Project 2: Secure PII Tokenization for LLMs (SPT-LLM)

Company Overview:

Analytical Data Systems empowers businesses by providing state-of-the-art software products, data processing systems, and AI-driven analytics solutions. Our experts are passionate about enabling companies to make informed decisions, optimize operations, and drive growth using data-driven insights. As a computer science student at a top engineering school, you have a unique opportunity to participate in our summer project, which aims to equip you with the skills and experience necessary to excel in the highly competitive world of data analytics, AI, and software development. Join us in our quest to revolutionize the way businesses harness the power of data and technology to unlock new opportunities, maximize value, and shape the future.

Description:

In this project, students will collaborate to create the Secure PII Tokenization processing for interaction with Large Language Models (SPT-LLM). A robust tokenization technique that enables secure interactions with large language models without compromising personally identifiable information (PII). The team will focus on designing a secure tokenization system capable of detecting and removing PII while preserving the integrity of the LLM's output. This project will cover the development of algorithms, back-end utilities, and tools to support the tokenization system, along with testing and evaluation of its security and effectiveness.

Technology: GPT-4, Langchain, Milivus or PineCode, Node, React, Python

Open Source Starting Point: https://github.com/mayooear/gpt4-pdf-chatbot-langchain

Objectives:

1. Design a secure tokenization system for handling PII: Students will work together to research and develop a secure tokenization system that can effectively detect and remove PII from input data without hindering the performance of LLMs. This system should be adaptable to various LLMs and compatible with different data formats.
2. Develop back-end utilities and tools to support the tokenization system: The team will create back-end utilities and tools that facilitate the integration of the tokenization system with various LLMs. These utilities will handle data ingestion, preprocessing, and evaluation, ensuring seamless interaction between the tokenization system and LLMs.
3. Test the tokenization technique in various LLM interactions: Participants will evaluate the performance of the tokenization system across different LLM applications and contexts, such as summarization, analysis across documents, and content generation. This testing process will provide valuable insights into the system's strengths, weaknesses, and areas for improvement.
4. Assess the system's security and effectiveness in protecting PII: The team will conduct a thorough evaluation of the tokenization system's security and its ability to protect PII in real-world scenarios. This assessment will help identify potential vulnerabilities and ensure the system meets the highest standards of privacy protection.

Why this project:

The SPT-LLM project provides a unique opportunity for students to contribute to the rapidly-growing field of AI and natural language processing while addressing critical privacy concerns. By participating in this project, students will gain hands-on experience with state-of-the-art technologies, techniques, and best practices for PII protection, setting them apart in the competitive job market.

Designed to be completed within a 5-week timeframe, this project offers an intensive, fast-paced learning experience tailored to ambitious computer science students. By tackling the challenge of PII protection in LLM interactions, students will not only gain valuable expertise but also make a meaningful impact on privacy and security within the AI landscape, laying the foundation for a successful career in the technology industry.

IP: I encourage students to leverage any learning or know-how gained on these projects for their own use. However, any code or data used in the development of the project will remain the property of Analytical Data Systems.