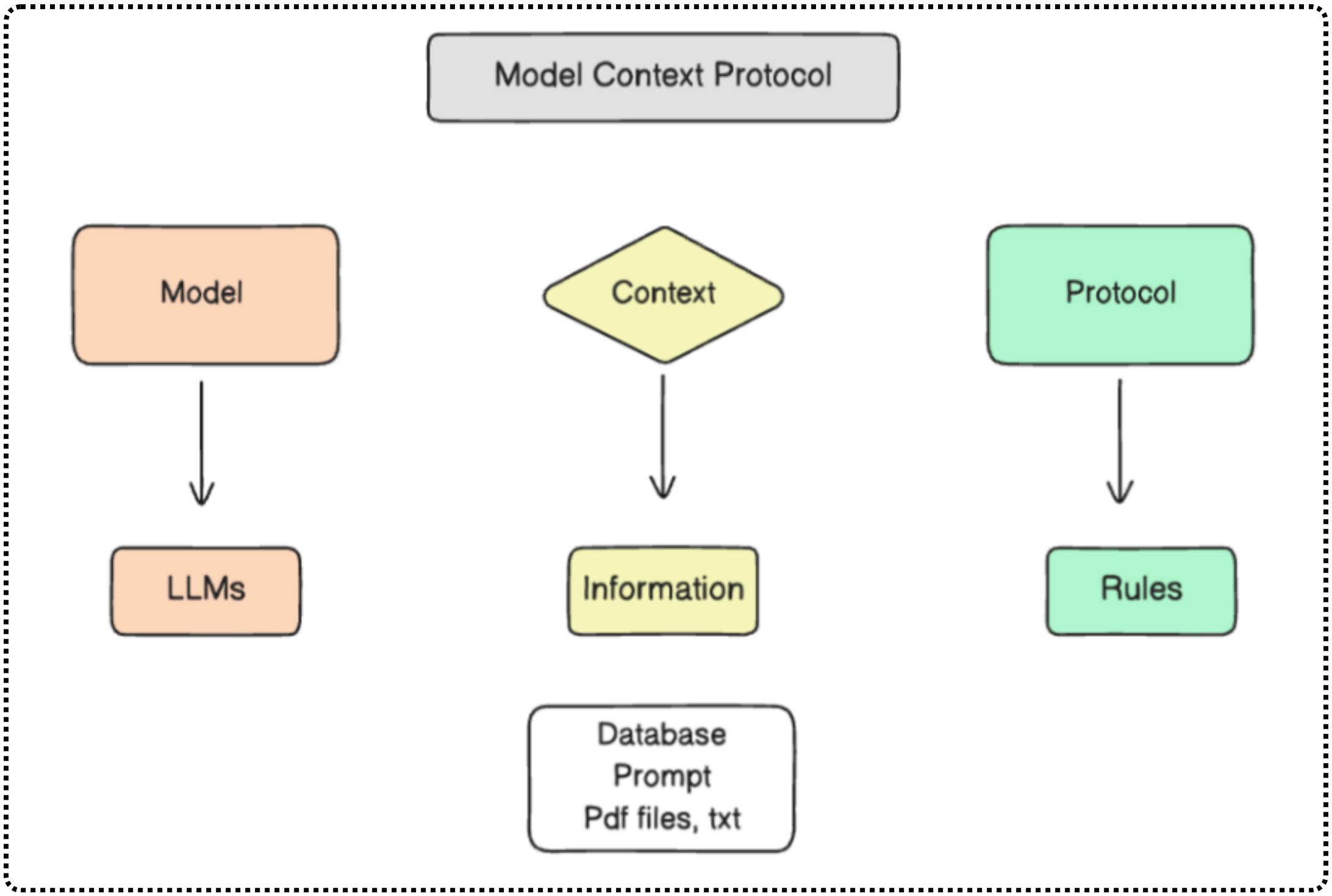
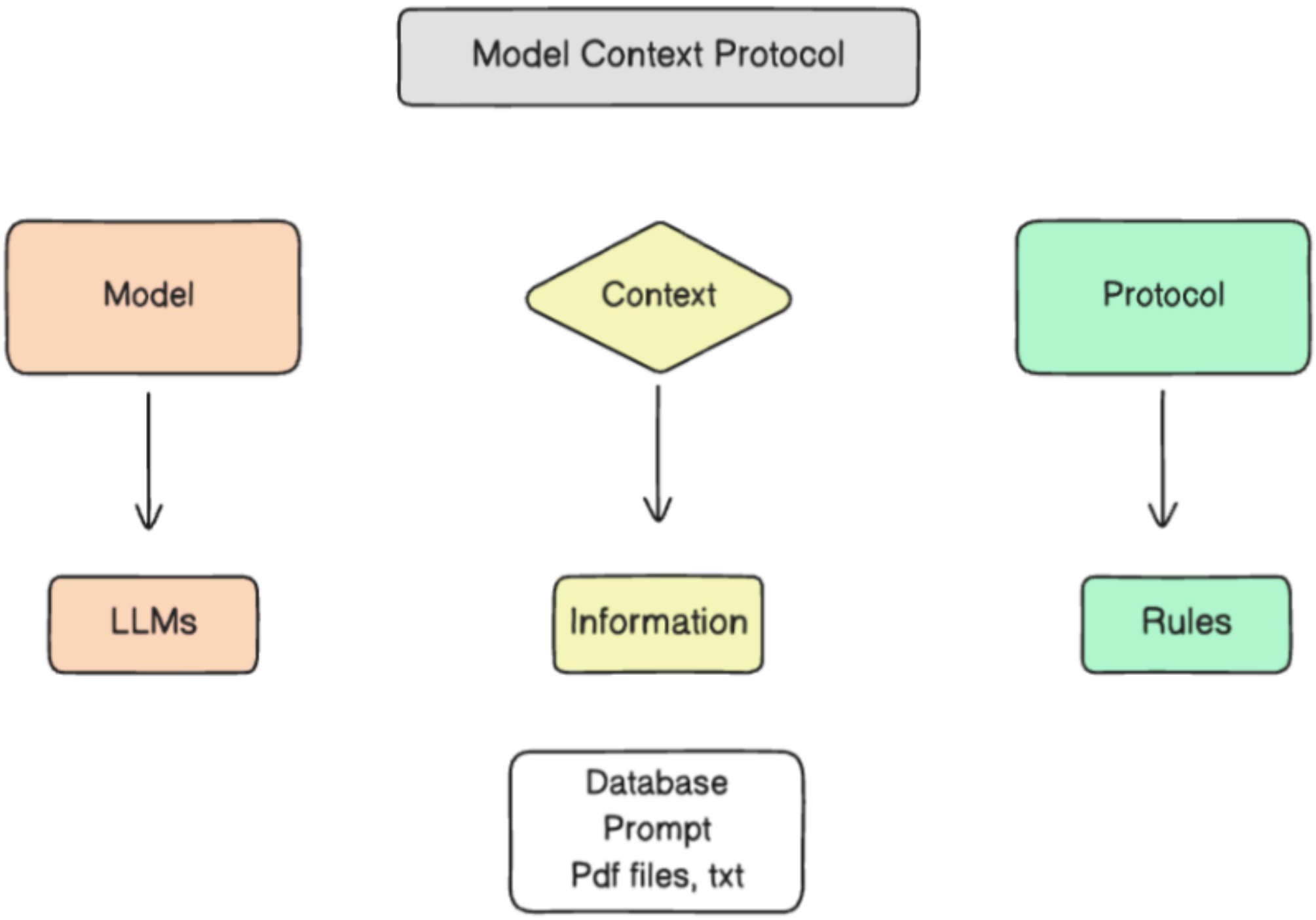
Analytics Vidhya

A Guide to Model Context Protocol(MCP)



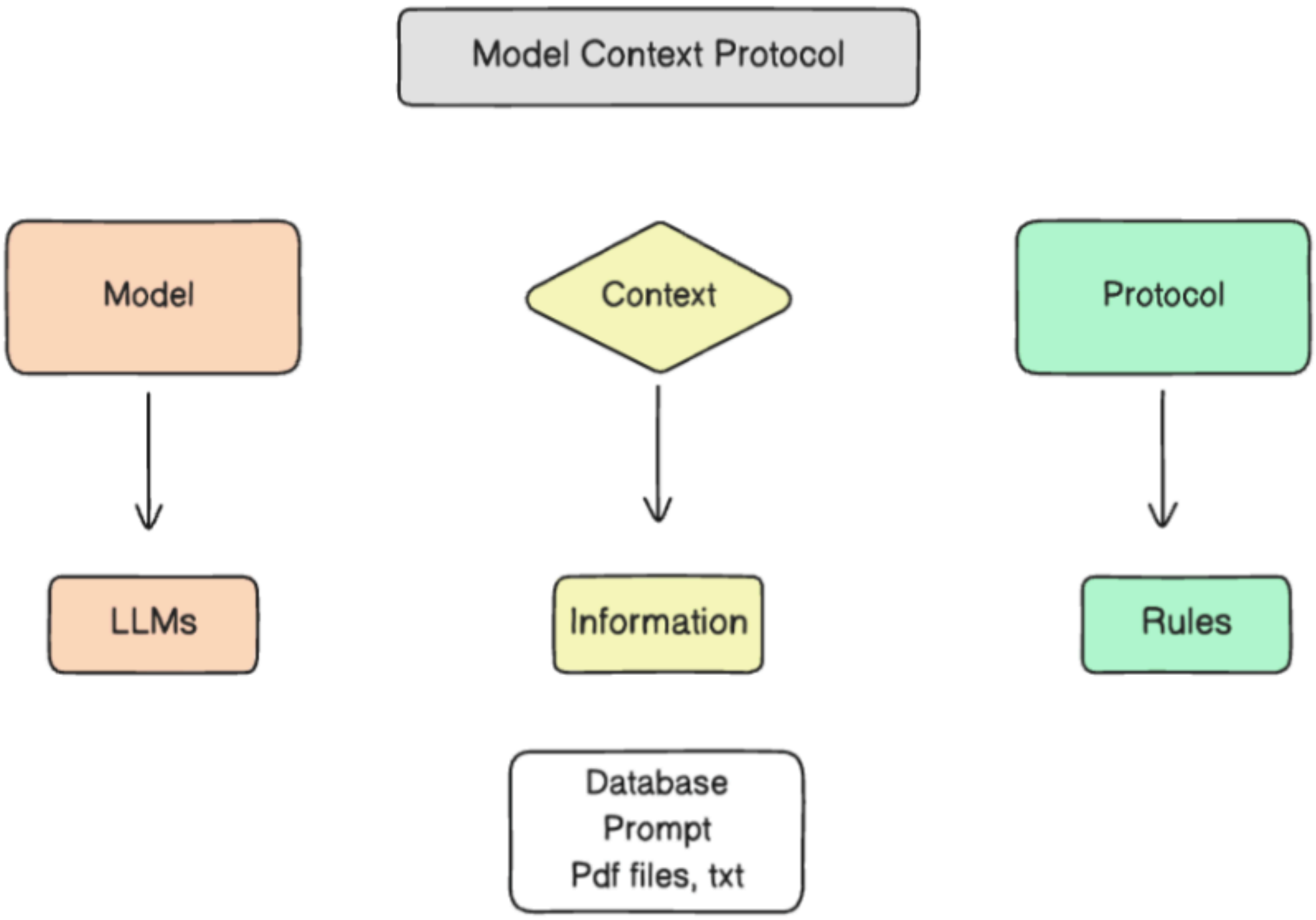
What is MCP?

- Model Context Protocol (MCP) is a powerful open standard that was launched by Claude's parent company, Anthropic, in November 2024. It allows Large Language Models (LLMs) like Claude or GPT to seamlessly access external content such as documents, databases, tools, local files or APIs, in a structured, secure, and scalable way.



What is MCP?

- Model Context Protocol (MCP) is a powerful open standard that was launched by Claude's parent company, Anthropic, in November 2024. It allows Large Language Models (LLMs) like Claude or GPT to seamlessly access external content such as documents, databases, tools, local files or APIs, in a structured, secure, and scalable way.



MCP at its core consists of three main components:

Model

It refers to the **LLM** (like Claude or GPT-4) that's responding to your inputs.

Context

It is the additional information the model needs to respond meaningfully. The source of this information can be documents, PDFs, prompts, or database entries.

Protocol

It represents a set of rules that lets the model access and use that context from structured sources.

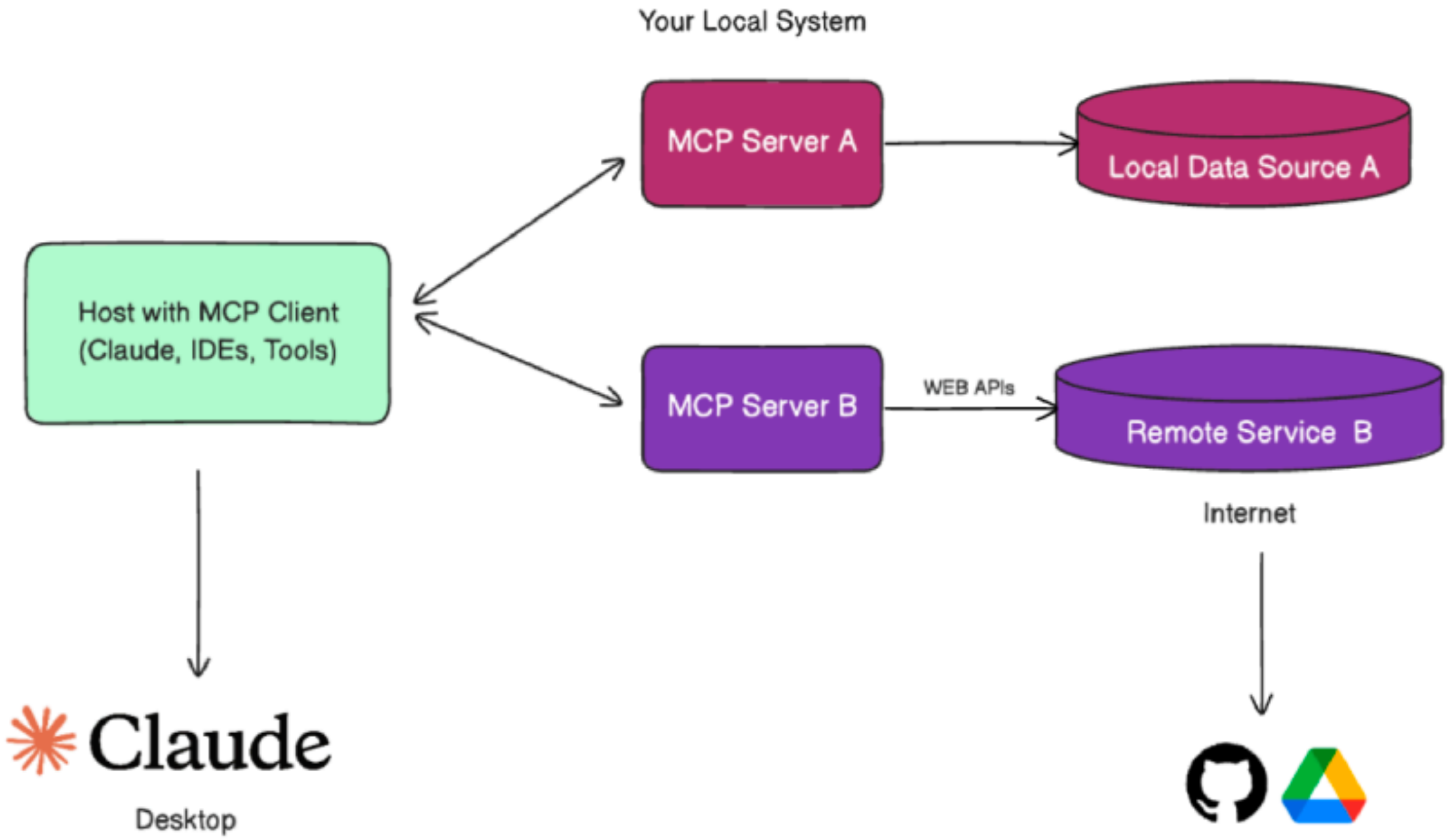
How Does MCP Work?

In its true essence, MCP standardizes the communication between the clients and servers, without needing custom code or manual data uploads. Clients and Servers can mean different things for different technologies, but for MCP, these are:.

- **Client**: This is the interface where the LLMs respond to you. This could be Claude's desktop app, your IDE, or a chatbot.

- **Server**: This is the system or data source (local or remote) that holds the context, for eg. Google Drive, GitHub, Gmail, your local files, PDFs, etc.

When you ask a question or give a command, the client sends a request to the server for the relevant information. The server then provides the necessary context (e.g., a file, email, or database), which the client uses to give you a response or complete a task. This process allows AI to efficiently work with real-time, dynamic data.



Thus, with MCP, the client (LLM interface) can automatically discover available servers (data sources), and request specific information based on your query.

For more information, you can visit this article

Generative AI Generative AI Application Intermediate

How to Use MCP: Model Context Protocol

Learn how to use MCP (Model Context Protocol) to connect LLMs lik

Anu Madan 25 Mar, 2025