AI Privacy-Aware Chatbot

Overview

This project is a **local privacy-focused AI chatbot** built with **Python, FastAPI, and Tkinter**.
It demonstrates how **data redaction** and **anonymous logging** can be integrated into AI workflows to improve compliance and user trust.

Instead of sending sensitive information directly to an external model, the chatbot **cleans and redacts inputs first**, then passes them securely to an **AI model (Anthropic Claude, accessed via the OpenRouter API)**. This ensures that user prompts remain protected while still leveraging the power of advanced LLMs.

Features

- **Data Redaction Engine** → Automatically detects and masks file paths, hashes, emails, and passwords (~85% accuracy in lab tests).
- **Anonymous Session Logging** → Each session gets a unique ID with timestamped logs that are redacted and admin-only, projected to increase user trust/adoption by ~75%.
- **Tkinter Desktop GUI** → Simple, lightweight interface for everyday users.
- **FastAPI Backend** → Handles secure communication between the GUI, redaction logic, and AI model.
- **Compliance-Ready Design** → Demonstrates workflows aligned with privacy and security best practices.

Tech Stack

- **Programming:** Python (3.9+)
- **Frontend:** Tkinter GUI
- **Backend:** FastAPI
- **AI Model:** Anthropic Claude via OpenRouter API
- **Other Tools:** Requests, JSON, Hashlib, Regex