

Florida International University
Knight Foundation School of Computing and Information Sciences

Software Engineering Focus

Final Deliverable

Customizing Cybersecurity Reports Using ChatGPT

Team Members: Pablo Hurtado, Javier Salgueiro, Carlos Pedroso

Product Owner(s): Masoud Sadjadi

Instructor: Masoud Sadjadi

The MIT License (MIT)
Copyright (c) 2016 Florida International University

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Abstract

This project encapsulates a comprehensive journey in integrating and enhancing OpenAI's GPT technology within a suite of applications, executed over a series of well-defined sprints. Each sprint was strategically planned with specific user stories, reflecting a progression from foundational learning to advanced application development.

Initially, the project focused on foundational aspects, including completing Nextcloud's App development tutorial and exploring ChatGPT's integration and API. This phase set the groundwork for subsequent technical advancements. The middle sprints concentrated on deeper integration, understanding OpenAI and LocalAI in the local cloud, and reviewing user feedback on existing integrations. A significant breakthrough was achieved with the development of a custom app featuring a smart picker for ChatGPT prompts, pushing the boundaries of AI application in user interfaces.

The project then progressed to more sophisticated endeavors, enriching report generation capabilities with GPT technology. This included integrating GPT-generated content into various report types and enhancing the overall user experience by enabling report customization and generating downloadable documents. Additionally, capabilities for editing report images were introduced, further enhancing the functionality.

In the final stages, the focus shifted to refining individual features, creating comprehensive video introductions, demos, and a detailed presentation of the project's journey and challenges. The culmination of the project was marked by the preparation of a poster and demos, effectively summarizing the evolution and achievements of the project.

This journey not only showcases the technical advancements in AI integration but also underscores a methodical and adaptive project management approach. The project's evolution from basic API connections to developing sophisticated, AI-enhanced features illustrates a successful blend of technology and strategy in software development.

Table of Contents

INTRODUCTION	5
CURRENT SYSTEM	5
PURPOSE OF NEW SYSTEM	5
USER STORIES	
IMPLEMENTED USER STORIES	7
PENDING USER STORIES	10
PROJECT PLAN	
HARDWARE AND SOFTWARE RESOURCES	12
SPRINTS PLAN	
.....	13
<i>Sprint 1</i>	
.....	13
<i>Sprint 2</i>	
.....	13
<i>Sprint 3</i>	
.....	14
<i>Sprint 4</i>	
.....	15
<i>Sprint 5</i>	
.....	16
<i>Sprint 6</i>	
.....	17
<i>Sprint 7</i>	
.....	18
SYSTEM DESIGN	
ARCHITECTURAL PATTERNS	20

SYSTEM AND SUBSYSTEM DECOMPOSITION	21
DEPLOYMENT DIAGRAM	22
DESIGN PATTERNS	22
...	22
SYSTEM VALIDATION	23
GLOSSARY	37
APPENDIX	38
APPENDIX A - UML DIAGRAMS	38
<i>Static UML Diagrams</i>	38
<i>Dynamic UML Diagrams</i>	40
APPENDIX B - USER INTERFACE DESIGN	52
APPENDIX C - SPRINT REVIEW REPORTS	69
APPENDIX D - USER MANUALS, INSTALLATION/MAINTENANCE DOCUMENT, SHORTCOMINGS/WISHLIST DOCUMENT AND OTHER DOCUMENTS	74
REFERENCES	80

INTRODUCTION

This project embarked on an innovative journey to integrate and enhance OpenAI's GPT technology within a range of applications. Set across a series of meticulously planned sprints, the endeavor aimed to explore the vast potential of AI in practical applications. Initially grounded in fundamental learning, the project focused on understanding and exploring ChatGPT's integration and API, establishing a robust foundation for future development. This phase was pivotal in laying the groundwork, enabling the team to delve into more advanced aspects of AI technology.

As the project progressed, it transitioned from basic explorations to complex implementations, involving the development of custom applications with smart ChatGPT prompts and enriching report generation capabilities. This shift marked a significant evolution in the project's scope, emphasizing not only the technical integration of AI but also a strong commitment to enhancing user experience and functionality. The culmination of these efforts was a series of demonstrations and a comprehensive documentation of the journey, showcasing the successful blend of AI technology with strategic project management and innovative application development.

Current System

The current system relies solely on Nextcloud, a widely adopted open-source file synchronization and sharing platform. Nextcloud serves as the core foundation upon which our innovative application will be built. Our approach involves leveraging Nextcloud's existing capabilities to create a seamless integration, thereby expanding and enhancing the platform's functionality. By harnessing Nextcloud's robust infrastructure and user-friendly interface, we aim to offer users an improved and unified experience within the Nextcloud ecosystem. This integration will transform Nextcloud into a versatile tool, capable of catering to a broader range of user needs, including enhanced productivity, streamlined data management, and heightened data security. Leveraging Nextcloud as our starting point ensures a solid foundation for our application, guaranteeing reliability and scalability in modern software environments.

Purpose of New System

The primary purpose of the new system is to seamlessly integrate and enhance OpenAI's GPT technology within various applications. This system aims to revolutionize how we interact with AI in software applications, specifically focusing on enriching cybersecurity reports. By incorporating advanced AI functionalities, such as ChatGPT prompts and smart pickers, the system offers enriched report generation capabilities, customizable user experiences, and enhanced report editing features. This integration not only demonstrates the technical prowess of AI but also underscores our commitment to improving usability and functionality. The system is designed to cater to the evolving needs of modern software environments, where AI can significantly augment efficiency and user engagement.

USER STORIES

The following section provides the detailed user stories that were implemented in this iteration of the Customizing Cybersecurity Reports Using ChatGPT project. These user stories served as the basis for the implementation of the project's features. This section also shows the user stories that are to be considered for future development.

Implemented User Stories

Throughout the project, the following user stories were methodically implemented, demonstrating a strategic progression in integrating and enhancing AI technology:

1. **Learning and Exploratory Phase:**
 - Complete Nextcloud's App development tutorial.
 - Explore existing ChatGPT integration and API.
2. **Integration and Understanding Phase:**
 - Install and understand OpenAI and LocalAI integration in the local cloud.
 - Review feedback on existing integrations.
3. **Custom Application Development:**
 - Develop a custom app with a smart picker for ChatGPT prompts.
 - Ideate apps utilizing OpenAI options through the smart picker.
4. **Report Enrichment and Customization:**
 - Enrich various report types using GPT.
 - Integrate GPT-generated content into reports and regenerate them for download.
5. **Enhancement of Functionality:**
 - Generate downloadable documents from reports/summaries.
 - Add editing capabilities for report images.
6. **Feature Refinement and Presentation:**
 - Enhance individual features.
 - Create videos, demos, and presentations detailing project challenges.
7. **Documentation and Showcase:**
 - Prepare a poster and demos summarizing the project's evolution and achievements.

PROJECT PLAN

Our project plan was meticulously designed to progressively integrate and enhance OpenAI's GPT technology within our application. We embarked on this journey with a series of strategically planned sprints, each focused on specific objectives and deliverables. The initial sprint laid the groundwork, focusing on learning essential technologies and exploring ChatGPT integration. Subsequent sprints built on this foundation, with efforts dedicated to enhancing OpenAI and LocalAI integrations, understanding API intricacies, and developing custom applications. A significant portion of the project was devoted to refining report generation capabilities, enriching user experience, and addressing technical challenges in API integration and image generation. The concluding sprints were pivotal in synthesizing our learnings and showcasing the project's evolution through detailed documentation and demonstrations. This structured yet flexible approach enabled us to navigate a spectrum of challenges, leading to the successful development of sophisticated, AI-enhanced features in our applications.

Sprints Plan

Sprint 1

In Sprint 1, our team, consisting of **Pablo Hurtado, Carlos Pedroso, and Javier Salgueiro**, successfully embarked on our project's initial phase, demonstrating effective planning and execution. The sprint commenced with a planning meeting where we estimated our team velocity at 30 and collectively decided to focus on three user stories: completing Nextcloud's App development tutorial, exploring existing ChatGPT integration, and investigating the ChatGPT API. The team dedicated itself to learning PHP, Javascript, and CSS, and made significant progress in understanding the integration methods of Nextcloud and ChatGPT.

Our retrospective meeting revealed our accurate velocity and story point estimation and adherence to work schedules. We noted the need for improved communication with the Product Owner and identifying more impactful enhancements for Nextcloud in future sprints. The sprint review meeting concluded with the acceptance of the first two user stories by the Product Owners, while the exploration of the ChatGPT API was deferred to a later sprint. This initial sprint laid a solid foundation for our project, with a focus on technical learning and groundwork for future development.

Sprint 2

In Sprint 2, our team successfully progressed in the project, focusing on key user stories such as installing OpenAI in the local cloud, understanding OpenAI API integration, and reviewing existing integration feedback for improvements. The sprint achievements included the efficient installation of the OpenAI integration and a deeper comprehension of its application interplay. Accurate estimations for team velocity and story points were noted, alongside adherence to schedules.

Key areas of improvement identified involved sourcing a team that would benefit from the integration. We gained insights into API Service Implementation, and the significance of Local Deployment for customization and testing. The sprint also highlighted some technical challenges, like the need for configurable timeout settings, improved error messaging, automated file conversion, transcription, image generation integration, and enhancing user experience with features like prompt history clearance. This phase marked substantial technical advancements, paving the way for more intricate developments in the forthcoming sprints.

Sprint 3

In Sprint 3, our team continued advancing our project with a focus on integrating OpenAI capabilities more seamlessly into our applications. The sprint began with a planning session where we estimated our team velocity at 36 and selected priority user stories. These included creating a custom app that enables a smart picker for ChatGPT prompts in a text box, and brainstorming ideas for apps utilizing OpenAI options through the smart picker. Throughout the sprint, we achieved the installation of the OpenAI integration locally and deepened our understanding of its interactions with other apps. Our retrospective highlighted our accurate estimation of team velocity and user story points, as well as consistent work schedules.

We delved into the specifics of the Smart Picker, an app that serves as an access layer to other app integrations or providers, including the OpenAI app. The integration of the OpenAI app with the Smart Picker showcased how GPT options can be made available in other apps. To utilize OpenAI integration in new apps, we learned that they only need to be integrated with the Smart Picker. The sprint was characterized by significant progress in understanding and integrating AI capabilities, laying the groundwork for more sophisticated applications and usage in future development phases.

Sprint 4

In Sprint 4, our team focused on enhancing report generation capabilities through the integration of OpenAI's GPT technology. The sprint began with a planning session, estimating our team velocity at 32. Key user stories selected for this sprint included:

1. Developing methods to enrich specific types of reports, with one report type per student.
2. Uploading documents and utilizing GPT (or our code) to detect the report type.
3. Providing the ChatGPT with a report template and specific prompts for enrichment.
4. Reintroducing GPT-generated text into the PDF according to the report type.

During the sprint, all team members committed to working on these user stories. The sprint review meeting concluded with the acceptance of all the implemented user stories by the product owners. The team successfully continued the development of the app, focusing on seamlessly integrating GPT technology for improved report customization and generation. This sprint marked a significant step in utilizing AI for practical applications in report processing, setting a strong foundation for future developments.

Sprint 5

In Sprint 5, our team focused on enhancing the functionality and user experience of our project. The key user stories for this sprint included generating downloadable documents from reports/summaries and adding capabilities to edit report images.

Throughout the sprint, all team members committed to these user stories, emphasizing the importance of both functionalities for the project. The sprint retrospective highlighted our accurate estimation of team velocity and user story points, as well as consistent adherence to work schedules. We identified strong communication and project progress as the main positives of this sprint.

The sprint review meeting concluded with all implemented user stories being accepted by the product owners. This sprint saw significant progress in developing features that enhance the practicality and usability of our project, laying a foundation for more advanced functionalities in future sprints.

Sprint 6

In Sprint 6, our team continued to focus on developing individual features, creating video introductions and demos for future improvements, and working on a presentation that describes the project's journey from initial API connection to its current state. This sprint involved addressing challenges such as API character limits, the limitations of Dall-E in generating company logos, and the need for human intervention in image generation due to varying quality outputs. We also highlighted learnings, including the necessity for specific prompts due to ChatGPT's non-deterministic nature.

All team members committed to working on these user stories, emphasizing collaborative efforts. The sprint concluded with a review meeting where all implemented user stories were accepted by the product owners. This phase marked a significant stride in refining our project, showcasing our ability to tackle technical challenges and improve upon our initial concepts, setting the stage for more advanced developments in upcoming sprints.

Sprint 7

In Sprint 7, the focus was on preparing a poster and demos to encapsulate the project's journey and achievements. The team estimated a velocity of 32 and unanimously agreed to work on these deliverables. Throughout the sprint, each team member dedicated approximately three hours daily, primarily focusing on the poster's development.

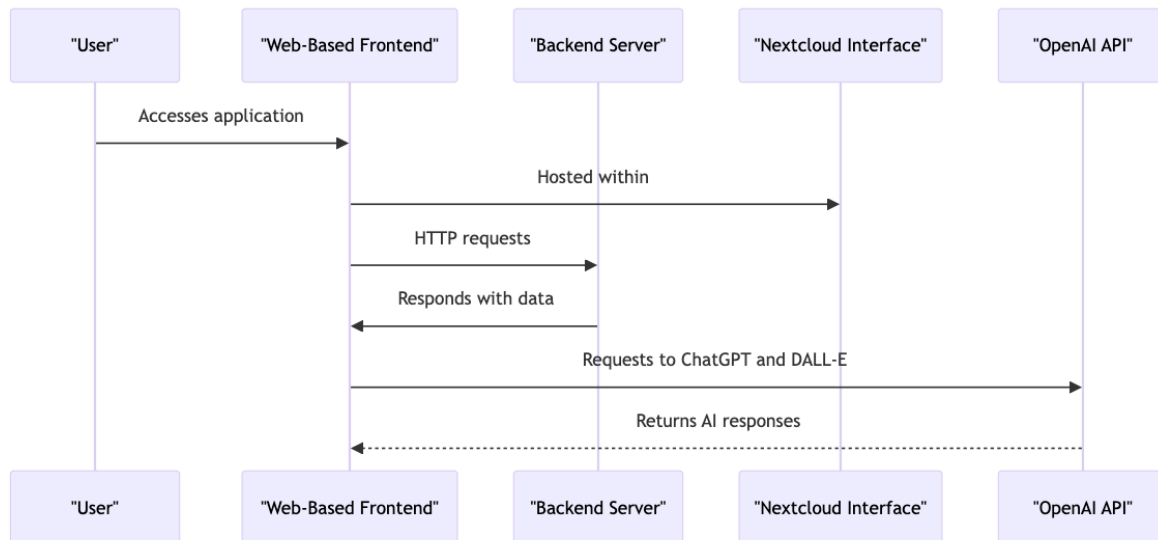
The daily scrum meetings consistently reported progress in the poster's creation, with all team members actively contributing and encountering no significant hurdles. This sprint was pivotal in synthesizing the project's journey, allowing the team to reflect on the challenges and successes experienced throughout the development process. It marked a significant step in documenting and showcasing the project's evolution and its technological advancements.

SYSTEM DESIGN

This section contains information on the design decisions that went into this project. The architecture patterns are outlined and explained. The entire system is shown in a package diagram and the subsystems are explained. Finally, the design patterns used in the project are discussed.

Architectural Patterns

Web-based Frontend



System Decomposition

Web-Based Application System

- This is the primary system, encompassing all components necessary for the application's functionality.

Subsystem Decomposition

Frontend Subsystem

- HTML, CSS, JavaScript: These technologies form the core of the frontend, handling the user interface and user experience.
- Framework/Library Integration: If any frameworks (like React, Angular, Vue) or libraries are used, they are part of this subsystem.

Backend Subsystem

- Server: Manages backend logic, database interactions, and API requests.
- Database: Stores and retrieves data as needed by the application.
- API Integration: Handles communication with external APIs, like OpenAI's ChatGPT and DALL-E.

Nextcloud Integration Subsystem

- Hosting Environment: The part of the system where the frontend is hosted.
- Nextcloud APIs: Interfaces for integrating with Nextcloud features, such as file storage, user management, etc.

OpenAI API Subsystem

- ChatGPT API: For text-based interactions and responses.
- DALL-E API: For generating images based on textual descriptions.

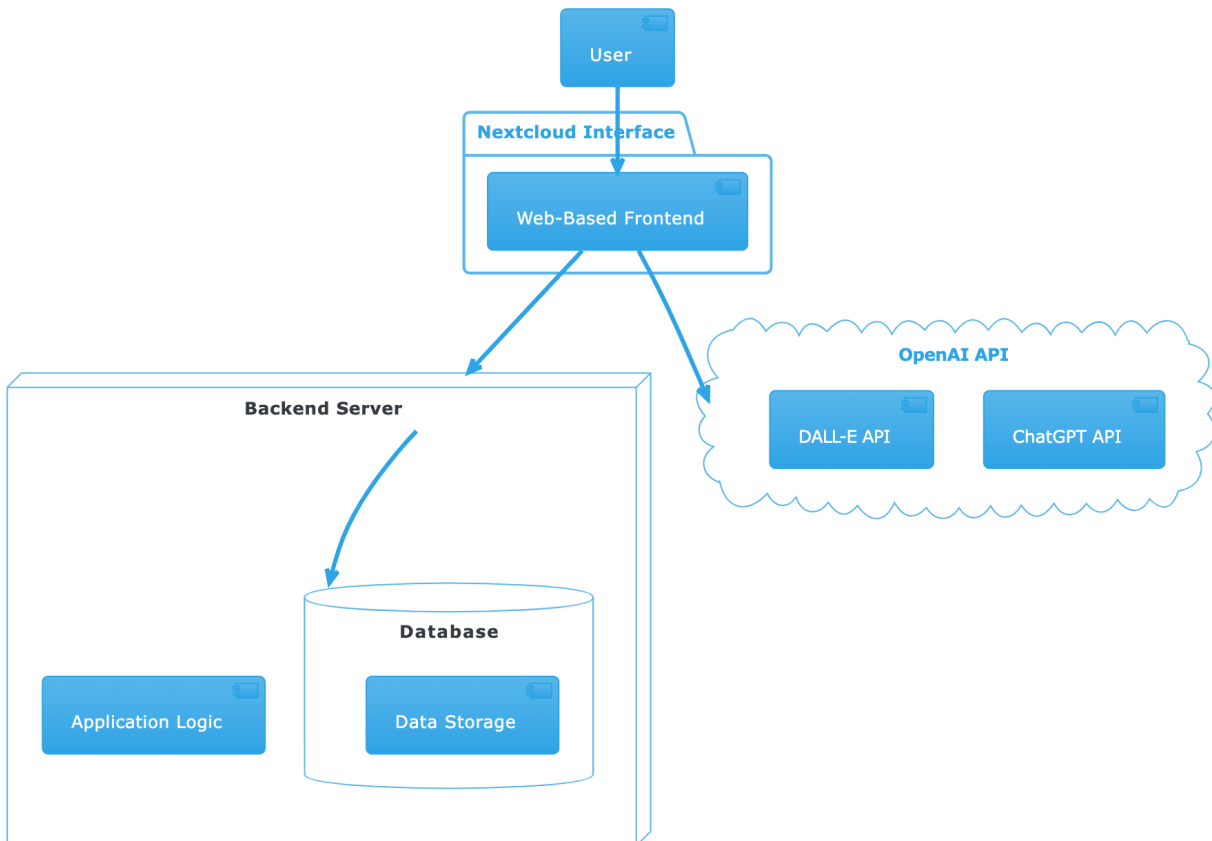
Network and Communication Subsystem

- HTTP/S Requests: Manages the requests and responses between the frontend, backend, and external APIs.
- Security and Authentication: Ensures secure data transmission and verifies user identities.

User Interface Subsystem

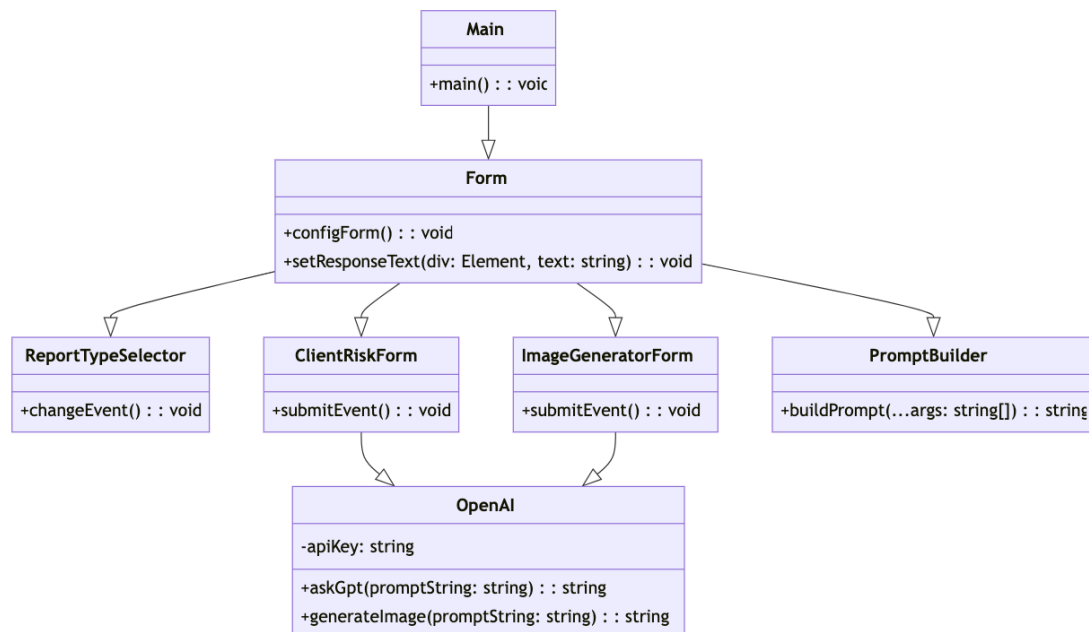
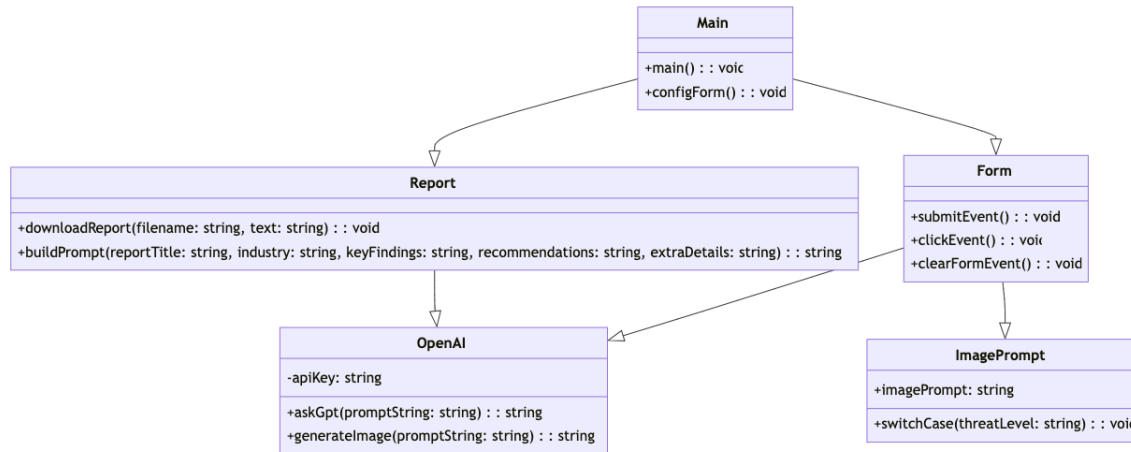
- Interactive Elements: Buttons, forms, and other interactive components.
- Visual Design: Layouts, color schemes, and overall aesthetics.
- Accessibility Features: Ensures the application is usable by people with various disabilities.

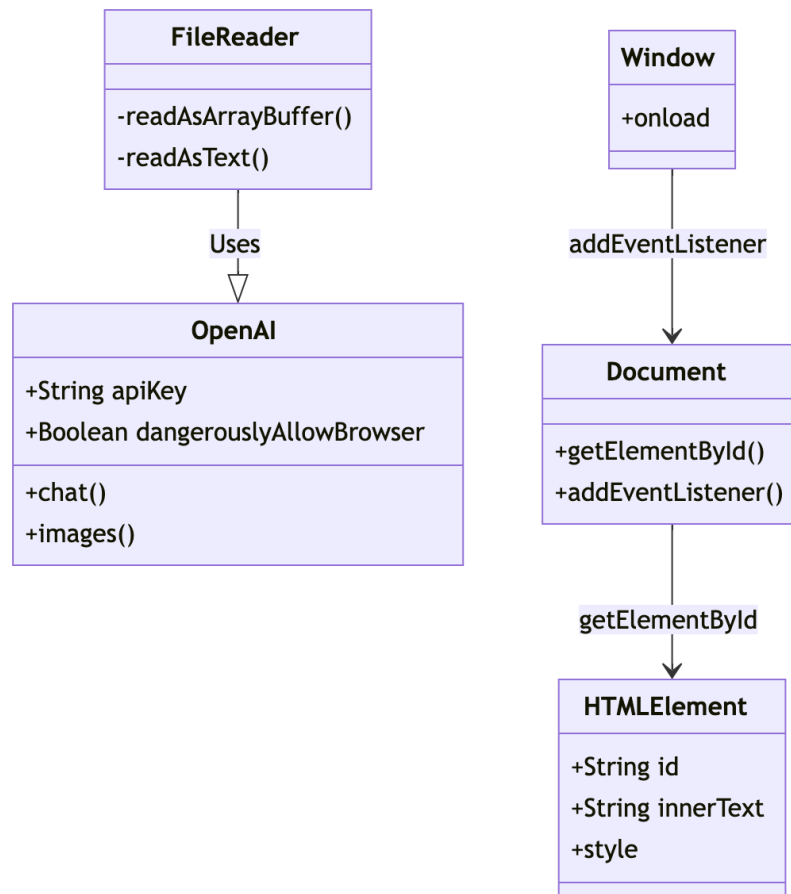
Deployment Diagram



SYSTEM VALIDATION

The system validation for our project involved a comprehensive series of tests and evaluations conducted over the course of the development sprints. Validation efforts included the successful installation and functioning of OpenAI and LocalAI integrations, rigorous testing of custom application features, and ensuring the seamless generation and customization of reports using GPT technology. User story acceptance by product owners at the end of each sprint served as a key validation metric. Additionally, the system underwent usability tests to ensure an intuitive user experience, especially concerning new features like the smart picker and report editing tools. The validation process also involved addressing technical challenges and refining features based on feedback, ensuring that the system met its intended goals effectively and efficiently.

APPENDIX**Appendix A - UML Diagrams**



Appendix B - User Interface Design

Appendix C - Sprint Review Reports

Sprint Review 1 Meeting Minutes

Date

Page 18 of 21

Attendees: Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Start time: 5:00 pm

End time: 5:30 pm

After a show and tell presentation, the implementation of the following user stories were accepted by the product owners: All.

- User Story 1: Complete Nextcloud's App development [tutorial](#).
- User Story 2: Explore existing ChatGPT integration.

The following ones were rejected and moved back to the product backlog to be assigned to a future sprint at a future Spring Planning meeting.

User Story 3: Explore ChatGPT API.

Sprint Review 2 Meeting Minutes

Attendees: Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Start time: 5:00 pm

End time: 5:30 pm

After a show and tell presentation, the implementation of the following user stories were accepted by the product owners:

- All.

The following ones were rejected and moved back to the product backlog to be assigned to a future sprint at a future Spring Planning meeting.

- N/A

Sprint Review 3 Meeting Minutes

Attendees: Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Start time: 4:30

End time: 5:00

After a show and tell presentation, the implementation of the following user stories were accepted by the product owners: All.

- Continue working on app

The following ones were rejected and moved back to the product backlog to be assigned to a future sprint at a future Spring Planning meeting.

- None

Sprint Review 4 Meeting Minutes

Attendees: Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Start time: 6:00PM

End time: 6:30PM

After a show and tell presentation, the implementation of the following user stories were accepted by the product owners: All.

- Brainstorm project ideas

The following ones were rejected and moved back to the product backlog to be assigned to a future sprint at a future Spring Planning meeting.

- None

Sprint Review 5 Meeting Minutes

Attendees: Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Start time: 6:30

End time: 7:00

After a show and tell presentation, the implementation of the following user stories were accepted by the product owners: All.

- Continue as planned

The following ones were rejected and moved back to the product backlog to be assigned to a future sprint at a future Spring Planning meeting.

- None

Sprint Review 6 Meeting Minutes

Attendees: Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Start time: 6:30

End time: 7:00

After a show and tell presentation, the implementation of the following user stories were accepted by the product owners: All.

- Continue as planned

The following ones were rejected and moved back to the product backlog to be assigned to a future sprint at a future Spring Planning meeting.

- None