DELVALLE
GRUPO EDUCATIVO

Astrid Glauser
Samuel Argueta
Dolan Cuellar
Alejandro Martínez

Proyecto 2

Cifrados de Información

Diseño de Arquitectura

Introducción

Desarrollar una aplicación de mensajería que utiliza mecanismos modernos de autenticación cifrado, firma digital, integridad de datos y almacenamiento seguro mediante blockchain.

Alcance: La aplicación ofrece funcionalidades de chat grupal y P2P, protegidas mediante algoritmos criptográficos

Requisitos

Funcionales:

- Autenticación segura con OAuth 2.0 (Google) y TOTP (Two-Factor Authentication).

- Chats grupales y P2P con cifrado de extremo a extremo.

- Firma digital e integridad de mensajes.

- Almacenamiento de mensajes en blockchain.

No funcionales:

- Seguridad en la transmisión y almacenamiento de datos.

- Escalabilidad para múltiples usuarios simultáneos.

- Mantenibilidad del código y modularidad.

Arquitectura general

Estilo arquitectónico: Cliente-servidor con separación de frontend y backend.

[Frontend (React)] -> [Backend (FastAPI)] -> [Blockchain Storage]

Componentes principales

Componente	Función principal
Frontend	Interfaz de usuario desarrollada en React, manejo de autenticación y comunicación con el backend.
Backend	API desarrollada en FastAPI, autenticación, cifrado y comunicación con blockchain.
Blockchain	Almacenamiento inmutable de mensajes para garantizar integridad y no repudio.

Tecnologías Utilizadas

- Lenguajes: Python (backend), JavaScript (frontend).

- Frameworks: FastAPI (backend), React (frontend).

- Autenticación: OAuth 2.0 con Google, TOTP.

- Cifrado y firma digital: Implementación de algoritmos criptográficos modernos.

- Blockchain: Uso de una cadena de bloques para almacenamiento seguro de mensajes.

Seguridad y manejo de errores

Seguridad:

- Cifrado de mensajes de extremo a extremo.

- Autenticación multifactor.

- Firma digital para garantizar la autenticidad de los mensajes.

Manejo de errores:

- Validación de entradas en frontend y backend.

- Manejo de excepciones y respuestas adecuadas en la API.

Despliegue

El sistema puede desplegarse en entornos locales o en la nube, utilizando contenedores Docker para facilitar la implementación y escalabilidad.

Conclusión

La arquitectura propuesta garantiza una comunicación segura entre usuarios, integrando mecanismos modernos de autenticación y almacenamiento inmutable mediante blockchain. La separación de responsabilidades entre frontend y backend facilita el mantenimiento y escalabilidad del sistema.