Retrieval-Augmented Generation with Qdrant and LLM Integration

Overview

This application implements a **Retrieval-Augmented Generation** (**RAG**) system, combining vector similarity search using **Qdrant** with reasoning-based text generation via **Groq's LLaMA model**. The system enables intelligent question answering over uploaded documents using advanced prompting strategies, providing interpretable outputs grounded in retrieved context.

System Architecture

Core Components

- Vector Store: Qdrant is used to store and search semantic vector representations of text chunks.
- **Embedding Model**: The all-MiniLM-L6-v2 model from sentence-transformers is used to generate 384-dimensional sentence embeddings.
- LLM Backend: Groq's hosted version of the meta-llama/llama-4-scout-17b-16e-instruct model is used for answer generation.
- Frontend Interface: Built with Streamlit, allowing interactive document uploads, query input, technique selection, and output display.

Functional Flow

A. Document Processing

1. Supported Formats: .txt, .pdf, .docx

2. Conversion Logic:

- PDFs processed using pdfplumber
- DOCX processed using python-docx
- Files are saved as .txt in a local directory (texts/)

3. Chunking Strategy:

 Token-based chunking with a fixed CHUNK_SIZE of 100 tokens and an OVERLAP of 30 to preserve context between segments.

4. Embedding and Storage:

- Each chunk is embedded using MiniLM and upserted into a Qdrant collection with associated metadata (chunk text and source filename).
- Collection is recreated upon DB rebuild to ensure consistency.

B. Querying and Reasoning

1. User Input:

- Users input natural language questions.
- Users select one or more prompting techniques to guide the LLM's reasoning.

2. Retrieval:

 Top-k (default 5) relevant chunks are retrieved via cosine similarity from Qdrant.

3. Prompt Engineering:

- Context is assembled from retrieved chunks.
- Prompting techniques are translated into specific instructions appended to the query.
- If "MCQ prompting" is selected, an additional structured format for multiple-choice questions is enforced.

4. LLM Interaction:

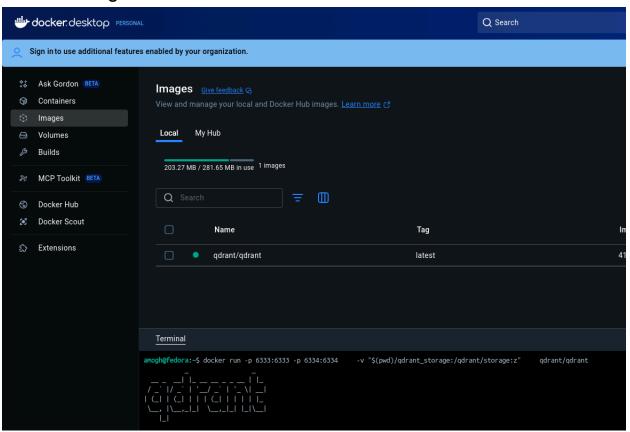
- A structured system/user prompt is sent to Groq's LLaMA model through their API.
- The model responds with either a direct answer or formatted MCQs depending on the prompt.

Prompting Techniques Supported

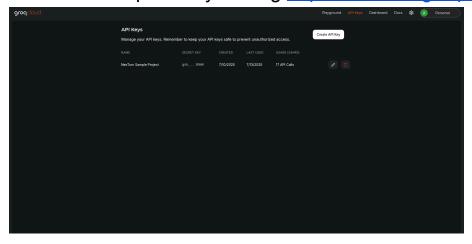
Technique	Description
Chain-of-Thoug hts	Step-by-step reasoning.
Tree-of-Thought s	Branching exploration paths before conclusion.
Role-based prompting	Assumes a relevant persona (e.g., expert, teacher).
ReAct prompting	Combines reasoning and action (e.g., verify, deduce).
Directional Stimulus	Injects guiding hints into context.
Step-Back prompting	Promotes re-evaluation of assumptions.
MCQ prompting	Converts context into MCQs with answer keys.

How to Use it

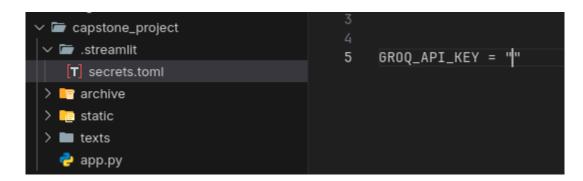
- Pull docker image for vector database by using docker pull qdrant/qdrant
- 2. Run the image



3. Generate Groq API key visiting https://console.groq.com/keys



4. Paste it into .streamlit/secrets.toml

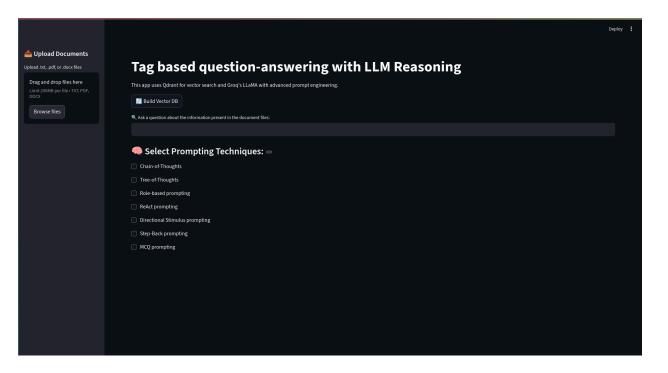


- 5. Run pip install -r requirements.txt to install necessary packages.
- 6. Run the app using streamlit run app.py

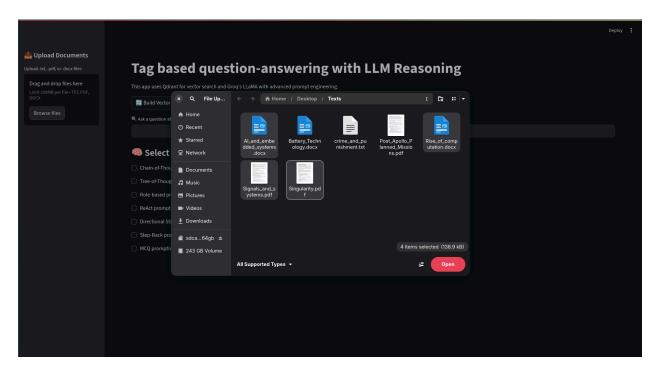
```
venvamogh@fedora:~/Desktop/Programs/capstone_project$ streamlit run app.py
You can now view your Streamlit app in your browser.

Local URL: http://localhost:8501
Network URL: http://172.16.2.25:8501
```

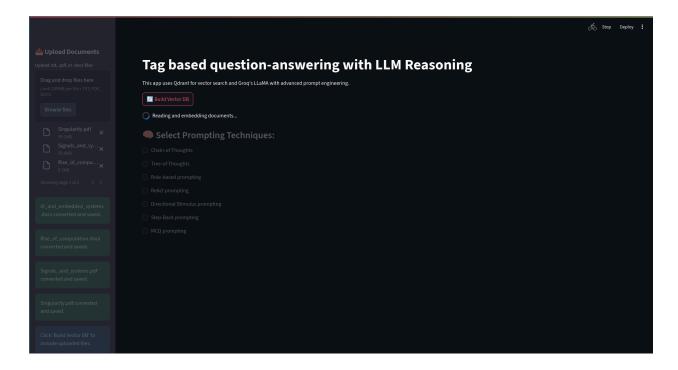
7. Open the browser where the app is running



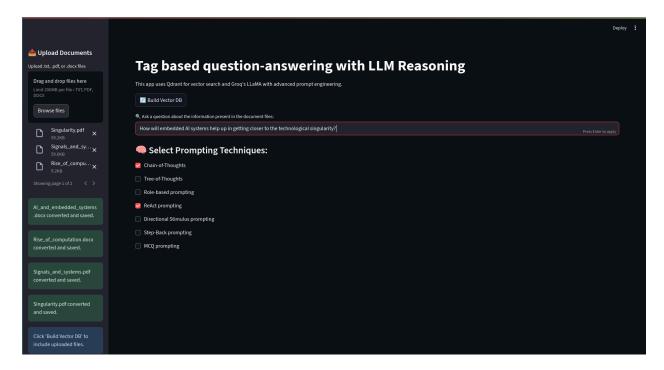
8. Select the files you want to query, the app can take .txt, .pdf and .docx files as input.



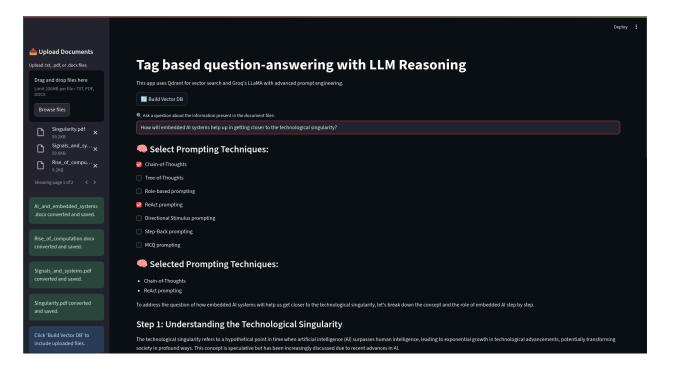
9. Once the files are uploaded, click Build Vector DB to build the vector database

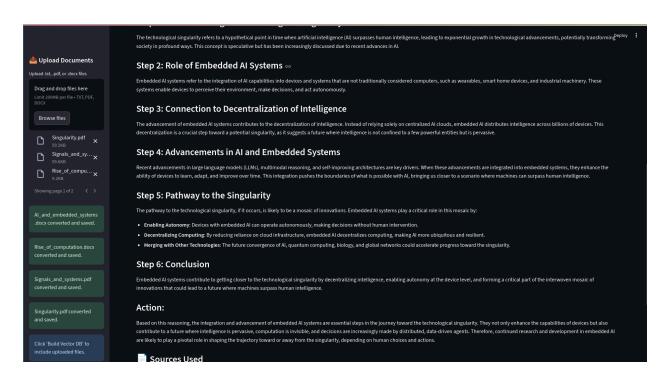


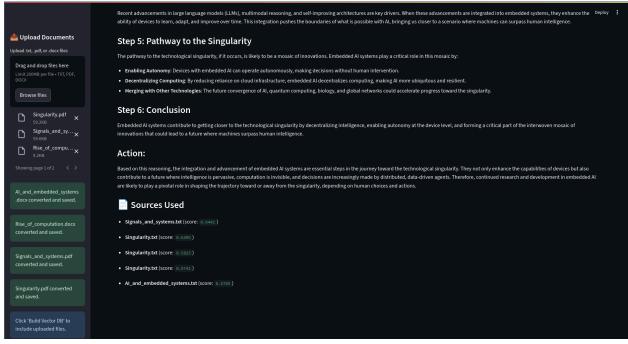
10. Once the vector database is built, select the tags from the list to select the kind of meta-prompt that is to be used to query the texts added and then the query.



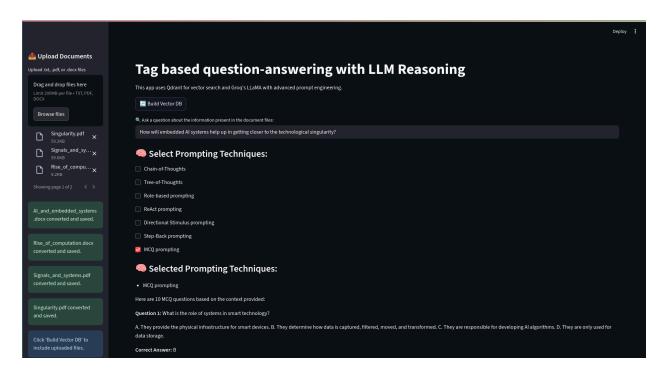
11. Output is generated.

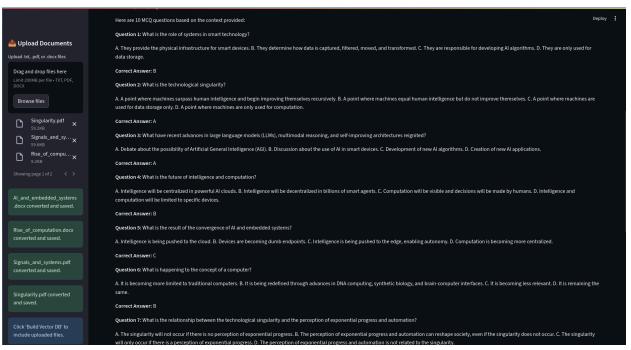


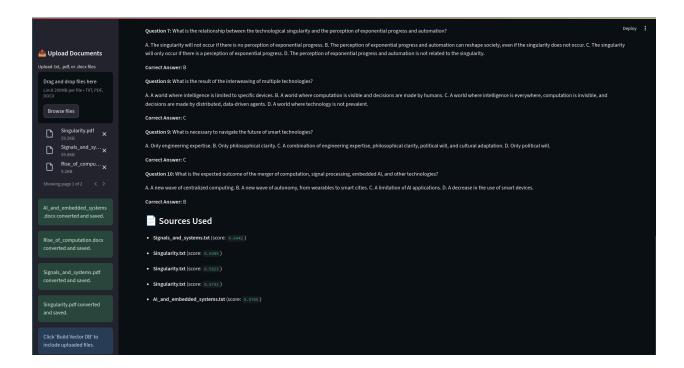




12. There is also a dedicated MCQ mode to generate 10 questions.







Design Strengths

- Modular and Extensible: Clean separation of concerns between chunking, embedding, storage, retrieval, and reasoning.
- Interactive UI: Simple Streamlit interface for experimentation and input customization.
- Advanced Prompting: Supports hybrid reasoning methods to guide LLM output.
- **Multi-format Document Support**: Accepts standard file formats with robust text extraction.

Limitations & Recommendations

Issue	Recommendation
Static Embedding Model	Consider upgrading to a more powerful embedding model like text-embedding-3-small if latency and cost permit.
No persistent state across sessions	Integrate persistent storage or session state to avoid repeated rebuilds.
Basic error handling	Improve API failure transparency (e.g., include status codes, retry logic).
Chunking is token-based, not semantic	Implement sentence-aware or semantic chunking using tools like nltk, spaCy, or langchain.text_splitter.
Prompt is purely template-based	Allow manual editing or preview of final prompt before submission.

Security Considerations

- API Key Management: Relies on st.secrets; ensure .streamlit/secrets.toml is properly secured.
- File Upload Handling: No malicious content scanning—consider sandboxing or filtering file types further.

• **LLM Output Filtering**: No post-processing of LLM output. For production, consider moderation or filtering.

Conclusion

This system demonstrates a practical and flexible implementation of retrieval-augmented generation using a local vector store and hosted LLM. It is well-suited for domain-specific document comprehension, educational tooling, or internal knowledge base querying. Future improvements could include deeper semantic processing, session-based tracking, and richer feedback integration from users.

Amogh K UmeshData Engineering BatchNexTurn Intern 2025