Overview

The Secure Online Communication Platform is a web-based application designed to facilitate secure communication and data exchange over the Internet. It emphasizes confidentiality, integrity of data, and secure cryptographic key management. This platform serves various online communication needs, focusing on security and privacy.

Website Structure and Functionalities

- **Home Page (/)**:
- **Overview Section**: Introduces the platform and its significance in secure communication.
- **Feature Highlights**: Summarizes key features like end-to-end encryption, secure messaging, and file transfer.
- **Navigation Links**: Links to login and register pages.
- **Access Control**: Redirects to the user's personalized page upon successful login.
- **Login Page (`/login`)**:
- **Function**: Allows existing users to log in using their username and password.
- **Security**: Implements bcrypt for password hashing, ensuring secure authentication.
- **User Feedback**: Displays error messages for invalid credentials.
- **Redirection**: On successful login, redirects to the user's personalized home page.
- **Registration Page (`/register`)**:
- **Function**: Enables new users to create an account.
- **RSA Key Generation**: Generates a unique RSA key pair for each user during registration.
- **Database Integration**: Stores username, hashed password, and RSA keys in the SQLite database.
- **Error Handling**: Provides feedback on username availability.
- **User's Personalized Home Page (/ after login)**:
- **Personalized Welcome**: Displays a greeting with the user's username.
- **Logout Functionality**: Includes a logout button for users to exit their session securely.
- **Logout Functionality (`/logout`)**:
- **Session Termination**: Clears the user session and redirects to the login page.

Security Features

- **End-to-End Encryption**:
- Currently, RSA keys are generated but not utilized for end-to-end encryption of messages or files.
- **User Authentication**:
- Securely implemented using bcrypt for password hashing.
- **Secure File Transfer and Messaging**:

- Not yet implemented. Future integration should include secure file upload/download and real-time messaging capabilities using end-to-end encryption.
- **Encrypted Storage**:
- User credentials and RSA keys are stored in the database, but no functionality for encrypted storage of user messages or files is currently implemented.
- **Key Management**:
- Generation and storage of RSA keys are implemented. However, there's a lack of mechanisms for key distribution, rotation, and revocation.
- **HTTPS Protocol**:
- The application should be configured to use HTTPS for secure data transmission, though this is not detailed in the current setup.

Missing Functionalities and Future Improvements

- **End-to-End Encryption for Communication**:
- Implement the use of stored RSA keys for encrypting messages and files.
- **Secure File Transfer and Real-Time Messaging**:
- Develop features for encrypted file sharing and real-time text messaging.
- **Advanced Key Management**:
- Implement secure methods for key distribution and management, including key rotation and revocation procedures.
- **Encrypted Data Storage**:
- Enhance the system to store user messages and files in an encrypted format.
- **Comprehensive User Dashboard**:
- Develop a dashboard for users to manage their settings, view message history, and handle files.
- **Admin Panel for User Management**:
- Create an admin interface for managing user accounts and access control.
- **API and Interface Security**:
- Ensure secure APIs for potential third-party integrations.
- **Scalability and Performance Optimization**:
- Optimize the platform for handling a large number of users and high-volume data transfer.
- **Compliance and Data Privacy**:
- Ensure the platform aligns with relevant data protection regulations and standards.

Conclusion

The Secure Online Communication Platform is a robust foundation for secure online interactions, with essential features like user authentication and RSA key management. However, to fully realize its potential and align with the initial project report, significant enhancements are needed, particularly in end-to-end encryption, secure messaging, file transfer, and advanced cryptographic key management. The platform's future development roadmap should focus on these areas to provide a comprehensive and secure communication experience.