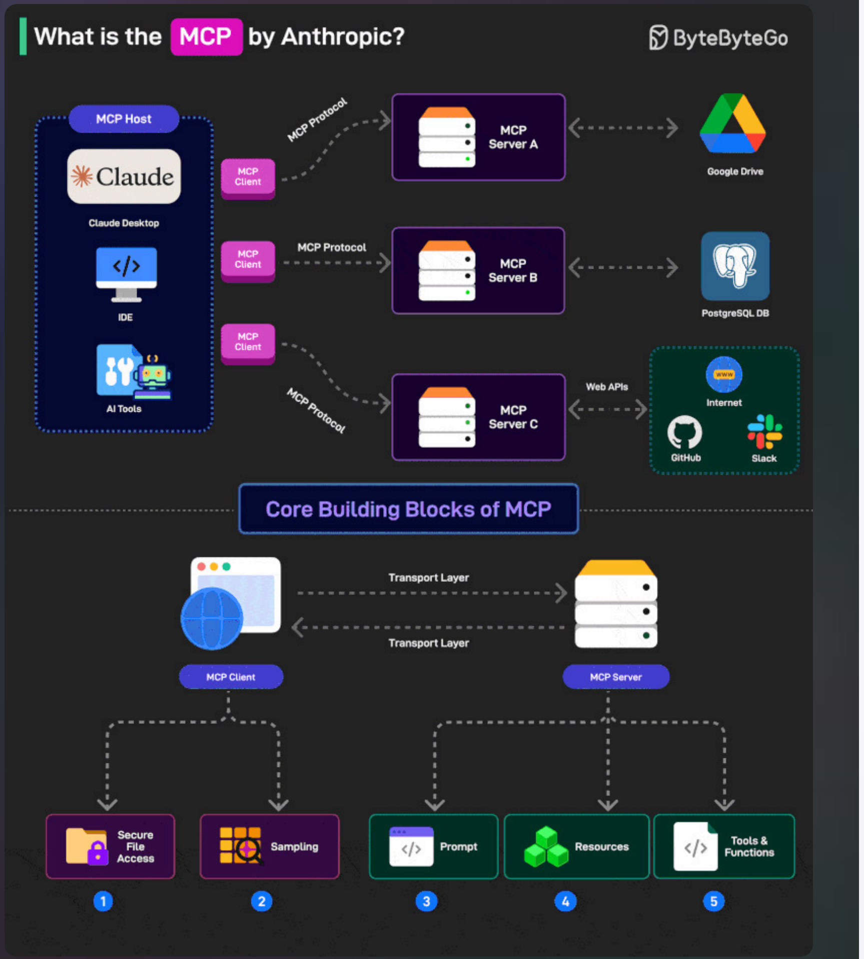
Understanding the Model Context Protocol (MCP)

Enabling Seamless AI-Tool Interaction

GM **by Govind Manoharan**



Challenges with Previous Approaches

Fragmented Integration

Complex manual interfaces for each service

Redundant Implementations

Function calling varied across platforms

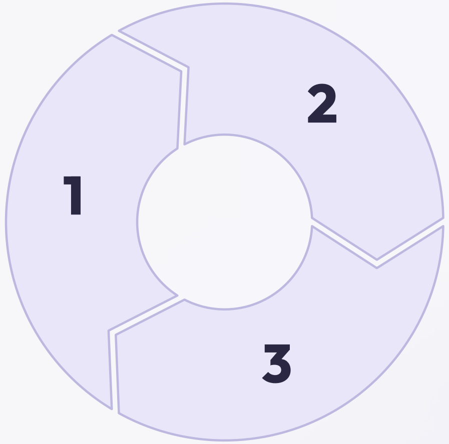
Manual API Wiring

Increased complexity and maintenance

RAG Limitations

Only passive information retrieval

Core Components of MCP Implementation



MCP Host

AI application environment

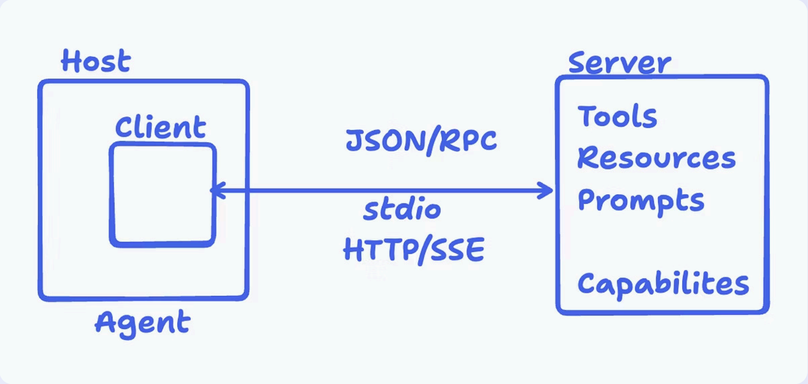
MCP Client

Intermediary managing communication

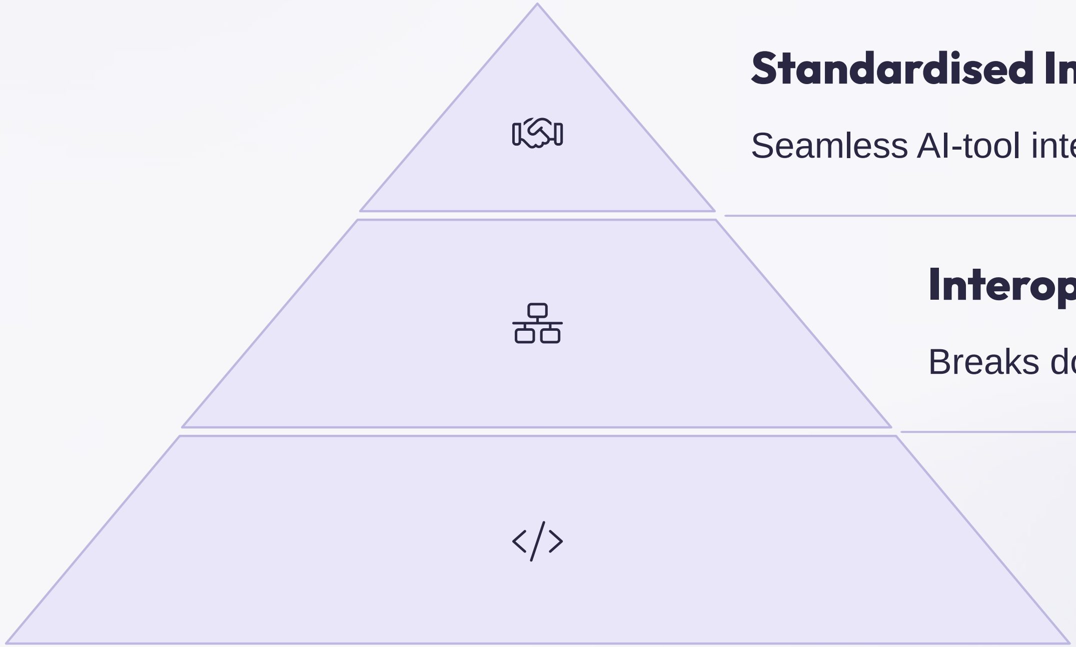
MCP Server

Access to external systems

- Tools
- Resources
- Prompts



Introducing MCP: A Standardised Solution



Standardised Interface

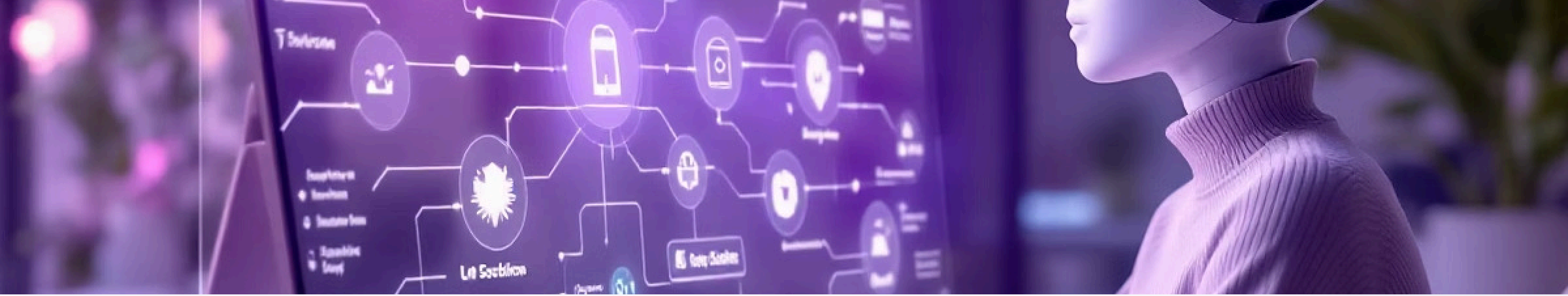
Seamless AI-tool interaction

Interoperability

Breaks down data silos

General-Purpose Protocol

Inspired by Language Server Protocol



Major Advantages of Using MCP

Improved Interoperability

Seamless interaction with multiple tools

Dynamic Tool Discovery

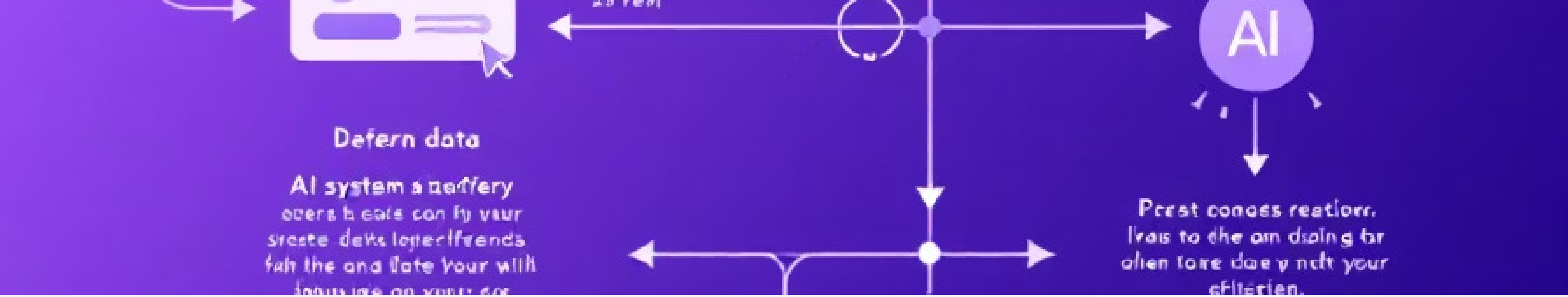
AI autonomously selects tools based on context

Simplified Development

Unified interfaces for AI applications

Enhanced Agent Capabilities

Both retrieval and action enabled



How MCP Works: The Workflow

Initial Request

User sends prompt to MCP client

Intent Analysis & Tool Selection

Client selects appropriate tools

API Invocation & Orchestration

Server processes information

Final Result

Client notifies user of results

Security Risks in Creation Phase

Security Risks

- Name collision
- Installer spoofing
- Code injection/backdoor

Mitigation Strategies

- Strict namespace policies
- Secure installation framework
- Code integrity verification

Security Risks in Operation Phase

Tool Name Conflicts

Similar names causing ambiguity

Slash Command Overlap

Identical commands causing unintended actions

Sandbox Escape

Breaking out of isolated environment

Conclusion

Promising Protocol

MCP standardizes AI-tool interactions

Address Security Risks

Crucial for sustainable growth

Stakeholder Collaboration

Essential for robust ecosystem

Continued Research

Enhance security, scalability, governance

Connect with Me

Email: govind.prem@gmail.com

LinkedIn: www.linkedin.com/in/govind-manoharan-a3205a12