Security Data Science

Adrian Rodriguez 21691

Lab 2

Nota: todos los notebooks fueron ejecutados localmente, los outputs demuestran dicha ejecución y realización de cada día.

1. ¿Hubo alguna aplicación o caso de uso de los LLMs que le llamó más la atención? ¿Por qué?

Me impresionaron particularmente los **agentes generativos**. La idea de darle a un LLM con herramientas para interactuar con bases de datos y ejecutar tareas específicas me parece bastante interesante. Me atrae la idea de cómo estos agentes pueden automatizar procesos complejos y tomar decisiones informadas en entornos dinámicos.

Otro aspecto que me llamó la atención es el uso de **embeddings para manejar grandes volúmenes de datos**. A menudo me he preguntado cómo proporcionar un contexto amplio a un LLM sin sobrepasar los límites de tokens de la ventana de contexto. Sin mencionar que el proceso fue bastante sencillo de realizar, la API de Gemini en Python es bastante intuitiva…

2. Proponga un caso de ciberseguridad que considere se puede solucionar mediante un LLM y describa de forma general cómo lo resolvería.

Propongo un modelo LLM que actúe como **filtro inteligente para logins**. Este modelo analizaría patrones de inicio de sesión y, basándose en la ubicación, actividad previa y otros factores, detectaría anomalías que sugieran un acceso no autorizado.

Además de marcar posibles riesgos, el modelo podría interactuar con el usuario mediante **preguntas de seguridad dinámicas**. A diferencia de las preguntas de seguridad estáticas tradicionales, el LLM podría generar preguntas personalizadas y relevantes para el contexto del intento de inicio de sesión, lo que aumentaría la seguridad y la confianza en la identidad del usuario.

Este enfoque permitiría:

- **Detección proactiva**: Identificar y bloquear accesos sospechosos antes de que causen daño.
- **Mayor seguridad**: Adaptar las preguntas de seguridad a cada situación, dificultando la suplantación de identidad.
- **Experiencia de usuario mejorada**: Evitar preguntas de seguridad tediosas y repetitivas, al tiempo que se mantiene un alto nivel de seguridad.