

Retrieval-Augmented Generation (RAG) Application

ENTER TEXT:

AIJack is an easy-to-use open-source simulation tool for testing the security of your AI system against hijackers. It provides advanced security techniques like Differential Privacy, Homomorphic Encryption, K-anonymity and Federated Learning to guarantee protection for your AI. With AIJack, you can test and simulate defenses against various attacks such as Poisoning, Model Inversion, Backdoor, and Free-Rider. We support more than 30 state-of-the-art methods. For more information, check our paper and documentation and start securing your AI today with AIJack.

ENTER PDF PATH:

ENTER QUESTION:

what is aijack used for?

SEND

OUTPUT:

AIJack is used for testing the security of Artificial Intelligence (AI) systems against various types of attacks, including: 1. Poisoning: Injecting malicious data into an AI model to manipulate its behavior. 2. Model Inversion: Reconstructing the original training data from a trained AI model. 3. Backdoor: Hiding a backdoor or trap in an AI model that can be exploited by attackers. 4. Free-Rider: Allowing unauthorized access to an AI system without permission. AIJack provides advanced security techniques like: 1. Differential Privacy 2. Homomorphic Encryption 3. K-anonymity 4. Federated Learning to simulate defenses against these attacks and protect AI systems from being hijacked or compromised.

Processing time: 78.31 seconds

Processing time: 78.26 seconds

Name	ID
Antonios Gerges Nageh	20221903971
Youssef Ibrahim Shehata	2103127
Hashem Ahmed Abdel Hafiz	20221445676
Hussein Hesham Ibrahim	20221372791
AbdelRahman Ahmed Fathi	20221441784
AbdelRahman Tarek Zaki	20221442265

Introduction

The advent of large language models (LLMs) like GPT-3 and LLaMA has revolutionized the field of natural language processing (NLP). These models have demonstrated remarkable capabilities in understanding and generating human-like text. However, they are not without limitations. One significant challenge is their reliance on static training data, which can lead to the generation of outdated or unsupported information. To address this, Retrieval-Augmented Generation (RAG) combines LLMs with information retrieval techniques, enhancing the accuracy and relevance of generated responses by integrating external data sources. This report details the development of a RAG-based web application, leveraging the Flask framework, for querying and providing contextually enriched answers.

Objectives

The primary objectives of this project are:

1. **Develop a User-friendly Web Application:** Create an intuitive web interface using Flask to facilitate user interactions with the RAG model.
2. **Integrate PDF Text Extraction:** Enable the application to extract and process text from uploaded PDF files to enhance the retrieval process.
3. **Implement Efficient Retrieval Mechanism:** Utilize advanced embedding and vector store techniques to store and retrieve relevant data efficiently.
4. **Leverage Advanced LLMs:** Use the Ollama LLaMA3 model to generate responses that are both accurate and contextually relevant.
5. **Provide Real-time Feedback:** Display the processing time for user queries, highlighting the efficiency of the system.

Methodology

The project employs a combination of Python libraries, **NLP techniques**, and **web development frameworks** to achieve its objectives. **The key components of the methodology include:**

1. **PDF Text Extraction:**
 - **The PyPDF2 library is employed to extract text from PDF files.** This allows users to upload documents that the system can then parse and utilize as part of the context for generating responses.
2. **Data Loading and Embedding Creation:**
 - **BeautifulSoup, a library for parsing HTML and XML documents,** is used to clean and process the extracted text data.
 - **The Ollama Embeddings model** is utilized to convert the text data into embeddings. These embeddings are then stored in Chroma, a vector store designed for efficient retrieval.
3. **RAG Model Implementation:**

- The RAG model combines the capabilities of retrieval systems and generative models. It retrieves relevant documents from the vector store and uses them as context for the LLM to generate responses.

4. Web Application:

- Flask is used to create the web application, providing routes for the homepage and query submission.
- The homepage route renders an HTML template for user input, while the submit route handles the form data, processes the query, and returns the response.
- The application supports both text input and PDF uploads, with the ability to handle various model parameters, including the weight assigned to the LLM.

User Interface

The user interface is designed to be intuitive and responsive, allowing users to interact with the RAG model seamlessly. **Key features include:**

- **Text Input Area:** Users can input text directly into a large text area for processing.
- **PDF Upload:** An option to upload PDF files, which are then processed to extract text.
- **Query Input:** A text input for users to enter their queries.
- **Model Weight Adjustment:** A numerical input to adjust the weight assigned to the LLM, providing flexibility in response generation.
- **Output Display:** The generated response is displayed in a styled output box, with real-time processing time shown.

The following elements contribute to the user interface:

- **Title and Icon:** A prominent title with an icon to represent the RAG Chatbot.
- **Form Container:** A form container that includes input fields for text, PDF path, question, and model weight.
- **Submit Button:** A submit button to process the query.
- **Output Box:** An output box to display the generated response.
- **Timer:** A timer to show the processing time for the query.

Benefits of RAG

- **Increased Accuracy and Up-to-date Responses:** By incorporating external data sources, RAG models can provide more accurate and timely answers, as they are not limited by the static training data of traditional LLMs.
- **Evidence-based Answers:** The use of verified sources ensures that the responses are based on reliable information, reducing the likelihood of misinformation.
- **Reduced Data Leakage:** Contextual retrieval helps ensure that the responses are based on relevant and appropriate information, minimizing the risk of irrelevant data being included.

Conclusion

This project successfully demonstrates the implementation of a Retrieval-Augmented Generation (RAG) model within a Flask web application. By leveraging advanced embedding techniques and efficient retrieval mechanisms, the application addresses key challenges of traditional LLMs, providing accurate, timely, and contextually relevant responses. The integration of PDF text extraction further enhances the system's capability to process and utilize diverse data sources, making it a robust solution for generating reliable answers.

Future Work

Future enhancements to this project could include:

- **Integration of Additional Data Sources:** Incorporating more sophisticated and diverse data sources for retrieval, such as real-time databases and APIs.
- **Advanced User Authentication:** Implementing advanced user authentication and data privacy measures to ensure secure access and protect sensitive information.
- **Exploration of Alternative LLMs:** Exploring additional LLM models and embedding techniques to further improve performance and response quality.
- **Enhanced User Interface:** Improving the user interface to provide a more seamless and interactive experience, including features like autocomplete for queries and dynamic response updates.
- **Scalability:** Optimizing the application for scalability to handle a larger number of simultaneous users and queries efficiently.

In summary, this project showcases the potential of RAG models in enhancing the capabilities of LLMs, offering a promising approach to generating accurate and relevant responses in various applications.