**TCP Client – Server**

# Mô tả

Ứng dụng giao tiếp client - server sử dụng socket. Có hỗ trợ:

- Multi-user

- Kết nối được mã hóa bằng TLS/SSL (sử dụng OpenSSL)

- Đăng nhập với tài khoản và mật khẩu

- Lưu lịch sử chat

- Có thể giám sát gói tin với `tcpdump` hoặc `Wireshark`

# Kiến trúc hệ thống

## Các thành phần chính

* Client application: Thiết lập kết nối tới server, gửi tin nhắn
* Server application: Xử lí kết nối từ các client, xác thực, lưu lịch sử tin nhắn
* OpenSSL: Bảo mật toàn bộ dữ liệu gửi/nhận bằng TLS
* Epoll: cho phép server xử lý nhiều client đồng thời
* Authenticate: xác thực từ file user.txt
* Logger: lưu lịch sử tin nhắn vào chat.log

## Luồng xử lý

* Bước 1: Khởi tạo server
* Bước 2: Khởi tạo client, kết nối đến server qua TCP
* Bước 3: Thực hiện TLS handshake
* Bước 4: Server yêu cầu đăng nhập → xác thực username/password
* Bước 5: Sau khi xác thực thành công:
  + Client có thể gửi/nhận tin nhắn
  + Server định tuyến tin nhắn đến các client khác
  + Ghi lịch sử vào chat.log
* Bước 6: Nếu client ngắt kết nối

## Dữ liệu hệ thống

* users.txt: Danh sách các username/password
* chat.log: Ghi lịch sử tin nhắn: người gửi, nội dung
* cert.pem, key.pem: Chứng chỉ bảo mật tự ký để mã hóa

## Công nghệ sử dụng

* Ngôn ngữ: C
* Giao tiếp: TCP Socket
* Đồng bộ I/O: epoll (Linux)
* Bảo mật: TLS/SSL (OpenSSL)

## Yêu cầu

### Yêu cầu chức năng

### Yêu cầu phi chức năng

# High Level Design (HLD)