

Projectech · projectech.in

Real-Time Encrypted Chat Application with Secure File Sharing

Title

Real-Time Encrypted Chat Application with Secure File Sharing

Abstract

This project presents a secure real-time chat application designed for private and group communication with encrypted messaging and file sharing capabilities. The system combines real-time communication technologies with security mechanisms to provide authenticated messaging, online presence tracking, typing indicators, media sharing, and searchable chat history.

Problem Statement

Modern communication platforms often depend on third-party services where users have limited control over privacy, customization, and data management. Educational institutions and organizations may require customized communication solutions with secure messaging and controlled access.

Objectives

1. Develop a real-time communication platform for one-to-one and group chats.
2. Implement secure message exchange using encryption techniques.
3. Enable file and image sharing within conversations.
4. Provide authentication, online status, and chat history features.
5. Demonstrate practical full-stack and cybersecurity concepts.

System Architecture

The system follows a client-server architecture. Users interact with the frontend interface, which communicates with a backend server through real-time communication protocols. The server manages authentication, message routing, encryption handling, file processing, and database operations.

Technologies Used

WebSocket, Socket.io, AES-256 Encryption, RSA Encryption, Database Management, Authentication, File Storage, Real-Time Communication.

Working Principle

1. Users register and authenticate into the application.
2. A real-time connection is established between clients and the server.
3. Messages are processed and protected using encryption methods.
4. Encrypted messages are delivered securely to intended recipients.
5. Files and images are uploaded and shared through chat sessions.
6. User activity updates such as typing and online status are synchronized instantly.

7. Conversation data is stored and retrieved from the database.

Key Features

- Real-time one-to-one messaging
- Group chat functionality
- Encrypted communication
- File and image sharing
- User authentication
- Online presence tracking
- Typing indicators
- Chat search and history management

Applications

- Educational communication platforms
- Organization-specific messaging systems
- Secure team collaboration tools
- Private communication applications
- Cybersecurity learning projects

Prerequisites

Basic knowledge of frontend and backend development, databases, APIs, networking concepts, and fundamental encryption concepts.

Limitations

- Security depends on correct encryption and key management.
- Large-scale deployment requires additional server optimization.
- Storage capacity depends on infrastructure.
- Advanced security auditing requires additional customization.
- Enterprise compliance features are not included by default.

Future Scope

Future enhancements may include voice/video calling, AI-assisted chat features, advanced user roles, mobile applications, cloud scaling, multi-device synchronization, and improved security auditing.

Conclusion

The Real-Time Encrypted Chat Application with Secure File Sharing demonstrates the integration of real-time networking, encryption, database management, and full-stack development. It provides a foundation for building customized secure communication platforms.