Project Safety and Reflection Report

Laura Kotalczyk[a], Manuel Mühlberger[a], Joana Silva[a], Eduardo Pinto[a] and Nils Harrer[a]

1. Safety of GenAI

1.1. Identified Risks

With the current setup of our service, we see two distinct areas bearing potential risks, namely, data privacy and security. The following paragraphs discuss these aspects in more detail.

1.1.1. Data Privacy Concerns

Since user data is a key asset of our service, data privacy, in particular, GDPR regulations are corner stones of our risk management.

1.1.2. Security Concerns

Since our service builds on a server-client architecture and uses an API to call the Vision Language Model (VLM) for meal nutrient estimation, our application is inherently vulnerable against malicious attacks, such as DDoS attacks or rate limit exceeding. As our service uses credit-based API calls to the VLM for meal logging, rate limit exceeding would not only result in availability problems, but also cause financial damage, if not properly handled.

1.2. Risk Mitigations

- output guardrails
- data privacy: “self-hosted” stuff, proxy, authentication, rate-limiting -> ddos, money abuse

1.2.1. Data Privacy Concerns

1.2.2. Security Concerns

To mitigate potential attack vectors concerning service availability, several mechanisms were implemented.

First of all, we established a user authentication mechanism based on JSON Web Tokens (JWT) and certificates, making sure only authenticated users could interact with our service, i.e. send requests to the VLM for meal nutrient estimation. This approach prevents direct public access to the VLM request endpoint, leveraging the server as a secure gateway for authenticated requests. A per-user rate limit - currently five requests daily - has been integrated into the development phase. This limit can easily be modified when the service is deployed to production.

2. Lessons Learned and Reflections

2.1. Team and Project Management

- aligning expectations
- team management
- architecture was hard
- AIs as black boxes, simpler prompts sometimes work better but there are multiple stellschrauben you can use to improve model results
- Prompting and data is very important, if your data is biased, incomplete, ambigiuous you cannot evaluate a model’s performance properly

*

- integrating GenAi into a consumer app involves lots of data privacy and security concerns

2.2. Architectural Design

2.3. Insights on GenAI and its Applications

... Our findings challenged the assumption that complexity yields superior results, demonstrating that simpler methods often outperform more complex ones in practical scenarios. We observed that high benchmark scores are not always indicative of real-world performance, as the effectiveness of GenAI is heavily context-dependent. Consequently, achieving the optimal configuration requires a systematic, experimental approach, adjusting prompts and parameters to identify the most impactful variables. While established techniques provide a foundation for improvement, the 'black-box' nature of AI as well as the large number of models, and corresponding set screws, makes this a tedious and time-consuming process, requiring significant iteration to reach high-quality results.

-Detail what worked well and what could be improved in future projects. Reflect on insights gained and how this project has influenced your understanding of GenAI and its applications

3. Acknowledgments of GenAI Usage

Generative AI was used in the process of writing this document in terms of improving the vocabulary used.

$$y = \alpha x + \beta \tau \int_0^x dx \tag{1}$$

where ...

$$x = \int_0^x dx \tag{2a}$$

$$(uv)' = u'v + v'u \tag{2b}$$

Eq. (2a) is a simple integral, while Eq. (2b) is the derivative of a product of two functions. These equations are grouped in Eq. (2).

3.1. Features

3.1.1. Table

Below is Table 1.

Table 1: Example

Header 1	Header 2	Header 3
Row 1	12.0	92.1
Row 2	16.6	104

3.1.2. Figures

Below is Fig. 1.

Figure 1: Typst logo - Credit: @fenjalien

3.1.3. Subfigures

Below are Figs. 2a and 2b, which are part of Fig. 2.

(a) (b)

Figure 2: (a) Left image and (b) Right image

A. Appendix A

A.1. Figures

In A.1

Figure A.1: Books cover

A.2. Subfigures

Below are A.2a and A.2b, which are part of A.2.

(a)

(b)

Figure A.2: (a) Left image and (b) Right image

A.3. Tables

In A.1

Table A.1: Example

Header 1	Header 2	Header 3
Row 1	12.0	92.1
Row 2	16.6	104

A.4. Equations

In (A.1)

$$y = f(x) \tag{A.1}$$

$$y = g(x)$$

$$y = f(x) \tag{A.2a}$$

$$y = g(x) \tag{A.2b}$$

References