Oracle SQLcl MCP server evaluation and resource limits

CERN openlab Summer Student Programme Lightning talks

David Benko

Supervisor: Andrzej Nowicki, Miroslav Potocky

18/08/2026

Motivation

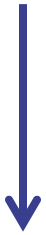
Problem description

We have a database of bike rentals at CERN, and we want to see who is likely to return their bike soon due to the end of their contract.

Motivation

Problem description

SQL



```
SELECT e.name, e.surname, e. affiliationend
FROM bikes b
LEFT JOIN employees e ON b.login = e.login
WHERE e.affiliationend <= '31-AUG-26'
FETCH FIRST 15 ROWS ONLY
```

Motivation

Problem description

SQL

Results

name	surname	affiliationend
Edwin	Ford	2026-08-21
Anton	Payne	2026-08-23
Max	Roberts	2026-08-30

What if we don‘t know SQL enough?

What if we don‘t know SQL enough?
If we are unfamiliar with the data model?

What if we don‘t know SQL enough?

If we are unfamiliar with the data model?

Or if we are just lazy?

What if we don‘t know SQL enough?

If we are unfamiliar with the data model?

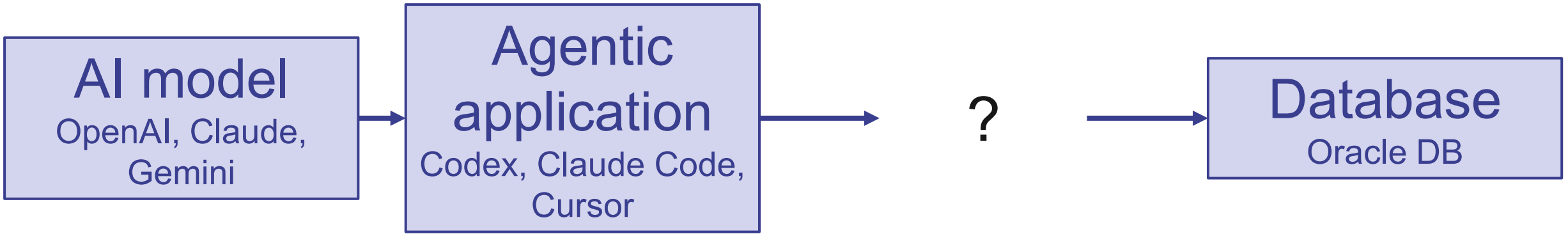
Or if we are just lazy?

AI agents can help us!

The goal

Let users query/modify Oracle DBs data from their LLMs

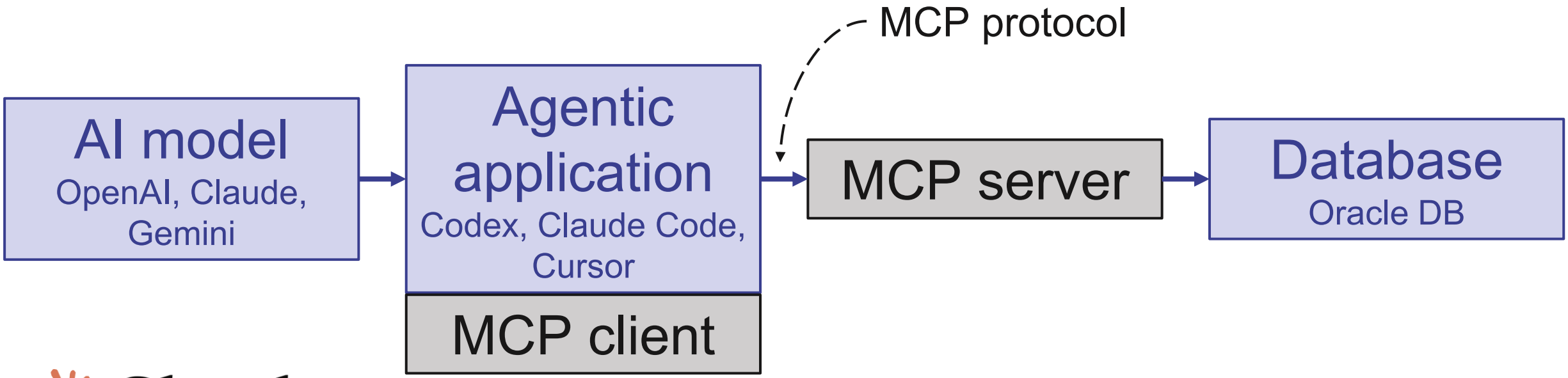
Architecture



Claude

ORACLE

Architecture



Too many options...

MCP server

Self-hosted? OCI? Local?

LLM

Self-hosted? Commercial?

Which specifically?

Performance? Data governance? Scaling? Ease of use?

MCP server deployment

The biggest problem

Authentication and permissions

- **Self-hosted and cloud solutions**: single DB account shared by all users
  - High permission granularity unfeasible
- **Users‘ machine deployment**: inherits user‘s permissions

MCP server deployment

Recommendation

- **Self-hosted** instance **per project or use-case** if needed
  - When all users share the same database privileges
  - Ideally read-only
  - Requires development time to set up
- **Local** (users‘ machine) **deployment** in **all other cases**
  - Flexibility
  - User‘s discretion and responsibility

What about the LLMs?

Let‘s check the benchmarks first

What about the LLMs?

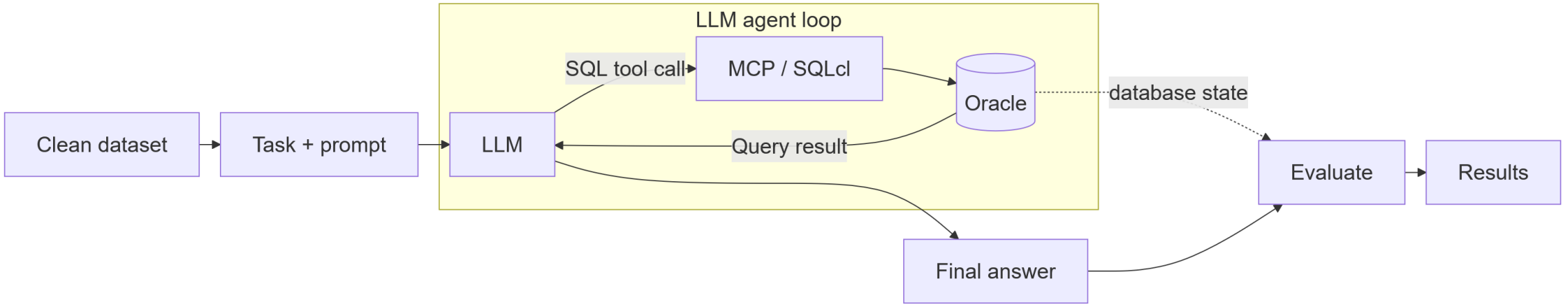
Let‘s check the benchmarks first

... there‘s no benchmark 😑

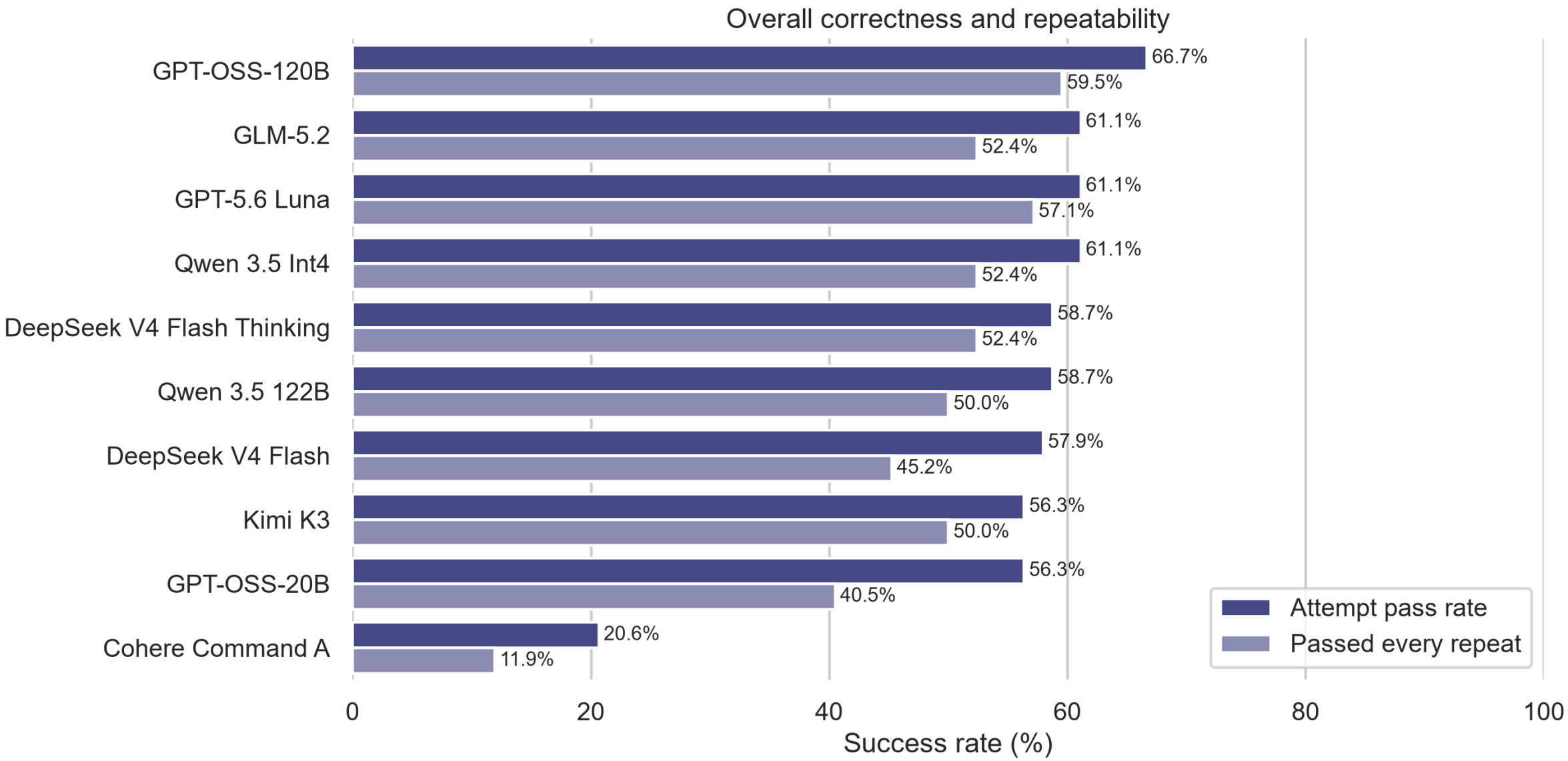
Benchmarking

Oracle-specific text-to-SQL benchmark

- New **benchmarking framework**
- Both **queries and management tasks**
  - Subset of LiveSQLBench Lite datasets + adaptation
- LLM prompted to work directly with the DB (SQLcl)
- 10 models, 3 datasets, 42 tasks, 3 repetitions per task per model



Benchmarking results



Benchmarking conclusions

- Oracle SQL is known well enough
  - Issues with quoting and adherence to the schema – self-recovery
- GPT-OSS-120B is the best general-purpose choice out of these 10 models
- The performance of OCI Cohere A model is very poor
- No model is sufficient for unattended use
- Flagship models remain to be benchmarked

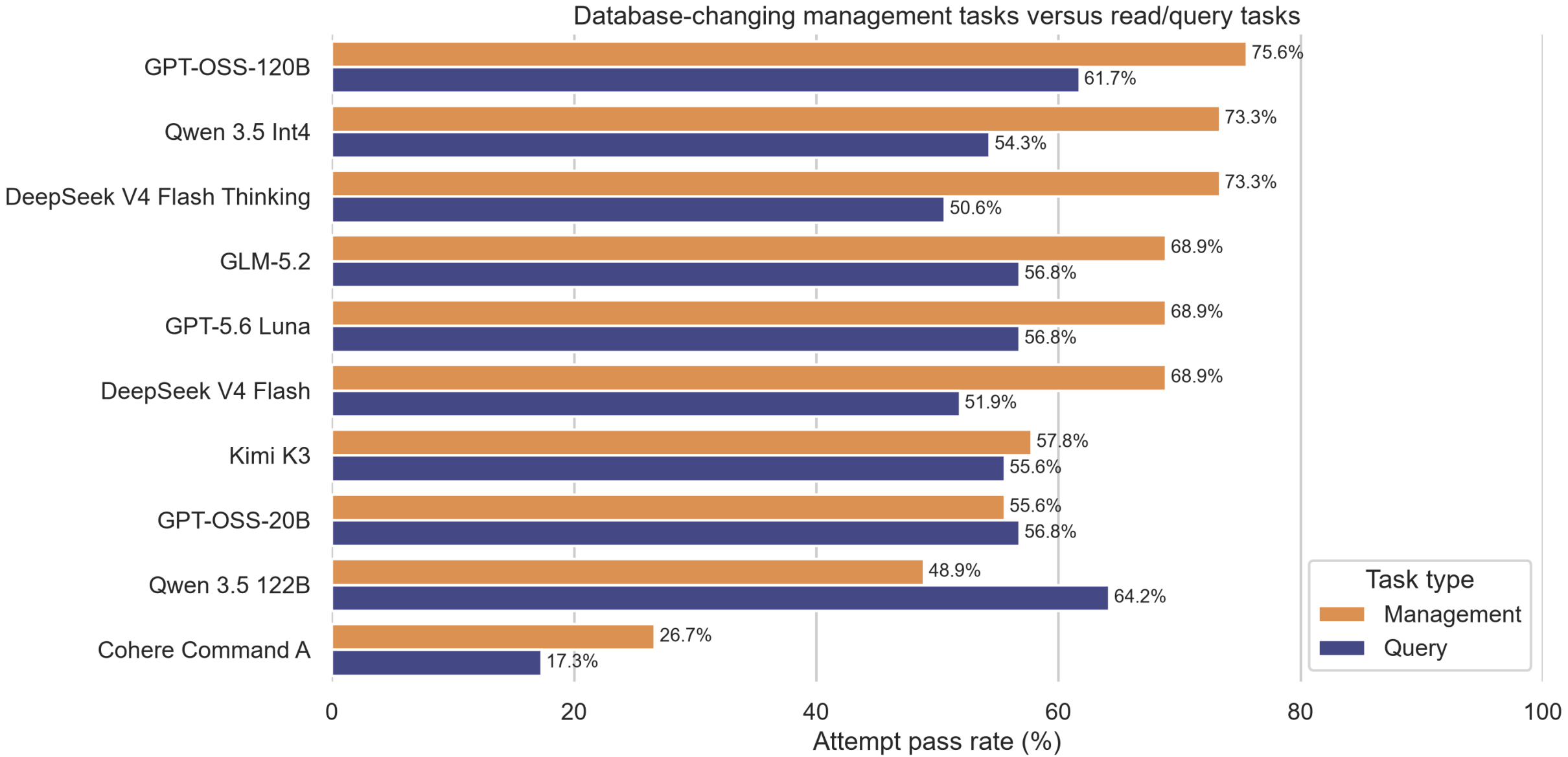
Next steps

Nearly two more weeks to go...

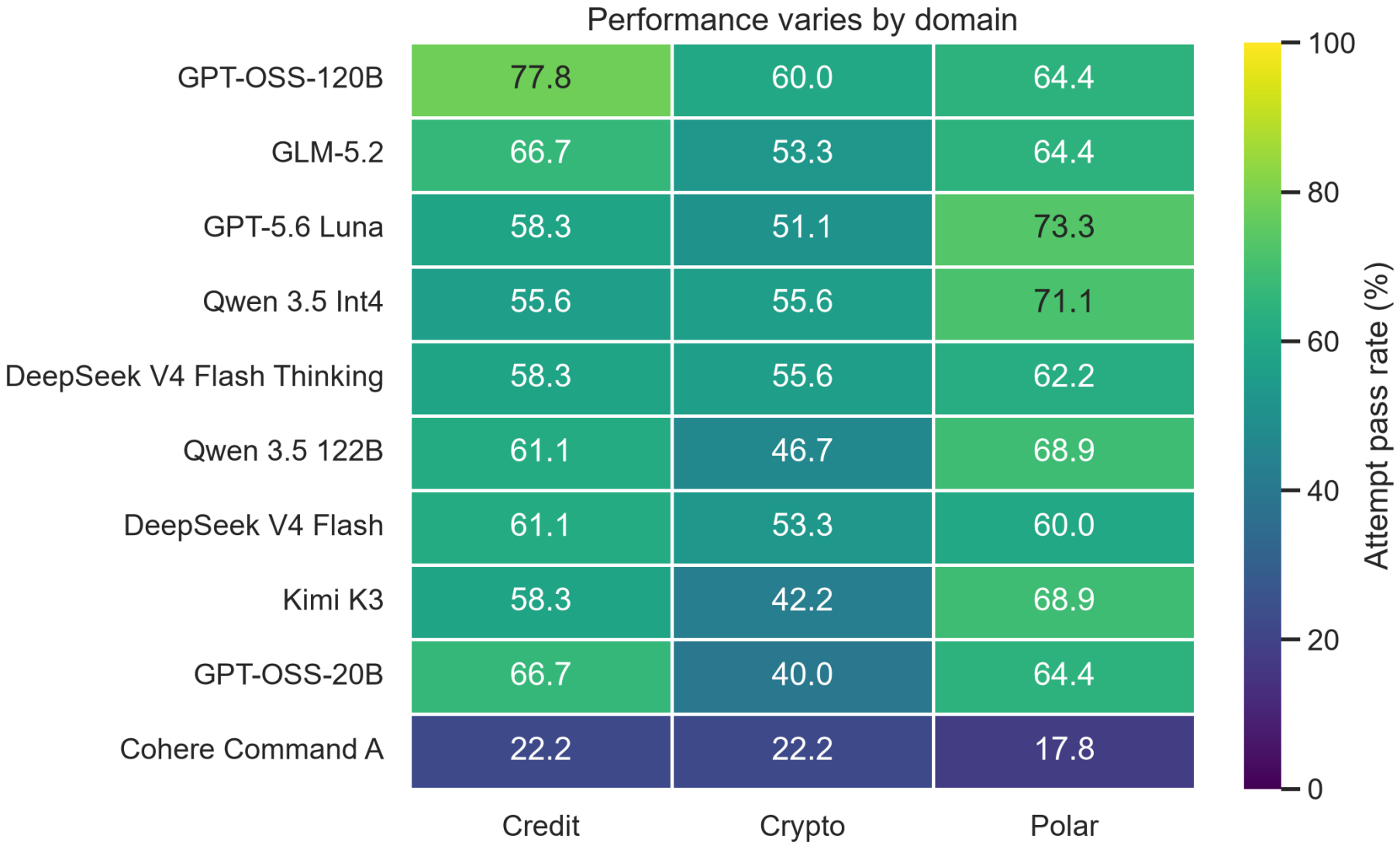
- Implement automatically applied DB **resource limits for database sessions** identified as running an AI/MCP based client

Questions?

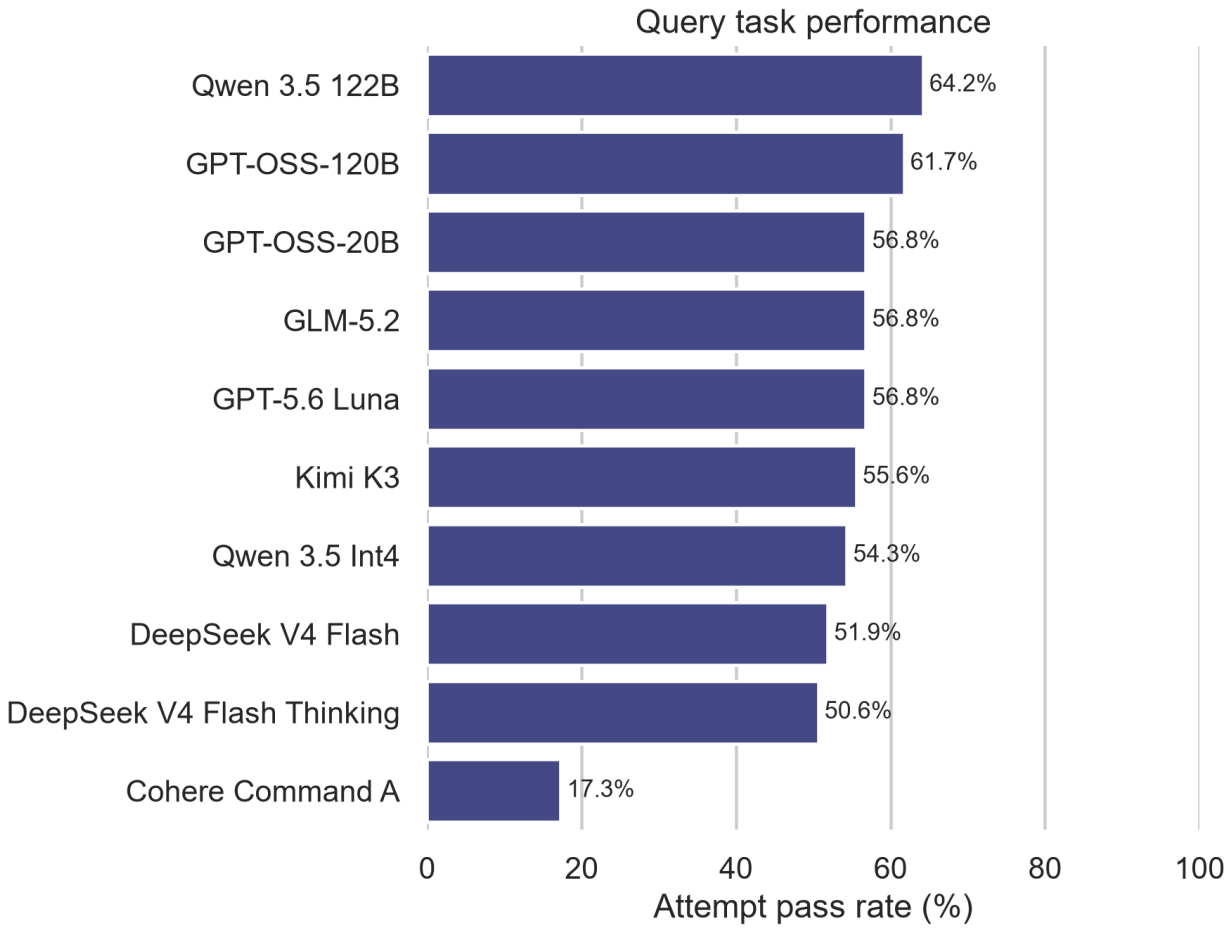
Benchmarking results

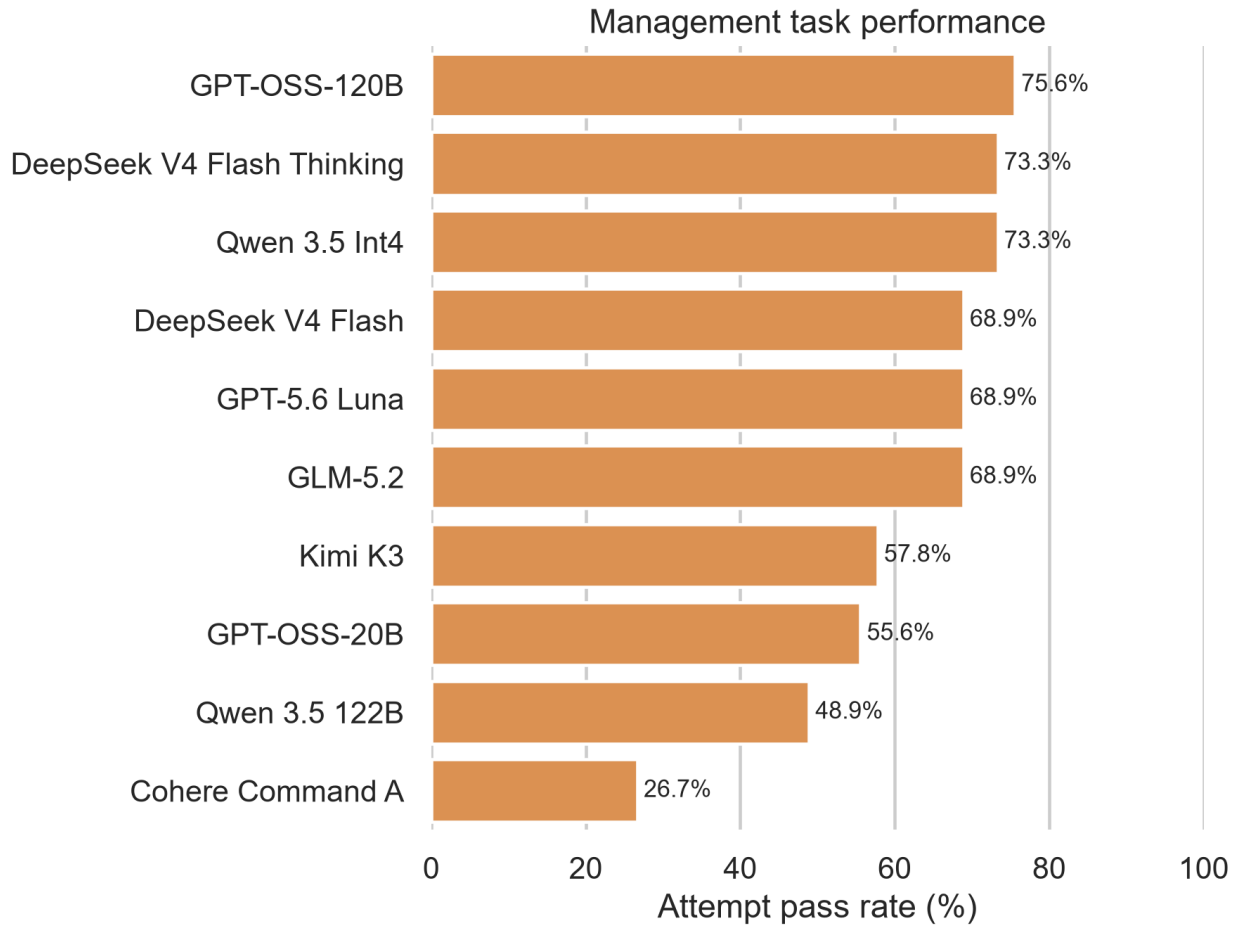


Benchmarking results

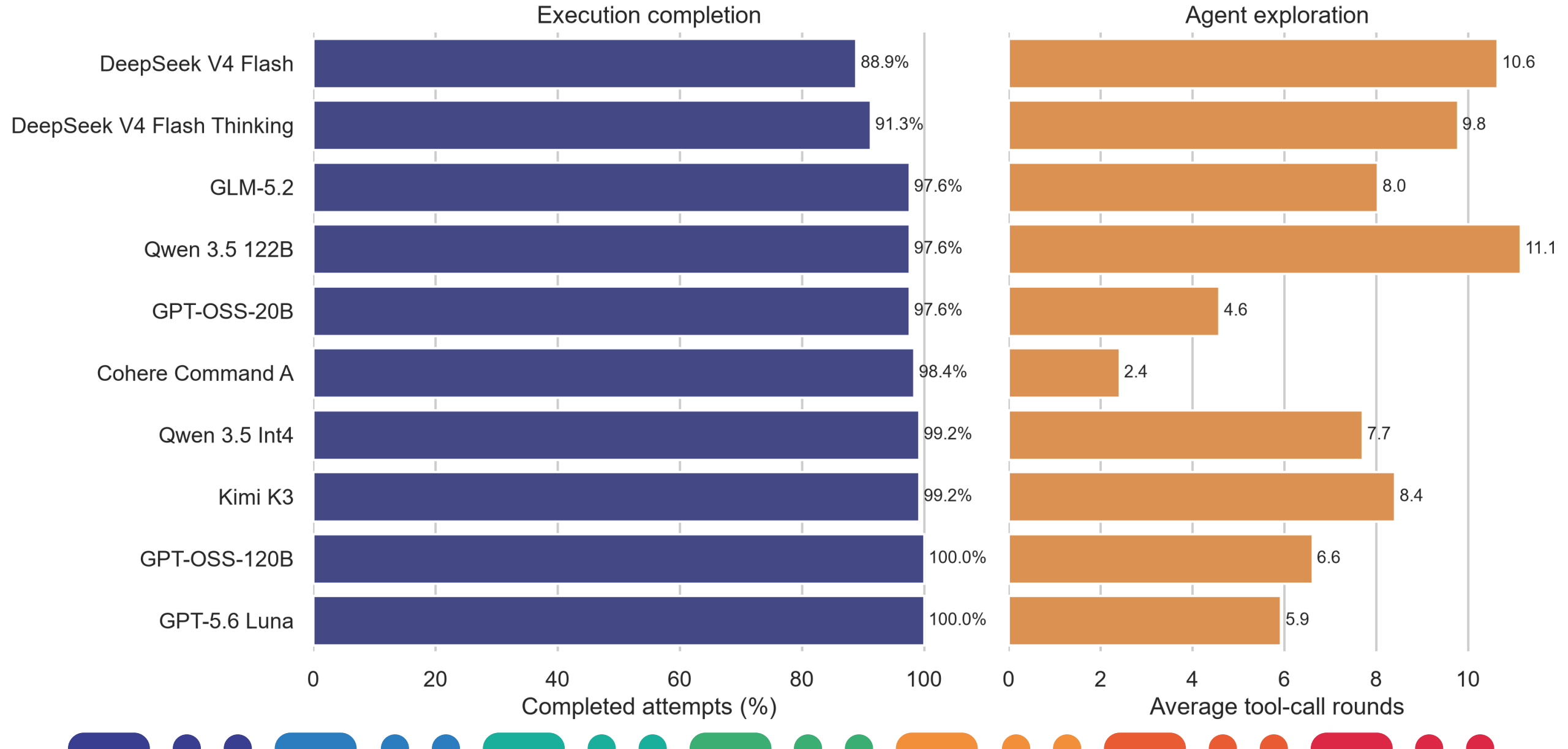


Benchmarking results

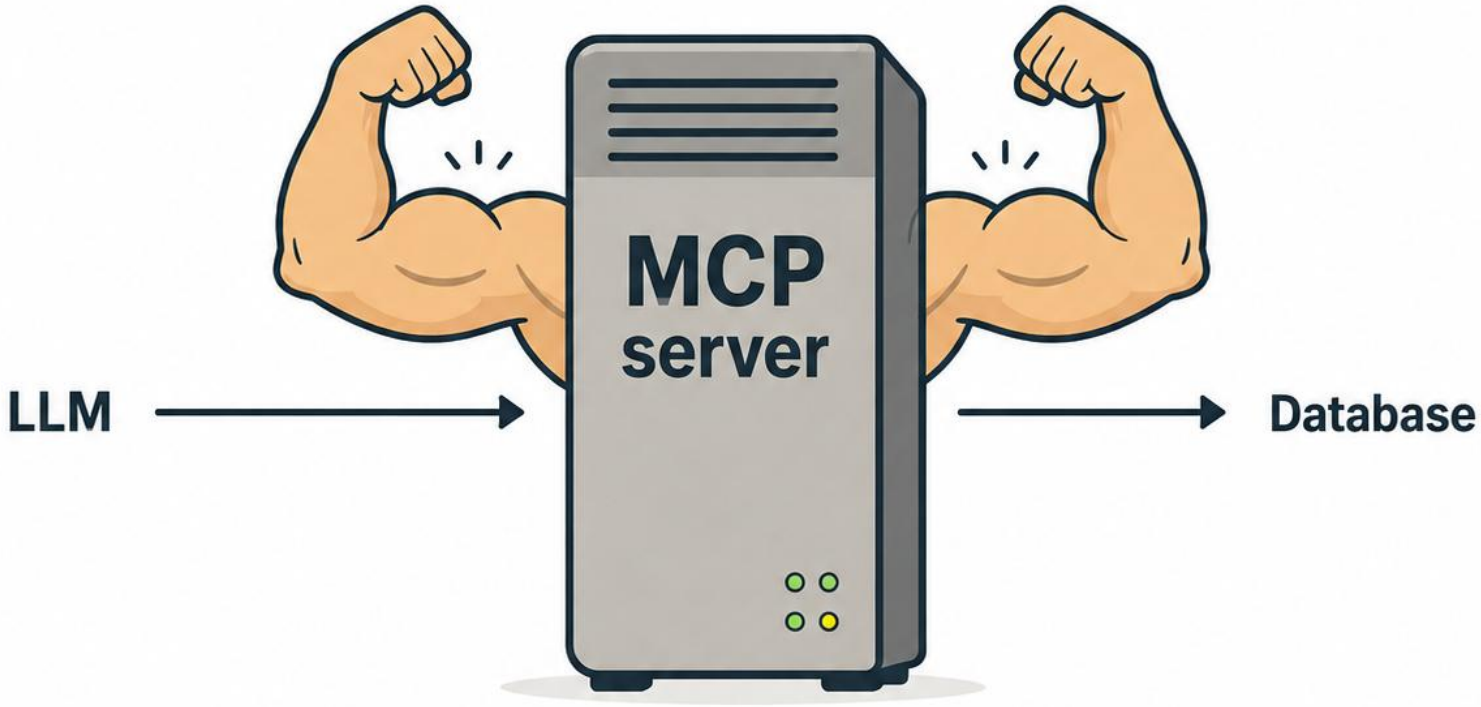




Benchmarking results



MCP server?



MCP server?