Secure Chat App with End-to-End Encryption

Introduction

The rapid growth of digital communication demands secure methods for transmitting sensitive data. To address this, we developed a Secure Chat App with end-to-end encryption (E2EE). This real-time chat system ensures that only the intended recipients can read the messages, enhancing privacy and data security.

Built as part of a cybersecurity internship, this application utilizes Flask, Socket.IO, and Python cryptography to implement encrypted message exchange and secure user authentication.

Abstract

This project presents a lightweight web-based chat application that offers secure messaging between users using end-to-end encryption. Each user can register and log in to the system securely. Messages exchanged are encrypted on the client side and decrypted only by the receiver, preventing any unauthorized access during transmission. This project demonstrates practical implementation of secure communications, session handling, and encrypted real-time data transfer.

Tools and Technologies Used

- Flask (Python) - Web framework for backend
- Flask-SocketIO - Real-time communication between users
- HTML/CSS/JS - Frontend interface with cybersecurity-themed UI
- bcrypt - Secure password hashing
- AES encryption - For securing chat messages
- Socket.IO - Enabling encrypted client-server messaging

Steps Involved in Building the Project

1. User Authentication:
   - Registration and login system using bcrypt-hashed passwords.
   - Session management using Flask.

2. Real-Time Communication:
   - Socket.IO integration for message exchange.

- Each user is connected to a unique room for private communication.

3. End-to-End Encryption:
   - Messages are encrypted on the sender's side using AES.
   - Only the recipient can decrypt and view the original message.

4. Frontend Design:
   - Cybersecurity-themed responsive UI for chat.
   - Message input, recipient targeting, and logout functionality.

5. Secure Chat Functionality:
   - Username auto-fetched from login.
   - Messages are visible only to the intended recipient.

Conclusion

This project demonstrates a practical and secure real-time communication system, integrating encryption techniques with modern web technologies. It reflects a foundational approach to implementing secure systems in cybersecurity, aligning with the current need for privacy-focused digital applications. The system can be expanded in the future to include file sharing, group chats, and stronger cryptographic protocols.