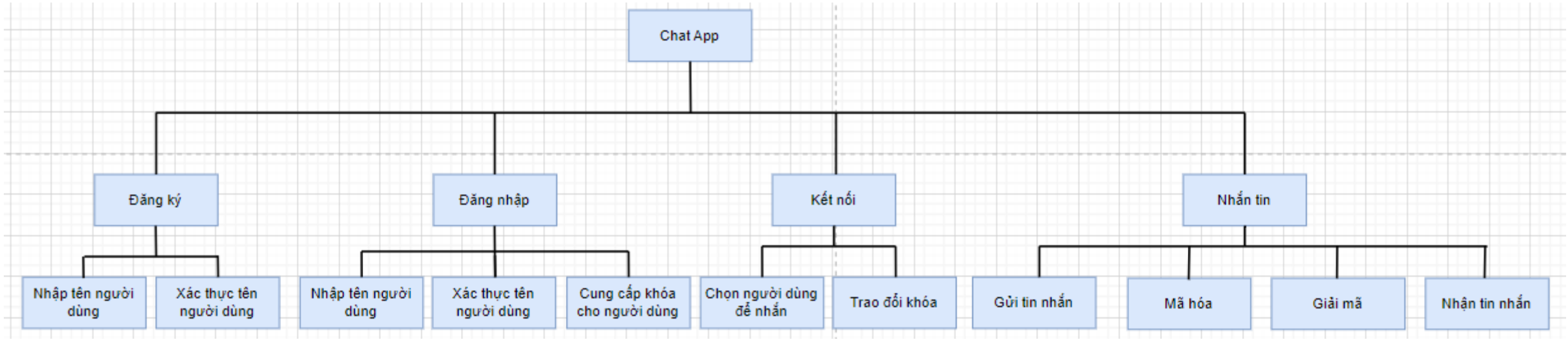
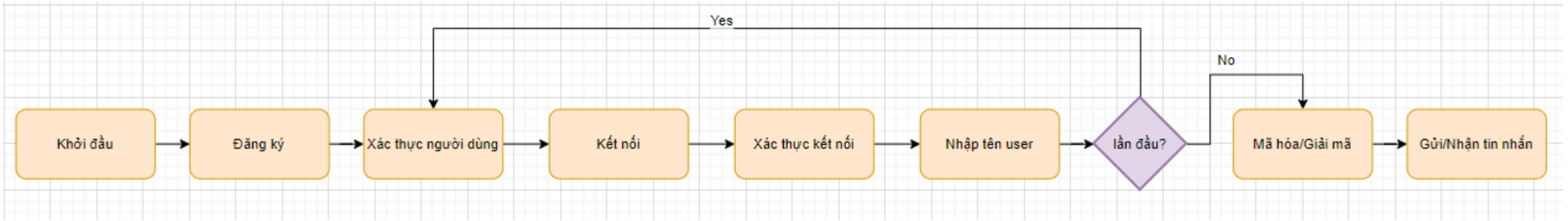
1. INTRODUCTION: Nhóm 10: 20127192_20127066

Mục tiêu	Xây dựng một ứng dụng nhắn tin cơ bản với các chức năng đăng nhập, xác thực trao đổi khóa an toàn và nhắn tin tích hợp mã hóa đầu cuối. Chương trình chat được xây dựng dựa trên mô hình client-server, nơi mà server quản lý các kết nối từ nhiều clients và chuyển tiếp thông điệp giữa chúng. Client gửi thông điệp tới server và nhận phản hồi. Server thì tiếp nhận các thông điệp từ các clients, xử lý chúng, và có thể phân phối các thông điệp đến các clients khác đảm bảo bảo mật mã hóa đầu cuối.	
Mô tả	Giao tiếp trực tiếp: Người dùng có thể gửi và nhận tin nhắn văn bản với nhau qua giao diện đơn giản và thân thiện. Quản lý người dùng: Chương trình hỗ trợ quản lý người dùng, cho phép họ đăng nhập và tham gia trò chuyện. Bảo mật: Dữ liệu được mã hóa và giải mã trước khi gửi và sau khi nhận, đảm bảo tính bảo mật trong quá trình truyền thông. Tính linh hoạt: Chương trình hỗ trợ nhiều người dùng cùng lúc. Client: Đại diện cho người dùng cuối, gửi và nhận tin nhắn từ server thông qua giao diện người dùng. Server: Quản lý kết nối từ các clients, xử lý tin nhắn và phân phối chúng đến các clients khác nếu cần. Giao thức truyền thông: Sử dụng giao thức TCP/IP để đảm bảo tính ổn định và toàn vẹn trong quá trình truyền thông.	
Thuật toán sử dụng	AES (Advanced Encryption Standard): Được sử dụng để mã hóa và giải mã dữ liệu, đảm bảo tính bảo mật trong quá trình truyền thông. TCP (Transmission Control Protocol): Sử dụng làm giao thức truyền thông chính giữa client và server, đảm bảo dữ liệu được truyền một cách đáng tin cậy và theo thứ tự. Diffie-Hellman: Sử dụng để tạo kênh truyền khóa an toàn đảm bảo bảo mật khi chia sẽ các khóa chung.	
Yêu cầu	**Chức năng**	**Phi chức năng**
	Xác thực: Tài khoản của người dùng phải hợp lệ trên hệ thống để sử dụng dịch vụ. **Tạo khóa**: Chương trình cung cấp cho người dùng dịch vụ tạo khóa trên máy người dùng **Lưu trữ**: Dữ liệu trao đổi được lưu tạm thời. **Gửi tin nhắn**: Khả năng gửi tin nhắn văn bản có bao gồm cả ký tự đặc biệt . **Thông báo**: hiển thị thông báo cho người dùng trả về kết quả của các sự kiện.	**Quản lý Phiên**: Đảm bảo việc quản lý phiên an toàn để ngăn chặn truy cập trái phép. **Giao diện thân thiện**: Hỗ trợ nhiều nền tảng và thiết bị, bao gồm cả ứng dụng di động. **Quản lý người dùng**: Kiểm soát và quản lý lưu lượng giúp vận hành tốt khi có số lượng người dùng cùng lúc quá cao. **Hiệu suất**: Sử dụng dịch vụ lưu trữ của bên thứ 3 để tối ưu khả năng lưu trữ mà vẫn đảm bảo an toàn.
Môi trường	Ngôn ngữ: Python Database framework: Flask, Flask-Session, fakerFlask-SQLAlchemy Tool nhắn tin: socket Thư viện hỗ trợ: Tkinter, Crypto, random, hashlib,...	

2. FUNCTION TREE



3. Flow


Yes
No
Khởi đầu
Đăng ký
Xác thực người dùng
Kết nối
Xác thực kết nối
Nhập tên user
lần đầu?
Mã hóa/Giải mã
Gửi/Nhận tin nhắn

4. TESTCASE

TEST CASES: Chat App

Test Case Name	Preconditions	Test Steps	Expected Results	Actual Results	Execution Status	Bug Severity	Bug Priority
Alice và Bob chưa trao đổi khóa và nhắn cho nhau (cả 2 đều online)	2 Người dùng phải là người dùng hợp lệ đã đăng ký thành công, chưa trao đổi khóa cho nhau'	B1: Bob chọn tên Alice ở cột bên phải B2: Alice chọn tên Bob B3: Bob nhắn tin cho Alice	Nếu 2 người dùng đã trao đổi khóa cho nhau và online có thể nhắn tin trực tiếp cho nhau	Đầu tiên, Bob chọn tên Alice ở cột bên phải, sẽ hiển thị thông báo "Bạn và người này cần cùng phòng để trao đổi khóa". Sau khi Alice chọn tên Bob, chatbox sẽ hiển thị "Bạn và người này đã trao đổi khóa thành công" và nhắn tin cho nhau	Pass	High	High
Alice và Bob đã có lịch sử nhắn tin trước đó và Alice nhắn tin cho Bob khi Bob đang offline	2 Người dùng phải là người dùng hợp lệ, đã có lịch sử nhắn tin trước đó, Bob offline	B1: Alice và Bob trao đổi khóa cho nhau B2: Alice và Bob nhắn cho nhau B3: Bob offline B4: Alice nhắn cho Bob	Khi một người dùng đang offline, nếu người nhắn và họ đã có lịch sử nhắn trước đó, thì người nhắn vẫn có thể nhắn được, và sau khi người nhận online trở lại thì các tin nhắn chưa đọc vẫn sẽ hiển thị lên đầy đủ.	Alice vẫn có thể nhắn được cho Bob, và sau khi Bob online trở lại thì các tin nhắn chưa đọc vẫn sẽ hiển thị lên đầy đủ.	Pass	Medium	Medium
Alice và Bob chưa trao đổi khóa, Alice nhắn tin cho Bob khi Bob đang offline	2 Người dùng phải là người dùng hợp lệ,chưa trao đổi khóa, Bob offline	B1: Alice chưa trao đổi khóa với Bob B2: Bob offline B3: Alice nhắn cho Bob	Khi chưa trao đổi khóa, người nhắn không thể nhắn cho người nhận dù bên kia đang online hay offline.	Cửa sổ chat của Alice sẽ hiển thị thông báo "Bạn và người này cần cùng phòng để trao đổi khóa"	Pass	High	High
Alice và Bob đã trao đổi khóa, Eve và Alice chưa trao đổi khóa và nhắn cho nhau	3 Người dùng hợp lệ	B1: Alice và Bob trao đổi khóa cho nhau B2: Alice và Bob nhắn cho nhau B3: Alice chưa trao đổi khóa với Eve B4: Eve nhắn cho Alice	Nếu người thứ 3 chưa trao đổi khóa sẽ không thể nhắn tin cho đối phương được và sau khi trao đổi khóa, các cặp khóa hoàn toàn không bị xáo trộn hay nhầm lẫn lẫn nhau.	Hiển thị thông báo bên Eve là "Bạn và người này cần cùng phòng để trao đổi khóa" và khi Alice chọn vào tên Eve, lúc này sẽ hiển thị thông báo "Bạn và người này đã trao đổi khóa thành công" và lúc này Alice và Eve có thể nhắn cho nhau.	Pass	High	High
Alice và Bob đã trao đổi khóa, Alice và Eve đã trao đổi khóa, nhưng Bob và Eve chưa trao đổi khóa và nhắn cho nhau	3 Người dùng hợp lệ	B1: Alice và Bob trao đổi khóa cho nhau B2: Alice và Bob nhắn cho nhau B3: Alice và Eve trao đổi khóa cho nhau B4: Alice và Eve nhắn cho nhau B5: Eve và Bob chưa trao đổi khóa cho nhau B6: Eve và Bob nhắn cho nhau	Nếu người thứ 3 chưa trao đổi khóa sẽ không thể nhắn tin cho đối phương được và sau khi trao đổi khóa, các cặp khóa hoàn toàn không bị xáo trộn hay nhầm lẫn lẫn nhau.	Hiển thị thông báo bên Eve là "Bạn và người này cần cùng phòng để trao đổi khóa" và khi Alice chọn vào tên Eve, lúc này sẽ hiển thị thông báo "Bạn và người này đã trao đổi khóa thành công" và lúc này Alice và Eve có thể nhắn cho nhau.	Pass	High	High
Alice với Bob đã trao đổi khóa, Alice với Eve đã trao đổi khóa và Bob với Eve đã trao đổi khóa, cả 3 nhắn tin lẫn nhau	3 Người dùng hợp lệ	B1: Alice và Bob trao đổi khóa cho nhau B2: Alice và Bob nhắn cho nhau B3: Alice và Eve trao đổi khóa cho nhau B4: Alice và Eve nhắn cho nhau B5: Eve và Bob trao đổi khóa cho nhau B6: Eve và Bob nhắn cho nhau	Các cặp khóa được trao đổi lẫn nhau, mà không bị nhầm lẫn trong quá trình nhắn giữa các người dùng trên.	Cả 3 cặp nhắn tin với nhau và không gây ra lỗi	Pass	High	High

1. APP SCREENS