**Cybersecurity AI Agent**

**Summary:**

This project presents a **Cybersecurity AI Agent** designed to provide intelligent, real-time insights and explanations related to the field of **cybersecurity**.  
Developed using **Gemini API**, **LangChain**, and **Gradio**, the agent can interpret user queries in natural language and respond with accurate, concise, and informative answers about cybersecurity threats, prevention methods, and awareness practices.

The system architecture consists of:

**Frontend (app.py)** — A Gradio-based user interface that allows users to interact with the AI agent easily.

**Backend (backend.py)** — Handles all processing and integrates **LangChain** with the **Gemini API** for intelligent response generation.

**.env file** — Stores environment variables, including the Gemini API key, ensuring secure and organized access to configuration data.

The AI agent assists users in understanding cybersecurity domains such as:

Common attack vectors (phishing, ransomware, DDoS, etc.)

Cyber hygiene and data protection practices

Threat analysis and risk prevention

General cybersecurity awareness

**Expected\_Outcome:**  
A smart, efficient, and easy-to-use **Cybersecurity Virtual Assistant** that helps users stay informed and vigilant against evolving cyber threats.

**Deployed Model Link:**

***->*** *<https://huggingface.co/spaces/Ithachi-maker/Cyber_SEcurity_Agent>*

Users can access the deployed web app directly via the above link to interact with the live Cybersecurity Agent.

**Local System Setup Instructions:**If you prefer to run the project locally, follow these steps:

1. **Create a virtual environment:**

python -m venv venv

1. **Activate the virtual environment:**
   1. On Windows:

venv\Scripts\activate

* 1. On macOS/Linux:

sourcevenv/bin/activate

1. **Install required dependencies:**

pip install -r requirements.txt

1. **Add your Gemini API key** in the .env file:

GEMINI\_API\_KEY=your-gemini-api-key

1. **Run the app:**

python app.py

1. **Open the generated local link** (shown in the terminal) to access the Cybersecurity Agent interface.

**Developer :**

|  |  |
| --- | --- |
| **Name** | **Role** |
| **[Soumya Subhra Datta,**  **RegNo: 43731131,**  **3rd Year, AI-A3]** | Developer (Full Stack AI & Deployment) |

**Folder Structure:**

**Cybersecurity\_AI\_Agent/**

**│**

**├── app.py # Gradio frontend interface**

**├── backend.py # LangChain + Gemini backend logic**

**├── .env # API key and configuration**

**├── requirements.txt # Python dependencies**

**└── Abstract.docx # Project summary and developer info**