Registered Module No: BUS5001

Individual Assessment:
Robotic Process Automation and Ai in The Cloud

Repo Link : https://github.com/ridutshanv/BUS5001_Assessment3_Chatbot.git

Video Link : 20251113_110702 1.mp4

[Ridutshan Vigneswaran]

[22349743]

Table of Contents

Q1. Build a Chatbot 1
  a) Functionalities Related to Tourism 1
  b) Ethical Considerations for Data Collection 1
  c) Chatbot Flow Design and Implementation 2
  d) Accessibility Considerations 4
  e) Demonstration Video 4
Q2. Evaluating Cloud Security 5
  a) Incident Summary 5
  b) Cloud Components and Deployment Model 5
  c) Preventive Measures and Recommendations 6
Q3. Using Large Language Models 7
  a) Model and Prompt Design 7
  b) Sample Results and Comparison 7
  c) Evaluation and Readiness 9
  d) Creation of Solution on Azure 10
Q4. Evaluating Cloud-Based Technology 12
  a) Key Functionalities Aligned with Academic Activities 12
  b) Demonstration of Functionalities in a Research Scenario 12
  c) Critical Evaluation 17

Q1. Build a Chatbot

a) Functionalities Related to Tourism

The chatbot created by Tourism Australia is a virtual assistant that will increase the interaction with the visitors and automate the information delivery. Five functionalities that were identified as core include:

- City and attraction information- It contains the details of the main attractions of major cities in Australia, including reviews on different attractions, their prices, timing, and the specific position.
- Travel Planning and Itinerary Support - This helps the tourists in constructing their own day plans depending on the interests, time and place.
- Accommodation and Transport Guidance- Suggests the local hotels, restaurants, and means of transport with links to booking when possible.
- Event and Festival Updates- Posts present or future events, concerts and local events schedules and ticket information.
- Emergency and Accessibility Help - Provides fast access to emergency contacts, embassy contacts, and accessibility services to differently disabled tourists.

These features contribute to the automatization of redundant queries and improves the visitor experience with a decrease in the cost of manual support.

b) Ethical Considerations for Data Collection

The interactions between the chatbots of Tourism Australia provide good behavioral and preference information. It is necessary to handle this information in an ethical manner. It is suggested that the following measures should be taken:

- Transparency of Data: Educate people that the conversations can be recorded to improve their analytics and the services.
- Consent and Opt-out: Ask users to give their consent before collecting their personal data and give them an option to refuse the sharing of data.
- Anonymization: Removal of identifiable information during storing of chat logs.
- Secure Storage: Data stored should be encrypted and be accessed by authorized personnel.

Bias and Fairness: The responses of the chatbot must be culturally diverse with no discriminatory elements as the chatbot might unintentionally discriminate against a particular group of people.

c) Chatbot Flow Design and Implementation

The implemented functionality focuses on **providing information about attractions across nine Australian cities**, including Sydney, Melbourne, Brisbane, Perth, Adelaide, Canberra, Darwin, Hobart, and Gold Coast.

Flow Overview

- **Intent: Introduction**
  Greets the user and introduces the chatbot's purpose ("Hi there! 👋 I'm your Tourism Australia Virtual Travel Companion. I currently support trip planning in popular destinations including Sydney, Melbourne, Brisbane, Perth, Adelaide, Cairns, and Canberra.").
- **Intent: City Selection**
  User selects or types a city name.
- **Intent: Attraction Information**
  The chatbot retrieves relevant places of interest (e.g., Sydney Opera House, Melbourne Zoo) and displays a short description, ticket price, opening hours, and location.
- **Intent: Follow-up Suggestions**
  Offers additional recommendations such as nearby attractions, restaurants, or transport links.
- **Intent: Farewell/Help**
  Ends the conversation or provides help options ("Would you like me to suggest something else?").

Conversation Example

User: what can you tell me about Melbourne?
Bot: Top attractions in Melbourne:

- Federation Square
- Royal Botanic Gardens
- Queen Victoria Market
- Great Ocean Road

• Melbourne Museum
Which one would you like details or directions for?

User: tell me about Federation Square
Bot: Federation Square (Melbourne)

Cultural precinct hosting galleries & events downtown.

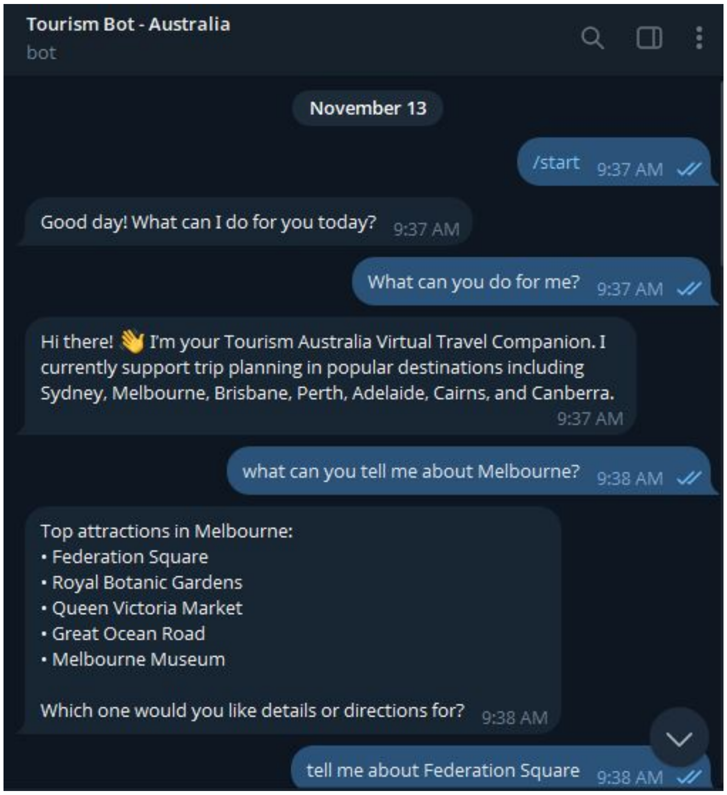
📍 Directions: https://www.google.com/maps/search/?api=1&query=-37.8179,144.9691

🎟️ Ticket: Free

🕐 Hours: 24 hours

Would you like info on another attraction?

This flow was implemented using **Dialogflow**, with separate **intents** for each city and **entity extraction** for attraction details. Context handling and fallback intents ensure smooth conversation flow. The chatbot was tested for language clarity, context switching, and user experience consistency.



Tourism Bot - Australia
bot

November 13

/start 9:37 AM

Good day! What can I do for you today? 9:37 AM

What can you do for me? 9:37 AM

Hi there! 👋 I'm your Tourism Australia Virtual Travel Companion. I currently support trip planning in popular destinations including Sydney, Melbourne, Brisbane, Perth, Adelaide, Cairns, and Canberra. 9:37 AM

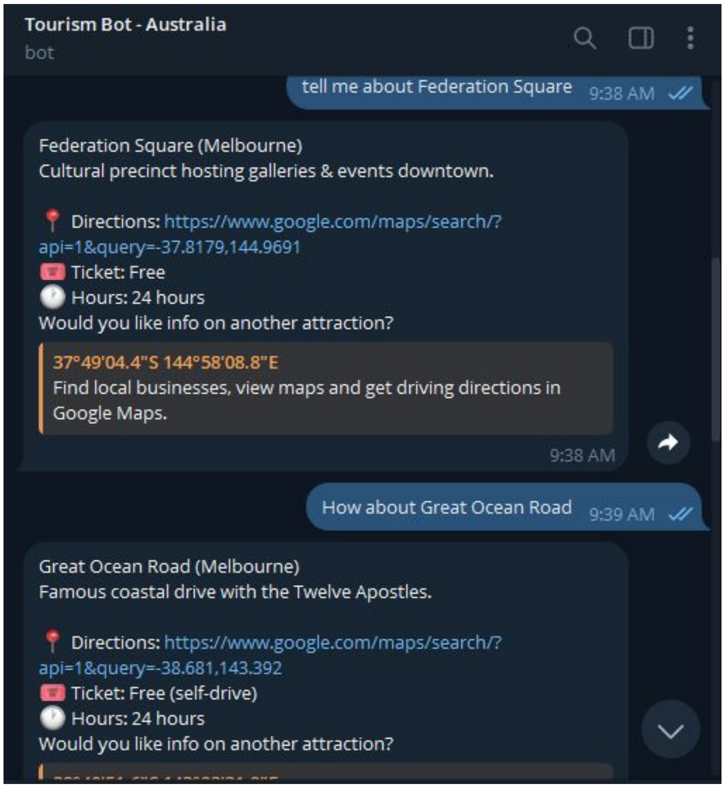
what can you tell me about Melbourne? 9:38 AM

Top attractions in Melbourne:
• Federation Square
• Royal Botanic Gardens
• Queen Victoria Market
• Great Ocean Road
• Melbourne Museum

Which one would you like details or directions for? 9:38 AM

tell me about Federation Square 9:38 AM

Figure 1 Chat Bot Conversation 1



tell me about Federation Square 9:38 AM

Federation Square (Melbourne)
Cultural precinct hosting galleries & events downtown.

📍 Directions: https://www.google.com/maps/search/?api=1&query=-37.8179,144.9691
🎟 Ticket: Free
🕐 Hours: 24 hours
Would you like info on another attraction?

37°49'04.4"S 144°58'08.8"E
Find local businesses, view maps and get driving directions in Google Maps.

9:38 AM

How about Great Ocean Road 9:39 AM

Great Ocean Road (Melbourne)
Famous coastal drive with the Twelve Apostles.

📍 Directions: https://www.google.com/maps/search/?api=1&query=-38.681,143.392
🎟 Ticket: Free (self-drive)
🕐 Hours: 24 hours
Would you like info on another attraction?

Figure 2 Chat bot conversation 2

d) Accessibility Considerations

The design of the chatbot is inclusive and accessible in:

- Multilingual Support: Have the capability to alternate between English and other popular languages.
- Text-to-speech and Speech-to-text Interaction: Text-to-speech and Speech-to-text Interactions are used by low-literacy or visually impaired users.
- Easy Interface: Large clickable buttons, clear choices and text are made concise making it easy to navigate through the interface.

e) Demonstration Video

Q2. Evaluating Cloud Security

Case Study: Capital One AWS S3 Data Breach (2019)

a) Incident Summary

What Happened:

In July 2019, Capital One, one of the largest financial institutions in the United States of America, was the victim of a data breach that revealed the personal data of more than 100 million customers. When a misconfigured AWS S3 bucket permitted some unauthorized access to sensitive data stored in the cloud, the breach took place.

Who Was Affected:

The United States and Canada customers, such as credit card, loan, and other financial products applicants.

What Data Was Compromised:

Names, address, credit rating and contact information.

- Bank account and Social Security Numbers.
- The information about transaction history and credit cards applications.

Root Cause:

An improperly configured Web Application Firewall (WAF) on AWS also allowed the attacker to use a Server-Side Request Forgery (SSRF) weakness, which allowed unlocking access to S3 bucket credentials.

b) Cloud Components and Deployment Model

Deployment Model:
Infrastructure as a Service (IaaS) Capital One deployed the AWS compute and storage infrastructure (EC2 and S3).

Cloud Services Involved:

- Amazon S3: Object storage that is utilized when storing customer data.
- AWS Identity and Access Management (IAM): Access control, which is misconfigured.

- AWS WAF: SSRF exploit was caused due to misconfiguration.

Shared Responsibility Failure.

- AWS (Provider): In charge of the security of the cloud (hardware, infrastructure).
- Capital One (Customer): In charge of cloud security (configuration, access policy).

Visual Diagram:

User → Web App → AWS WAF (Misconfigured) → EC2 Instance → S3 Bucket (Data Exfiltration)

c) Preventive Measures and Recommendations

1. Strict Access Controls Use IAM policies that are least privilege; do not use public S3 bucket policies.
2. Ongoing Configuration Auditing: Use AWS Config, Security Hub and CloudTrail to audit configuration drifts.
3. Network Layer Protection: Use VPC endpoints to access S3 privately rather than via the internet.
4. Encryption and Key Management: Use S3 encryption (SSE-S3 or SSE-KMS) to secure data at rest.
5. Penetration Testing and SSRF Prevention: Web apps should be tested on a regular basis to determine vulnerabilities and prevent unnecessary metadata access.

With such best practices, organizations can reduce significantly the exposure to cloud security misconfigurations, and align themselves with the data protection regulations like the ISO 27001 and GDPR.

Q3. Using Large Language Models

a) Model and Prompt Design

An OpenAI-based LLM was implemented to create an automation system to classify customer complaints and direct them to the relevant support team. To have structured JSON outputs and similar extraction of fields, a custom prompt template named TELECOM_PROMPT was created.

Prompt Template:

You are an assistant for a telecommunications provider.

Your task is to analyze customer messages and return a structured JSON with the following fields:

For each message, extract:

- issue_category: ["Billing", "Network", "Technical Support", "Account Access", "General Enquiry"]
- urgency_level: ["Low", "Medium", "High", "Critical"]
- sentiment: ["Positive", "Neutral", "Negative"]
- followup_required: "Y" or "N"
- recommended_team: e.g. "Billing Team", "Network Operations", "Technical Support", "Customer Care"
- followup_reason: brief human-readable reason

This structured format helps integrate directly into workflow systems such as CRM or ticketing dashboards.

b) Sample Results and Comparison

Example Input:

“I’ve been charged twice for the same service. This is really frustrating and I want a refund.”

OpenAI Model Output:

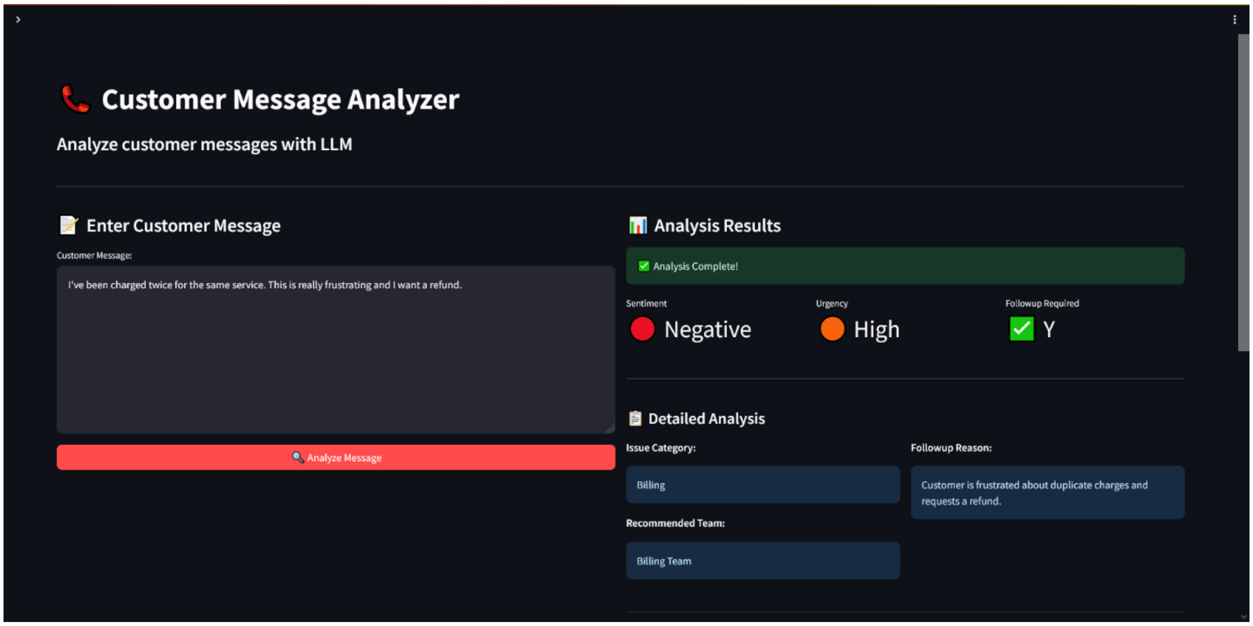
```
{
  "message": "I’ve been charged twice for the same service. This is really frustrating and I want a refund.",
  "analysis": {
    "issue_category": "Billing",
    "urgency_level": "High",
    "sentiment": "Negative",
    "followup_required": "Y",
    "recommended_team": "Billing Team",
    "followup_reason": "Customer is requesting a refund for duplicate charges, indicating urgency."
  }
}
```

pydantic model configuration was used to ensure strict output generation following the needed JSON format with the exclusion of irrelevant text. The LLM demonstrated:

Higher detention of context specific categories (e.g. Billing vs Account Access).

- Improved sentiment and urgency prediction.
- Limited formatting mistakes or illusions because of immediate limitations.

The rule-based model was poor on mixed topic messages and was unrefined in urgency recognition.



☎ Customer Message Analyzer

Analyze customer messages with LLM

Enter Customer Message

Customer Message:

I've been charged twice for the same service. This is really frustrating and I want a refund.

Analysis Results

☑ Analysis Complete!

Sentiment: 🔴 Negative

Urgency: 🟠 High

Followup Required: ✅ Y

Detailed Analysis

Issue Category: Billing

Followup Reason: Customer is frustrated about duplicate charges and requests a refund.

Recommended Team: Billing Team

Figure 3 Analyzed message from the Customer message analyzer

c) Evaluation and Readiness

The implementation of OpenAI shows a high potential of limited production applications under controlled circumstances. It provides precise classification, interpretable JSON results as well as scalable enterprise workflow integration.

Nevertheless, there are a few enhancements that are suggested to be made prior to full implementation:

- Add Retrieval-Augmented Generation (RAG): With the help of RAG, the model questions only accepted domain-specific repositories (e.g., inner policy or service manuals) and reduces the chances of hallucination to minimum, and no customer information is shared with external APIs.
- Apply the Access Controls: Limit the use of models using authenticated endpoints and use of encrypted messages.
- Add Moderation and Validation Layers: The altered automation of the detection and filtering of unsafe or biased outputs prior to logging or escalation.
- Fine-Tuning Domain Data: Fine-tuning with anonymized historical tickets can help increase the accuracy of context and maintain privacy.

On the whole, the solution is ready to be deployed in production to pilot with active privacy-enhancing methods, i.e., RAG pipelines, data masking, and on-premise hosting of models in secure cloud settings.

d) Creation of Solution on Azure

The system can also be developed by using the Azure end-to-end automation and scalability services in order to deploy the prototype to the cloud. The primary parts are described with the way they are interconnected as follows:

1. Data Ingestion Layer

The company communication channels are linked with Azure Graph API and Azure Logic Apps which connect to emails, live chats, and customer feedback forms.

These services monitor new messages on-line and retrieve message content to be processed.

Azure Blob can be used to store all incoming messages in temporary storage so that they can be backed up and audited.

2. Processing and AI Layer

An application written in Python (with the help of OpenCV to process images and Pydantic to validate the RosesGalleriesJSON) is used to provide a custom application, which is available in the form of a container and implemented with the help of Azure Container Apps or Azure Functions.

The app will automatically get activated to process a new data when it arrives.

The application is linked with Azure OpenAI Service to use the Large Language Model (LLM) that will analyze each message and determine the type of issue, the level of urgency, the sentiment, the confidence, and sensitivity.

The result of the processing is returned in structured form, in JavaScript language, and is verified by Pydantic to maintain data quality.

3. Storage and Routing Layer

The resulting JSON data is saved in the Azure Cosmos DB or Azure SQL Database.

Each classified message may then be directed to the corresponding support team depending on its type and priority (e.g. Billing → Billing Queue, Network → Network Operations).

4. Observation and Visualization.

Azure monitor and application insights are used to monitor the performance of the system, the response times, and model precision.

Power BI dashboards demonstrate the trends of complaints, sentiment distribution, and urgency levels to allow the management to define the areas that require improvement.

5. Security and Governance

Azure Key Vault provides storage of sensitive credentials like API keys.

ROLE-Based Access Control (RBAC) is the paradigm that is used to make sure that only authorized users are allowed to access classified data or make adjustments to the configuration.

Pipeline Flow:

Emails / Chats / Forms

↓

Azure Graph API + Logic App (Ingestion)

↓

Azure Container App / Azure Function (OpenCV + Pydantic App)

↓

Azure OpenAI Service (LLM Analysis)

↓

Validated JSON Results → Cosmos DB / SQL Database

↓

Logic App or Service Bus (Routing to Support Teams)

↓

Azure Monitor + Power BI (Performance and Trend Monitoring)

Q4. Evaluating Cloud-Based Technology

a) Key Functionalities Aligned with Academic Activities

Google NotebookLM is an AI-based note-taking and research assistant, combining the use of large language models with source-grounded knowledge management. It allows users to index, summarize and engage with academic content uploaded therein, streamlining the research processes in higher education.

Functionality	**Description**	**Academic Use Case**
Document Summarization	Generates concise bullet-point or paragraph summaries from uploaded PDFs, lecture notes, or academic papers.	Helps researchers and students quickly review long journal articles or technical documents.
Question Answering from Sources	Enables users to ask contextual questions directly from uploaded sources (e.g., “What are the main findings of this paper?”).	Supports targeted information retrieval for literature reviews.
Concept Extraction and Topic Mapping	Identifies and connects related terms, entities, and themes across documents.	Aids in developing conceptual frameworks and identifying gaps in literature.
Source Referencing and Citation Context	Provides direct links to source text, ensuring credibility and transparency.	Helps maintain academic integrity through traceable citations.
Collaborative Note Organization	Organizes multiple notebooks by topic, storing summaries, highlights, and AI Q&A.	Facilitates multi-project management and ongoing research collaboration.
Audio Summary Generation	Converts textual summaries into brief audio notes.	Enhances accessibility and auditory learning for researchers on the move.

b) Demonstration of Functionalities in a Research Scenario

Scenario Used: *Synthesizing Literature and Preparing a Research Summary*

NotebookLM was tested on the basis of its usefulness in literature consolidation in a research project on AI and Machine Learning developments. Several peer-reviewed articles were uploaded and the system was put to the test in the areas of summarization, concept mapping, and citation verification. The workflow and finding are as shown below:

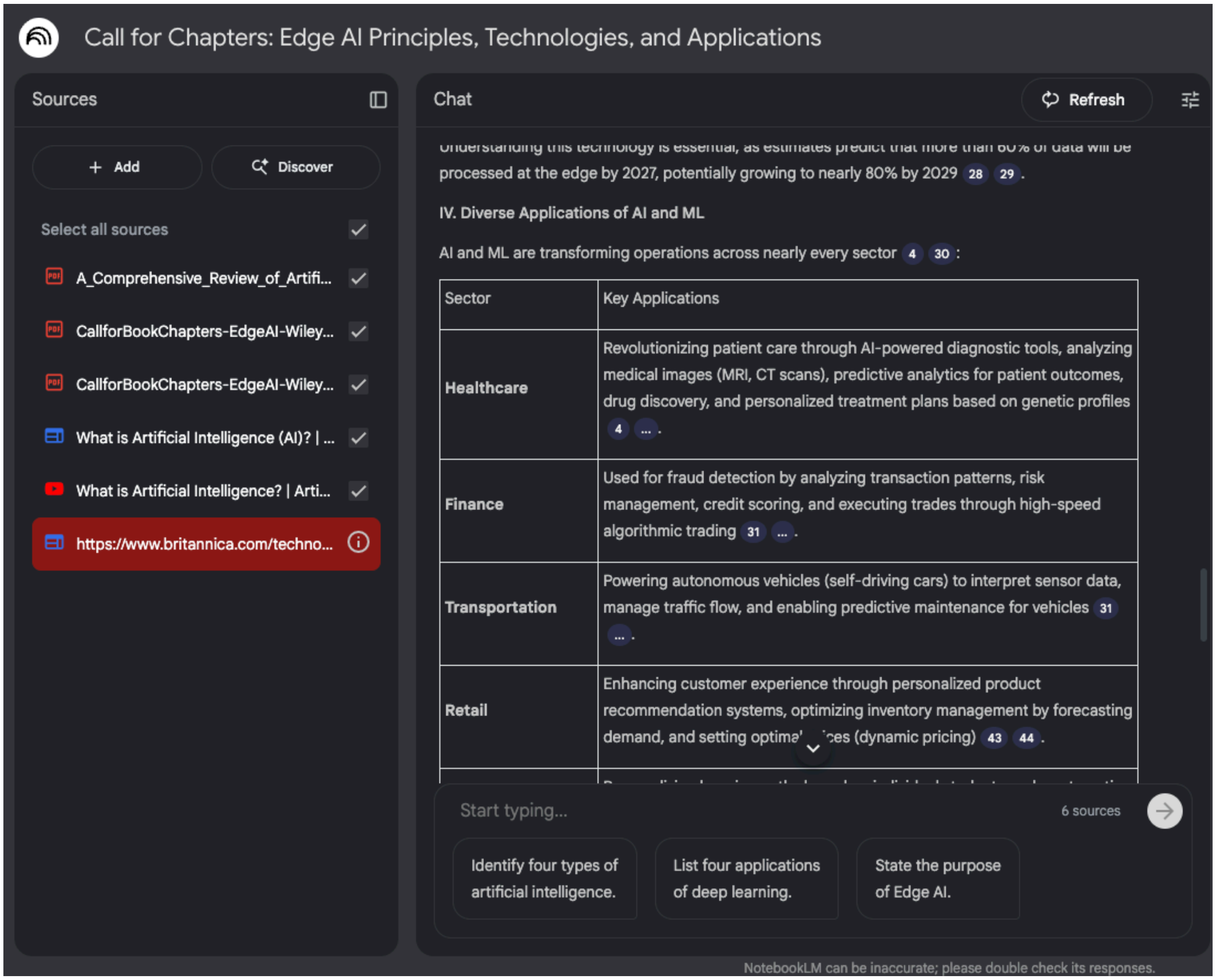
Feature Testing and Observations

Feature Tested	Prompt or Action Used	NotebookLM Output Summary	Accuracy & Relevance (1–5)	Usefulness in Academic Workflow	Limitations / Observed Issues
Summarization	"Summarize this paper in 5 bullet points."	Produced a coherent and structured summary highlighting key AI/ML concepts, applications, challenges, and future trends.	4	Very helpful for literature review and exam preparation — condenses complex information into clear points.	Missed citation details; some generalization of technical depth.
Question Answering	"What is the difference between AI and ML?"	Explained AI as a broader concept and ML as a subset with structured comparison points.	5	Very useful for conceptual understanding in coursework or tutorials.	None significant; occasionally too formal or repetitive.
Trend Analysis / Future Directions	"What are the upcoming concepts that have to release?"	Gave a detailed breakdown of future AI directions like AGI, Federated Learning, Quantum AI, and Ethical AI.	5	Excellent for research insights and writing introductions for papers.	Some speculative content; minor factual confidence issues.
Source Extraction /	Checked sources	Listed academic references,	4	Very useful for bibliography	Did not provide complete

Reference Linking	mentioned in generated text.	journals, and authors clearly with structured categorization (books, papers, reports).		tracking in research projects.	citation formatting (APA/IEEE).
Thematic Summary / Consolidation	"Create a summary of content."	Produced an integrated, structured academic-style summary with clear sections (fundamentals, applications, challenges, future trends).	4	Ideal for academic synthesis, assignment writing, and presentation preparation.	Slight redundancy; needed user editing for conciseness.

All outputs and versioned experiment files were documented in a GitHub repository for verification and reproducibility.

GitHub Repository Link: [Insert GitHub link here]



Call for Chapters: Edge AI Principles, Technologies, and Applications

Sources

+ Add

Discover

Select all sources ✓

- A_Comprehensive_Review_of_Artifi... ✓
- CallforBookChapters-EdgeAI-Wiley... ✓
- CallforBookChapters-EdgeAI-Wiley... ✓
- What is Artificial Intelligence (AI)? | ... ✓
- What is Artificial Intelligence? | Arti... ✓
- https://www.britannica.com/techno...

Chat

Refresh

Understanding this technology is essential, as estimates predict that more than 60% of data will be processed at the edge by 2027, potentially growing to nearly 80% by 2029 [28] [29].

IV. Diverse Applications of AI and ML

AI and ML are transforming operations across nearly every sector [4] [30]:

Sector	Key Applications
Healthcare	Revolutionizing patient care through AI-powered diagnostic tools, analyzing medical images (MRI, CT scans), predictive analytics for patient outcomes, drug discovery, and personalized treatment plans based on genetic profiles [4] [...].
Finance	Used for fraud detection by analyzing transaction patterns, risk management, credit scoring, and executing trades through high-speed algorithmic trading [31] [...].
Transportation	Powering autonomous vehicles (self-driving cars) to interpret sensor data, manage traffic flow, and enabling predictive maintenance for vehicles [31] [...].
Retail	Enhancing customer experience through personalized product recommendation systems, optimizing inventory management by forecasting demand, and setting optima' ices (dynamic pricing) [43] [44].

Start typing...

6 sources

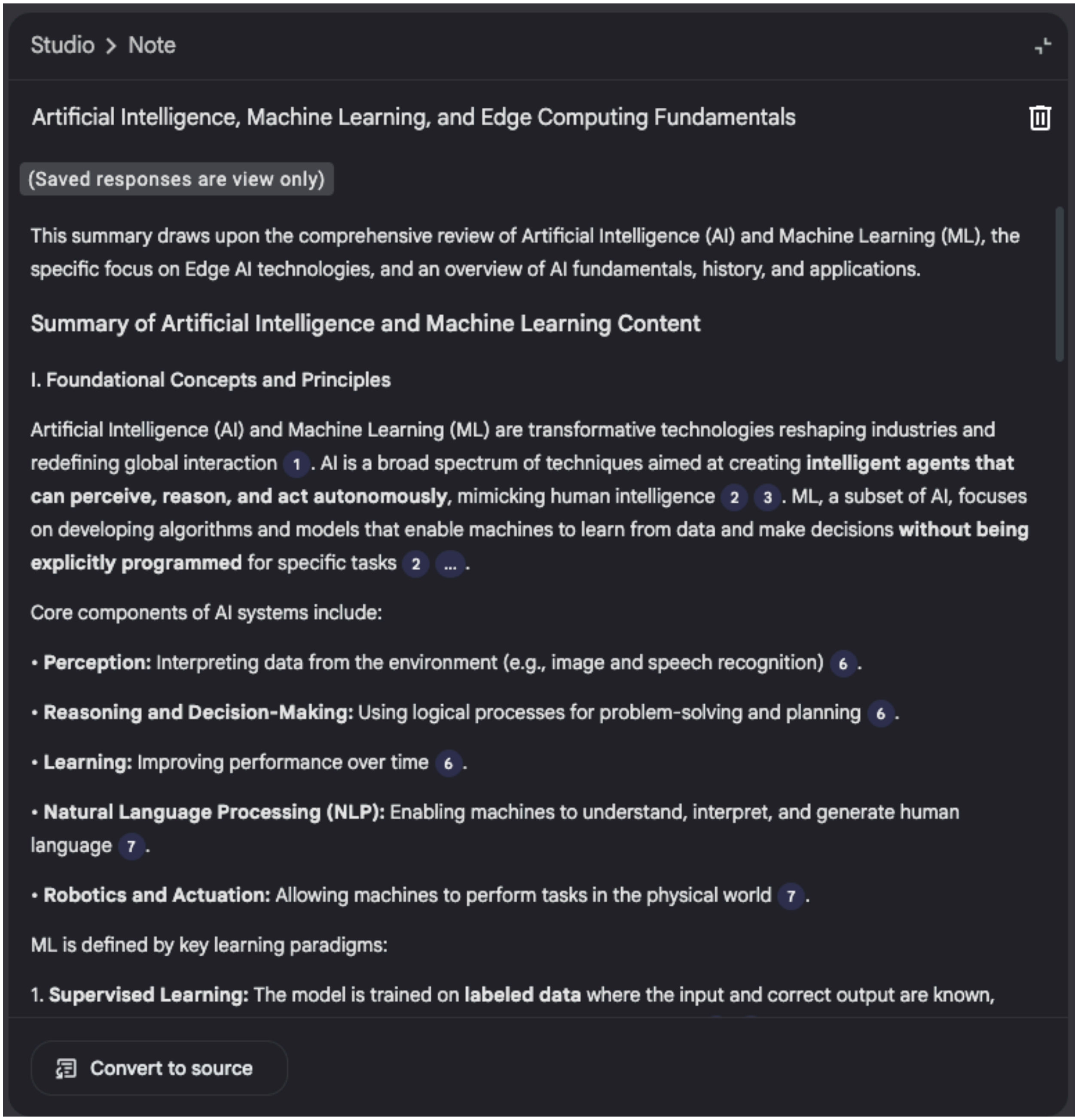
Identify four types of artificial intelligence.

List four applications of deep learning.

State the purpose of Edge AI.

NotebookLM can be inaccurate; please double check its responses.

Figure 4 NotebookLM interface displaying uploaded research sources and AI-assisted extraction of application domains of AI and ML across sectors such as healthcare, finance, and transportation. Demonstrates the system's document management and contextual question-answering capabilities.



Artificial Intelligence, Machine Learning, and Edge Computing Fundamentals

This summary draws upon the comprehensive review of Artificial Intelligence (AI) and Machine Learning (ML), the specific focus on Edge AI technologies, and an overview of AI fundamentals, history, and applications.

Summary of Artificial Intelligence and Machine Learning Content

I. Foundational Concepts and Principles

Artificial Intelligence (AI) and Machine Learning (ML) are transformative technologies reshaping industries and redefining global interaction ①. AI is a broad spectrum of techniques aimed at creating **intelligent agents that can perceive, reason, and act autonomously**, mimicking human intelligence ② ③. ML, a subset of AI, focuses on developing algorithms and models that enable machines to learn from data and make decisions **without being explicitly programmed** for specific tasks ② … .

Core components of AI systems include:

- **Perception:** Interpreting data from the environment (e.g., image and speech recognition) ⑥.
- **Reasoning and Decision-Making:** Using logical processes for problem-solving and planning ⑥.
- **Learning:** Improving performance over time ⑥.
- **Natural Language Processing (NLP):** Enabling machines to understand, interpret, and generate human language ⑦.
- **Robotics and Actuation:** Allowing machines to perform tasks in the physical world ⑦.

ML is defined by key learning paradigms:

1. **Supervised Learning:** The model is trained on **labeled data** where the input and correct output are known,

Figure 5 Example of AI-generated structured summary in NotebookLM synthesizing content from multiple uploaded sources on Artificial Intelligence, Machine Learning, and Edge Computing fundamentals. Highlights summarization, conceptual extraction, and reference linking features.

c) Critical Evaluation

Overall Evaluation Summary

Criterion	Evaluation	Evidence / Notes
Accuracy & Relevance	High accuracy with structured and relevant academic output. Responses aligned well with uploaded materials and were contextually consistent.	Summarization and comparison tasks showed no major factual errors; cross-checked against uploaded content.
Usefulness in Academic Workflows	Excellent support for summarization, concept clarification, and literature synthesis.	Helped condense multi-source material for AI/ML research; suitable for coursework and report writing.
Limitations / Concerns	Occasionally verbose or speculative; lacks formal citation output.	Example: “upcoming concepts” responses included speculative terms such as “self-aware machines.”
Bias or Hallucination Risks	Low bias detected but slight tendency to overgeneralize missing details.	—
Recommendation	Suitable for limited academic use (study aids and summarization); better used with human verification for formal publication or citation work.	Combine with verified academic sources and manual proofreading before submission.

Summary and Recommendation:

NotebookLM can be of considerable value to the academic research support - especially in summarizing, organizing, and synthesizing complicated literature. It saves time used in manual reading and is contextually relevant. Nevertheless, to reduce chances of overgeneralization or incomplete citing, the results are to be cross-verified with the original sources before being included in the academic publication.