Project Plan and Accomplished Progress for Blitz Chatbot

Project Duration:

Start Date: July 1, 2024

End Date: August 31, 2024

Milestones

Milestone 1 : Planning and Requirements Gathering

Start Date: July 1

End Date: July 7

Objective:

1. Define the project scope, functional, and non-functional requirements.
    - Start Date: July 1
    - End Date: July 3
2. Identify user stories, use cases, and technical constraints.
    - Start Date: July 3
    - End Date: July 5
3. Plan project timeline and allocate resources efficiently.
    - Start Date: July 5
    - End Date: July 6
4. Conduct feasibility analysis for various chatbot frameworks and models.
    - Start Date: July 6
    - End Date: July 7

Accomplishments:

- Clarified project goals and objectives, focusing on developing a multilingual chatbot for library FAQs.
- Defined both functional and non-functional requirements based on user stories and identified use cases.
- Created a requirements document listing key features and system constraints.

Deliverables:

- Requirements document outlining project goals, functional features, non-functional requirements, user stories, and use cases.
- Feasibility analysis report comparing language models and retrieval methods.
- Project plan with a timeline.

Milestone 2 : Design Phase

Start Date: July 8

End Date: July 14

Objective:

1. Develop the system architecture and chatbot interaction design.
    - Start Date: July 8
    - End Date: July 10
2. Select the appropriate language and embedding models based on feasibility analysis.
    - Start Date: July 10
    - End Date: July 11
3. Design a modular architecture for easy maintenance and scalability.
    - Start Date: July 11
    - End Date: July 12
4. Plan for multilingual capabilities and security features (e.g., prompt injection protection).
    - Start Date: July 12
    - End Date: July 14

Accomplishments:

- Created a flowchart outlining the chatbot's interaction process.
- Designed sequence and use case diagrams to visualize interactions between users and the chatbot.
- Evaluated language and embedding model options for chatbot performance, initially considering Mistral 7B.
- Chose RAG for retrieval-based responses to improve reliability in information retrieval.

Deliverables:

- System architecture diagram depicting the chatbot's design.
- Interaction flowchart and sequence diagrams for chatbot-user interactions.
- Design documents detailing selected language models, embedding models, and RAG (Retrieval-Augmented Generation) methodology.
- Security design plan addressing potential vulnerabilities, including prompt injection.

Milestone 3 : Implementation Phase

Start Date: July 15

End Date: August 7

Objective:

1. Develop the core functionalities of the chatbot, including language model integration and real-time response generation.
    - Start Date: July 15
    - End Date: July 25
2. Implement retrieval-augmented generation (RAG) for reliable FAQ responses.
    - Start Date: July 25
    - End Date: August 1
3. Integrate multilingual support for both English and Arabic.
    - Start Date: August 1
    - End Date: August 3
4. Establish user authentication and security measures, including prompt injection protection.
    - Start Date: August 4
    - End Date: August 7

Accomplishments:

- **Language Model Setup:** Initially used Mistral 7B, then transitioned to LLaMA 3.1 for improved performance. Eventually, Aya was adopted for better Arabic query handling.
- **Embedding Models:** Started with Mxbai-Embed-Large, later switched to Nomic Embed for its efficiency.
- **RAG Implementation:** Developed APIs using Ollama, Langchain, and ChromaDB for retrieval-augmented generation then transitioned to Dify.
- **Authentication Integration:** Implemented user authentication features using Google and email/password.
- **Prompt Injection Protection:** integrated Prompt Injection detection APIs.

Deliverables:

- Functional chatbot with multilingual support for English and Arabic.
- Implemented RAG solution using APIs developed with Ollama, LangChain, and ChromaDB (later transitioned to Dify).
- Authentication system with Google sign-in and email/password registration.
- Basic prompt injection detection APIs integrated into the system.

Milestone 4 : Testing Phase

Start Date: August 8

End Date: August 20

Objective:

1. Conduct comprehensive testing, including functional, performance, security, and user acceptance testing.
    - Start Date: August 8
    - End Date: August 15
2. Validate chatbot performance in real-world scenarios (e.g., library FAQs, membership assistance).
    - Start Date: August 15
    - End Date: August 18
3. Ensure that all implemented features meet defined requirements and quality standards.
    - Start Date: August 18
    - End Date: August 20

Accomplishments:

- **Performance Testing:** Ensured response times were under 10 seconds, with peak load times below 15 seconds.
- **Security Testing:** Validated the system's defenses against prompt injection and other vulnerabilities.
- **User Testing:** Conducted usability tests with library staff, collecting feedback for improvements.
- **Functional Testing:** Verified that all features, such as multilingual support, real-time responses, and FAQ handling, met the functional requirements.

Milestone 5 : Documentation and Final Review

Start Date: August 21

End Date: August 31

Objective:

1. Prepare comprehensive documentation covering the entire project lifecycle, including planning, design, implementation, and testing.
    - Start Date: August 21
    - End Date: August 25
2. Review system performance and make final adjustments based on user feedback and test results.
    - Start Date: August 25
    - End Date: August 28
3. Propose recommendations for future improvements and potential integrations.
    - Start Date: August 29
    - End Date: August 31

Accomplishments:

- Prepared detailed documentation covering all aspects of the project, including requirements, design, implementation, and testing.
- Finalized recommendations for future improvements (e.g., exploring larger models, hybrid search integration).

Deliverables:

- Detailed documentation covering requirements, design, implementation, testing procedures, and deployment instructions.
- Finalized user manual for library staff and chatbot administrators.
- Recommendations document for future improvements, such as exploring larger models or integrating hybrid search methods.

Completed Requirements

Requirements:

1. **Multilingual Support:** Implemented for both English and Arabic.
2. **FAQ Handling:** Answered frequent inquiries regarding library services, membership, hours, and facilities.
3. **Real-Time Responses:** Achieved response times of under 10 seconds.
4. **User Authentication:** Integrated Google and email/password authentication.
5. **Security Against Prompt Injection:** Implemented basic protections.
6. **Context Awareness:** Maintained conversational context during sessions.
7. **Membership Assistance:** Assisted with membership inquiries and renewals.

Gantt Chart