Grado en Ingeniería Informática

Criptografía y seguridad informática 25/26

Grupo 81

Práctica 1

«OmniMessenger: Envío de mensajes en masa»

Denis Loren Moldovan — 100522240

Jorge Adrian Saghin Dudulea — 100522257

Profesor

Lorena Gonzalez Manzano

Tabla de Contenidos

1. Propósito y estructura

La aplicación consiste en el envío masivo de mensajes, usando servicios como Telegram (Bots), Whatsapp (Business) y Gmail (Conexión al correo correspondiente). Esta almacena en un servidor todos los mensajes, junto con las plataformas conectadas donde se van a distribuir, y la hora cuando se ha subido en una base de datos privada. Después, el servidor genera una cola con estos mensajes y los va distribuyendo de forma ordenada, reduciendo la carga acorde a los límites de cada plataforma.

El servicio se basa en una aplicación web, la cual actúa como interfaz para todas las acciones disponibles para el usuario. Por otro lado, se usa como servidor un script escrito en Python, la cual gestiona las sesiones de los usuarios, y almacena toda la información en una base de datos.

Para el acceso a todos los servicios, se ha usado Caddy como proveedor de archivos, y proxy reversa a todos los servicios de la aplicación. Por otro lado, se ha usado PostgreSQL para la base de datos y Adminer para la visualización de la base de datos. Finalmente, para asegurar el funcionamiento, se ha contenerizado toda la aplicación usando Docker.

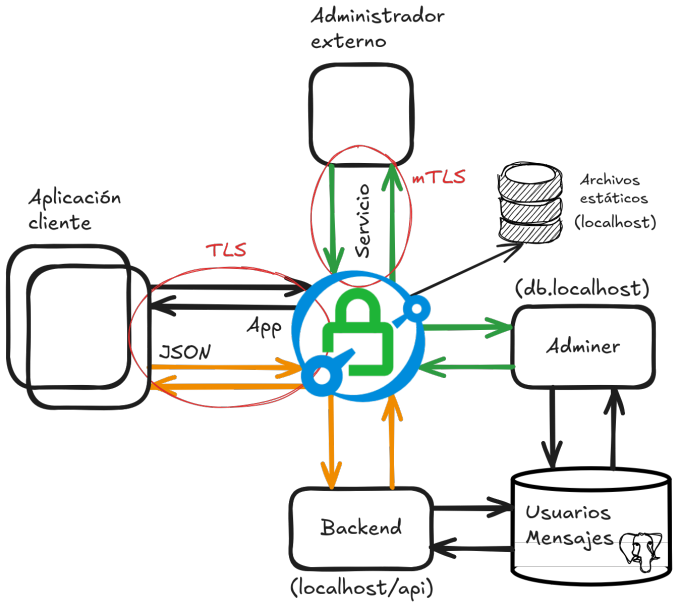

Figura 1: Diseño de la aplicación

Para ejecutar la aplicación, primero hay que descargar y configurar Docker. Después, hay que construir la imagen personalizada usando `./setup.sh`, y finalmente ejecutar la aplicación usando `./run.sh`. Para detenerlo, hay que ejecutar `./down.sh`.

La página principal se encontrará en `https://localhost`, y el gestor de la base de datos en `https://db.localhost`. El certificado requerido para poder acceder al gestor se encuentra en `Docker/conf/mTLS/Client/keystore.p12`, el cual hay que instalar en el navegador.

2. Uso de cifrado simétrico y asimétrico

3. Uso de Códigos de Autenticación de Mensajes (MAC)

4. Pruebas realizadas