Informe sobre el Sistema de Chat con Historial Protegido por Contraseña

Descripción General

Este informe describe un sistema de chat basado en TCP que permite la comunicación entre múltiples clientes y un servidor. El sistema guarda el historial de mensajes y protege el acceso a este historial mediante contraseñas. La implementación incluye funcionalidades para manejar mensajes públicos y privados, así como la gestión de conexiones de clientes.

Funcionamiento del Sistema

1. Servidor de Chat (Server)

- Aceptación de Conexiones: El servidor escucha en una dirección IP y puerto específicos. Cuando un cliente se conecta, el servidor solicita un nombre de usuario y una contraseña.
- Almacenamiento Seguro de Contraseñas: Las contraseñas de los usuarios se almacenan utilizando hashing SHA-256 para garantizar la seguridad.
- Gestión de Mensajes: El servidor maneja mensajes públicos, mensajes privados dirigidos a usuarios específicos y solicitudes de historial de mensajes.
- Protección del Historial: Para acceder al historial de mensajes, el usuario debe proporcionar su contraseña. El servidor verifica esta contraseña antes de enviar el historial.

2. Cliente de Chat (Client)

- Conexión y Autenticación: El cliente se conecta al servidor, proporcionando un nombre de usuario y una contraseña.
- Interacción con el Servidor: El cliente puede enviar mensajes públicos, enviar mensajes privados a usuarios específicos y solicitar el historial de mensajes. Al solicitar el historial, el cliente debe proporcionar su contraseña para autenticación adicional.
- Recepción de Mensajes: El cliente está diseñado para recibir y mostrar mensajes en tiempo real desde el servidor.

3. Descripción TécnicaSHA-256

SHA-256 es un algoritmo de hash de una sola vía, lo que significa que es computacionalmente impracticable invertir el proceso y recuperar la entrada original a partir del hash generado. Este algoritmo se utiliza ampliamente en aplicaciones de seguridad, incluida la protección de contraseñas, la integridad de los datos y las firmas digitales.

Importación del módulo hashlib:

hashlib es una biblioteca estándar de Python que proporciona una interfaz para muchos algoritmos de hashing, como SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, y MD5.

Instrucciones de Ejecución

1. Configuración del Servidor

- Asegúrese de que Python esté instalado en su sistema.
- Guarde el archivo llamado `server_TCP.py`: en una ruta donde podra ejecutarlo Por ej Escritorio
- Ejecute el servidor desde la ubucacion del archivo con el comando:
  python server_TCP.py
- Para poder deterner el servidor puede ejecutar Ctr+C una vez que se hayan desconectado todos los usuarios de la misma red lan

2. Configuración del Cliente

- Guarde el archivo llamado `client_TCP.py`: en una ubicación donde pueda ejecutarse
- Comparta el archivo a otros ususarios que quieran entrar al servidor una vez compartida siga el paso anterior
- Ejecute el cliente con el comando:
  - python server_TCP.py
- Al ingresar le solicitara una direcion ip por defecto sera el del ususario que contega el archivo server_TCP
- para poder mencontrar la direcion ip ejecute uno los sigientes comando en la terminal bash
  - ifconfig
  - ip -a

  verifique en la cecion donde dice por ej wlp2s0 dentro mire inet donde tendra su direcion ip
- Una vez ingresado le pedira un Ususario y una contraseña si ya previamente te registrasete le solisitara la contraseña de verificacion

3. Comandos del serviror

- Para poder salir del servidor debe ingresar por consola
  - ‘exit’
- Para enviar mensajes privados se sugiere utulizar el carácter @ segido del ususario que este disponibre en el servidor
  - @User ‘mesage’
- Para poder ver el historial del usuario incluyendo los mensajes privados debe ejecutar por consola
  - history

  se visualizara los mensajes publicos del servidor que incluye a los usuarios activos y no activos incluyendo los mensajes privados del ususario que ejecute el comando

Conclusión

El sistema de chat implementado permite la comunicación segura entre múltiples clientes y protege el acceso al historial de mensajes mediante