

Project Report – Amit Meena

Project 1: Custom Chatbot Interface for LLaMA and Mistral Models

Objective:

- Build a **custom chatbot UI** where users interact with **LLaMA 2**, **LLaMA 3.2**, and **Mistral** models.

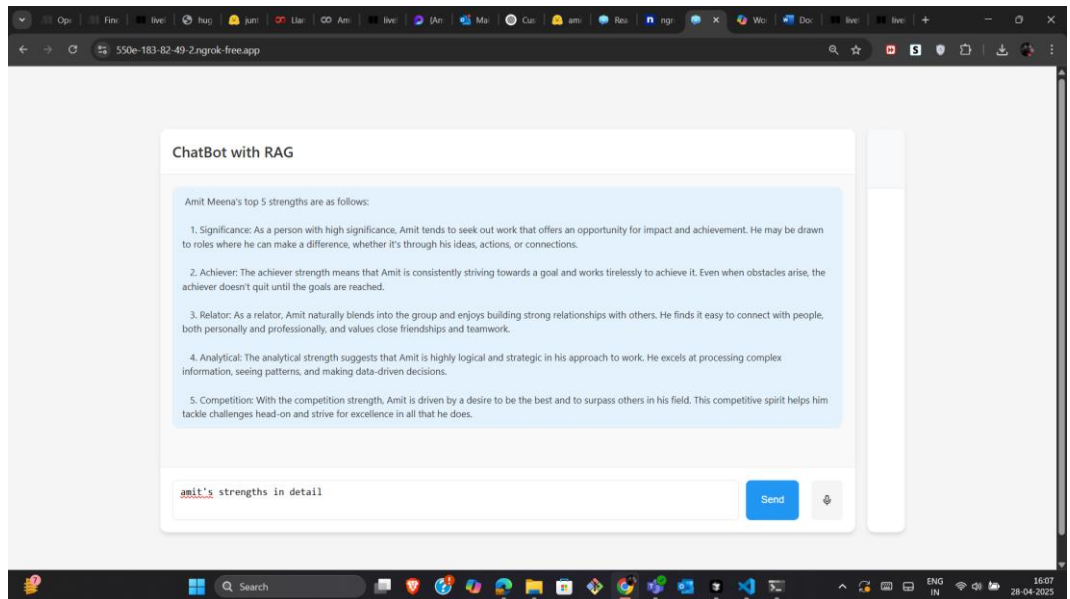
Implementation:

1. **Model Setup:**
 - a. Downloaded and hosted **LLaMA 2**, **LLaMA 3.2**, and **Mistral** models locally.
 - b. Optimized loading and memory management for efficient inference.
2. **Backend (Python):**
 - a. Developed a Flask-based backend API to handle user prompts and generate model responses.
 - b. Integrated an optional retrieval step (RAG) **before** querying the model (detailed in Project 2).
3. **Frontend (React):**
 - a. Built an intuitive chatbot UI in React.
 - b. Features include:
 - i. Real-time conversation flow.
 - ii. Model selection (user can choose between LLaMA 2, LLaMA 3.2, and Mistral).
 - iii. Support for additional retrieved context (RAG responses injected dynamically).
 - iv. API communication through the **Ngrok URL**.
4. **Testing:**
 - a. Validated both direct model responses and RAG-enhanced responses.
 - b. Optimized for low latency and smooth user experience.

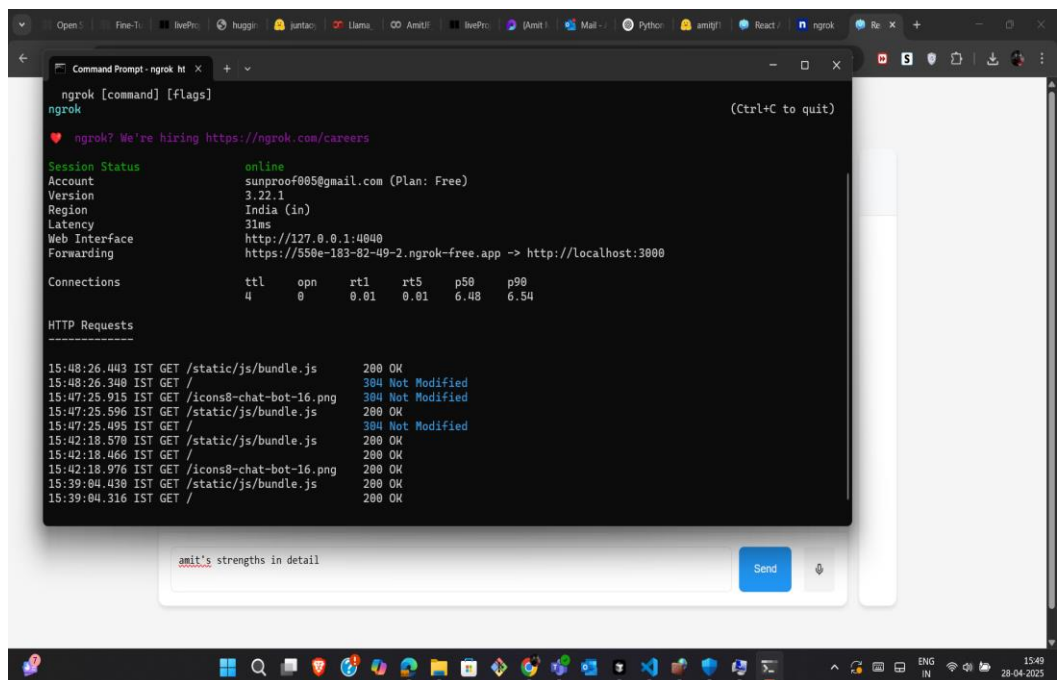
Note: This chatbot is tightly coupled with a **Retrieval-Augmented Generation (RAG)** system for better, context-aware answers (see Project 2).

Screenshots:

a. React Chatbot Interface:



b. Flask API Exposed via Ngrok:



Project 2: Retrieval-Augmented Generation (RAG)

System Integration

Objective:

- Implement **Retrieval-Augmented Generation (RAG)** to improve the accuracy and relevance of model outputs.

Implementation:

1. Vector Database Creation:

- a. Processed large sets of domain-specific documents.
- b. Converted documents into vector embeddings using transformer-based embedding models.
- c. Indexed embeddings into a **FAISS-based** vector database.

2. Retrieval Pipeline:

- a. On receiving a user query:
 - i. Search the vector database for the most relevant documents.
 - ii. Retrieve top-k matches as context snippets.
 - iii. Append these snippets to the user prompt.

3. Response Generation:

- a. The model (LLaMA or Mistral) generates its answer **based on both** the user's query **and** the retrieved context.
- b. This ensures more **informed and accurate** responses, especially for domain-specific or fact-based questions.

4. Integration with Chatbot:

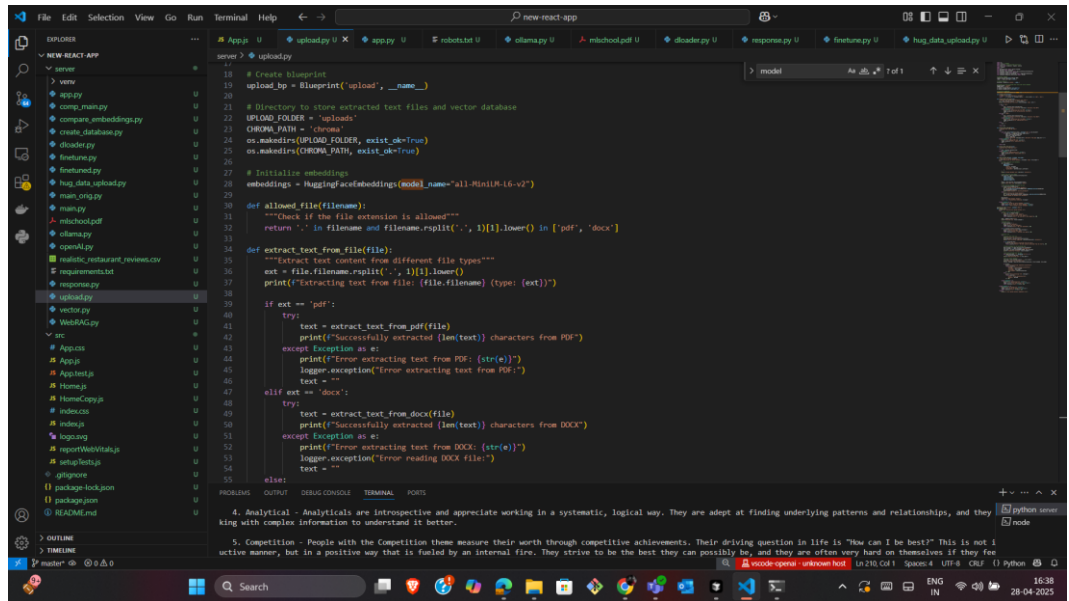
- a. Seamlessly connected the RAG pipeline with the chatbot backend.
- b. User can interact without noticing the retrieval step, but benefits from smarter outputs.

5. Testing:

- a. Compared RAG-enhanced outputs vs standard model outputs.
- b. Found significant improvement in answer relevance and factual correctness.

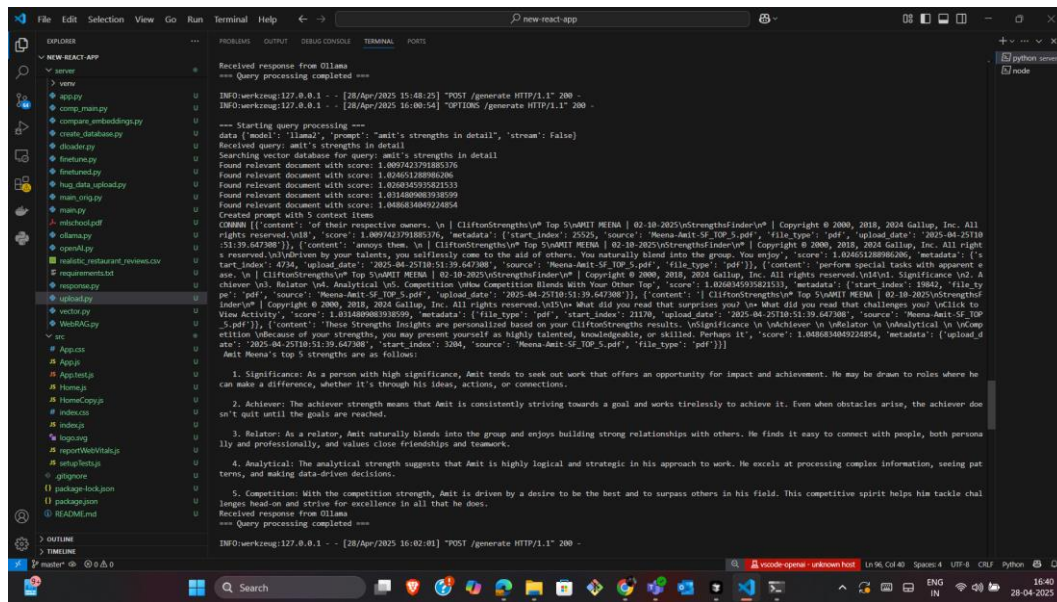
6. Screenshots:

a. *Vector Database Setup (CHROMA DB):*



```
server > upload.py
18 # Create blueprint
19 upload_bp = Blueprint('upload', __name__)
20
21 # Directory to store extracted text files and vector database
22 UPLOAD_FOLDER = 'uploads'
23 CHROMA_PATH = 'chroma'
24 os.makedirs(UPLOAD_FOLDER, exist_ok=True)
25 os.makedirs(CHROMA_PATH, exist_ok=True)
26
27 # Initialize embeddings
28 embeddings = HuggingFaceEmbeddings(model_name="all-MiniLM-L6-v2")
29
30 # Main endpoint
31 @upload_bp.route('/upload', methods=['POST'])
32 def upload():
33     """Check if the file extension is allowed"""
34     return '...'
35
36 def extract_text_from_file(file):
37     """Extract text content from different file types"""
38     ext = file.filename.rsplit('.', 1)[1].lower()
39     print(f"Extracting text from file: {file.filename} (type: {ext})")
40
41     if ext == 'pdf':
42         try:
43             text = extract_text_from_pdf(file)
44             print(f"Successfully extracted {len(text)} characters from PDF")
45         except Exception as e:
46             print(f"Error extracting text from PDF: {str(e)}")
47             logger.exception("Error extracting text from PDF:")
48             text = ""
49     elif ext == 'docx':
50         try:
51             text = extract_text_from_docx(file)
52             print(f"Successfully extracted {len(text)} characters from DOCX")
53         except Exception as e:
54             print(f"Error extracting text from DOCX: {str(e)}")
55             logger.exception("Error reading DOCX file:")
56             text = ""
57     else:
58         text = ""
59
60     return text
61
62 def extract_text_from_pdf(file):
63     """Extract text from PDF file"""
64     pdf_reader = PyPDF2.PdfReader(file)
65     text = ""
66     for page in pdf_reader.pages:
67         text += page.extract_text()
68     return text
69
70 def extract_text_from_docx(file):
71     """Extract text from DOCX file"""
72     doc = Document(file)
73     text = doc.text
74     return text
75
76 def save_to_vector_db(text, filename, file_type):
77     """Save text to vector database"""
78     print(f"Saving text to vector database: {filename} (type: {file_type})")
79
80     # Create a document with metadata
81     doc = Document(
82         page_content=text,
83         metadata={
84             "source": filename,
85             "file_type": file_type,
86             "upload_date": datetime.now().isoformat()
87         }
88     )
89     print(f"Created document with {len(text)} characters")
90
91     # Split the text into chunks
92     text_splitter = RecursiveCharacterTextSplitter(
93         chunk_size=100,
94         chunk_overlap=50,
95         length_function=len,
96         add_start_index=True,
97     )
98     chunks = text_splitter.split_documents([doc])
99     print(f"Split text into {len(chunks)} chunks")
100
101     # Load existing database or create new one
102     if os.path.exists(CHROMA_PATH):
103         print("Loading existing Chroma database")
104         db = Chroma(persist_directory=CHROMA_PATH, embedding_function=embeddings)
105         db.add_documents(chunks)
106         print("Added documents to existing database")
107     else:
108         print("Creating new Chroma database")
109         db = Chroma.from_documents(chunks, embeddings, persist_directory=CHROMA_PATH)
```

b. *Retrieved Context Added to Prompt:*



Project 3: Dataset Creation and Fine-tuning of LLaMA Model

Objective:

- Create a custom dataset.
- Upload it to Hugging Face.
- Fine-tune the LLaMA model to adapt it to specific tasks/domains.

Implementation:

1. Dataset Creation:

- a. Designed a structured dataset (e.g., instruction-response pairs, domain-specific Q&A).
- b. Ensured high data quality with clear formatting (JSONL/CSV).

2. Uploading to Hugging Face:

- a. Uploaded the dataset to my Hugging Face account for accessibility and versioning.

3. Fine-tuning:

- a. Fine-tuned the LLaMA model using the custom dataset.
- b. Techniques used:
 - i. LoRA (Low-Rank Adaptation) for efficient fine-tuning.
 - ii. Hyperparameter tuning (learning rate, batch size, epochs) for optimal results.

4. Results:

- a. Achieved a more specialized LLaMA model that performed better on custom task domains.
- b. Improved coherence, task adherence, and response specificity.

Screenshot - Custom Dataset Example(Hugging Face upload):

The screenshot shows the Hugging Face dataset card for 'amitjf111/first-finetuning-validate-chemistry-questions'. The dataset is licensed under gpl-3.0 and is currently in the 'Dataset card' view. The 'Dataset Viewer' section shows a split of 1 train (933 rows). The 'input' column is a string of length 39, and the 'output' column is a string of length 213. The 'output' column contains JSON objects with a 'valid' key, all set to true. The 'Downloads last month' section shows 0 downloads. The 'Size of downloaded dataset files' is 418 kB, and the 'Size of the auto-converted Parquet files' is 51.2 kB. The 'Number of rows' is 933.

input	output
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }
Determine if the input is a question related to chemical science. If it is, return a JSON object with...	{ 'valid': true }

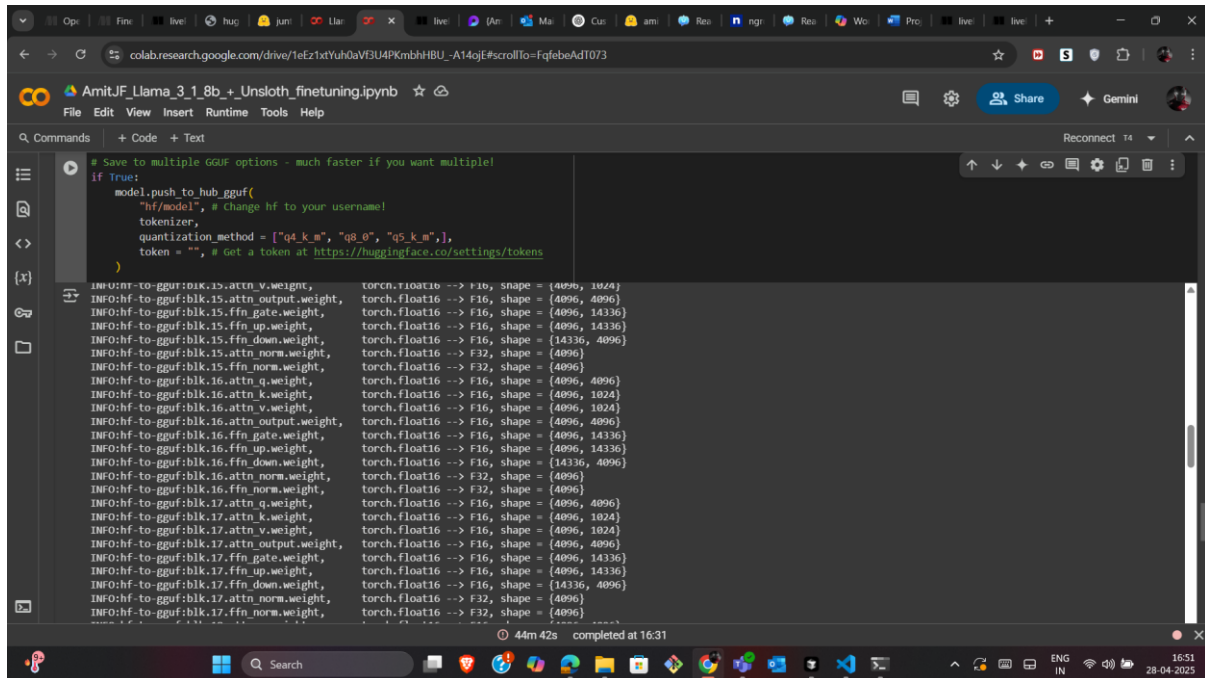
Screenshot – use while finetuning:

The screenshot shows a Google Colab notebook titled 'AmitJF_Llama_3_1_8b + Unsloth finetuning.ipynb'. The code defines a 'formatting_prompts_func' that takes examples of instructions, inputs, and outputs, and returns a list of formatted prompts. The code then loads the dataset from Hugging Face and maps the formatting function to the dataset. The progress bar shows the following status:

Task	Progress	Count	Speed
README.md	100%	925/925	00:00:00.00, 21.9KB/s
finetune.json	100%	418k/418k	00:00:00.00, 5.65MB/s
Generating train split	100%	933/933	00:00:00.00, 7863.48 examples/s
Map	100%	933/933	00:00:00.00, 14011.10 examples/s

The notebook also includes a section for training the model, with instructions on how to use Hugging Face TRL's SFTTrainer and how to set the number of training epochs and maximum steps.

Screenshot - Fine-tuning Logs:



```
# Save to multiple GGUF options - much faster if you want multiple!
if True:
    model.push_to_hub_gguf(
        "hf/model", # Change hf to your username!
        tokenizer,
        quantization_method = ["q4_k_m", "q8_0", "q5_k_m"],
        token = "", # Get a token at https://huggingface.co/settings/tokens
    )

INFO:hf-to-gguf:blk.15.attn.v.weight, torch.float16 --> F16, shape = (4096, 1024)
INFO:hf-to-gguf:blk.15.attn.output.weight, torch.float16 --> F16, shape = (4096, 4096)
INFO:hf-to-gguf:blk.15.ffn_gate.weight, torch.float16 --> F16, shape = (4096, 14336)
INFO:hf-to-gguf:blk.15.ffn_up.weight, torch.float16 --> F16, shape = (4096, 14336)
INFO:hf-to-gguf:blk.15.ffn_down.weight, torch.float16 --> F16, shape = (14336, 4096)
INFO:hf-to-gguf:blk.15.attn_norm.weight, torch.float16 --> F32, shape = (4096)
INFO:hf-to-gguf:blk.15.ffn_norm.weight, torch.float16 --> F32, shape = (4096)
INFO:hf-to-gguf:blk.16.attn.q.weight, torch.float16 --> F16, shape = (4096, 4096)
INFO:hf-to-gguf:blk.16.attn.k.weight, torch.float16 --> F16, shape = (4096, 1024)
INFO:hf-to-gguf:blk.16.attn.v.weight, torch.float16 --> F16, shape = (4096, 1024)
INFO:hf-to-gguf:blk.16.attn.output.weight, torch.float16 --> F16, shape = (4096, 4096)
INFO:hf-to-gguf:blk.16.ffn_gate.weight, torch.float16 --> F16, shape = (4096, 14336)
INFO:hf-to-gguf:blk.16.ffn_up.weight, torch.float16 --> F16, shape = (4096, 14336)
INFO:hf-to-gguf:blk.16.ffn_down.weight, torch.float16 --> F16, shape = (14336, 4096)
INFO:hf-to-gguf:blk.16.attn_norm.weight, torch.float16 --> F32, shape = (4096)
INFO:hf-to-gguf:blk.16.ffn_norm.weight, torch.float16 --> F32, shape = (4096)
INFO:hf-to-gguf:blk.17.attn.q.weight, torch.float16 --> F16, shape = (4096, 4096)
INFO:hf-to-gguf:blk.17.attn.k.weight, torch.float16 --> F16, shape = (4096, 1024)
INFO:hf-to-gguf:blk.17.attn.v.weight, torch.float16 --> F16, shape = (4096, 1024)
INFO:hf-to-gguf:blk.17.attn.output.weight, torch.float16 --> F16, shape = (4096, 4096)
INFO:hf-to-gguf:blk.17.ffn_gate.weight, torch.float16 --> F16, shape = (4096, 14336)
INFO:hf-to-gguf:blk.17.ffn_up.weight, torch.float16 --> F16, shape = (4096, 14336)
INFO:hf-to-gguf:blk.17.ffn_down.weight, torch.float16 --> F16, shape = (14336, 4096)
INFO:hf-to-gguf:blk.17.attn_norm.weight, torch.float16 --> F32, shape = (4096)
INFO:hf-to-gguf:blk.17.ffn_norm.weight, torch.float16 --> F32, shape = (4096)
```

Conclusion

This project series involved end-to-end development: setting up strong foundation models, creating an interactive chatbot, augmenting it with retrieval for smarter responses, and fine-tuning a model for even more targeted performance.

The experience covered key real-world AI production workflows like serving large models, building retrieval pipelines, integrating frontends, and model personalization.