Privacy-Focused Raspberry Pi-based AI Assistant Leveraging On-Device Machine Learning

Nithun Selva, Clio Zhu

Abstract

With the recent advancements in artificial intelligence and machine learning, personal digital assistants are becoming more mainstream. However, these often lack a personalized touch and raise substantial privacy and ethical concerns. Our project explores developing a private and intelligent AI assistant powered by a Raspberry Pi 5. This assistant is designed to address the growing discomfort in human-robot interactions and the ethical dilemmas arising from rapid technological advancements.

Our primary goals include: Privacy-Centric Design: Employs state-of-the-art on-device machine learning to ensure user data remains private and secure. This means no internet connection is necessary, as everything is run locally. Multifunctional Capabilities: Supports translation, multilingual chatting, and image generation using locally run pre-trained large language models. User-Friendly and Intuitive: Prioritizes ease of use without compromising functionality, offering a secure and personalized user experience.

1 Introduction

With the recent advancements in artificial intelligence and machine learning, personal digital assistants are becoming more mainstream. However, these often lack a personalized touch and raise substantial privacy and ethical concerns. Our project explores developing a private and intelligent AI assistant powered by a Raspberry Pi 5. This assistant is designed to address the growing discomfort in human-robot interactions and the ethical dilemmas arising from rapid technological advancements.

Our primary goals include: Privacy-Centric Design: Employs state-of-the-art on-device machine learning to ensure user data remains private and secure. This means no internet connection is necessary, as everything is run locally. Multifunctional Capabilities: Supports translation, multilingual chatting, and image generation using locally run pre-trained large language models. User-Friendly and Intuitive: Prioritizes ease of use without compromising functionality, offering a secure and personalized user experience.

1.1 Background

Initial Surveys

As the focus of our project is deeply rooted in understanding and addressing user needs, we initiated our efforts by conducting a comprehensive survey. This survey was designed to gather detailed insights into how potential users interact with and perceive current AI technologies.

1.2 Architecture

This project is programmed to be as modular as possible, both in the hardware and software. Each model is a self-contained class, which makes it quite easy to test different models. We use a Raspberry Pi 5 with a 5" round touchscreen and a microphone in a customized 3D-printed enclosure. The user interface is designed to have minimal UI elements to enhance ease of use.

Our testing phase is comprehensive, evaluating the assistant's performance in various scenarios to ensure that privacy, ease of use, accuracy, and user satisfaction are all up to our high standards. We conduct iterative tests to fine-tune the device based on user feedback and performance data, continuously refining our system to meet the needs of our users better.

As the Pi doesn't have native hardware for accelerating ML workloads, we use a workstation in Davis with an RTX 4090 communicating with the Raspberry Pi to process tasks. This approach allowed us to enhance performance without compromising data privacy/integrity.

Our framework is designed around the following advanced AI models: OpenAI Whisper: transcribing audio inputs into text, recognizing the language, and translating it when necessary. Google Gemma (7B): classifies inputs to determine whether they are for image generation, translation, or chat. We used few-shot prompting to improve predictions. Mistral (7B): Generates chat/text prompt outputs. Meta NLLM: For language translations. Stable Diffusion XL: For image generation tasks.

Figure 1: Picture of devicet.

- One
- Two
- There

1. One
2. Two
3. There

Item 1: Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

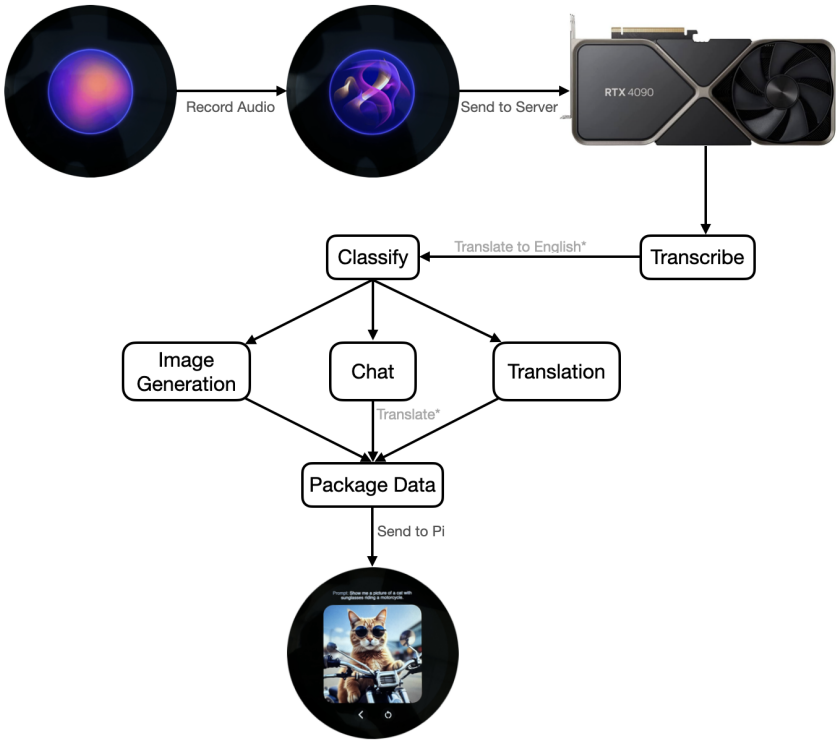

Figure 2: How the server works.

Item 2: Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Item 3: Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

The correlation analysis of user satisfaction metrics underscores the importance of the structure of a response, with a significant correlation, highlighting that users value clear and logical answers the most. Speech recognition accuracy and response time also affect satisfaction, indicating that effective communication and speed are key to a positive user experience. Other features like image generation, though beneficial, are less critical to overall satisfaction.

2 Results

User Experience Enhancements: Users appreciated the quick responsiveness and user-friendly interface of the assistant. Improvements could include reducing distractions from background noise and updating the database more frequently. Feature Additions: Several suggestions for new features were mentioned, such as better handling of multilingual interactions, more basic informational queries, and improvements in image generation capabilities, particularly

concerning copyright issues. Future improvements could include fine tuning the models (particularly the classifier), as we are currently only running pre-trained models. Privacy and Trust: Given the focus on privacy it might be beneficial to include more explicit information or features that reassure users about how their data is being handled and protected.

Acknowledgements

We want to thank Prof. Ying Li for her invaluable feedback and her guidance throughout this project.
We would also like to thank MuleWorks for help with 3D printing the enclosure for our device.

References

[1] Shin, Jong-Gyu, Ga-Young Choi, Han-Jeong Hwang, and Sang-Ho Kim (2021), "*Evaluation of Emotional Satisfaction Using Questionnaires in Voice-Based Human-AI Interaction*," Applied Sciences 11, no. 4: 1920. https://doi.org/10.3390/app11041920

[2] Carmody, J., Shringarpure, S. and Van de Venter, G. (2021), "*AI and privacy concerns: a smart meter case study*," Journal of Information, Communication and Ethics in Society, Vol. 19 No. 4, pp. 492–505. https://doi.org/10.1108/JICES-04-2021-0042