UbuCon India 2026

#2026

#UbuConIndia2026

Beyond Tool Sprawl: Practical Discovery and Governance for MCP Agents.

arul.sg

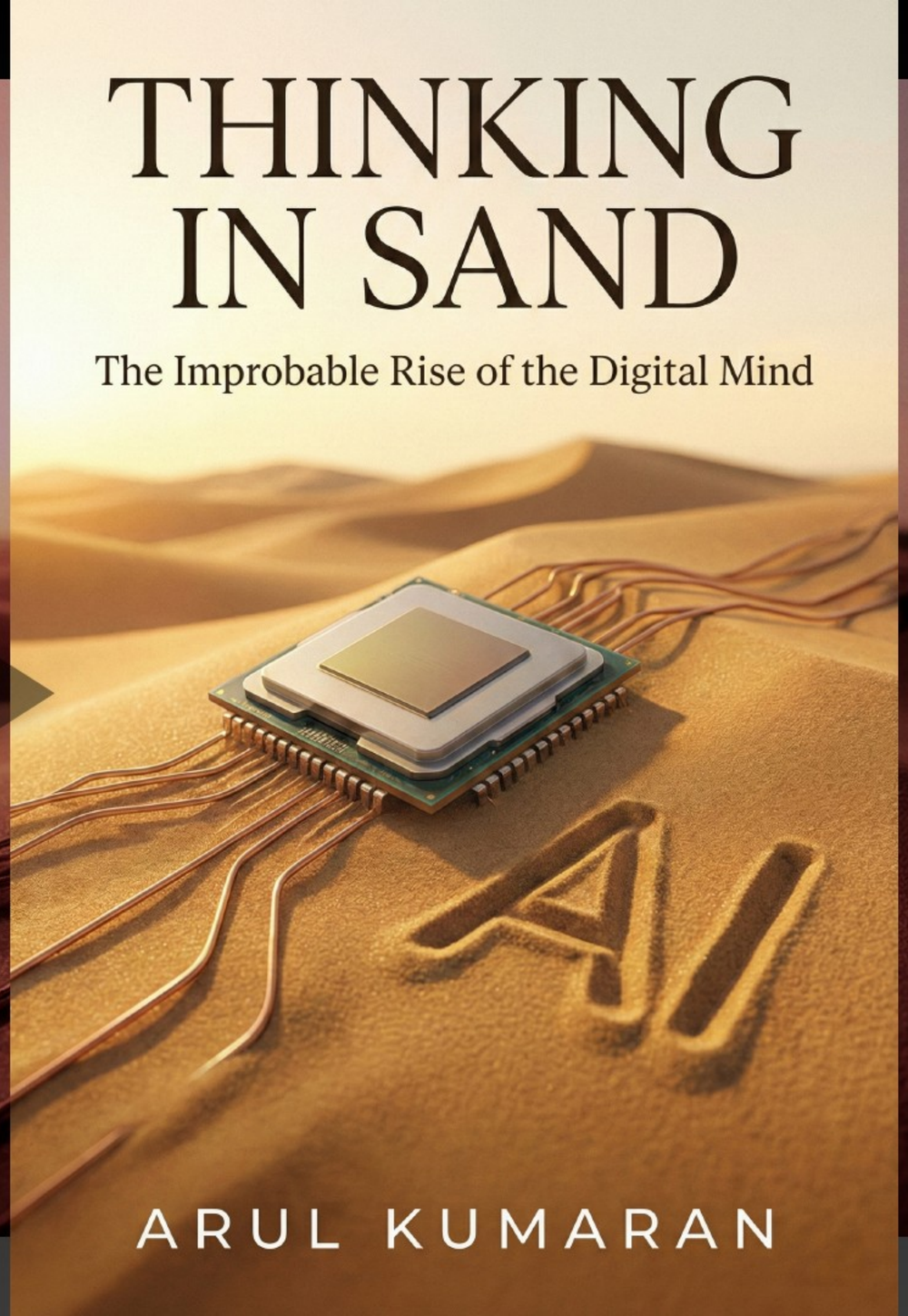


Canonical Qualcomm penpot

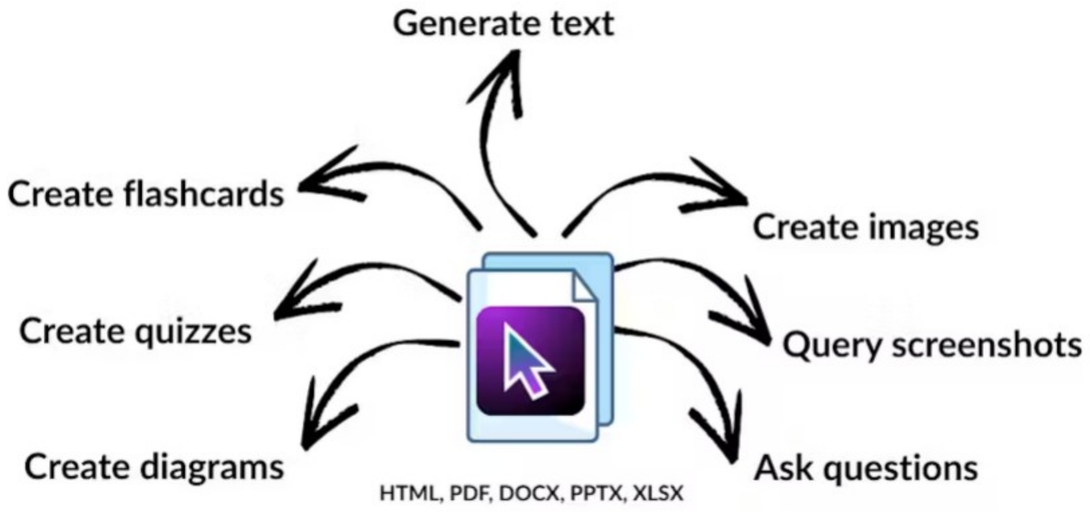


Thinking in Sand

This book argues that artificial intelligence is not replacing human intelligence. It is restructuring power. As machines gain perception, creativity, and agency, leverage shifts toward those who understand how to design systems rather than merely operate them. In the Hybrid Intelligence era, the most powerful individuals will be those who architect the partnership between human intent and machine scale.



Mighty Cursor

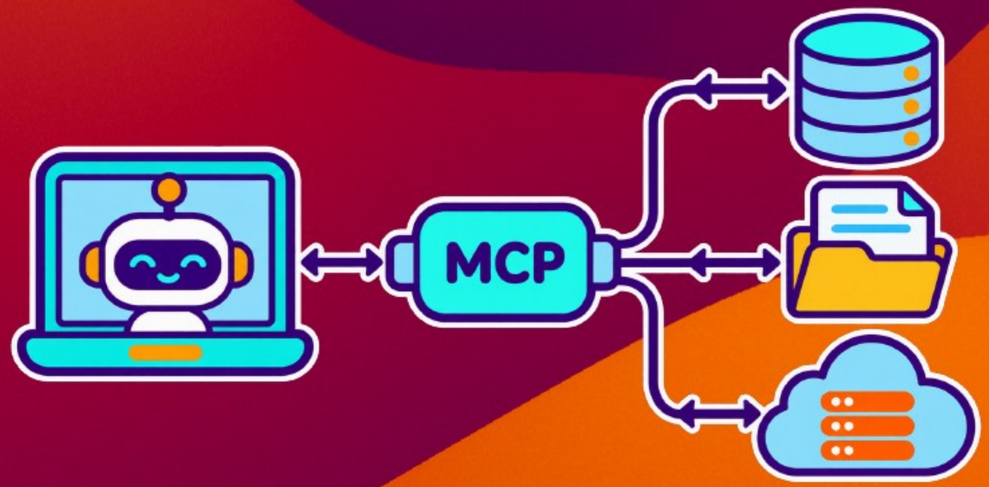


A Mac Application that brings AI home


SAPIEN
GENO

MCP connects AI to systems

A common protocol for tools and context



- Introduced in November 2024
- One protocol connects clients and servers
- Tools, resources and prompts

Problem 1: Tool definitions

A growing catalog fills context



- Many clients expose schemas up front
- Descriptions compete for context
- Cost depends on the host and catalog

Is MCP dead?

Why some agents use the terminal



- Large tool catalogs sparked criticism
- A terminal agent can discover commands on demand
- Command help and output still use context

Find tools when needed

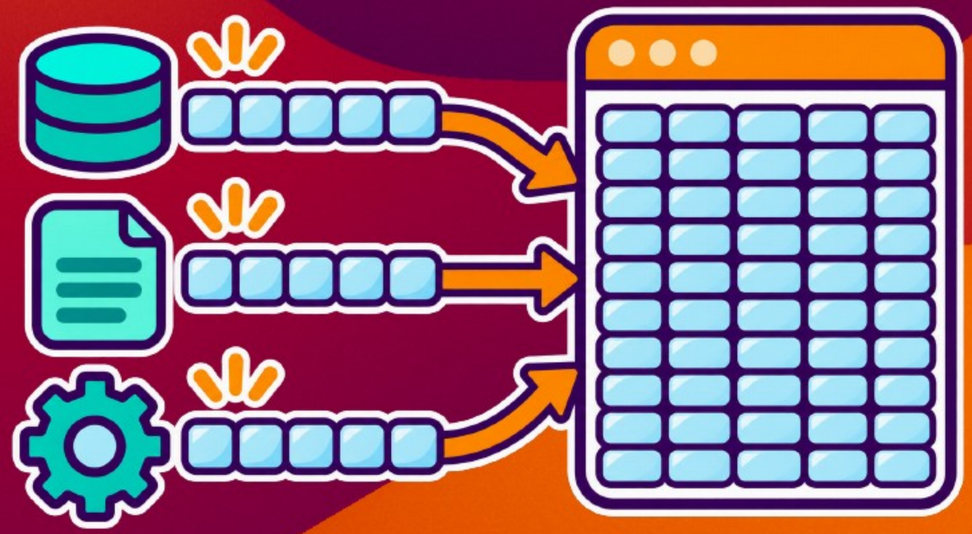
Search before loading full schemas



- Search by keywords or vector similarity
- Return relevant candidates and schemas
- Review relevance and permissions

Problem 2: Results add up

Intermediate outputs return to the model



- A multi-step task can pass large results
- Each model turn consumes context
- Filter data before returning it

Code mode: compose tool calls

Code handles the intermediate steps



- Write a small program to call tools
- Filter, join and loop in execution
- Return only what the model needs

Cloudflare and Anthropic

Two approaches to the same constraints



- Cloudflare: typed APIs and Code Mode
- Anthropic: Tool Search and programmatic calls
- Both can reduce context sent to the model

NCP: discovery and gateway checks

One implementation across configured MCP servers



- Find relevant tools across servers
- Track health; exclude unhealthy servers
- Request confirmation for some modifying actions

Discovery is not permission

Governance remains a separate concern



- Read access can be limited
- Changes may need approval
- Enforce policy at execution

Choose for the task

Discovery, execution, governance



- Small catalog: direct calls can be enough
- Many tools: discover on demand
- Multi-step work: consider code execution
- Enforce access and observe calls

Questions?

Connect on LinkedIn