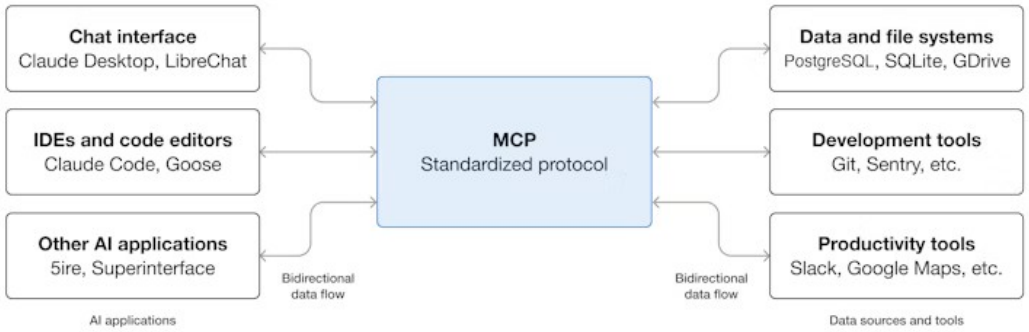
HOCH SCHULE OFFEN BURG

**Forschungsmaster**
**Projekt Thema**

IMLA

# Model Context Protocol (MCP) in der HSO LLM Infrastruktur




Das **Model Context Protocol** hat sich in den letzten Monaten zum de facto Standard bei der Interaktion von Sprach- und Visionmodellen (LLMs und VLMs) mit externen Datenquellen und Werkzeugen entwickelt. Zwischenzeitlich gibt es eine Vielzahl von Toolboxen und Libraries welche einfache Umsetzungen von MCP Servern erlauben. Weitestgehend ungeklärt ist hingegen wie sich MCP basierte Dienste in komplexe Multi-User Infrastrukturen einbinden und Orchestrieren lassen. Dies soll in der Arbeit anhand der HSO LLM Infrastruktur untersucht und prototypisch umgesetzt werden.

## Betreuer

**Prof. Dr.-Ing. Janis Keuper**
- janis.keuper@hs-offenburg.de
- https://www.keuper-labs.org

## Beteiligte Institute und Firmen

Das Projekt am **I**nstitute for **M**achine **L**earning and **A**nalytics im Rahmen des BMBF geförderten Forschungsprojekts LLM-Praxis durchgeführt.

## Ziele des Projekts

- Systematische Analyse und Evaluation aktueller MCP Frameworks
- Konzeption einer zentralen MCP Lösung in der HSO LLM Infrastruktur unter Betrachtung der Teilaspekte:
  - Authentifizierung
  - Ressourcen Orchestrierung
  - Accounting
  - Security

## Diese Werkzeuge/Qualifikationen werden erlernt

- Theorie und Praxis aktueller Methoden zu LLMs und VLMMs
- Praktische Entwicklung Python inf MCP/LLM Tools Pipelines in realen Projekten
- Methoden angewandter Forschung in realen Projekten

## Literatur + Weiterführende Informationen

- BMBF Projekt: https://www.llm-praxis.de/
- HSO Infrastruktur: https://llm-proxy.imla.hs-offenburg.de/info/
- IMLA: https://imla.hs-offenburg.de/