VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

B.Tech. Winter Semester 2024-25
School Of Computer Science and Engineering (SCOPE)

Project Work
Information Security

Slot: B1+TB1
Faculty Name: Santhi H.
Team Name: Cryptonite
Team Number: 7

Contents

1 Team Members

Divya Lakshi H: 22BCE2544
Apurva Mishra: 22BCE2791
Taware Harsh Vilas: 22BCE2878
Tanmay Patel: 22BCE2911
Mohammad Faiz Khan: 22BCE2995

2 Title

P2P Chat

3 Aim

To develop a peer to peer chat application which is end to end encrypted and does not require login to ensure complete user privacy

4 Objectives

- **Key Exchange**: Implement a method for securely exchanging encryption keys between peers using the shared secret phrase without relying on a central server.
- **End-to-End Encryption**: Ensure all messages are encrypted from sender to recipient, preventing any intermediary from reading them.
- **Peer Discovery**: Develop a decentralized mechanism for peers to discover each other using the shared secret phrase.
- **Secure Messaging**: Implement a secure messaging protocol that handles message delivery, order, and potential loss.
- **User Interface**: Create a user-friendly web interface for sending and receiving messages, managing connections, and setting up the chat.

5 Planned Salient Features

- **Secret Phrase Based Connection**: Users connect using a shared secret phrase.
- **End-to-End Encryption**: All communication is end-to-end encrypted.
- **Decentralized Peer Discovery**: No central server is required for finding peers.
- **Open Source**: Make the application open source to allow for community review and improvement.

6 Required Technologies

- **Programming Language**: Rust and Javascript
- **Networking Libraries**: Iroh
- **User Interface Framework**: React
- **Version Control**: Git