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

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

□]□

A picture containing logo

Description automatically generated

**BÁO CÁO: THIẾT KẾ HỆ THỐNG**

**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

Nguyễn Quang Thuận 19127571

Hoàng Hữu Minh An 20127102

Trần Hoàng Minh Quang 20127299

Ho Chi Minh, 26-01-2024

Contents

[I. Thông tin nhóm: 3](#_Toc157175793)

[II. Data Model: 3](#_Toc157175794)

[III. Processing Model: 4](#_Toc157175795)

[IV. Tham khảo: 6](#_Toc157175796)

1. **Thông tin nhóm:**

|  |  |
| --- | --- |
| **Họ và tên** | **Mã số sinh viên** |
| Hoàng Duy Thành Long | 19127200 |
| Nguyễn Quang Thuận | 19127571 |
| Hoàng Hữu Minh An | 20127102 |
| Trần Hoàng Minh Quang | 20127299 |

1. **Data Model:**

A diagram of a company

Description automatically generated

User(Public key, email, password)

* Khóa chính: Public key
* Thuộc tính:
  + Public key: một chuỗi kí tự được cấp tự động cho User một lần duy nhất
  + Email: địa chỉ email của User
  + Password: mật khẩu của User

Chữ ký(Public key, Signature, ngày tạo, thuật toán mã hóa)

* Khóa chính : Public key
* Khóa Phụ : Signature, ngày tạo , thuật toán mã hóa
* Thuộc tính:
  + Signature : Được lưu dưới dạng chuỗi hoặc binary
  + Ngày tạo : Ngày, tháng , năm , giờ, phút , giây khi người dùng tạo
  + Thuật toán mã hóa : Bao gồm các thuật toán mã hóa như RSA, DSA, ... khi thực hiện quá trình mã hóa và giải mã

Lịch sử chia sẻ(Người gửi, Ngày chia sẻ, Người nhận, Thuật toán mã hóa, Kích thước, Phân loại)

* Khóa chính: Người gửi, Ngày chia sẻ (1 Người gửi có thể mã hóa nhiều file, cần có thêm thuộc tính Ngày chia sẻ để phân biệt lịch sử chia sẻ của người dùng).
* Khóa phụ: Người nhận, Người gửi.
* Thuộc tình:
  + Người gửi: chứa thông tin Public key của người gửi. Có thể truy xuất đến bảng User và Chữ ký thông qua thuộc tính Người gửi.
  + Ngày chia sẻ: Ngày, Tháng, Năm cùng với Giờ, Phút, Giây mã hóa file.
  + Người nhận: chứa thông tin Public key của người nhận. Có thể truy xuất đến bảng User và Chữ ký thông qua thuộc tính Người nhận.
  + Thuật toán mã hóa: chứa thông tin tên của thuật toán phù hợp với file muốn mã hóa như DES, 3DES, AES,...
  + Kích thước: chứa thông tin kích thước của file (không vượt quá 20 Mb).
  + Phân loại: chứa thông tin về định dạng của file (file.docx, file.xls, file.mp4, file.mov,...) hoặc mail nếu người dùng muốn mã hóa việc chuyển mail.
* Quan hệ:
* User chỉ sở hữu 1 chữ ký và ngược lại
* User có nhiều lịch sử chia sẻ hoặc không có lịch sử chia sẻ nào. 1 lịch sử chia sẻ file chỉ có duy nhất một user.

1. **Processing Model:**

* **Level 0:**

A diagram of a machine

Description automatically generated

* User:
  + Input: Private key, file (đã được mã hóa hoặc giải mã) từ Halt system
  + Output: Thông tin User (email, mật khẩu), file cho Halt system
* Halt System:
  + Input: Thông tin User (email, mật khẩu), file từ User. Public key, Signature từ Database
  + Output: Private key, file (đã được mã hóa hoặc giải mã) cho User. Thông tin User cho Database
* Database:
  + Input: Thông tin User từ Halt system
  + Output: Public key và Signature cho Halt system
* **Level 1:**

A diagram of a computer

Description automatically generated

1. Đăng nhập:
   * User sẽ gửi thông tin về email, password cho hệ thống, hệ sẽ tìm kiếm từ Thông tin User (email, password). Tiến hành kiểm tra email và password, nếu hợp lệ cho phép người dùng đăng nhpa65 vào hệ thống, nếu sai thì từ chối. Ở quá trình này, thực hiện xác thực người dùng.
2. Đăng kí:
   * Nhận vào gửi thông tin User
   * Gửi thông tin User và Public key cho Đăng kí chữ kí số
   * Lưu lại thông tin User
3. Đăng kí chữ kí số:
   * Nhận vào thông tin User và Public key
   * Lưu lại Public key và signature
4. Tìm kiếm:
   * Nhận thông tin người nhận từ user
   * Tra cứu email người nhận qua database thông tin user
   * Gửi email người nhận về cho user sau khi tìm được
5. Chia sẻ file:
   * Người dùng đưa vào hệ thống file
   * Chia sẻ file sẽ thực hiện cho người dùng nhập thông tin người nhận có tồn tại trong hệ thống
   * Sau khi thực hiện xong sẽ trả về thông tin người nhận, và file đến quá trình mã hóa.
6. Gửi mail:
   * Người dùng nhập vào hệ thống thông tin email người nhận có tồn tại trong hệ thống.
   * Trả vể thông tin người nhận đến quá trình mã hóa.
7. Giải mã:
   * Nhận private key cũng như các thứ cần giải mã như : file , email , ...
   * Yêu cầu user xác nhận chữ ký để tiến hành giải mã
   * Database chữ ký gửi trả signature và kiểm tra tính hợp lệ của chữ ký để tiến hành giải mã
   * Giải mã các file và đưa qua xử lý file cho người dùng sử dụng theo nhu cầu cá nhân .
8. Mã hóa:
   * Nhận thông tin người nhận, kèm theo file hoặc mail cần được mã hóa.
   * Lưu lại thông tin mã hóa trong Lịch sử chia sẻ.
   * Gửi private key (AES) cho user.
   * Sau khi mã hóa, file đã mã hóa sẽ chuyển đến bước Xử lý file để tiến hành các bước tiếp theo.
9. Xử lý file:
   * Nhận vào file đã mã hóa hoặc file đã giải mã.
   * Gửi file về cho user, lúc này user có thể tải xuống.
10. **Tham khảo:**

[1]: [What is Data Flow Diagram? (visual-paradigm.com)](https://www.visual-paradigm.com/guide/data-flow-diagram/what-is-data-flow-diagram/)

[2]: [What is Entity Relationship Diagram (ERD)? (visual-paradigm.com)](https://www.visual-paradigm.com/guide/data-modeling/what-is-entity-relationship-diagram/)

Cảm ơn thầy/cô và các bạn đã xem