

Umsetzung von KI-Transferprojekten

Praxisbericht zu Risiken und Herausforderungen

Reinhold von Schwerin¹, Daniel Schaudt² und Alexander Hafner³

Abstract: Dieser Beitrag beschreibt den Wissenstransfer im Rahmen der Entwicklung eines Retrieval-Augmentation Generation (RAG) Systems durch das DASU – Transferzentrum für Digitalisierung, Analytics & Data Science Ulm. Das Projekt, dessen Entwicklung im Oktober 2023 in Kooperation mit Industriepartnern begann, zielt darauf ab, unternehmerisches Wissensmanagement mithilfe großer Sprachmodelle zu unterstützen. Der Bericht thematisiert sowohl technische als auch organisatorische Risiken und Herausforderungen bei der Entwicklung von KI-Systemen im Allgemeinen und erläutert, wie diese im DASU-Projekt konkret adressiert wurden. Ziel dieses Beitrags ist es, insbesondere kleinen und mittleren Unternehmen (KMU) praxisnahe Einblicke in die Potenziale und Grenzen von KI-Implementierungen zu geben.

Keywords: Digitalisierung, Digitale Transformation, Risikomanagement, Maschinelles Lernen, Künstliche Intelligenz

1 Motivation

Im Kontext der digitalen Transformation und des Einsatzes von künstlicher Intelligenz (KI) sehen sich Unternehmen mit Herausforderungen konfrontiert, die ihre Wettbewerbsfähigkeit unmittelbar beeinflussen. Die Nutzung und Integration von Technologien des maschinellen Lernens birgt zwar beträchtliche Chancen zur Steigerung der Effizienz bestehender Prozesse, ist jedoch auch mit erheblichen Risiken verbunden. Die Notwendigkeit, digitale Technologien nicht nur zu adaptieren, sondern auch effektiv in diese bestehenden Prozesse zu integrieren, stellt insbesondere KMU vor komplexe Herausforderungen. Zudem erfordert der erfolgreiche Transfer und die Anwendung von KI in realen Anwendungsfällen nicht nur technologisches Know-how, sondern auch ein tiefgreifendes Verständnis über die vorherrschende Organisation und Unternehmenskultur. Um sich diesen Herausforderungen in Transferprojekten zu stellen, verwendet das DASU – Transferzentrum für Digitalisierung, Analytics & Data Science Ulm [DA24] eine allgemein gültige Systematik zur Identifikation möglicher Risiken in KI-Projekten. Der vorliegende Praxisbericht beleuchtet, wie das DASU im Rahmen der

¹ DASU, Olgastraße 94, 89073 Ulm, reinhold.vonschwerin@dasu.digital; Technische Hochschule Ulm, Albert-Einstein-Allee 53-55, 89081 Ulm, reinhold.vonschwerin@thu.de

² DASU, Olgastraße 94, 89073 Ulm, daniel.schaudt@dasu.digital

³ Technische Hochschule Ulm, Albert-Einstein-Allee 53-55, 89081 Ulm, alexander.hafner@thu.de

Entwicklung eines Retrieval-Augmentation Generation (RAG) Systems diese Risiken adressiert.

2 Projektbeschreibung: Retrieval-Augmented Generation Chatbot-System

Das DASU, eine Stiftung bürgerlichen Rechts, unterstützt KMU bei der digitalen Transformation durch gemeinsame Transferprojekte. Eines dieser Projekte ist die Entwicklung eines Retrieval-Augmentation Generation (RAG) Chatbot-Systems, das lokal und ohne Internetanbindung betrieben werden kann. Die Entwicklung dieses Systems erfolgt in Kooperation mit zwei Industriepartnern, wobei das DASU primär für die Konzepterstellung sowie für die wissenschaftlich fundierte (Weiter-)Entwicklung der KI-Komponenten zuständig ist.

Inspiriert wurde das Projekt maßgeblich durch die Etablierung großer Sprachmodell-Anwendungen wie *ChatGPT* der Firma OpenAI [Op24] und der Frage, wie ebendiese Technologie für andere Unternehmen sicher und wertschöpfend eingesetzt werden kann. Abbildung 1 zeigt die webbasierte Oberfläche des Systems, mithilfe derer Anwender mit dem Sprachmodell interagieren können.

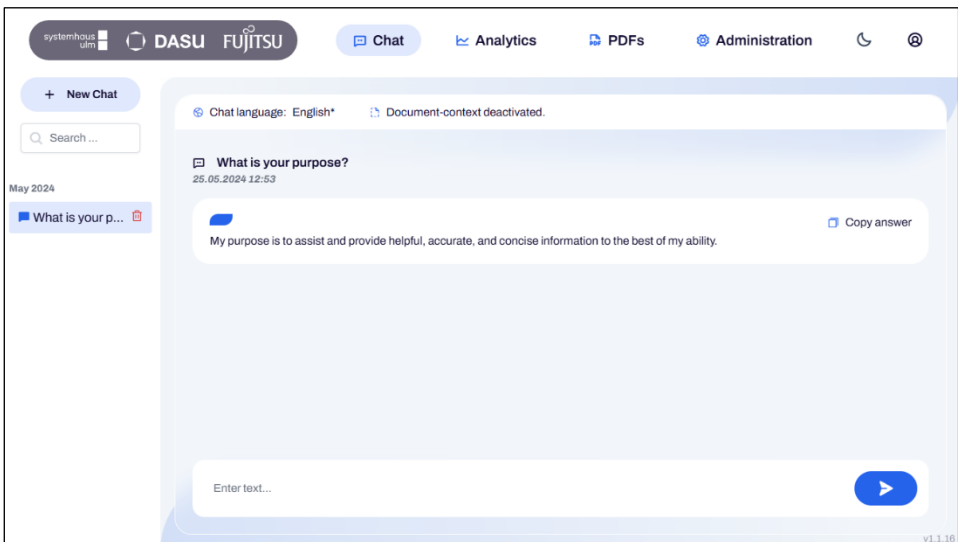


Abb. 1: Grafische Benutzeroberfläche des Chatbot-Systems

Der primäre Anwendungsfall, der zu Beginn durch das Projekt bedient werden soll, ist die Möglichkeit eines optimierten Wissensmanagements. Unternehmen verwalten in der Regel eine Vielzahl strukturierter und unstrukturierter Daten, die in textueller Form

relevante Informationen enthalten können. Das Projektziel besteht in der Bereitstellung eines Systems, welches den Zugriff auf die Gesamtheit der Informationen in natürlicher Sprache ermöglicht, ohne dass diese die Datenhoheit der Unternehmen verlassen.

3 Risiken bei KI-Transferprojekten

Die Implementierung von KI-basierten Anwendungen in Unternehmensprozessen erfordert ein tiefgreifendes Verständnis der vielfältigen Risiken, die während der Implementierung dieser Technologien auftreten können. Das DASU verwendet hierfür ein Gliederungsschema, welches mögliche Risiken in organisatorische und technische Kategorien aufteilt. Abbildung 2 zeigt dieses Schema.

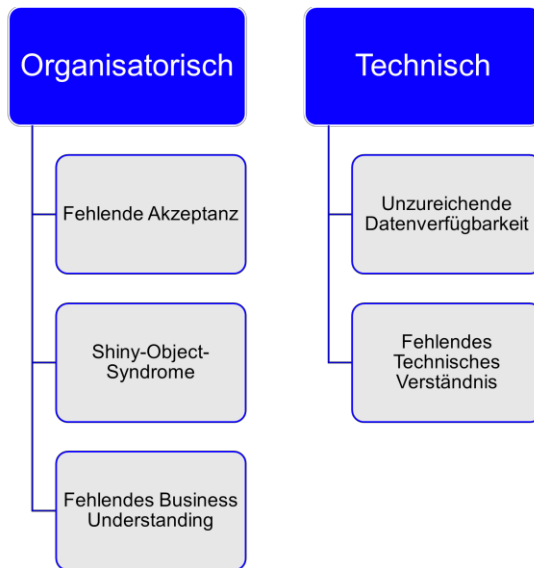


Abb. 2: Ausgewählte Risiken bei der Entwicklung von KI-Projekten

Es sei an dieser Stelle darauf hingewiesen, dass die aufgeführten Risiken weder vollständig noch priorisiert sind. Die Aufstellung dient dazu, ein Bewusstsein für die Herausforderungen zu schaffen, die den Erfolg von KI-Projekten beeinträchtigen können. Die Relevanz der Risiken variiert je nach Transferprojekt und kann zwischen verschiedenen Anwendungsfällen unterschiedlich ausgeprägt sein. Die Identifikation und das Management dieser Risiken erfordern daher eine individuelle Herangehensweise, die die spezifischen Rahmenbedingungen und Anforderungen jedes Unternehmens und Projekts berücksichtigt.

3.1 Fehlende Akzeptanz

Die Akzeptanz von KI-Systemen durch Endanwender stellt eine zentrale organisatorische Herausforderung dar. Oft herrscht ein grundlegendes Misstrauen gegenüber KI-Anwendungen, bedingt durch ein Unverständnis der verwendeten Methoden und Modelle sowie durch die Wahrnehmung der Systeme als undurchschaubare Blackboxes. Diese Wahrnehmung, verstärkt durch eine oft mangelhafte Erklärbarkeit und Dokumentation, erhöht die Unsicherheit und erschwert es Anwendern sowie Entscheidungsträgern, Vertrauen in die Technologie zu entwickeln. Zudem kann die Einführung von KI-Technologien interne Widerstände hervorrufen, da Mitarbeiter befürchten, ihre Arbeitsplätze könnten gefährdet oder ihre Fähigkeiten entwertet werden. Solche Ängste können die Bereitschaft zur Nutzung von KI erheblich mindern.

Herangehensweise im Projekt:

Die Ergebnisse von Gesprächen mit potenziellen Endanwendern zeigen, dass die Einführung eines Chatbot-Systems für optimiertes Wissensmanagement nicht unmittelbar zu Befürchtungen bezüglich Arbeitsplatzverlust führt. Obwohl viele Nutzer bereits Erfahrungen mit großen Sprachmodellen haben, bleibt die Skepsis gegenüber den Antworten des Chatbots, insbesondere bezüglich ihrer Genauigkeit und Herkunft, bestehen. Um diese Bedenken zu mindern und die Akzeptanz zu fördern, hat das DASU ein umfangreiches Schulungskonzept entwickelt. Dieses Konzept zielt darauf ab, verschiedenen Nutzergruppen – von Systemadministratoren über Key-User bis hin zu Standard-Usern – den effektiven Umgang mit dem System beizubringen und die Verbindung zwischen Nutzeranfragen und Antwortqualität zu verdeutlichen.

3.2 Shiny-Object-Syndrome

Das Shiny-Object-Syndrom beschreibt die Anziehungskraft neuer Technologien, die häufig zu deren unüberlegtem Einsatz führt, selbst wenn sie nicht die optimale Lösung für ein Problem darstellen. Unternehmen neigen mitunter dazu, die Fähigkeiten von KI zu überschätzen und setzen sie für Aufgaben ein, für die regelbasierte Lösungen angemessener wären. Diese Tendenz, den technologischen Fortschritt über praktische Problemorientierung zu stellen, kann zu einer Diskrepanz zwischen den tatsächlichen Anforderungen des Unternehmens und den eingesetzten Technologien führen. Der Wunsch, als innovativ wahrgenommen zu werden, verstärkt dieses Risiko zusätzlich.

Herangehensweise im Projekt:

Der zunehmende Bekanntheitsgrad öffentlich zugänglicher Chatbot-Systeme hat zu einer allgemein erhöhten Nachfrage von Unternehmen geführt, die diese Technologie einsetzen möchten. Das DASU reagiert auf diese Entwicklung mit speziellen Workshops, die darauf abzielen, den Bedarf eines Unternehmens an einem Chatbot-System klar zu definieren. Im Fokus dieser Workshops steht der Anwendungsfall des Wissensmanagements, wobei sowohl der praktische Nutzen als auch die Grenzen von RAG-basierten Chatbots

demonstriert werden. Zusätzlich haben Unternehmen die Möglichkeit, das System in einer eigenen Testumgebung mit persönlichen, domänenspezifischen Daten zu testen. Die genannten Maßnahmen zielen darauf ab, die Erwartungen der Unternehmen an die Technologie sowie die geplanten Investitionen realistisch zu bewerten.

3.3 Fehlendes Business Understanding

Ein Mangel an Verständnis der geschäftlichen Anforderungen stellt ein weiteres organisatorisches Risiko beim Einsatz von KI zur Unterstützung bestehender Unternehmensprozesse dar. Eine präzise Definition der Projektziele und -anforderungen ist entscheidend, um effektive KI-Lösungen zu entwickeln. Fehlt ein klares Verständnis der Geschäftsziele, könnten die resultierenden KI-Systeme an den tatsächlichen Bedürfnissen des Unternehmens vorbeigehen. Des Weiteren ist ein tiefgreifendes Verständnis der verfügbaren Daten und deren Bedeutung erforderlich, um die Projektziele zu erreichen. Ohne dieses Wissen besteht die Gefahr, dass unpassende oder fehlerinterpretierte Daten für das Modelltraining verwendet werden, was zu ineffektiven und möglicherweise irreführenden KI-Modellen führt. Dies tritt besonders häufig auf, wenn die Kommunikation zwischen technischen Teams und Geschäftsexperten unzureichend ist.

Herangehensweise im Projekt:

Trotz der technischen Expertise des DASU sind detaillierte Einblicke in die operativen Prozesse und Dokumente verschiedener Unternehmensbereiche begrenzt. Um einer Entwicklung vorzubeugen, die nicht an den tatsächlichen Bedürfnissen potenzieller Endanwender ausgerichtet ist, wurden in Zusammenarbeit mit verschiedenen externen Partnern spezifische Einsatzszenarien eines RAG-basierten Chatbot-Systems entwickelt. Ein Beispiel hierfür ist die Nutzung der Anwendung zur Bereitstellung von Nutzer- und Wartungshandbüchern, wobei die Inhalte dieser Handbücher durch Servicepersonal in natürlicher Sprache abgefragt werden können. Diese Kooperationen erlauben Tests und Bewertungen des Systems unter Einsatz echter Unternehmensdaten und ermöglichen direktes Feedback durch Domänenexperten.

3.4 Unzureichende Datenverfügbarkeit

KI-Entwickler sehen sich häufig mit dem Problem konfrontiert, nicht über ausreichendes Datenvolumen zu verfügen, das zur Entwicklung robuster und effektiver Modelle erforderlich wäre. Ein weiteres technisches Risiko liegt in der Repräsentativität der Daten: Oft reflektieren diese nicht die Realität oder die Variabilität des Zielumfelds, was dazu führen kann, dass Modelle unter Laborbedingungen funktionieren, aber im praktischen Einsatz versagen. Hinzu kommen Fragen der rechtlichen und ethischen Zulässigkeit der Datennutzung sowie der sichere Zugriff auf Daten unter Einhaltung geltender Datenschutzbestimmungen.

Herangehensweise im Projekt:

Das DASU hat sich bei der Entwicklung des Chatbot-Systems gegen das Training oder Fine-Tuning eines großen Sprachmodells entschieden, da die erforderlichen Datenmengen und Rechenkapazitäten aktuell in KI-Transferprojekten mit KMU weder realisierbar noch gerechtfertigt sind. Stattdessen nutzt das Projekt ein RAG-basiertes System mit vortrainierten Modellen. Des Weiteren gewährleistet das DASU den Schutz unternehmerischer Daten, indem das System ausschließlich lokal und ohne Internetanbindung betrieben wird. Diese Maßnahme stellt sicher, dass auch in sensiblen Branchen wie dem Gesundheitswesen die Datenschutz- und Datensicherheitsanforderungen erfüllt werden.

3.5 Fehlendes Technisches Verständnis

In Unternehmen mit geringer Erfahrung im produktiven Einsatz von KI-Technologien stellt ein mangelndes technisches Verständnis ein weiteres, mögliches Risiko dar. Im Unterschied zu klassischen Softwareprojekten erfordern KI-Projekte spezielle Kenntnisse, etwa in statistischen Methoden, um nachhaltigen Erfolg zu gewährleisten. Fehlen diese Spezialkenntnisse, kann die Auswahl unpassender KI-Methoden zu ineffizienten Lösungen führen. Zudem birgt eine unzureichende Planung für die Integration von KI-Systemen in bestehende IT-Strukturen und Prozesse weitere Risiken für eine nachhaltige Anwendungsentwicklung.

Herangehensweise im Projekt:

Die Entwicklung des RAG-basierten Chatbot-Systems erfolgt in Kooperation mit Industriepartnern, die spezifische Fachkompetenzen einbringen, um eine umfassende und effiziente Aufteilung notwendiger Fähigkeiten und Erfahrungen zu gewährleisten. Das DASU-Team verfügt über Expertise in den Bereichen KI, maschinelles Lernen, natürliche Sprachverarbeitung, Datenbanken und Statistik. Die Industriepartner erweitern dieses Know-how um Spezialwissen in den Bereichen Hardware, Nutzererfahrung, Webdesign, Enterprise-Integration, Systemadministration und Softwarequalität. Diese ganzheitliche Herangehensweise gewährleistet den erfolgreichen Transfer von KI-Technologien in die unternehmerische Praxis, indem sie fachliche Lücken schließt und die erfolgreiche Integration in bestehende IT-Strukturen ermöglicht.

Literaturverzeichnis

- [DA24] DASU, Transferzentrum für Digitalisierung, Analytics & Data Science Ulm, www.dasu.digital, Stand: 21.06.2024.
- [Op24] OpenAI, Inc., www.openai.com, Stand: 21.06.2024.