Cyber Guardian

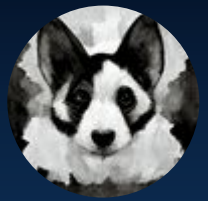
By Crestian AI

Crestian AI Team

Priyank Shah

Prijen Khokhani

Darshak Kakani



Jenis Donda

Poojan Patel

Harsh Agheda

Problem Statement

- In today's world, stay informed about cybersecurity threats is crucial for individuals and organization. On top of that, **accessing latest relevant information** poses a significant challenge.
- For chatbot, we have to use LLM models. So **accuracy** and managing their **cost** is very crucial challenge.
- The challenge is clear: How do we stay alert with **latest news** with better **accuracy** without losing valuable time?

Solution

- CyberGuardian autonomously **collects and delivers the latest information** from diverse news sources.
- We leverage **Trulens** for evaluating and tracking our model responses. It provides different metrics like **answer relevance, groundedness, context relevance** by monitoring the application’s AI interaction.
- We can measure **costing and tokens** for every request so we can ensure scalability and affordability for our users.

Tools/Technologies

Llama Index

MongoDB

TruLens

OpenAI

GPT-4

Streamlit

Market Opportunity

Enterprise Security

CyberGuardian provides **real-time update** on cyber attacks, compliance support through regulatory news insights, and actionable information for effective mitigation strategies.

Growing Cyber Threats

CyberGuardian offers real-time threat updates, **enhancing incident response and insights** for growing cyber threats.

Integrations with SOAR

CyberGuardian enhances a SOAR platform by providing **real-time alerts, incident context enrichment** and updated threat intelligence for more efficient security workflows.

Subscription Revenue

Offers **premium**, up-to-date cyber security news and insights through subscription models.

Project Architecture

1

Chatbot UI

Takes input from the user and show the response from the bot

2

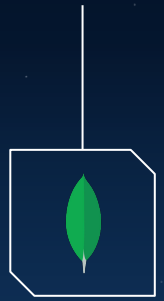
GPT-4

Used to embeddings the chunks and also give response from mongoDB vectores

3

MongoDB

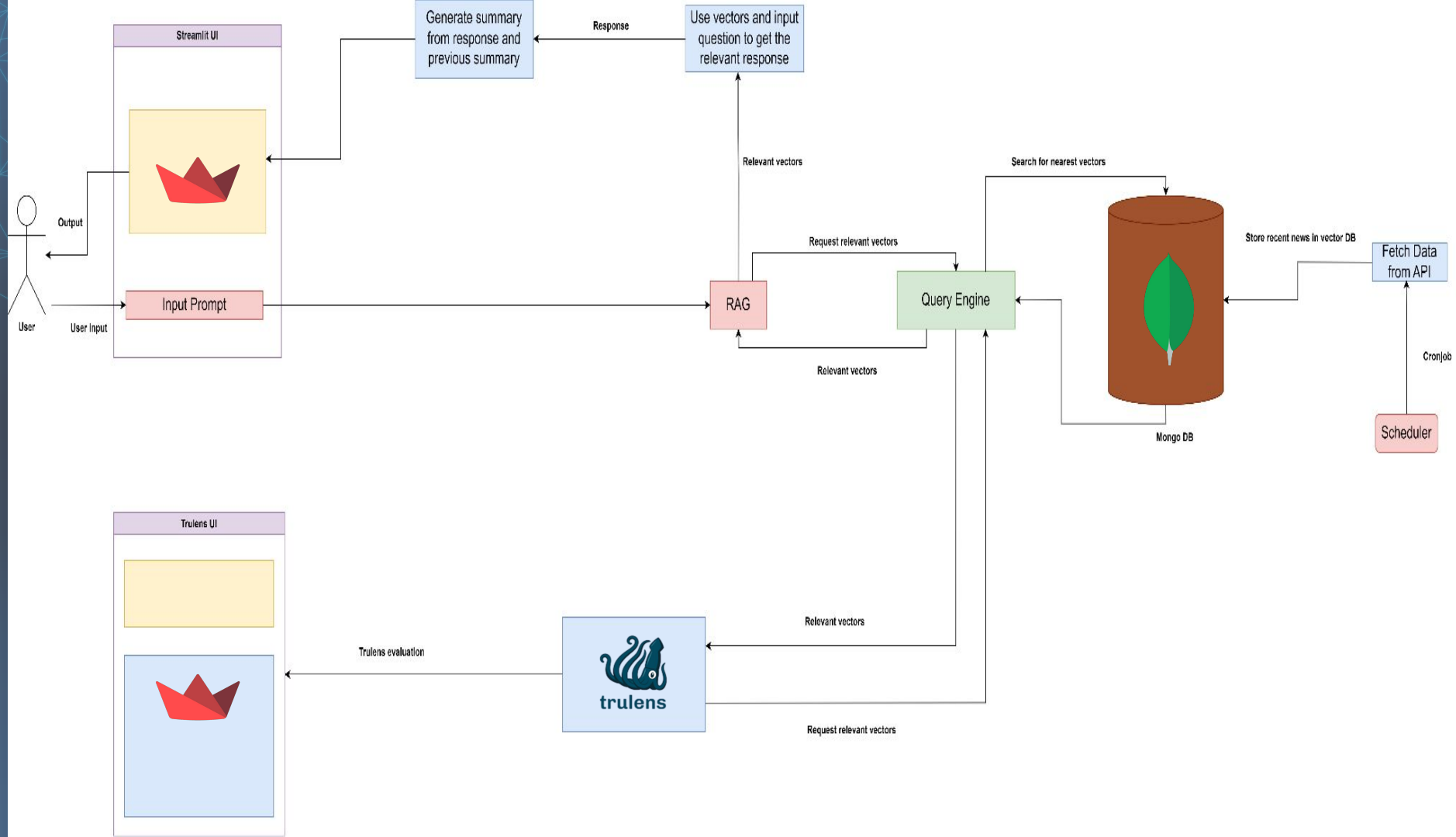
Used to store embeddings vectors



4

TruLens

Evaluating and tracking model responses


Streamlit UI
Generate summary from response and previous summary
Response
Use vectors and input question to get the relevant response
Relevant vectors
Search for nearest vectors
Output
Request relevant vectors
Store recent news in vector DB
Fetch Data from API
Input Prompt
RAG
Query Engine
User
User Input
Relevant vectors
Cronjob
Mongo DB
Scheduler
Trulens UI
Relevant vectors
Trulens evaluation
trulens
Request relevant vectors

Advantages

Latest Updates

Provide latest updates on cybersecurity threats, news and trends

1

2

Personalized Recommendations

Offer recommendations tailored to user's interest and need

Cost Effective

With using of trulens we accurately assess costs associated with model usage, ensuring efficient resource allocation

3

4

Accuracy and relevancy

Cyber Guardian ensure relevancy and accuracy of model outputs, optimizing decision making processes

Limitations

Limited Domain Knowledge

Cyber Guardian have cyber security domain so apart from that it can not be able to answer or not be accurate

1

2

Context Limit

With using of LLM models, always there will be context limit so we can store limited previous chat summary

Costing

The cost may rise substantially based on the pricing of the underlying LLM.

3

4

Accuracy and relevancy

It may face limitations in accuracy due to rapidly evolving threats and data quality, and in relevance due to the challenges in contextual understanding of cyber security news.

Future Expansion

Recommendations

Integrate user profiles to personalized news recommendations based on user preferences or interaction patterns.

Multimedia

Incorporate multimedia content such as videos, images, infographics, or interactive elements to enrich the user experience.

SOAR

Integrating the Cyber Guardian with SOAR platforms for incident response and seamless automation.

Community Engagement

Foster a community around the bot by enabling users to share insights, discuss cybersecurity topics, or collaborate on threat analysis and response efforts.

Thank you