

Teoría:

1.

Para resolver el problema de clasificar y organizar los correos en diferentes categorías, se puede implementar una solución de procesamiento de lenguaje natural (NLP) utilizando técnicas de aprendizaje automático. Aquí se presenta una metodología detallada para abordar este problema.

Metodología

- Recolección y Preparación de Datos

Preprocesamiento de datos: Limpiar los correos electrónicos eliminando ruido como firmas, saludos, y elementos HTML. Convertir el texto a un formato utilizable eliminando caracteres especiales y aplicando técnicas de tokenización.

- Análisis Exploratorio de Datos (EDA)

Realizar un análisis exploratorio para entender la distribución de las palabras y frases clave en cada categoría.

Utilizar visualizaciones como nubes de palabras y gráficos de frecuencia de términos.

- Selección y Extracción de Características

Utilizar técnicas de extracción de características como TF-IDF para convertir los correos en vectores numéricos.

Considerar la utilización de técnicas avanzadas como embeddings de palabras para capturar el contexto semántico.

- División del Conjunto de Datos

Dividir los datos en conjuntos de entrenamiento y prueba (80% entrenamiento, 20% prueba) para evaluar el rendimiento del modelo.

- Selección de Modelos y Entrenamiento

Probar varios algoritmos de clasificación de texto como Naive Bayes, SVM y modelos basados en redes neuronales como LSTM y transformers.

Realizar una validación cruzada para ajustar hiperparámetros y seleccionar el mejor modelo basado en métricas de rendimiento como precisión, recall y F1-score.

- Evaluación y Validación

Evaluar el modelo seleccionado en el conjunto de prueba.

Ajustar y optimizar el modelo basado en los resultados de la evaluación.

- Implementación

Desarrollar una interfaz para integrar el modelo de clasificación con el sistema de correos de la empresa.

Configurar un servicio en la nube para manejar las solicitudes de clasificación en tiempo real.

- Monitoreo y Mantenimiento

Implementar un sistema de monitoreo para seguir el rendimiento del modelo en producción.

Actualizar y reentrenar el modelo periódicamente con nuevos datos para mantener su precisión.

Arquitectura del Proyecto

- Recolección y Almacenamiento de Datos

Utilizar servicios como Azure Blob Storage para almacenar los correos históricos.

Utilizar un servicio de base de datos relacional como SQL para almacenar metadatos y resultados de clasificación.

- Procesamiento y Preprocesamiento

Implementar scripts de preprocesamiento utilizando Python y bibliotecas como NLTK, SpaCy, o Hugging Face Transformers.

Utilizar servicios de computación en la nube para ejecutar tareas de preprocesamiento y clasificación.

- Entrenamiento del Modelo

Utilizar instancias de computación de alto rendimiento con GPUs para entrenar los modelos.

Almacenar modelos entrenados en un servicio de almacenamiento en el Blob Storage .

- Despliegue del Modelo

Desplegar el modelo utilizando servicios de contenedores como Docker y Kubernetes.

Utilizar un servicio de inferencia de modelos en tiempo real.

- Integración y Monitoreo

Integrar el servicio de clasificación con el sistema de correos de la empresa mediante APIs RESTful.

Implementar monitoreo continuo utilizando servicios como AWS CloudWatch para rastrear el rendimiento y detectar anomalías.

Recursos Necesarios

- Recursos Humanos

Un equipo de científicos de datos para el desarrollo y entrenamiento de modelos.

Ingenieros de software para la integración y despliegue del sistema.

Analistas de datos para la validación y monitoreo continuo.

- Recursos Tecnológicos

Instancias de computación en la nube con capacidad GPU para el entrenamiento del modelo.

Almacenamiento en la nube para datos y modelos.

Herramientas de monitoreo y administración de modelos.

Esta solución permitirá clasificar eficientemente los correos en las categorías especificadas, mejorando la organización y gestión del área de compras en la empresa.

2.

Sí, es posible que el modelo esté sufriendo de drift. Debemos validar que las entradas hayan cambiado.

Para ello debemos validar que la recolección de datos recientes y antiguos, esto implica comparar los datos actuales de entrada con los datos históricos que se usaron para entrenar el modelo, así como recolectar un conjunto de predicciones recientes del modelo y compararlas con las salidas reales observadas. Repetimos el análisis estadístico para evaluar los ajustes de distribución y algunas pruebas estadísticas.

Con esto anterior podemos identificar las causales del driftt, para corregirlo debemos reentrenar el modelo. Recolectar y etiquetar datos recientes que representen mejor el estado actual del entorno. Crear un conjunto de datos actualizado combinando datos históricos con datos recientes y reentrenar el modelo utilizando el conjunto de datos actualizado para capturar las nuevas tendencias y patrones.

Como método de mejora podríamos establecer un sistema de monitoreo que permita detectar el drift de manera temprana y automática, o también podríamos establecer una frecuencia de “mantenimiento” del modelo.

3.

Para asegurar que las respuestas del chatbot basado en GPT-3.5 estén siempre relacionadas a obtener cierta información particular del usuario y no desvíen hacia temas irrelevantes, se pueden implementar varias estrategias como utilizar prompts Específicos y mantener o alinear al usuario al contexto del chatbot.

Por ejemplo, en lugar de preguntas abiertas como "¿En qué puedo ayudarte?", utilizar prompts como "Por favor, proporciona tu nombre completo" o "¿Cuál es tu dirección de correo electrónico?"

Hay que asegurar que cada respuesta del modelo mantenga el contexto de la conversación. Utilizar prompts que incluyan el historial reciente de la conversación para mantener el enfoque.

Otras estrategias para robustecer el chatbot puede ser ajustar la temperatura del modelo a un valor bajo para que las respuestas sean más deterministas y menos “creativas”.

Implementar reglas que validen si la respuesta del modelo está alineada con el objetivo. Si no lo está, se puede generar una nueva respuesta o redirigir la conversación.