**TRƯỜNG ĐẠI HỌC QUỐC GIA TP – HỒ CHÍ MINH**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

□]□

A picture containing logo

Description automatically generated

**BÁO CÁO: USE-CASE**

**ĐỒ ÁN: ỨNG DỤNG WEB TRAO ĐỔI DỮ LIỆU ĐA PHƯƠNG TIỆN BẢO MẬT**

**GIẢNG VIÊN:** Nguyễn Đình Thúc

Nguyễn Văn Quang Huy

Ngô Đình Hy

**LỚP:** 20CNTThuc

**SINH VIÊN:** Hoàng Duy Thành Long 19127200

Lê Võ Huỳnh Thanh 20127072

Hoàng Hữu Minh An 20127102

Trần Tiến Hoàng 20127424

Ho Chi Minh, 19-01-2024

Contents

[I. Thông tin nhóm: 3](#_Toc156666901)

[II. Mục tiêu đồ án: 3](#_Toc156666902)

[III. Nội dung: 4](#_Toc156666903)

[IV. Mô hình Use-case: 4](#_Toc156666904)

[V. Chức năng: 5](#_Toc156666905)

[**1.** **Use-case: Signup** 5](#_Toc156666906)

[**2.** **Use-case: Login** 5](#_Toc156666907)

[**3.** **Use-case: Tìm kiếm** 6](#_Toc156666908)

[**3.1.** **Tìm kiếm người dùng** 6](#_Toc156666909)

[**3.2.** **Tìm kiếm thư mục, dữ liệu mã hóa** 6](#_Toc156666910)

[**4.** **Use-case: Chia sẻ file** 7](#_Toc156666911)

[**4.1.** **Use-case: Ký** 7](#_Toc156666912)

[**4.2.** **Use-case: Sinh khóa** 8](#_Toc156666913)

[**4.3.** **Use-case: Mã hóa** 8](#_Toc156666914)

[**5.** **Giải mã** 8](#_Toc156666915)

[**5.1.** **Use-case: Giải mã** 8](#_Toc156666916)

[**5.2.** **Tải file lên** 9](#_Toc156666917)

[**5.3.** **Tải file xuống** 10](#_Toc156666918)

[**5.4.** **Xác thực chữ ký** 10](#_Toc156666919)

[**6.** **Use-case: Đăng ký chữ ký số** 10](#_Toc156666920)

[VI. Tham Khảo 11](#_Toc156666921)

1. **Thông tin nhóm:**

|  |  |
| --- | --- |
| **Họ và tên** | **Mã số sinh viên** |
| Hoàng Duy Thành Long | 19127200 |
| Lê Võ Huỳnh Thanh | 20127072 |
| Hoàng Hữu Minh An | 20127102 |
| Trần Tiến Hoàng | 20127424 |

1. **Mục tiêu đồ án:**

Mục tiêu đồ án hướng tới một trang web **Halt** trao đổi thông tin như cuộc trò chuyện bí mật của Messenger nhưng sẽ toàn vẹn hơn và an toàn hơn. Halt sẽ cho phép người dùng trao đổi thông tin an toàn và riêng tư với người khác. Khi bạn sử dụng tính năng này, file của người dùng sẽ được mã hóa đầu cuối, tức là chỉ có người dùng và người nhận mới có thể đọc được. Người dùng cũng có thể thiết lập thời gian cho file tự xóa sau một khoảng thời gian nhất định, hoặc tắt cuộc trò chuyện khi họ muốn.

Quá trình mã hóa và sinh khóa của **Halt** dựa trên chuẩn mã hóa nâng cao AES (Advanced Encryption Standard). AES là một giải thuật mã hóa khóa đối xứng, tức là sử dụng cùng một khóa để mã hóa và giải mã. AES có thể sử dụng khóa có độ dài 128, 192 hoặc 256 bit. Quá trình mã hóa và giải mã của AES bao gồm nhiều vòng lặp, trong đó mỗi vòng lặp gồm nhiều bước biến đổi dữ liệu theo các quy tắc nhất định.

Để sinh khóa cho AES, **Halt** sử dụng giao thức Signal, một giao thức mã hóa đầu cuối mã nguồn mở. Giao thức Signal sử dụng giải thuật mã hóa khóa bất đối xứng RSA để tạo ra các khóa công khai và bí mật cho mỗi người dùng. Khóa công khai được chia sẻ với người khác, còn khóa bí mật được giữ riêng tư. Bên cạnh đó sẽ kết hợp với chữ kí số và chứng thực để tăng cường bảo mật so với các ứng dụng trao đổi thông tin trên thị trường hiện tại. Khi hai người dùng muốn tạo cuộc trò chuyện bí mật, họ sẽ trao đổi khóa công khai của nhau và sử dụng khóa bí mật của mình để tạo ra một khóa chung. Khóa chung này sẽ được sử dụng làm khóa cho AES256.

1. **Nội dung:**

Cuối cùng, đồ án sẽ là một trang web giúp người dùng có thể trao đổi, chia sẽ thông tin (file, email) qua internet có bảo mật. Trang web sẽ có những chức năng tối ưu, giao diện đơn giản giúp người dùng dễ dàng thực hiên các thao tác.

1. **Mô hình Use-case:**

A diagram of a diagram

Description automatically generated

Actor:

* User: người sử dụng dịch vụ
* Admin system: người quản lý hệ thống

1. **Chức năng:**
2. **Use-case: Signup**

|  |  |
| --- | --- |
| **Tên Use case** | Signup |
| **Đặc tả** | Người dùng có thể đăng kí một tài khoản ở trên Halt |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Ở trang homepage, người dùng có thể nhấn vào nút “signup”   # Đăng kí qua tài khoản google or facebook  # Đăng kí qua mẫu có sẵn   1. Người dùng điển đầy đủ thông tin. 2. Nhấn nút “submit” để tiếp tục đăng kí 3. Người dùng sẽ nhận một đoạn code từ tin nhắn điện thoại để xác thực tài khoản. 4. Người dùng trở về trang home. |
| **Tình huống khác** | **# Đăng kí qua mẫu có sẵn**  **Tình huống 1: nhập sai hoặc thiếu thông tin bắt buộc.**   1. Từ b2, nếu người dùng không nhập đủ các thông tin bắt buộc hoặc nhập sai dăng thông tin quay lại b1.   **Tính huống 2: Người dùng nhập sai mã code từ tin nhắn.**   1. Từ b3, người dùng nhập sai thông tin mã code sẽ không thực hiện các bước còn lại, mỗi mã code có giới hạn thời gian. Người dùng có thể chọn gửi lại tin nhắn để có mã code mới.   **# Đăng kí qua tài khoản google hoặc facebook**  **Tình huống 1: Người dùng đã có tài khoản trước đó**   1. Người dùng vào trang home với tài khoản đã đăng kí trước đó |
| **Điều kiện trước** | Người dùng vào trang homepage |
| **Điều kiện sau** | Xuất hiện tin nhắn thông báo đăng kí tài khoản thành công |

1. **Use-case: Login**

|  |  |
| --- | --- |
| **Tên Use case** | Login |
| **Đặc tả** | Người dùng có thể đăng nhập bằng tài khoản đã đăng kí |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Ở trang homepage, người dùng có thể nhấn vào nút “login”   # Đăng nhập qua tài khoản google hoặc facebook  # Đăng nhâp qua mẫu có sẵn   1. Người dùng điển đầy đủ thông tin. 2. Nhấn nút “login” để tiếp tục 3. Người dùng trở về trang home. |
| **Tình huống khác** | **# Đăng nhập qua tài khoản google hoặc facebook**  **Tình huống 1: Chưa có tài khoản**   1. Người dùng sẽ phải đăng kí nếu chưa có tài khoản   **# Đăng nhập qua mẫu**  **Tình huống 1: Người dùng nhập sai thông tin**   1. Người dùng phải nhập lại mẫu   **Tình huống 2: Người dùng quên mật khẩu**   1. Người dùng nhấn vào “forget password” ở trên màn hình. Nếu tồn tại tài khoản, người dùng sẽ nhận được mail để tới trang có thể thay đổi mật khẩu. |
| **Điều kiện trước** | Người dùng phải có tài khoản |
| **Điều kiện sau** | Người dùng đăng nhập thành công |

1. **Use-case: Tìm kiếm**
   1. **Tìm kiếm người dùng**

|  |  |
| --- | --- |
| **Tên Use case** | Tìm kiếm người dùng |
| **Đặc tả** | Người dùng có thể tìm kiểm người dùng khác |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Ở trang homepage, người dùng nhấn vào ô tìm kiếm để tìm kiếm người trao đổi dữ liệu 2. Người dùng chọn xác nhận dựa trên tên hoặc ID và tiến hành trao đổi dữ liệu. |
| **Tình huống khác** | **Tình huống 1: nhập sai hoặc thiếu thông tin bắt buộc.**   1. Từ b2, nếu người dùng không nhập đủ các thông tin bắt buộc hoặc nhập sai dăng thông tin quay lại b1. |
| **Điều kiện trước** | Người dùng vào ô tìm kiếm |
| **Điều kiện sau** | Hiển thị được người tìm kiếm và có thể tiến hành trao đổi thông tin |

* 1. **Tìm kiếm thư mục, dữ liệu mã hóa**

|  |  |
| --- | --- |
| **Tên Use case** | Tìm kiếm file |
| **Đặc tả** | Người dùng có thể tìm kiểm những tệp tin mã hóa |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Ở trang homepage, người dùng nhấn vào ô tìm kiếm để tìm kiếm file trao đổi dữ liệu 2. Người dùng chọn xác nhận dựa trên tên file dữ liệu đã trao đổi. |
| **Tình huống khác** | **Tình huống 1: nhập sai hoặc thiếu thông tin bắt buộc.**   1. Từ b2, nếu người dùng không nhập đủ các thông tin bắt buộc hoặc nhập sai dăng thông tin quay lại b1. |
| **Điều kiện trước** | Người dùng vào ô tìm kiếm |
| **Điều kiện sau** | Hiển thị được file dữ liệu |

1. **Use-case: Chia sẻ file**
   1. **Use-case: Ký**

|  |  |
| --- | --- |
| **Tên Use case** | Ký |
| **Đặc tả** | Ký vào file mả người dùng muốn gửi đi |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Tạo một yêu cầu ký với việc chọn file đa phương tiện cần ký. 2. Website hiển thị cho người dùng file đa phương tiện và yêu cầu xác nhận việc ký. 3. Người dùng xác nhận việc ký. 4. Website tiến hành ký số trên file đa phương tiện dựa trên chữ ký đã đăng ký và gán thêm thông tin về người dùng và thời gian ký. 5. Sau khi quá trình ký hoàn tất, website hiển thị thông báo ký thành công và cung cấp link tải file ký về máy tính của người dùng. 6. Người dùng tải file ký về máy tính để sử dụng hoặc gửi đi qua bên thứ ba. |
| **Tình huống khác** | * **Tình huống 1: Người dùng không đăng nhập vào tài khoản của mình.**  1. Website yêu cầu người dùng đăng nhập hoặc tạo tài khoản mới để tiếp tục tiến trình ký.  * **Tình huống 2: Người dùng không xác nhận việc ký.**  1. Người dùng không xác nhận việc ký và thoát khỏi trang web hoặc hủy bỏ yêu cầu ký. 2. Trở lại trạng thái trước đó, không thực hiện việc ký file đa phương tiện.  * **Tình huống 3: Quá trình ký thất bại.**  1. Website thông báo cho người dùng biết về lỗi ký và yêu cầu thử lại hoặc liên hệ với quản trị viên để được hỗ trợ. 2. Người dùng có thể thử lại quy trình ký hoặc tìm giải pháp khác để ký file đa phương tiện. |
| **Điều kiện trước** | Người dùng ấn vào link ký trên website và đăng ký chữ ký trước đó |
| **Điều kiện sau** | Thông báo thành công và dưa ra các tùy chọn như gửi file qua mail hoặc lưu file về máy ... |

* 1. **Use-case: Sinh khóa**

|  |  |
| --- | --- |
| **Tên Use case** | Sinh khóa |
| **Đặc tả** | Sử dụng các thuật toán sinh khóa để thực hiện chức năng mã hóa |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Người dùng gửi file dữ liệu đi đến người nhận 2. Hệ thống tạo khóa mã hóa thông qua sử dụng thuật toán sinh khóa để tạo khóa bí mật 3. Khóa công khai được trả về cho người dùng để sử dụng trong quá trình mã hóa file |
| **Tình huống khác** | **Tình huống 1: nếu không sinh khóa được**   1. Ở bước 1, nếu người dùng gửi file lỗi thì sẽ trở về trang chủ 2. Ở bước hai nếu hệ thống không sinh khóa được thì sẽ hiển thị lỗi tạo khóa |
| **Điều kiện trước** | Người dùng phải có tài khoản, kết nối tới một người dùng có tồn tại và đó phải là kết nối an toàn |
| **Điều kiện sau** | Khóa được sinh ra sẽ dùng để mã hóa thông tin dữ |

* 1. **Use-case: Mã hóa**

|  |  |
| --- | --- |
| **Tên Use case** | Mã hóa |
| **Đặc tả** | Mã hóa file để sinh ra bản mã |
| **Vai trò** | User |
| **Các bước thực hiện** | Người dùng nhấn nút upload file bản rõ. Server tạo ra khóa đối xứng và tạo ra bản mã của file. |
| **Tình huống khác** | **Người dùng chưa điền form thì sẽ hiện thông báo** |
| **Điều kiện trước** | Người dùng đã đăng nhập, đã chọn chức năng sinh khóa |
| **Điều kiện sau** | Tồn tại file mã hóa ở server |

1. **Giải mã**
   1. **Use-case: Giải mã**

|  |  |
| --- | --- |
| **Tên Use case** | Giải mã |
| **Đặc tả** | Người dùng tiến hành giải mã file sau khi nhận file mã hóa từ người gửi hoặc sau khi đã tải file mã hóa lên. |
| **Vai trò** | User |
| **Các bước thực hiện** | # Người dùng đã nhận thông báo kết nối thành công có file gửi tới trong kênh kết nối.   1. Người dùng nhấn vào thông báo nhận được file từ người gửi 2. Người dùng sẽ được chuyển đến giao diện trang giải mã file. Hệ thống sẽ tự dộng giải mã khóa bí mật của A từ thuật toán RSA hện lên cho người dùng thấy. 3. Người dùng tải file đã mã hóa 4. Người dùng nhấn chọn nút giải mã file 5. Người dùng sẽ nhận được thông báo giải mã file thành công nếu giải mã thành công.   # Người dùng chủ động chọn file để giải mã   1. Ở trang home, người dùng nhấn vào nút “giải mã” 2. Được chuyển đến giao diện phù hợp, người dùng có thể chọn file mới bằng cách nhấn vào nút “upload file” 3. Người dùng nhập khóa bí mậ nhận được từ kênh kết nối vào 4. Người dùng nhập vào thông tin khóa đã được mã hóa 5. Nhấn và nút giải mã, để tiến hành giải mã file nếu giải mã thành công sẽ nhận được thông báo. |
| **Tình huống khác** | **# Người dùng chủ động chọn file**  **Tính huống 1: Khi người dùng không nhập khóa bí mật từ kênh kết nối, không tải file lên, không nhập thông tin khóa.**   1. Người dùng sẽ nhận dược thông báo mình chưa nhập đủ thông và sẽ trở lại bước phù hợp. |
| **Điều kiện trước** | Người dùng phải nhập đủ các thông tin cần thiết có trong hệ thống như file mã hóa, thông tin khóa bí mật từ kênh kết nối, thông tin khóa. |
| **Điều kiện sau** | Người dùng nhận thông báo nhận thông báo giải mã khóa thành công |

* 1. **Tải file lên**

|  |  |
| --- | --- |
| **Tên Use case** | Tải file lên |
| **Đặc tả** | Người dùng có thể upload file và key lên server để nhờ giải mã |
| **Vai trò** | User |
| **Các bước thực hiện** | Người dùng nhấn nút upload để tải file mã hóa và key lên server |
| **Tình huống khác** | **Tình huống 1: người dùng không điền đủ form để gửi lên server** |
| **Điều kiện trước** | Người dùng có tài khoản |
| **Điều kiện sau** | Xuất ra đường dẫn để tải file giải mã xuống |

* 1. **Tải file xuống**

|  |  |
| --- | --- |
| **Tên Use case** | Tải file xuống |
| **Đặc tả** | Người dùng có thể tải file xuống từ server |
| **Vai trò** | User |
| **Các bước thực hiện** | Người dùng nhấn nút tải xuống |
| **Tình huống khác** | **Không đúng đường dẫn đến file thì sẽ hiện thông báo không tồn tại** |
| **Điều kiện trước** | Người dùng đã upload file mã hóa lên server để giải mã |
| **Điều kiện sau** | File giải mã được tải xuống máy người dùng |

* 1. **Xác thực chữ ký**

|  |  |
| --- | --- |
| **Tên Use case** | Xác thực chữ ký |
| **Đặc tả** | Xác thực chủ sở hữu của file |
| **Vai trò** | User |
| **Các bước thực hiện** | Người dùng điền form thông tin cần xác thực, sau đó nhấn nút xác thực |
| **Tình huống khác** | **Người dùng điền thiếu form** |
| **Điều kiện trước** | File đã được kí bởi chủ sở hữu, file đã được tải lên, file đã được ký |
| **Điều kiện sau** | Thông báo xác thực chủ sở hữu |

1. **Use-case: Đăng ký chữ ký số**

|  |  |
| --- | --- |
| **Tên Use case** | Đăng ký chữ ký số |
| **Đặc tả** | Người dùng có thể đăng kí một chữ ký số trên Halt |
| **Vai trò** | User |
| **Các bước thực hiện** | 1. Người dùng truy cập vào trang Halt để đăng ký chữ ký số.Người dùng chọn mục đăng ký chữ ký số trong menu hoặc trang chủ của trang Halt. 2. Trang Halt yêu cầu người dùng cung cấp thông tin cá nhân như tên đầy đủ, địa chỉ email, số điện thoại, v.v. 3. Sau khi người dùng điền đầy đủ thông tin, trang Halt gửi một email xác nhận đến địa chỉ email mà người dùng đã cung cấp. 4. Người dùng mở email và nhấp vào liên kết xác nhận trong email để xác nhận đăng ký. 5. Trang web xác nhận và gửi một tài liệu yêu cầu người dùng cung cấp các tài liệu cần thiết để xác minh danh tính, ví dụ như CMND, giấy phép lái xe, v.v. 6. Người dùng quét hoặc chụp ảnh các tài liệu cần thiết và tải lên trang web. 7. Trang web xử lý và xác minh thông tin từ các tài liệu người dùng tải lên. 8. Sau khi thông tin được xác minh thành công, trang web sẽ yêu cầu người dùng tạo mật khẩu và lưu trữ chữ ký số. 9. Người dùng tạo mật khẩu và lưu trữ chữ ký số, thông tin này sẽ được truyền mã hóa và lưu trữ an toàn trên trang web. 10. Quá trình đăng ký chữ ký số hoàn thành và người dùng có thể sử dụng chữ ký số trên trang web để truyền file đa phương tiện. |
| **Tình huống khác** | **Tình huống 1: Xác minh danh tính không thành công**   1. Nếu thông tin từ các tài liệu người dùng tải lên không hợp lệ hoặc không đủ để xác minh danh tính, trang web sẽ yêu cầu người dùng cung cấp thông tin hoặc tài liệu bổ sung. 2. Người dùng cung cấp thông tin hoặc tải lên tài liệu bổ sung để xác minh danh tính. 3. Quá trình này có thể tiếp tục cho đến khi danh tính được xác minh thành công hoặc người dùng không thể cung cấp thông tin hoặc tài liệu đủ để xác minh.   **Tình huống 2: Đăng ký bị hủy bỏ**   1. Trong quá trình xác minh danh tính và tạo mật khẩu, người dùng có thể quyết định hủy bỏ quá trình đăng ký chữ ký số. 2. Trong trường hợp này, quá trình đăng ký sẽ kết thúc và chữ ký số không được tạo và lưu trữ trên trang web. 3. Người dùng có thể quay trở lại quá trình đăng ký bất cứ lúc nào |
| **Điều kiện trước** | Người dùng vào trang homepage vào nhấn vào link đăng ký chữ ký số |
| **Điều kiện sau** | Xuất hiện tin nhắn thông báo đăng kí chữ ký số thành công |

1. **Tham Khảo**

[1]: [Bản vẽ Use Case (Use Case Diagram) - iViettech - iViettech](https://iviettech.vn/blog/543-ban-ve-use-case-use-case-diagram.html)

[2]: [Mã hóa đầu cuối: Bảo mật tối ưu cho trò chuyện (bản thử nghiệm) - Zalo Help](https://help.zalo.me/huong-dan/chuyen-muc/nhan-tin-va-goi/nhan-tin/ma-hoa-dau-cuoi-bao-mat-toi-uu-cho-tro-chuyen/)

[3]: [Home - MEGA](https://mega.io/)

Cảm ơn thầy/cô và các bạn đã xem