AI Agent爆火后，MCP到底是个什么神器?

原创 猕猴桃 探索AGI 2025年03月08日 18:00 湖北

嘿，大家好！这里是一个专注于前沿AI和智能体的频道~

随着Agent的爆火，MCP这个词被提及的次数也越来越多了，所以到底什么是MCP呢？今天给家人们简单介绍一下，不涉及非常技术性的内容~

2024年11月，Anthropic开源Model Context Protocol (MCP)协议。拆解MCP的三个单次分别是：

- **Model**：指各类AI模型，如GPT、Claude等
- **Context**：指提供给模型的额外资料或上下文
- **Protocol**：指一种通用标准或规范

也就是说，MCP是一种使AI模型能够无缝对接外部资料的标准协议。AI Agent要发挥真正价值，必须能够操作外部工具，而软件程序的本质就是对数据进行操作。

举个例子：当你在AI驱动的IDE（如Cursor或Windsurf）中写好代码后，若想直接向GitHub提交Pull Request，传统方式下这是不可能的。即使AI非常智能，没有外部工具接口，它也无法完成这类任务。开发者必须手动打开GitHub、创建PR并添加描述。

而有了MCP，AI可以直接完成这些流程。本质上，在GitHub发送PR就是在特定代码库中创建PR相关数据。通过MCP服务器将AI IDE连接到GitHub，AI Agent就能在完成代码后直接创建PR。

为什么需要MCP?

你可能会问："这不就是让AI调用GitHub的API吗？为什么需要MCP？"

关键问题在于：没有MCP，AI模型如何知道正确调用GitHub的API？如果直接询问AI"如何调用GitHub API发送PR"，它可能基于过时的训练数据回答，或者产生幻觉。

以前一直采用"函数调用"(function calling)的方式解决这个问题，开发者定义特定函数和调用方式，让模型按规定格式传参并调用。那么，既有函数调用，为何还需MCP?

主要区别在于标准化。function calling让开发者自由定义函数及调用方式，虽然灵活，但当不同开发者采用不同方式时，就会出现"无法通用"的问题，导致普及困难且需要重复开发。

Anthropic开源MCP是，希望它成为类似USB-C的存在——一个通用标准，让各种设备都能通过同一接口连接，不会因更换设备而无法使用相同的接头。

就像苹果最终放弃专有的Lightning接口转而采用USB-C一样，MCP的存在让AI应用能轻松切换不同模型，同时让模型轻松对接各种数据源和工具。

MCP的核心价值在于提供标准化接口，让AI开发者能更轻松地将AI模型与外部资源和工具连接起来，从而构建更强大、更实用的AI应用。

好了，这就是我今天想分享的内容。如果你对构建AI智能体感兴趣，别忘了点赞、关注噢~

探索AGI
目前专注于大模型agent的产品落地方向，未来不确定~
136篇原创内容

公众号