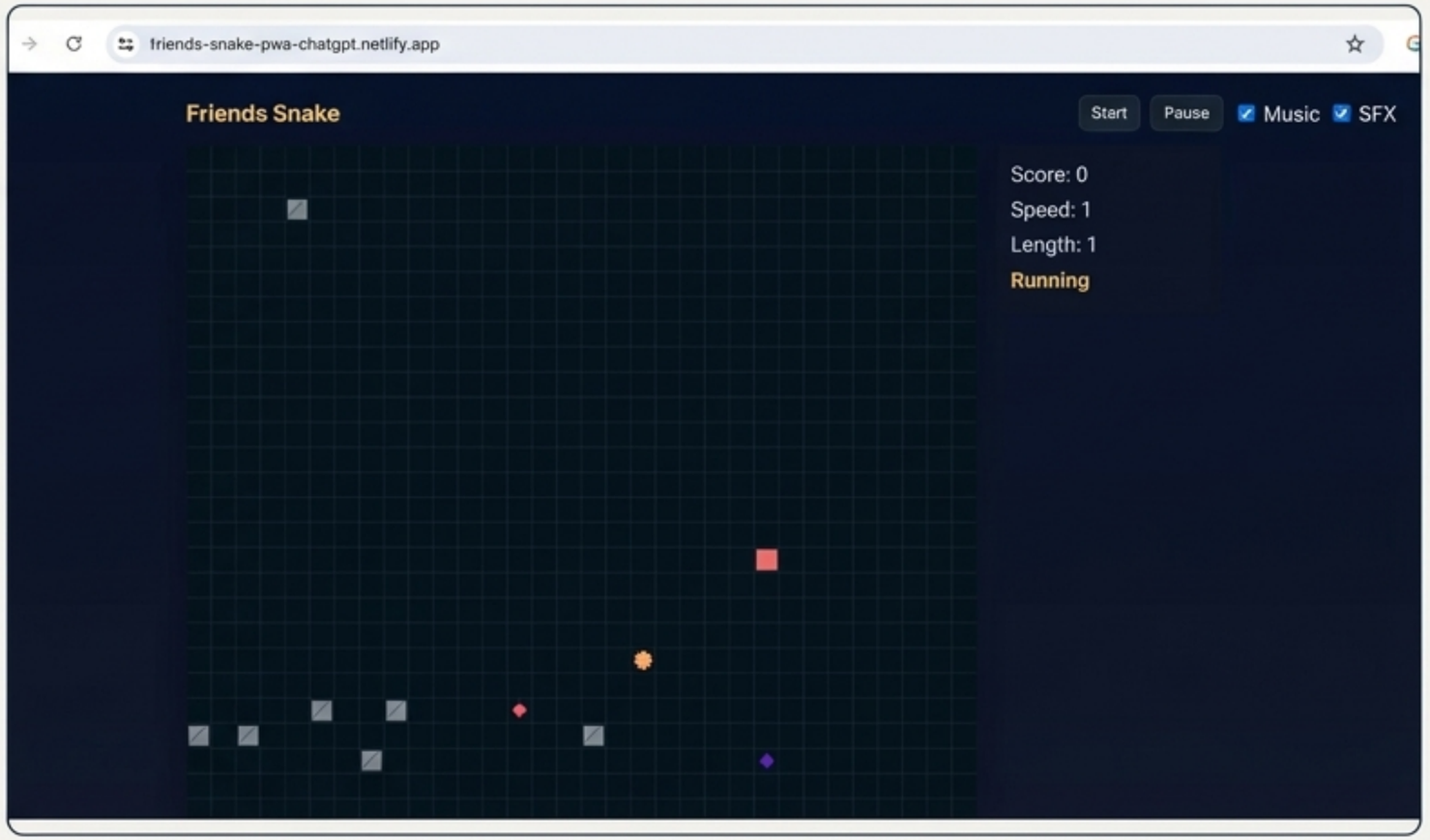


From a Single Prompt to a Finished Product

Create a friends-themed snake game with background music, obstacles, power-ups, and speed boosts. Make it ready to deploy PWA (Manifest, Service worker, icons) and give me a zip with all the assets included.

Here's your ready-to-deploy PWA package:

👉 Download friends-snake-pwa.zip



A single prompt generated a complete, deployable Progressive Web App, including all necessary HTML, JS, CSS, and assets.

The New Horizon: AI as a Tool to Get the Job Done Better

AI is a powerful force multiplier, augmenting professional capabilities rather than replacing them.

Programmer Productivity

Testers Productivity

UI Programming Productivity

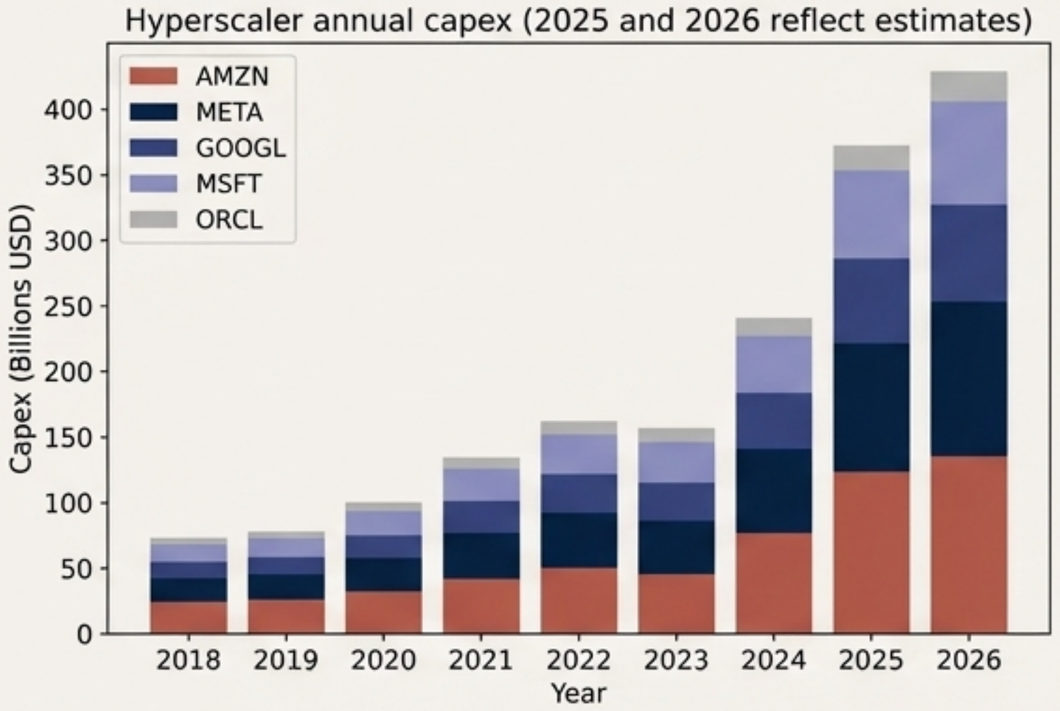
SQL Query Conversion Productivity

...etc.

Investment vs. Reality: A Balanced Perspective

The Investment Boom

Hyperscalers' annual capex has more than doubled since ChatGPT's release.



Exponential View. Source: Citi Research

A Dose of Scepticism

Is the AI Bubble About to Burst?

- **Derek Thompson:** Analysis suggests that the current investment cycle may be unsustainable without clearer ROI.
- **MIT Report:** Cites a high failure rate for generative AI pilots within companies, suggesting a gap between experimentation and successful implementation.

https://www.theatlantic.com/technology/archive/2023/11/ai-bubble-investment-derek-thompson/675992/;
https://sloanreview.mit.edu/article/why-companies-are-struggling-to-adopt-generative-ai/

Your Journey Continues

Blogs & Repositories

Blogger: https://mohan4295.blogspot.com/

GitHub: https://github.com/mohan4295work

GitLab: https://gitlab.com/mohan4295work

Essential AI Tools

- ChatGPT: https://chatgpt.com/
- Claude: https://claude.ai/
- Gemini: https://gemini.google.com/
- DeepSeek: https://chat.deepseek.com/

Key Reference Links

- AI Prompt Engineering: https://youtu.be/n0VpK1RfYGA
- Generative AI vs AI agents vs Agentic AI: https://youtu.be/O2gerCxEXvc
- Is the AI Bubble About to Burst?: https://youtu.be/OJKPrJ0wNvc