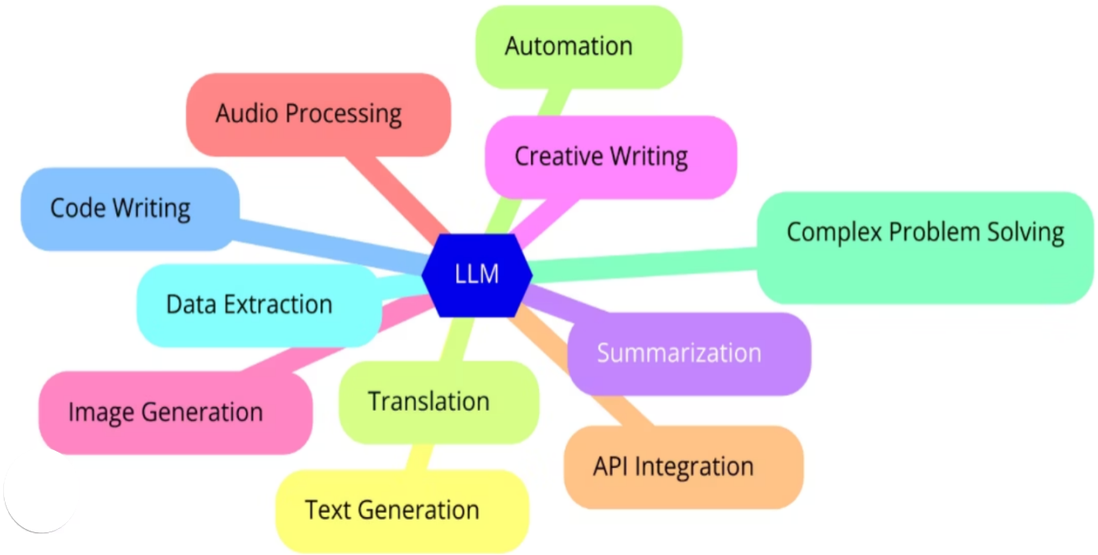
Evolution of Large Language Models

Exploring the technological journey from simple text prediction to sophisticated AI reasoning systems and the emergence of Model Context Protocol (MCP) as the next frontier.

LLM - Capabilities, Limitations, Path to MCP

Core Functions of LLMs



Early LLMs had significant functional constraints, limiting their real-world utility.

Early Limitations

First versions of ChatGPT-3 couldn't perform basic actions like sending emails on user's behalf.

MCP Significance

Understanding these limitations reveals why Model Context Protocol represents the next evolutionary leap for LLMs.

RAG - Retrieval Augmented Generation

Query Processing

System analyzes what information is needed from the user query

Information Retrieval

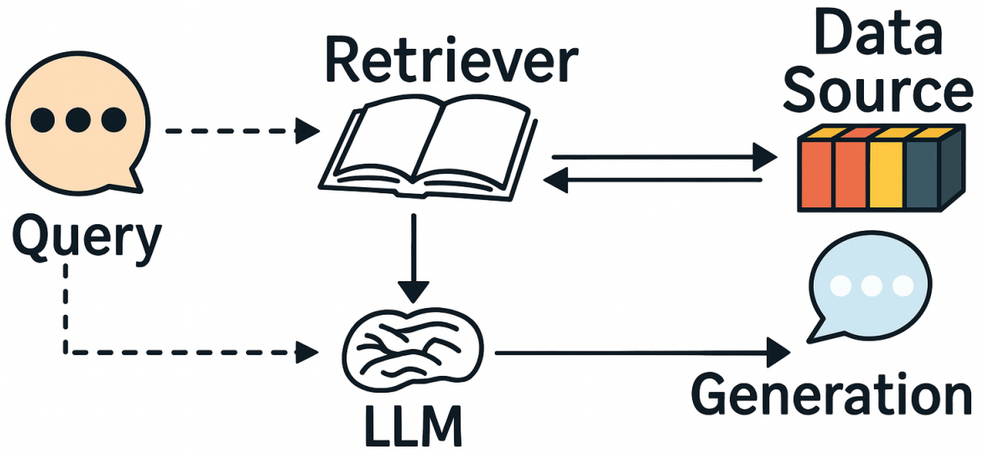
Search through databases, documents or knowledge bases

Context Integration

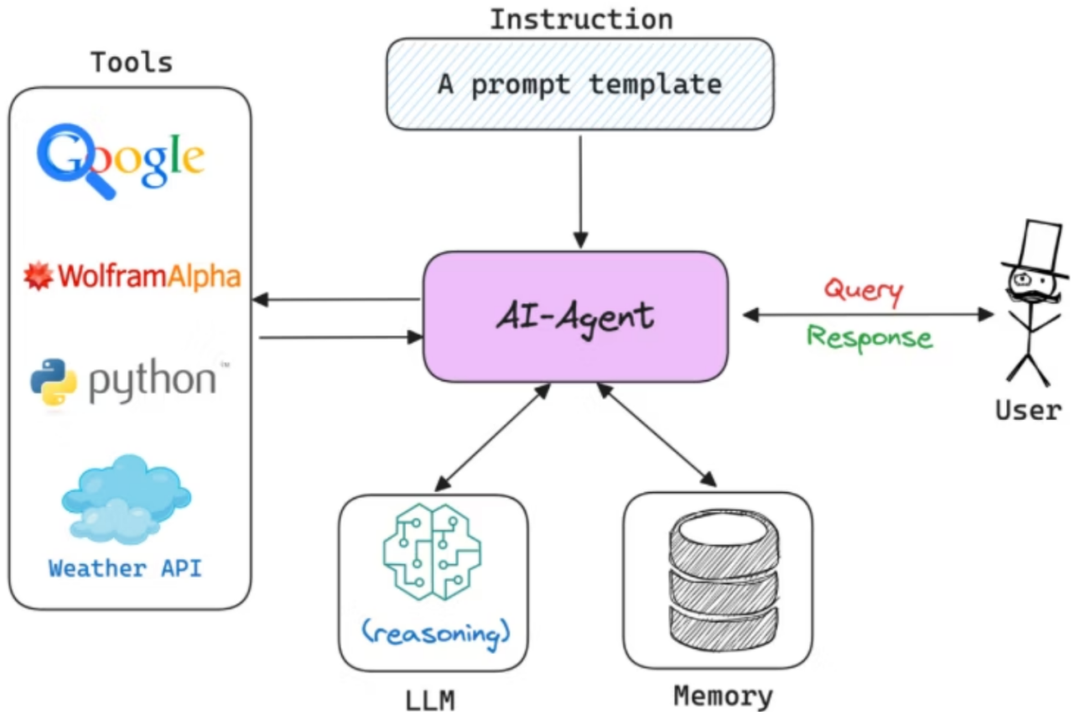
Retrieved information is fed to LLM as additional context

Enhanced Response

LLM generates more accurate, knowledge-grounded responses



AI Agents: Extending LLM Capabilities



AI Agents Defined

Systems that combine LLMs with external tools to perform complex tasks autonomously

Tool Categories

- External API tools
- Code execution engines
- Information retrieval systems
- DevOps infrastructure tools

Tools Integration and Challenges

1

Real-World Examples

Modern AI systems like Perplexity effectively demonstrate the evolution of LLMs with integrated tools for real-time information access.

2

The Complexity Challenge

While individual tool integrations work well, building comprehensive AI assistants becomes exponentially complex with each new capability.

3

Scaling Problems

Current approaches require custom integration for each tool, creating maintenance burden and inconsistent user experiences.

MCP - Model Context Protocol

The Next Evolution in LLM Architecture

A standardized approach for connecting LLMs to the external world

Foundation for MCP : Client-Server Architecture

Client

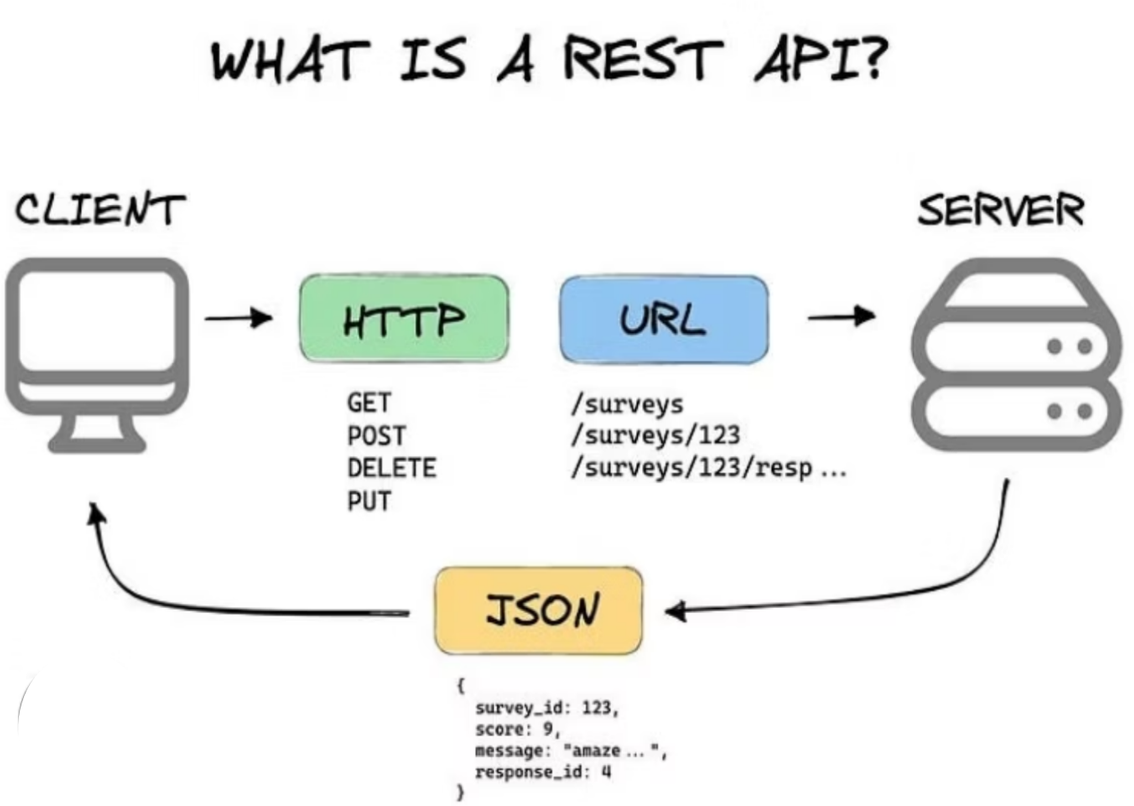
Any computer, application, or device that requests services or resources from a server.

Server

Powerful computer or software system that provides services and resources to clients upon request.

Communication

Standardized protocols enable reliable data exchange between client and server components.



REST API and LLM Limitations

REST API Standards

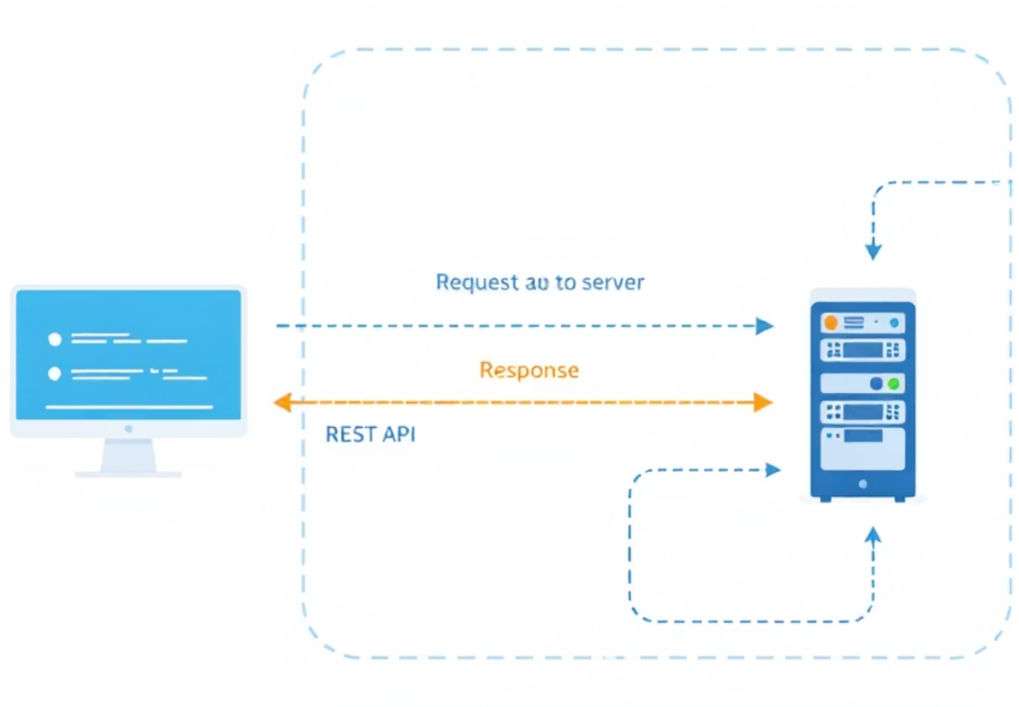
- Representational State Transfer (REST)
- Stateless request/response model
- Resource-oriented architecture
- Uses HTTP methods (GET, POST, PUT, DELETE)
- Returns structured data (JSON, XML)

Why Standards Matter

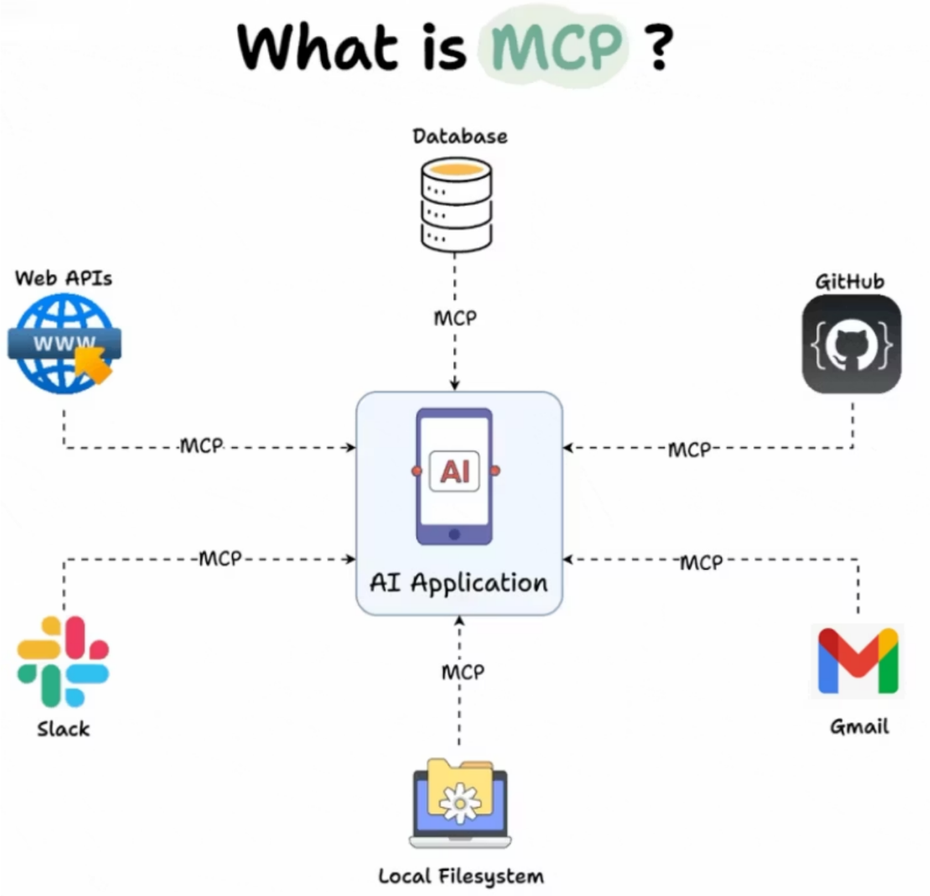
REST APIs provide a standardized way for software systems to communicate, enabling:

- Interoperability between diverse systems
- Predictable behavior and documentation
- Scalable, maintainable integrations

Engineering Principle:
Software engineering relies on standards and established protocols to create reliable, maintainable systems.



MCP - Model Context Protocol



Key Components

AI Application

Core AI at center of the architecture, handling user interactions and coordinating with external services

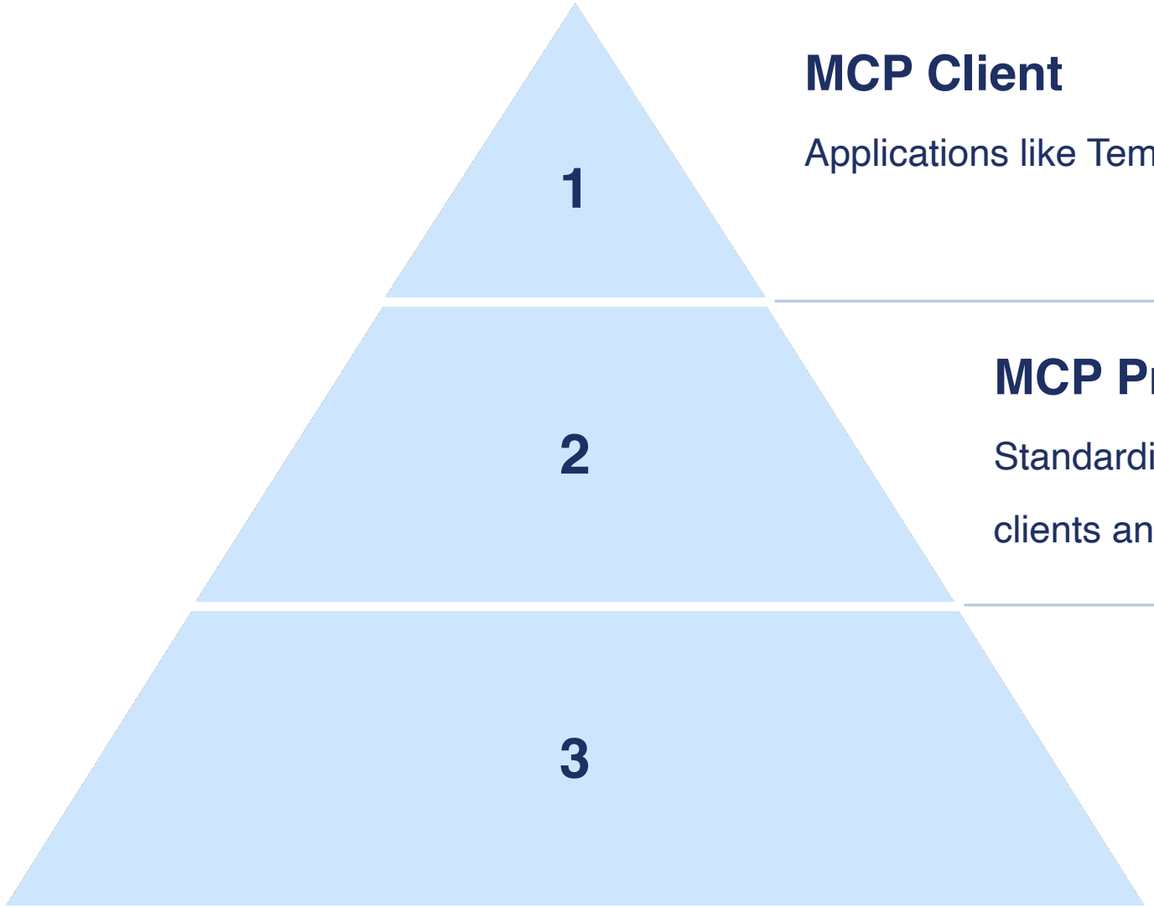
External Services

Specialized tools including databases, web APIs, GitHub repositories, and other functional systems

Standardized Protocol

Common language allowing LLMs to discover, understand, and utilize external capabilities consistently

MCP - Architecture Components



MCP Client

Applications like Tempo, WindSurf, and FirstServe serving as the LLM-facing interface

MCP Protocol

Standardized communication layer enabling two-way connections between clients and servers

MCP Server

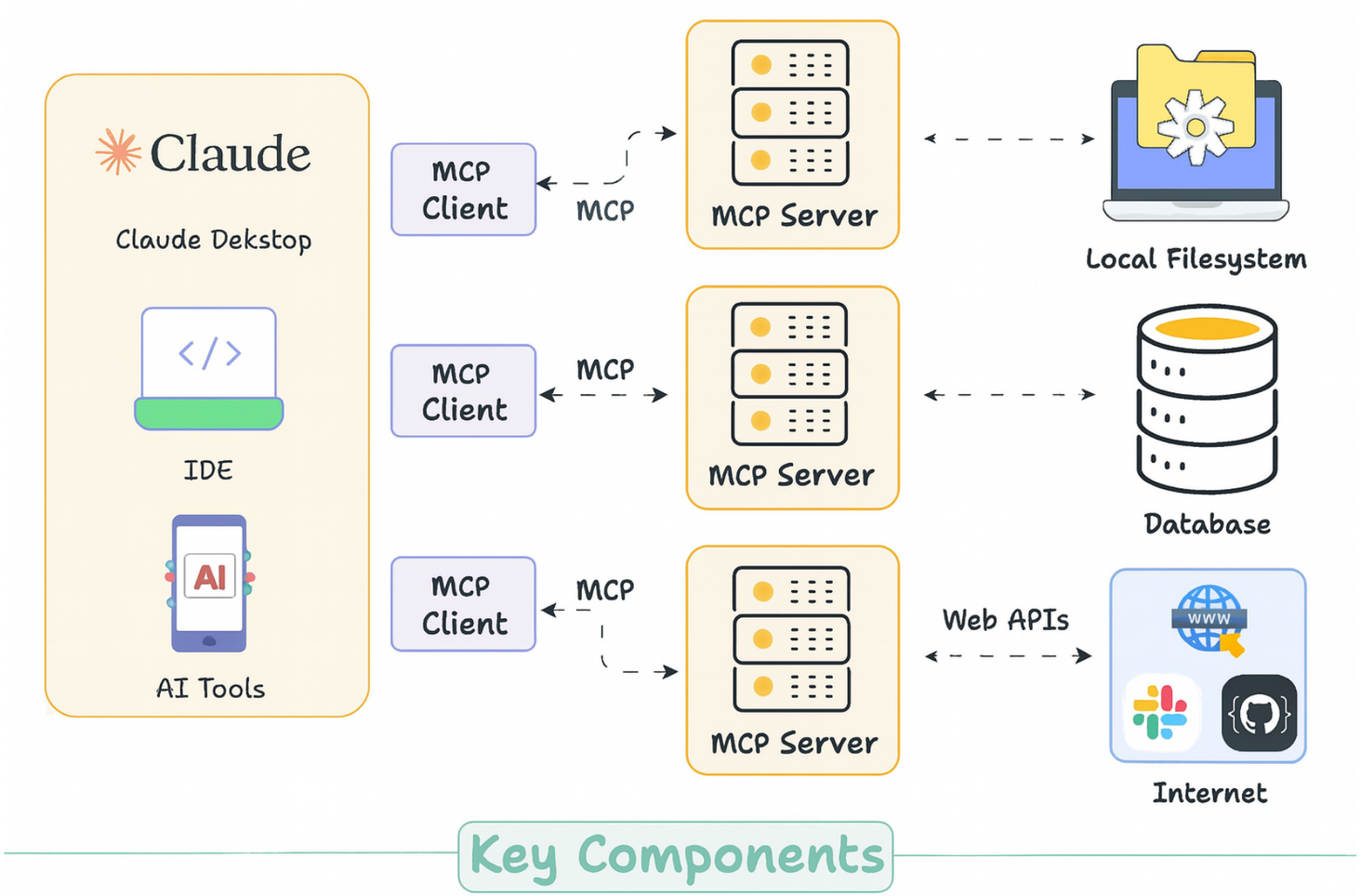
Component translating external services and capabilities into a format the client can understand

MCP creates a standardized ecosystem that enables LLMs to interact with external services through a unified interface

MCP - Complete Architecture

The Model Context Protocol creates a standardized ecosystem that enables LLMs to discover and utilize external capabilities consistently across different implementations.

Benefits: MCP eliminates the need for custom integrations between each LLM and external service, significantly reducing complexity while improving scalability and innovation.



MCP - Communication

MCP Client

The Host Application integrating with host Client Layer that manages communication between host and communication protocol.

MCP Transport

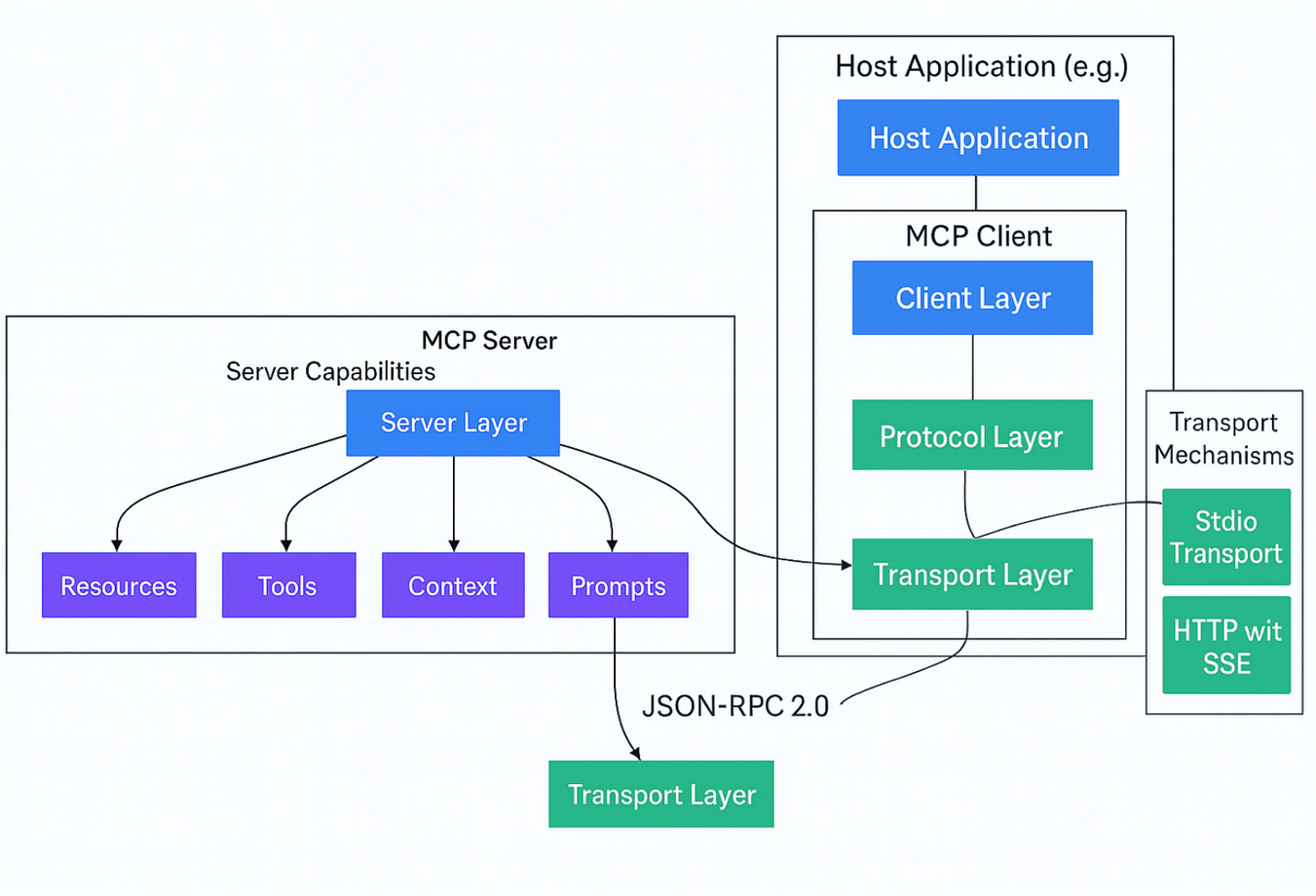
Interfaces with the client via supported transport mechanisms (like HTTP or Stdio).

MCP Server

MCP Server acts as the resource provider, with capabilities that include Resources, Tools, Context,Prompts

Protocol Layer

Responsible for structuring the communication using JSON-RPC 2.0.



MCP - Server Components

Tools

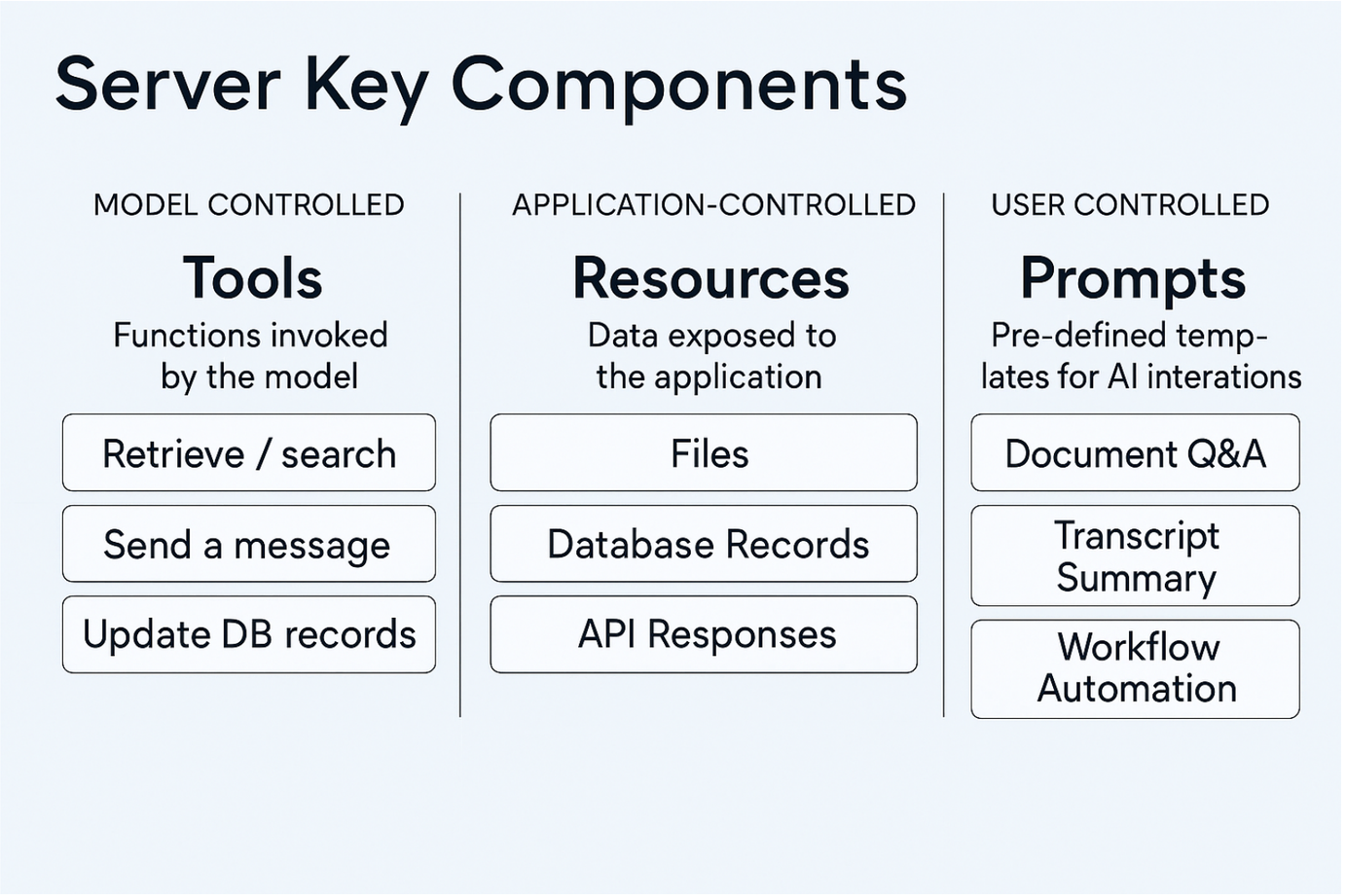
Model-controlled functions that enable the AI to take actions like retrieving data, sending messages, or updating database records

Resources

User-controlled templates that standardize AI interactions for specific use cases like document Q&A, transcript summaries, and workflow automation.

Prompts

MCP Server acts as the resource provider, with capabilities that include Resources, Tools, Context,Prompts



MCP - Transport Types

Stdio Transport

Local Transport

- Uses standard input/output streams
- Ideal for local process communication
- Used in commard-line tools and integrations
- Limited to same-machine

HTTP with SSE

Original Remote Transport

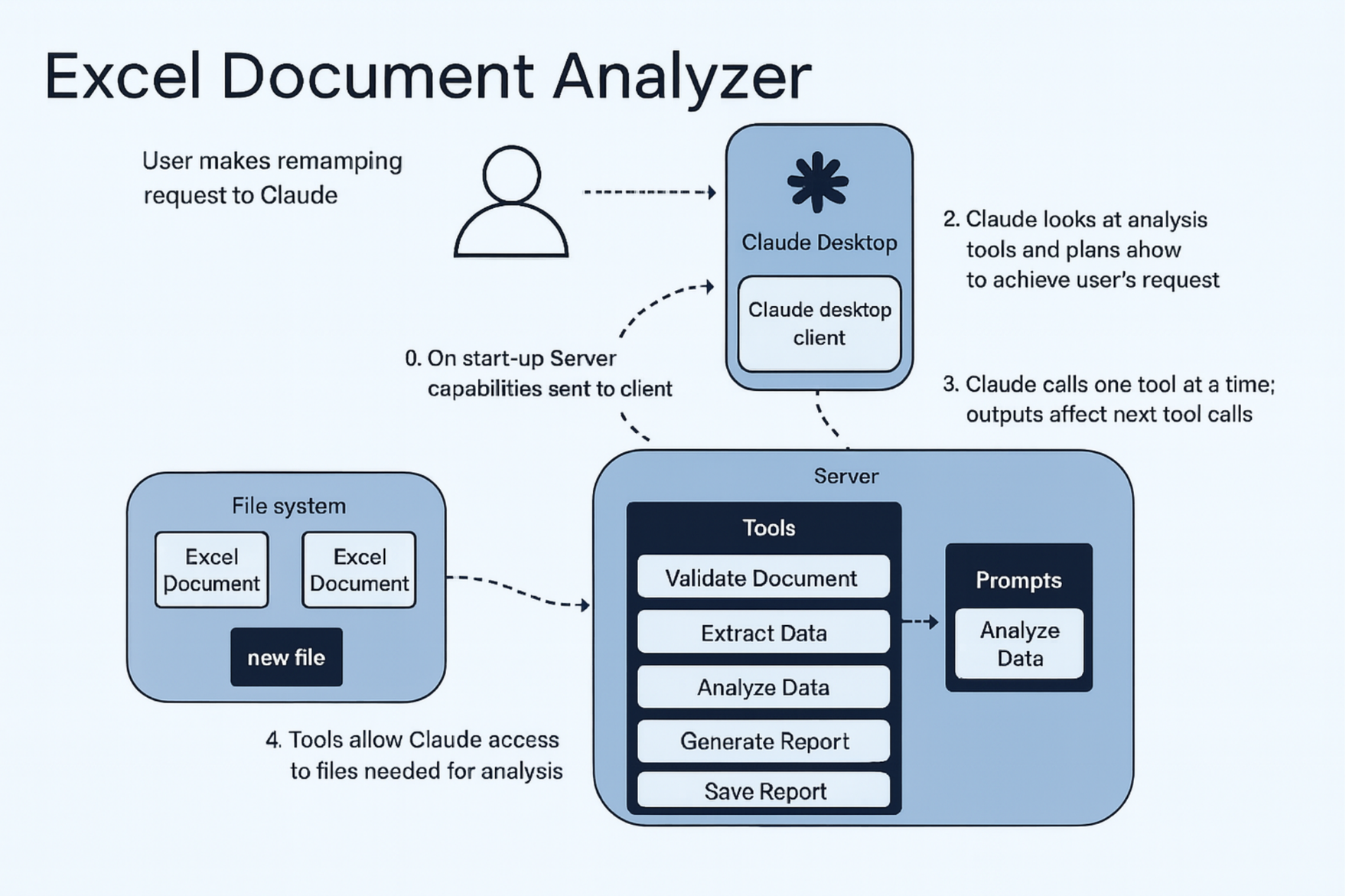
- Server-Sent Events for server→client streaming
- HTTP POST for client→server messages
- Enabled remote MCP servers
- Requires maintaining constant connection state

Streamable HTTP

Released March 2025

- Enables stateless server architecture
- No requirementryer long-term connections
- More flexiple for cloud and serveriess deployment
- Ideal for modern web architecture

MCP - Flow


Excel Document Analyzer
User makes remamping request to Claude
Claude Desktop
Claude desktop client
2. Claude looks at analysis tools and plans ahow to achieve user's request
0. On start-up Server capabilities sent to client
3. Claude calls one tool at a time; outputs affect next tool calls
Server
File system
Excel Document
Excel Document
new file
Tools
Validate Document
Extract Data
Analyze Data
Generate Report
Save Report
Prompts
Analyze Data
4. Tools allow Claude access to files needed for analysis