KIDA
AI for Food and Agriculture

Gefördert durch:
Bundesministerium für Landwirtschaft, Ernährung und Heimat
aufgrund eines Beschlusses des Deutschen Bundestages

Projektträger
Bundesanstalt für Landwirtschaft und Ernährung

KIDA-AIChat

Chatbot auf eigener Plattform ermöglicht sichere Textverarbeitung

- **Nutzung von öffentlich zugänglichen Chatbots kann den Schutz von vertraulichen Daten gefährden**
- **KIDA-Lösung erleichtert den Arbeitsalltag bei gleichzeitiger Gewährleistung von Datensicherheit**
- **Verwendung einer gemeinsamen Lösung spart Ressourcen**

Hintergrund und Fragestellung

Große Sprachmodelle (LLMs) gewinnen fortlaufend an Relevanz im Arbeitsalltag. Sie können viele Arbeitsschritte erleichtern und beschleunigen, jedoch bieten kommerzielle, öffentlich zugängliche Anwendungen oft keinen hohen Schutz z.B. für sensible Forschungsdaten, vertrauliche Verwaltungsunterlagen oder unveröffentlichte Strategiepapiere. Ziel des **KIDA-AIChats** ist es, den Mitarbeitenden der sieben Einrichtungen im KIDA-Verbund eine **benutzerfreundliche und datenschutz-konforme Nutzung** eines Chatbots zu ermöglichen, ohne dass jede Einrichtung eine eigene Lösung finden und leistungsfähige Hardware dafür bereitstellen muss.

Vorgehensweise

Der AIChat wurde von KIDA-Beteiligten aus der **Open-Source-Software** „Open WebUI“, „Ollama“ und später „vLLM“ zusammengestellt. Dadurch konnte schnell ein einsatzfähiges Produkt erstellt werden, das kontinuierlich von der Community weiterentwickelt wird. Anschließend wurde der AIChat auf dem KIDA-Cluster des Julius-Kühn-Instituts (JKI) für alle Einrichtungen im KIDA-Verbund zur Verfügung gestellt. Die Lösung hat folgende Merkmale:

1) Der AIChat kann auf der eigenen oder der Verbund-Infrastruktur betrieben werden. Dadurch müssen keine Daten auf externen Cloudservern verarbeitet werden, wie es in der Regel bei öffentlich zugänglichen Chatprogrammen der Fall ist. Jede Einrichtung kann ihn **innerhalb ihrer jeweiligen geschützten IT-Infrastruktur** einsetzen, um die uneingeschränkte Hoheit über die **Datensicherheit** zu behalten. Dies trifft auch auf die Bereitstellung durch das JKI zu, indem jede Einrichtung ihre eigene Instanz in ihrem Netzwerk erhält.

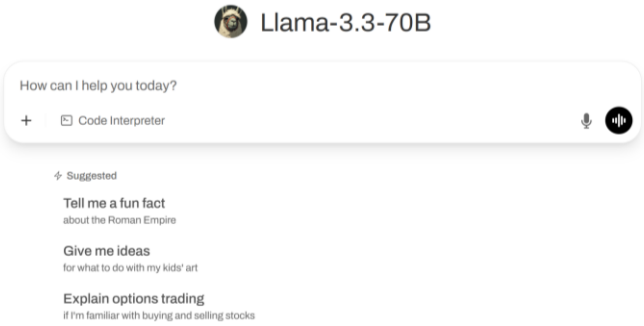
2) Der Einsatz im Verbund nutzt die Rechenleistung optimal aus und ermöglicht Einrichtungen die **Nutzung, ohne eigene Ressourcen** wie Grafikkarten bereitstellen zu müssen.

3) Die Anwendung besitzt durch die Verwendung von Open WebUI eine **benutzerfreundliche Oberfläche**. Nutzende benötigen keine Programmierkenntnisse, um den AIChat bedienen zu können.

4) Die AnwenderInnen können (mehrere) **Dokumente** zum Chat hinzufügen. Sie können **Fragen** dazu stellen und sich eine **Zusammenfassung** erstellen lassen. Der KIDA-AIChat kann auch zum **Übersetzen** von Texten verwendet werden.

5) Es können verschiedene aktuelle Sprachmodelle von Llama oder Mistral eingebunden werden.

6) Die individuellen Chats von Nutzenden sind **personalisiert** und nicht für andere zugänglich.



Ergebnisse und Schlussfolgerungen

Der KIDA-AIChat ermöglicht den Forschenden und Beschäftigten eine **datenschutzkonforme Verarbeitung von Texten**. Er ist durch die gemeinsame Entstehung und Bereitstellung **ressourceneffizient**. Zudem bietet er eine präzise **Steuerbarkeit** bei gleichzeitig großer **Gestaltungsfreiheit** durch die Einrichtungen und macht diese so unabhängig von externen Anbietern. Der KIDA-AIChat stärkt so nachhaltig die Leistungsfähigkeit der beteiligten Einrichtungen.

Kontakt	Informationen
KIDA-Teams Produktivsetzung, KI-Beratung & Infrastruktur: kida@bmleh.bund.de	**KIDA-Bearbeitende** (alphabetisch): Steffen Albrecht (KIDA, FLI), Ahsan Ali (KIDA, BfR), Aileen Bahl (KIDA, BfR), Sebastian Fischer (KIDA, JKI), Maria Heinze (KIDA, JKI), Marko Henning (KIDA, Thünen), Emanuel Hesse (KIDA, JKI), Cristina Ortiz Cruz (KIDA, MRI), Jacob Schmieder (KIDA, DBFZ) **Team-Leitungen:** Marco Selig (KIDA Produktivsetzung, DBFZ), Micha Schneider (KIDA KI-Beratung, Thünen), Boris Orywahl-Wild (KIDA Infrastruktur, BVL)