TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN 01:

WEBSITE TRAO ĐỔI DỮ LIỆU SỐ ĐA PHƯƠNG TIỆN CÓ BẢO MẬT

GV hướng dẫn:

Nguyễn Đình Thúc

Sinh viên thực hiện:

20127192 - Trần Anh Huy

20127066 – Nguyễn Nhật Quân

20127299 – Trần Hoàng Minh Quang

Thành phố Hồ Chí Minh, ngày 28 tháng 3 năm 2024

1. TỔNG QUAN

1.1. THÔNG TIN NHÓM: NHÓM 10

MSSV	Họ tên	Email
20127192	Trần Anh Huy	20127192@student.hcmus.edu.vn
20127066	Nguyễn Nhật Quân	20127066@student.hcmus.edu.vn
20127299	Trần Hoàng Minh Quang	20127299@student.hcmus.edu.vn

1.2. CÁC CÔNG VIỆC ĐÃ HOÀN THÀNH

STT	Công việc	Tiến độ
1	Hoàn thiện code	100%
2	Triển khai các test case	100%
3	Viết báo cáo	100%
4	Đánh giá nhận xét	100%
5	Slide báo cáo cuối kỳ	100%

2. NỘI DUNG

2.1. GIỚI THIỆU

2.1.1 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, Viber,... Nhưng được 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 thuật 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.

2.1.1 Mô tả:

Cài đặt Website trao đổi tin nhắn và dữ liệu số đa phương tiện có bảo mật thông qua các room chat.

- 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.
- Người dùng mang tính tương đối với 2 vai trò người gửi và người nhận, tuy thuộc vào tính huống và hoàn cảnh.
- Người gửi và người nhận tham gia Chatroom và xác minh nhau thông qua việc trao đổi Publickey.
- Người dùng tham gia vào các phòng chat có thể 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.
- Hai bên có thể trao đổi thông qua tin nhắn và có thể đính kèm tệp dữ liệu số đa phương tiện. Trong đó người gửi sẽ thực hiện gửi file dữ liệu, file sẽ được mã hóa sử dụng AES và tạo chữ ký sử dụng RSA và SHA. Người nhận sẽ nhận file và thực hiện giải mã sử dụng AES, giải mã chữ ký bằng RSA và xác nhận nguồn gốc với SHA. Nếu xác nhận chữ ký 4 chính xác, thì việc gửi file mã hóa đã đúng và hoàn thành.
- Chatroom giữa 2 người sẽ có thời hạn lưu trữ là 07 ngày kể từ ngày tạo, và sẽ được tự động xóa sau khi hết thời hạn.

2.2. YÊU CẦU

2.2.1 Yêu cầu 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
- 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.

2.2.2 Các thành phần chính:

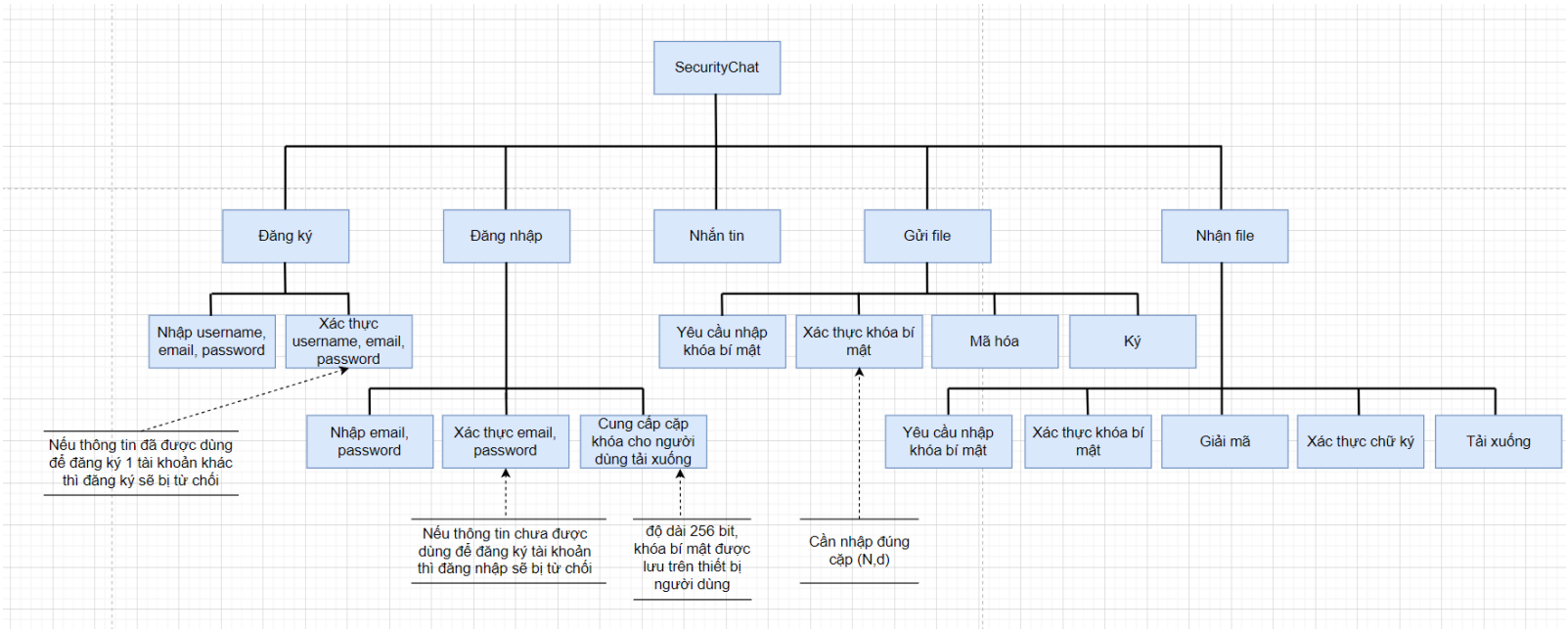
- Quản lý Phiên: Đảm bảo việc quản lý phiên an toàn để ngăn chặn truy cập trái phép.
- Tương thích di động: Hỗ trợ nhiều nền tảng và thiết bị, bao gồm cả ứng dụng di động
- Tìm kiếm hiệu quả: Cung cấp khả năng tìm kiếm nhanh chóng và sát nhất với từ khóa.
- Backup và Phục hồi: Hệ thống sao lưu thường 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 từ nền tảng khác và tích hợp 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.

2.2.3 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

2.3. FUNCTION TREE:



Một số lưu ý:

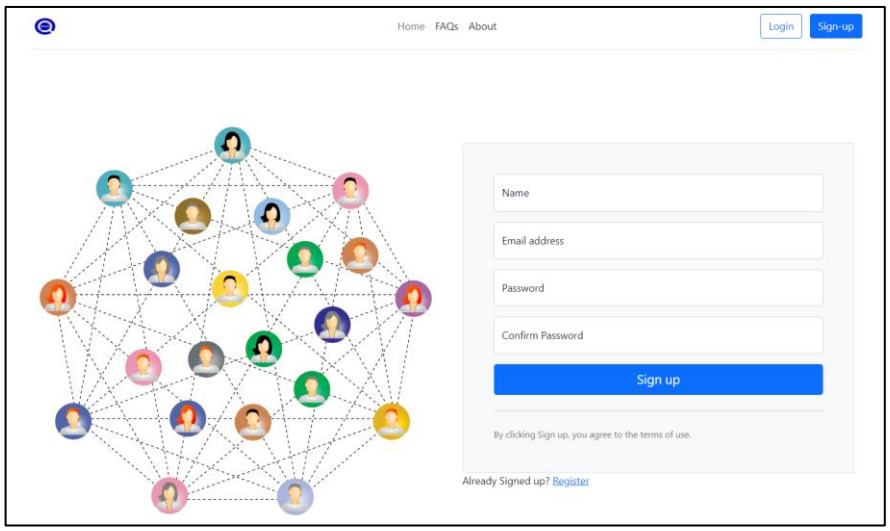
1. Trong quá trình đăng ký, nếu 1 miền thông tin nào đó bị thiếu, sẽ hiển thị thông báo lỗi và yêu cầu người dùng nhập vào đầy đủ thông tin.
2. Sau khi người dùng nhập đầy đủ thông tin, chương trình tiến hành xác thực xem các thông tin có hợp lệ hay không, có từng được sử dụng hay không.
3. Chương trình cung cấp dịch vụ cho phép người dùng tạo cặp khóa (độ dài 256bit) trên thiết bị người dùng.
4. Khi chương trình yêu cầu nhập khóa bí mật, người dùng cần nhập đúng cặp nhân tố (N,d), nếu sai một trong 2 đều sẽ giải mã thất bại.

2.4. TEST CASES:

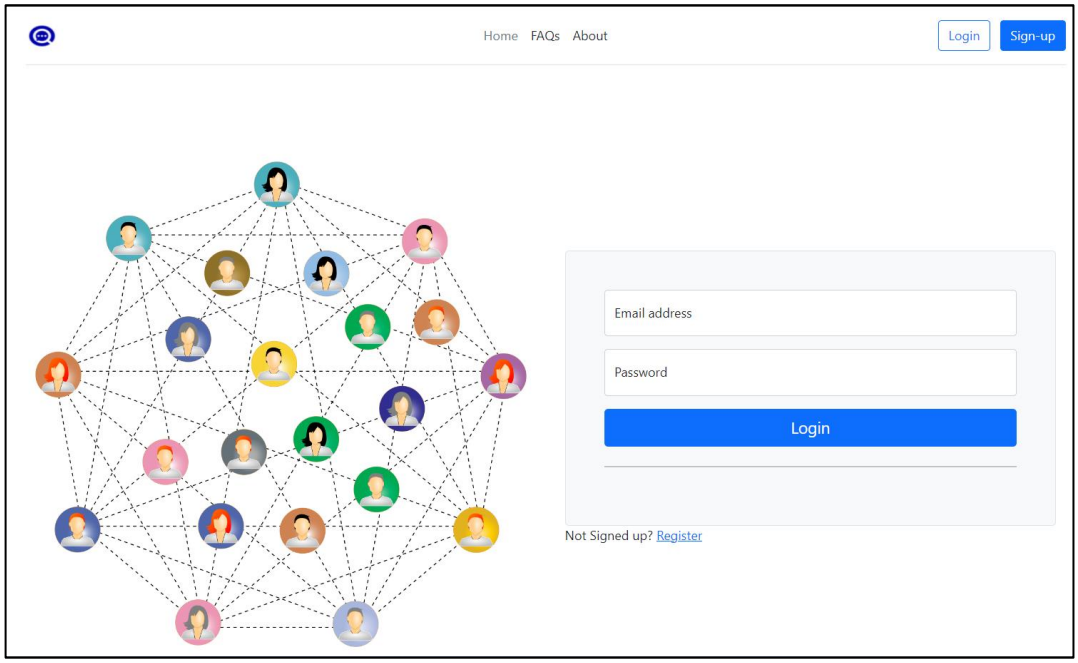
TEST CASES: Securitychat

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	
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

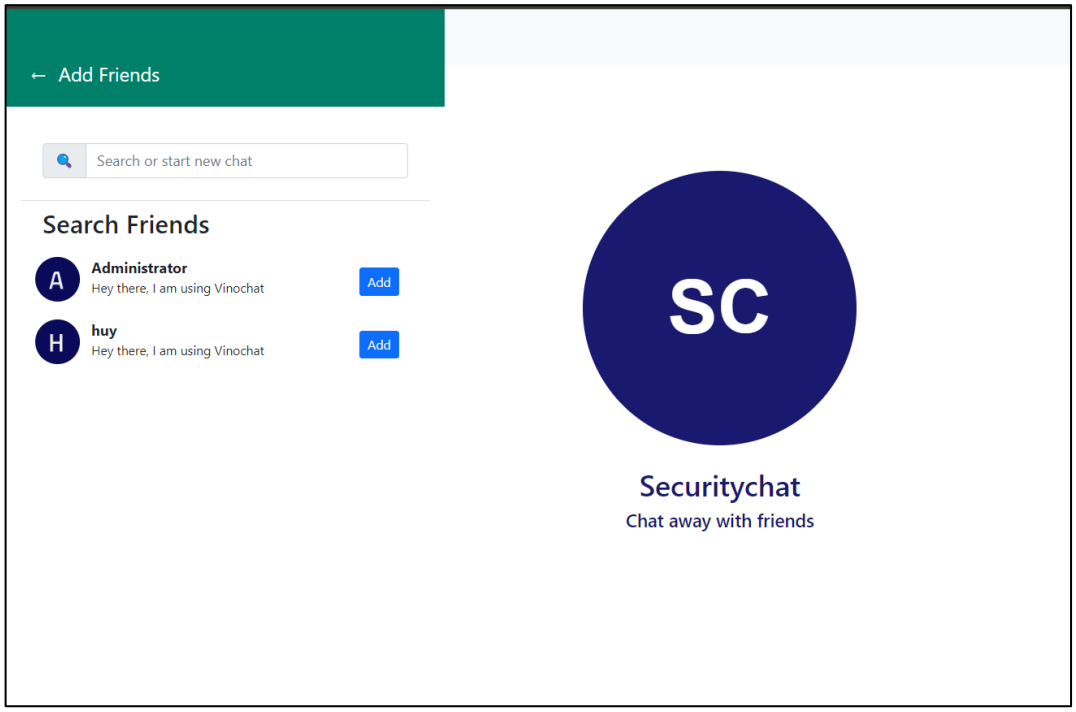
2.5. MỘT SỐ GIAO DIỆN MÀN HÌNH CHƯƠNG TRÌNH:



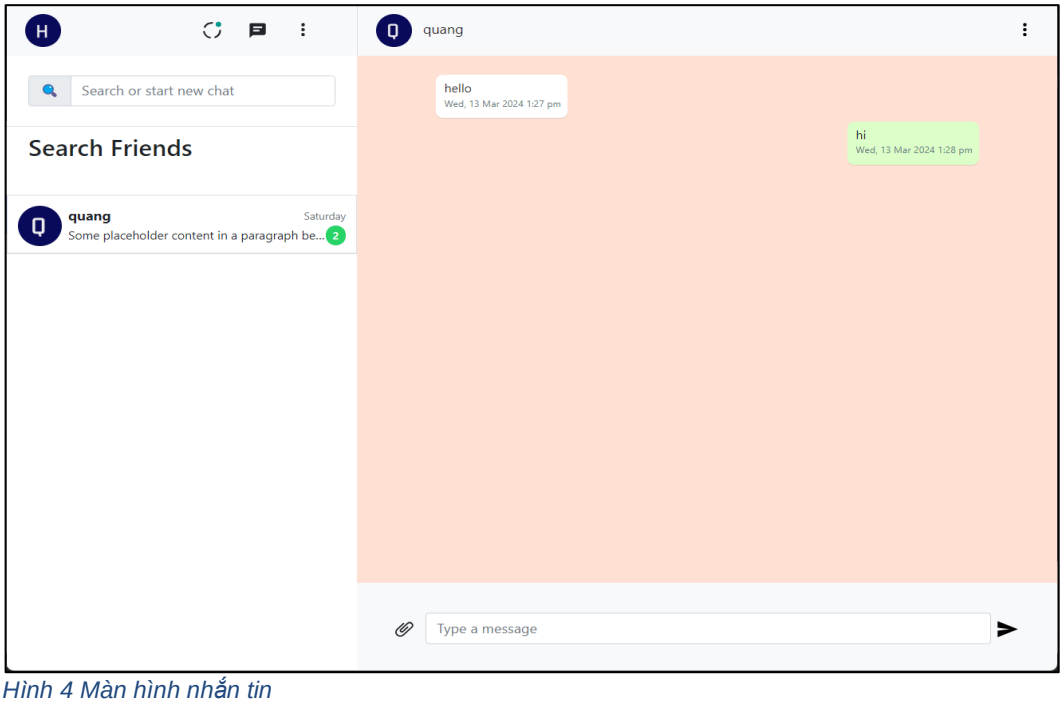
Hình 1 Màn hình đăng ký



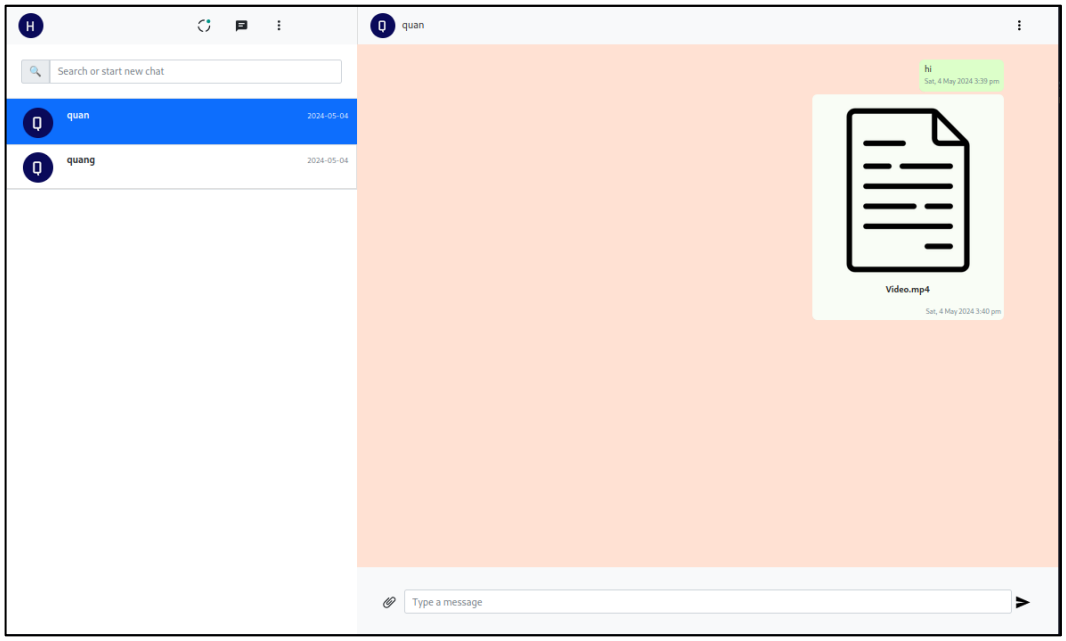
Hình 2 Màn hình đăng nhập



Hình 3 Màn hình thêm bạn



Hình 4 Màn hình nhắn tin



Hình 5 Màn hình gửi file mã hóa

2.6. ĐÁNH GIÁ QUÁ TRÌNH LÀM VIỆC:

Qua quá trình thực hiện đồ án Website trao đổi tin nhắn và dữ liệu số đa phương tiện có bảo mật thông qua các room chat, nhóm cảm thấy đây là một đồ án rất thực tế, do đó nhóm cũng gặp một số khó khăn nhất định. Tuy nhiên nhóm vẫn tuân thủ và hoàn thành theo phương hướng và kế hoạch đã đề ra ban đầu. Bên cạnh đó, việc sắp xếp thời gian làm việc nhóm cũng gặp đôi chút khó khăn. Tuy nhiên, sau cùng nhóm cũng đã hoàn thành được nội dung tìm hiểu và có được sản phẩm demo thực tế đáp ứng đủ các yêu cầu được đặt ra.
Nhìn chung, nhóm cảm thấy đây là một chủ đề rất hay và mang tính thực tế cao mang lại kinh nghiệm thực tiễn

quý giá trong việc triển khai hệ thống bảo mật.Trong tương lai, có thể sẽ ứng dụng rộng rãi hơn và hoàn toàn có thể cải tiến và tích hợp thêm được các công nghệ mới.

2.7. KẾT LUẬN:

Đồ án đã hoàn thành thành công với các yêu cầu đặt ra. Hệ thống cung cấp một giải pháp an toàn và đáng tin cậy cho việc trao đổi thông tin và dữ liệu số giữa các người dùng. Việc sử dụng các công nghệ mã hóa tiên tiến như AES, RSA, và SHA đảm bảo tính bảo mật và an toàn cho dữ liệu. Giao diện người dùng thân thiện và cơ chế quản lý khóa hiệu quả đã tăng cường trải nghiệm người dùng và tính thực tiễn của hệ thống. Việc triển khai chatroom với thời hạn lưu trữ 7 ngày đáp ứng được nhu cầu sử dụng thực tế. Nhìn chung, đồ án không chỉ đáp ứng được mục tiêu ban đầu mà còn mang lại trải nghiệm thực tiễn và kiến thức quý giá cho quá trình triển khai hệ thống bảo mật trong các dự án tương lai.

3. NGUỒN THAM KHẢO

STT	Link tham khảo
1	https://www.geeksforgeeks.org/simple-chat-room-using-python/
2	https://www.youtube.com/watch?v=k4mjF4sPITE
3	https://flet.dev/docs/tutorials/python-realtime-chat/
4	https://www.youtube.com/watch?v=YDZPp0EnzEA
5	https://www.pubnub.com/blog/building-a-modern-chat-application-with-python/
6	https://www.linkedin.com/pulse/how-build-simple-client-server-chat-application-python-kurkoglu/
7	https://www.youtube.com/watch?v=NIduVsNC8X0

HẾT