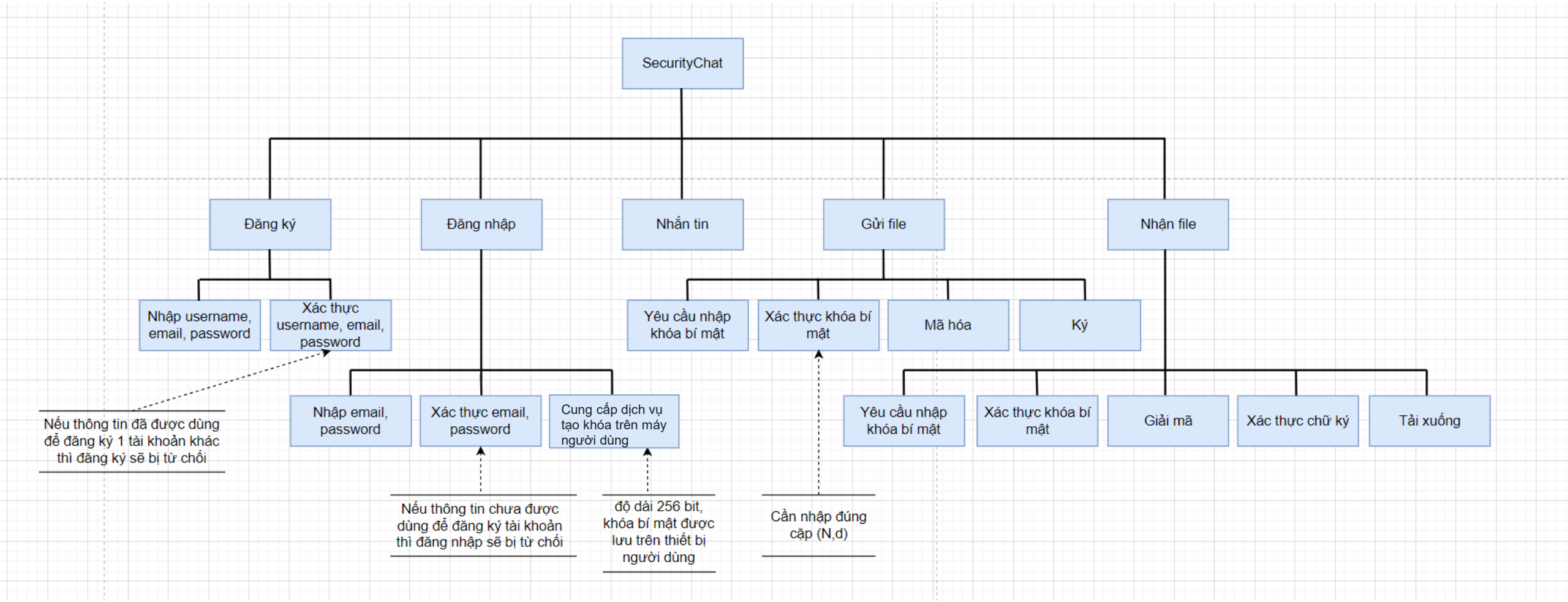
1. INTRODUCTION: Nhóm 03: 20127192_20127066_20127299

Mục tiêu	Xây dựng một website trao đổi tin nhắn có thể đính kèm tệp dữ liệu số đa phương tiên có các yêu cầu bảo mật như sau: Website có chức năng gửi nhận tin nhắn tương tự như các ứng dụng Messenger, Skype,... Nhưng xây dựng ở mức độ cơ bản các chức năng và các yêu cầu bảo mật. Website cho phép người dùng trao đổi thông tin an toàn và riêng tư với người khác thông qua một Chatroom cho 2 người. Các file đính kèm sẽ được mã hóa với các thuật toán AES, RSA, và được ký tên xác nhận nguồn gốc với thật toán SHA. Dữ liệu trao đổi qua lại trong Chatroom sẽ chỉ được lưu trữ tạm thời, và sau một khoảng thời gian cố định kể từ ngày bắt đầu Chatroom, dữ liệu sẽ tự động được xóa. Các dữ liệu về Publickey, PrivateKey và các file được lưu trữ cục bộ. Webiste sẽ chỉ quản lý thông tin các nhân của các người dùng đã đăng ký thành công.	
Mô tả	Cài đặt Website trao đổi tin nhắn và dữ liệu số đa phương tiện có bảo mật. Người dùng khi đăng ký tài khoản thành công, sẽ được cung cấp dịch vụ tạo một cặp khóa gồm Public Key và Private Key trên máy người dùng. Người dùng tìm bạn, thêm bạn, tham gia vào các phòng chat và nhắn tin cho nhau và cũng có thể đính kèm tệp dữ liệu số đa phương tiện được mã hóa và khi người gửi và nhận tải về hay tải lên đều cần xác thức bằng Private Key.	
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:** Người dùng tạo cặp khóa công khai và bí mật trên máy người dùng từ dịch vụ do chương trình cung cấp trên máy người dùng. **Lưu trữ**: Dữ liệu trao đổi được lưu tạm thời chúng trong vòng 7 ngày. **Gửi tin nhắn**: Khả năng gửi văn bản, hình ảnh, video, tệp âm thanh và tệp đính kèm khác. **Tải lên và Tải xuống**: Cho phép người dùng tải lên các tệp đính kèm từ thiết bị của họ. **Mã hóa Tệp**: Mã hóa tệp đính kèm để đảm bảo an toàn và bảo mật dữ liệu. **Thông báo**: Hiển thị thông báo cho người dùng theo các kết quả thực hiện các sự kiện.	**Quản lý Phiên**: Đảm bảo việc quản lý phiên an toàn để ngăn chặn truy cập trái phép. **Tương thích di động**: Hỗ trợ nhiều nền tảng và thiết bị, bao gồm cả ứng dụng di động **Tìm kiếm hiệu quả**: Cung cấp khả năng tìm kiếm nhanh chóng và sát nhất với từ khóa. **Backup và Phục hồi**: Hệ thống sao lưu thường xuyên để bảo vệ dữ liệu khỏi mất mát. **Quản lý lưu lượng người dùng**: Kiểm soát và quản lý lưu lượng giúp website có thể vận hành tốt khi có số lượng người dùng cùng lúc quá cao. **Tích hợp Mạng xã hội**: Cho phép chia sẻ nhanh chóng từ nền tảng khác và tích hợp với các dịch vụ mạng xã hội. **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. **Khả năng sử dụng**: Có hướng dẫn sử dụng rõ ràng, đáng tin cậy, giao diện thân thiện với người dùng.
Môi trường	Ngôn ngữ: Python, html, css, javascript Máy chủ: localhost Kali linux Database framework: Flask, Flask-Session, fakerFlask-SQLAlchemy Tool nhắn tin: flask_socketio, gevent, gevent-websocket Thư viện hỗ trợ: Pillow 9.5, Crypto	

2. FUNCTION TREE



3. TESTCASE

TEST CASES: Securitychat

Test Case Name	Preconditions	Test Steps	Input Data	Expected Results	Actual Results	Execution Status	Bug Severity	Bug Priority	Notes
Đăng ký thiếu thông tin	Thông tin dùng để đăng ký chưa được dùng để đăng ký tài khoản nào khác	B1: Nhấn vào "Register" để đăng ký B2: Nhập Thông tin tên vào cột "Name" B3: Bỏ trống thông tin "Email address" B4: Nhập mật khẩu và nhấn vào nút "Sign up"	Tên và mật khẩu dùng để đăng ký	Đăng ký không thành công	Hiển thị thông báo lỗi "Please provide your email", đăng ký không thành công	Pass	Low	Low	
Đăng nhập sai email/mật khẩu	Tài khoản đã đăng ký thành công	B1: Nhấn vào "Login" để đăng nhập B2: Nhập email vào cột "Email address" B3: Bỏ trống thông tin "Password" B4: Nhập mật khẩu và nhấn vào nút "Login"	Email dùng để tạo tài khoản	Đăng nhập không thành công	Hiển thị thông báo lỗi "Invalid username and/or password!", đăng nhập không thành công	Pass	High	High	
Thêm bạn đã tồn tại	2 Người dùng phải là người dùng hợp lệ đã đăng ký thành công	B1: Nhấn vào nút thêm bạn trên menu B2: Nhập tên người dùng muốn tìm B3: Nhấn vào nút "Add"	Tên người dùng muốn tìm	Thêm bạn thành công	Trạng thái người dùng trong mục tìm kiếm chuyển sang "Added", thêm người dùng thành công	Pass	Medium	Medium	Nếu tên người dùng chưa tồn tại, thanh tìm kiếm không hiển thị kết quả
Nhắn tin với ký tự đặc biệt	2 Người dùng phải là người dùng hợp lệ đã đăng ký thành công đang chat với nhau	B1: Nhấn vào thanh chat và gõ chuỗi ký tự đặc biệt B2: Nhấn gửi tin nhắn B3: Làm mới lại trang	Chuỗi "!@#$%^&*()_+"	Tin nhắn vẫn gửi đi không gặp lỗi	Tin nhắn vẫn gửi đi không gặp lỗi	Pass	Medium	Medium	

4. TESTCASE

TEST CASES: Securitychat

Test Case Name	Preconditions	Test Steps	Input Data	Expected Results	Actual Results	Execution Status	Bug Severity	Bug Priority	Notes
Gửi file đa phương tiện	2 người dùng hợp lệ, đang chat, file đa phương tiện đang tồn tại trên máy người gửi	B1: Nhấn vào nút gửi file B2: Chọn file đa phương tiện muốn gửi B3: Nhấn vào "Open file" để gửi file B4: Nhập khóa bí mật người gửi B5: Gửi file thành công	File "Hello.mp4"	File đã được mã hóa và gửi cho người nhận	File đã được mã hóa và gửi cho người nhận	Pass	High	High	
Xóa tin nhắn đã nhắn	2 Người dùng hợp lệ đang chat với nhau, tin nhắn đã được chat	B1: Nhấn nút mũi tên của 1 tin nhắn đã nhắn B2: Chọn lựa chọn "Delete Message" B3: Hiển thị thông báo pop up xác nhận xóa B4: Nhấn nút "Delete Message" B5: Làm mới lại trang		Xóa tin nhắn thành công	Tin nhắn đã xóa không còn hiển thị trong chatbox, Xóa tin nhắn thành công	Pass	Low	Low	
Nhập key mã hóa sai	2 Người dùng hợp lệ đang chat với nhau, file đa phương tiện chưa được mã hóa	B1: Chọn file đa phương tiện muốn gửi B2: Nhập sai khóa bí mật người gửi B3: Nhấn nút gửi file	Chuỗi khóa bí mật sai "12345678"	File không được gửi	File không được gửi	Pass	High	High	Cần nhập đúng cả 2 yếu tố của khóa bí mật người gửi (N,d) để mã hóa đúng
Nhập key giải mã sai	2 Người dùng hợp lệ đang chat với nhau, file đa phương tiện đã được gửi và mã hóa	B1: Nhấn vào file muốn tải xuống trong chatbox B2: Nhập sai khóa bí mật người nhận	Chuỗi khóa bí mật sai "12345678"	File tải về bị lỗi, tải về không thành công	Hiển thị File tải về dạng "tên file.htm" bị lỗi, tải về không thành công	Pass	High	High	Cần nhập đúng cả 2 yếu tố của khóa bí mật người nhận (N,d) để giải mã đúng

1. POC SCREENS