

Private AI for Research: Secure, Scalable and Automated

Wednesday 16 July 2025 10:03 (3 minutes)

We present a privacy-preserving research environment integrating offline Large Language Models (LLMs), AI agents, and scalable infrastructure. By deploying private LLMs via Ollama and containerized workflows on Kubernetes, researchers can automate tasks like literature review, code generation, and secure data processing without compromising sensitive information. AI agents—coordinated through n8n—enhance productivity by orchestrating multi-step research workflows, such as relevance scoring of abstracts and deep content summarization. Designed with biomedical applications in mind, the environment enables responsible use of clinical and omics data in line with the stringent data governance requirements at the University Medical Center Hamburg-Eppendorf (UKE).

I want to give a Lightning Talk

yes

Author: HEINS, Sven (Universität Hamburg)

Presenter: HEINS, Sven (Universität Hamburg)

Session Classification: Lightning Talks