Implementing an MCP Server

- Kavith *(Most definitely not an MCP expert)*

Seriously though, what *is* MCP?

- JSON-RPC (JSON-Remote Procedure Call); lightweight, stateless protocol

```
--> {"jsonrpc": "2.0", "method": "subtract", "params": [42, 23], "id": 1}
<-- {"jsonrpc": "2.0", "result": 19, "id": 1}
```

Terminology	What it is/ does	Examples
Host	LLM-integrated apps. Can generate tool calls.	Cursor, Windsurf, Goose, Claude Desktop,etc.
MCP Client	Library in the host that maintains a **stateful** session per MCP server.	MCP SDK
MCP Server	Lightweight wrapper in front of a tool.	GitHub MCP Server, Daft MCP
Tool	A callable function. It’s discoverable by the client at runtime.	get_pull_request, get_rental_properties

Demo Time

Things I’m weary of

- MCP is just a thin wrapper around existing endpoints/ data sources
- It’s *somewhat* limited by the LLM
- Not many officially hosted MCP servers yet
  - Feels like installing Android APKs or strange browser extensions
  - Even if not malicious, it could expose sensitive data accidentally
  - Would recommend self-built MCP servers > 3rd party hosted ones

Thanks!

Email*: xyz@kavith.xyz*