**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**KHOA CÔNG NGHỆ THÔNG TIN**



**PHÁT TRIỂN PHẦN MỀM TRONG THẺ THÔNG MINH**

Đề tài:

**XÂY DỰNG THẺ GỬI XE SỬ DỤNG SMART CARD**

NHÓM 3

*Giảng viên hướng dẫn*: **Cao Thanh Vinh**

*Sinh viên thực hiện*: Nguyễn Văn Thanh - CT050443

Hứa Trung Hiếu - CT050417

Đinh Công Tuấn - CT050453

Vũ Tuấn Kiệt - CT050427

Trần Văn Hiệp - CT050415

**Hà Nội,** **2025**

**MỤC LỤC**

[LỜI CẢM ƠN 2](#_Toc187319782)

[LỜI NÓI ĐẦU 3](#_Toc187319783)

[CHƯƠNG 1: PHÂN TÍCH THIẾT KẾ 4](#_Toc187319784)

[1.1. Yêu cầu hệ thống 4](#_Toc187319785)

[1.1.1. Mục tiêu hệ thống 4](#_Toc187319786)

[1.1.2. Yêu cầu chức năng 4](#_Toc187319787)

[1.1.3. Mô tả tổng quan hệ thống 4](#_Toc187319788)

[1.2 Thiết kế hệ thống 5](#_Toc187319789)

[1.2.1 Usecase tổng quát 5](#_Toc187319790)

[1.2.2 Usecase chi tiết 6](#_Toc187319791)

[1.2.2.1 Chức năng kết nối 6](#_Toc187319792)

[1.2.2.2 Chức năng tạo thông tin 6](#_Toc187319793)

[1.2.2.3 Chức năng đăng nhập 8](#_Toc187319794)

[1.2.2.4 Chức năng sửa thông tin 10](#_Toc187319795)

[1.2.2.5 Chức năng đổi mã PIN 12](#_Toc187319796)

[1.2.2.6 Chức năng nạp tiền 14](#_Toc187319797)

[1.2.2.7 Chức năng mở khóa thẻ 16](#_Toc187319798)

[1.2.2.8 Chức năng quẹt thẻ 17](#_Toc187319799)

[1.3 Thiết kế cơ sở dữ liệu 20](#_Toc187319800)

[1.3.1 Bảng user 20](#_Toc187319801)

[1.3.2 Bảng history\_input\_output 21](#_Toc187319802)

[CHƯƠNG 2: CÀI ĐẶT VÀ THỰC NGHIỆM 22](#_Toc187319803)

[2.1 Thiết kế giao diện 22](#_Toc187319804)

[2.1.1 Giao diện kết nối với Applet 22](#_Toc187319805)

[2.1.2 Giao diện nhập mã pin 22](#_Toc187319806)

[2.1.3 Giao diện khởi tạo thẻ 23](#_Toc187319807)

[2.1.4 Giao diện trang chủ 23](#_Toc187319808)

[2.1.5 Giao diện cập nhật thông tin 24](#_Toc187319809)

[2.1.6 Giao diện nạp tiền 24](#_Toc187319810)

[2.1.7 Giao diện đổi mã pin 25](#_Toc187319811)

[2.1.8 Giao diện quản lí bãi đỗ xe 25](#_Toc187319812)

[2.1.9 Giao diện quản lịch sử ra vào 26](#_Toc187319813)

[2.2 Cơ chế xử lý 26](#_Toc187319814)

[2.2.1. Mã PIN 26](#_Toc187319815)

[2.2.2. Mã hóa dữ liệu 26](#_Toc187319816)

[2.2.3. Tạo ID thẻ 27](#_Toc187319817)

[2.2.4. Xử lý hình ảnh 27](#_Toc187319818)

[2.2.5. Xác thực thẻ 27](#_Toc187319819)

[CHƯƠNG 3: TỔNG KẾT 29](#_Toc187319820)

[3.1 Tổng kết 29](#_Toc187319821)

[3.2 Kết quả các thành viên trong nhóm đạt được 29](#_Toc187319822)

[3.3 Hạn chế 29](#_Toc187319823)

# LỜI NÓI ĐẦU

Trong cuộc sống hiện đại, sự gia tăng nhanh chóng của các phương tiện giao thông đòi hỏi các giải pháp quản lý bãi xe hiệu quả và thông minh. Việc sử dụng các hệ thống quản lý bãi xe truyền thống, như ghi chép bằng tay hoặc sử dụng vé giấy, không chỉ tốn kém thời gian mà còn dễ dẫn đến sai sót và khó khăn trong việc kiểm soát lưu lượng xe. Những vấn đề này đặc biệt rõ rệt tại các khu vực đô thị, trung tâm thương mại, trường học, và các khu vực công cộng có lưu lượng xe ra vào lớn.

Thẻ thông minh (Smart Card) đã và đang trở thành một công cụ hữu ích trong việc hiện đại hóa quy trình quản lý bãi xe. Với khả năng lưu trữ thông tin an toàn và tốc độ xử lý nhanh chóng, hệ thống gửi xe sử dụng thẻ thông minh mang lại nhiều lợi ích vượt trội như tăng cường hiệu quả quản lý, đảm bảo tính bảo mật, và nâng cao trải nghiệm người dùng. Không chỉ giúp giảm thiểu sai sót trong quy trình, hệ thống còn mang lại sự tiện lợi và tính chuyên nghiệp, góp phần xây dựng hình ảnh hiện đại cho các tổ chức sử dụng.

Xuất phát từ nhu cầu thực tế và tiềm năng ứng dụng cao của công nghệ thẻ thông minh, nhóm chúng em đã chọn đề tài: **“Xây dựng thẻ gửi xe sử dụng Smart Card”**. Đề tài nhằm nghiên cứu, thiết kế và phát triển một hệ thống quản lý bãi xe sử dụng thẻ thông minh, đáp ứng các yêu cầu về hiệu quả, bảo mật và tiện ích. Qua đó, chúng em hy vọng hệ thống này sẽ trở thành một giải pháp hữu ích, ứng dụng thực tiễn vào đời sống hàng ngày.

Bố cục đề tài được chia làm 3 chương như sau:

**Chương 1:** PHÂN TÍCH THIẾT KẾ

**Chương 2:** CÀI ĐẶT VÀ THỰC NGHIỆM

**Chương 3:** TỔNG KẾT

# CHƯƠNG 1: PHÂN TÍCH THIẾT KẾ

## 1.1. Yêu cầu hệ thống

### 1.1.1. Mục tiêu hệ thống

Hệ thống quản lý thẻ thông minh gửi xe được xây dựng nhằm mục đích:

* Tự động hóa quy trình gửi xe: Loại bỏ sự phụ thuộc vào giấy tờ hoặc vé gửi xe truyền thống, thay thế bằng thẻ thông minh.
* Bảo mật dữ liệu: Sử dụng các cơ chế mã hóa và xác thực để bảo vệ thông tin người dùng.
* Nâng cao hiệu suất: Giảm thời gian xử lý khi đăng ký, xác thực và quản lý thẻ.
* Tạo trải nghiệm thân thiện: Đảm bảo hệ thống dễ sử dụng và phù hợp với cả người dùng lẫn người quản lý.

### 1.1.2. Yêu cầu chức năng

Hệ thống cần đáp ứng các chức năng sau:

1. Đăng ký thẻ thông minh:

* Tạo mã PIN cho người dùng (6 – 10 ký tự).
* Gắn ID thẻ tự động cho mỗi thẻ.
* Lưu trữ thông tin thẻ và public key vào cơ sở dữ liệu.

2. Xác thực thẻ:

* Kiểm tra mã PIN người dùng.
* Sử dụng chữ ký RSA để xác thực thông tin giữa thẻ và server.

3. Quản lý mã hóa:

* Sử dụng AES để mã hóa dữ liệu nhạy cảm trên thẻ.

4. Lưu trữ ảnh vào thẻ.

5. Thay đổi thông tin trên thẻ.

6. Đổi mã pin.

7. Nạp tiền vào thẻ.

8. Quản lý lịch sử ra vào .

### 1.1.3. Mô tả tổng quan hệ thống

Hệ thống bao gồm các thành phần chính sau:

1. Thẻ thông minh:

* Được lập trình bằng Java Card để lưu mã PIN, private key, và thông tin thẻ.
* Hỗ trợ xác thực và mã hóa.

2. Server quản lý:

* Lưu trữ cơ sở dữ liệu người dùng, public key và các giao dịch.
* Xử lý xác thực và đăng ký thẻ.

3. Cơ sở dữ liệu:

* Lưu thông tin thẻ, public key
* Lịch sử ra vào gửi xe

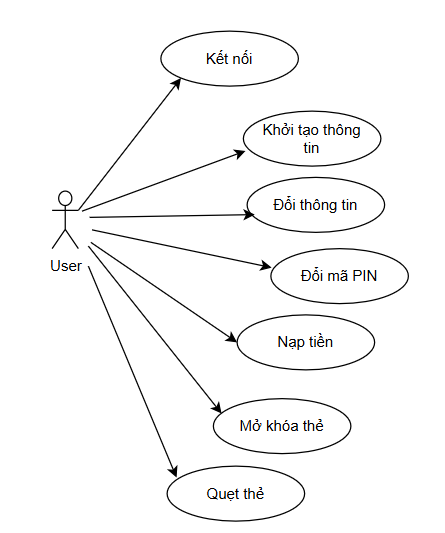
4. Giao diện người dùng:

- Cho phép đăng ký và thay đổi thông tin trong thẻ

Trang hiển thị thông tin quản lý lịch sử ra vào.

## 1.2 Thiết kế hệ thống

### 1.2.1 Usecase tổng quát

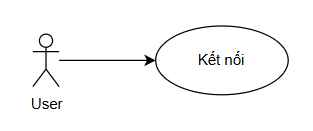


Hình 1. 1 Biểu đồ usecase tổng quát

### 1.2.2 Usecase chi tiết

#### 1.2.2.1 Chức năng kết nối

a. Biểu đồ usecase chi tiết



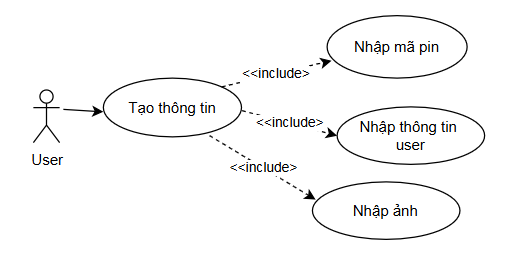
Hình 1.2 Biểu đồ usecase chi tiết của chức năng kết nối

b. Đặc tả

|  |  |
| --- | --- |
| Usecase | Kết nối thẻ |
| Tác nhân chính | User |
| Mô tả | User kết nối thẻ với hê thông |
| Tiền điều kiện | User chạy chương trình applet |
| Luồng điều kiện chính | 1. User chọn chức năng kết nối thẻ  2. Kết nối thành công với applet |

#### 1.2.2.2 Chức năng tạo thông tin

a. Biểu đồ usecase chi tiết

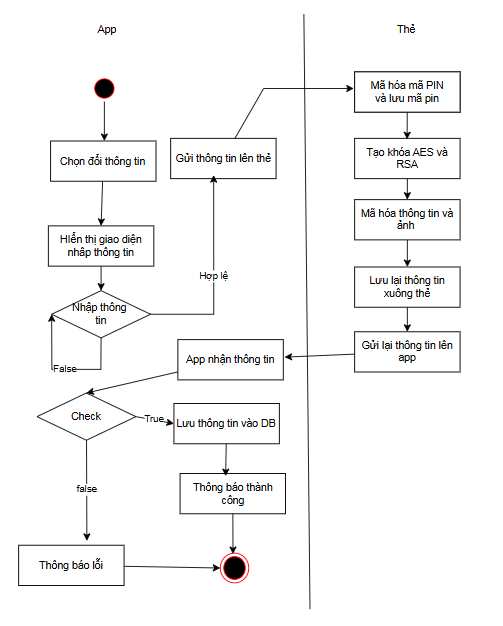


Hình 1.3 Biểu đồ use case chi tiết của chức năng tạo thông tin

b. Đặc tả usecase

|  |  |
| --- | --- |
| Usecase | Tạo thông tin thẻ |
| Tác nhân chính | User |
| Mô tả | Người dùng nhập mã pin, thông tin cá nhân và ảnh đê tạo thông tin |
| Tiền điều kiên | User đăng nhập vào hệ thông |
| Luồng sự kiện  chính | 1. User chọn chức năng tạo thông tin  2. Hệ thống hiển thị form nhập thông tin  3. User nhập mã PIN, thông tin và ảnh  4. Hệ thống kiểm tra các thông tin (PIN, thông tin , ảnh) hợp lệ  5. Hệ thống lưu thông tin xuống thẻ thành công  6. Hệ thống lưu lại thông tin vào DB  7. Hệ thống thông báo tạo thông tin thành công |
| Luồng sự kiện thay thế | TH1. Mã PIN không hợp lệ  - Hệ thống thông báo lỗi  - User nhập lại mã PIN  TH2 Thông tin hoặc ảnh không hợp lệ  - Hệ thống thông báo lỗi thông tin  - User sửa lại thông tin hoặc tải lại ảnh |
| Hậu điều kiên | - Thông tin được lưu thành công trong hệ thống |

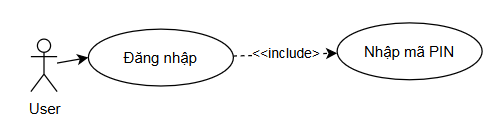
c. Biểu đồ hoạt động



Hình 1.4 Biểu đồ hoạt động của chức năng tạo thông tin

#### 1.2.2.3 Chức năng đăng nhập

a. Biểu đồ usecase chi tiết

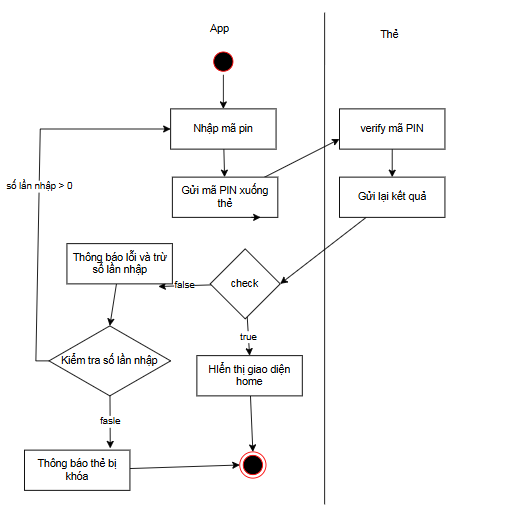


Hình 1.5 Biểu đồ usecase chi tiết của chức năng đăng nhập

b.Đặc tả

|  |  |
| --- | --- |
| Usecase | Đăng nhập |
| Tác nhân chính | User |
| Mô tả | Người dùng nhập mã PIN để truy cập vào hệ thống |
| Tiền điều kiên | User đã có thẻ và đăng ký thông tin |
| Luồng sự kiện  chính | 1. User nhập mã PIN vào form  2. Hệ thống kiểm tra mã PIN  3. Mã PIN chính xác  4. Chuyển người dùng vào giao diện home |
| Luồng sự kiện thay thế | TH1. Mã PIN không hợp lệ  - Số lần nhập sẽ bị trừ đi 1  - Người dùng nhập lại mã PIN  TH2. Nhập sai 3 lần  - Thẻ bị khóa thông tin |
| Hậu điều kiên | - Người dùng đăng nhập thành công |

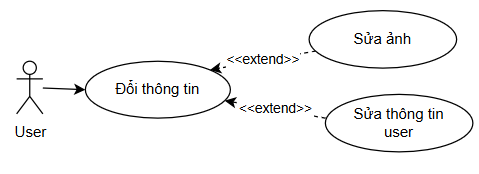
c. Biểu đồ hoạt động



Hình 1.6 Biểu đồ hoạt động của chức năng đăng nhập

#### 1.2.2.4 Chức năng sửa thông tin

a. Biểu đồ usecase chi tiết

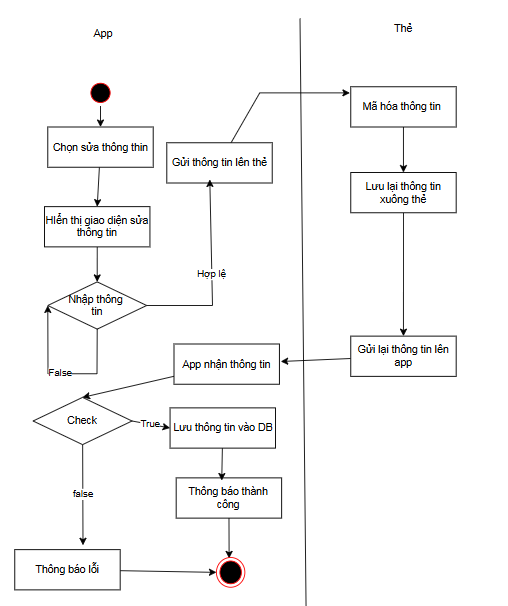


Hình 1.7 Biểu đồ usecase chi tiết của chức năng sửa thông tin

b. Đâc tả

|  |  |
| --- | --- |
| Usecase | Chỉnh sửa thông ti |
| Tác nhân chính | User |
| Mô tả | Người dùng sửa thông tin cá nhân |
| Tiền điều kiên | User đăng nhập vào hệ thống. |
| Luồng sự kiện  chính | 1. User chọn chức năng sửa thông tin  2. Hệ thống hiển thị form sửa thông tin  3. User nhập lại các mục cần sửa  4. Hệ thống kiểm tra các thông tin (thông tin , ảnh) hợp lệ  5. Hệ thống lưu thông tin xuống thẻ thành công  6. Hệ thống lưu lại thông tin vào DB  7. Hệ thống thông báo tạo thông tin thành công |
| Luồng sự kiện thay thế | TH1. Thông tin hoặc ảnh không hợp lên  - Hệ thống thông báo lỗi  - User nhập lại thông tin hoặc ảnh |
| Hậu điều kiên | - Thông tin được lưu thành công trong hệ thống |

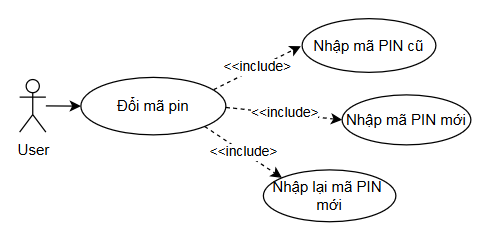
c. Biểu đồ hoạt động



Hình 1.8 Biểu đồ hoạt động của chức năng sửa thông tin

#### 1.2.2.5 Chức năng đổi mã PIN

a. Biểu đồ usecase chi tiết

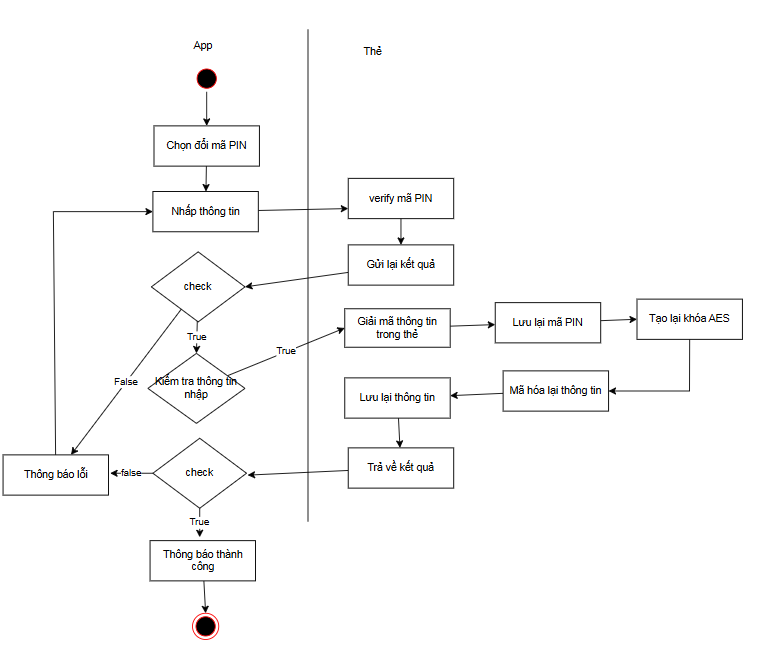


Hình 1.9 Biểu đồ usecase chi tiết của chức năng đổi mã PIN

b. Đặc tả

|  |  |
| --- | --- |
| Usecase | Thay đổi mã pin |
| Tác nhân chính | User |
| Mô tả | Người dùng thay đổi mã PIN |
| Tiền điều kiên | User đăng nhập vào hệ thống. |
| Luồng sự kiện  chính | 1. User chọn chức năng đổi mã PIN  2. Hệ thống hiển thị form đổi mã PIN  3. User lại mã PIN cũ, mã PIN mới  4. Hệ thống kiểm tra mã PIN  5. Hợp lệ lưu lại mã PIN xuống th |
| Luồng sự kiện thay thế | TH1. Nhập sai mã PIN cũ  - Hệ thống thông báo mã PIN sai  - User nhập lại mã PIN  TH2. Mã PIN cũ và mã PIN mới trùng nhau  - Hệ thống thông báo mã PIN bị trùng.  - User nhập lại mã PIN.  TH3. Mã PIN mới và nhập lại khác nhau  - Thông báo mã PIN không khớp  - User nhập lại mã PIN |
| Hậu điều kiên | - Mã PIN được lưu thành công xuống thẻ. |

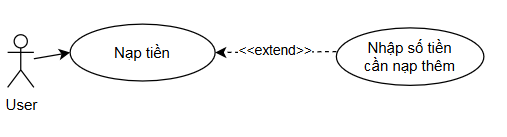
c. Biểu đồ hoạt động



Hình 1.10 Biểu đồ hoạt động của chức năng đổi mã PIN

#### 1.2.2.6 Chức năng nạp tiền

a. Biều đồ usecase chi tiết

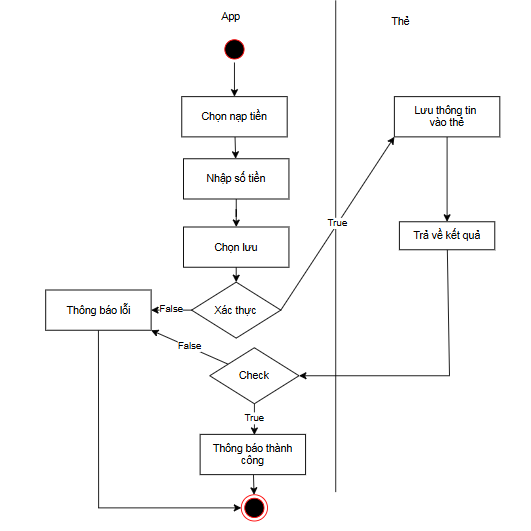


Hình 1.11 Biểu đồ usecase chi tiết của chức năng nạp tiền

b. Đặc tả

|  |  |
| --- | --- |
| Usecase | Nạp tiền |
| Tác nhân chính | User |
| Mô tả | Người dùng nạp thêm tiền vào thẻ. |
| Tiền điều kiên | User đăng nhập vào hệ thống. |
| Luồng sự kiện  chính | 1. User chọn chức năng nạp tiền  2. Hệ thống hiển thị form nạp tiền.  3. User nhập số tiền cần nạp thêm.  4. Hệ thống tính toán lại số tiền.  5. Hệ thỗng thực hiện xác thực (thành công)  5. Hệ thống lưu lại tiền vào thẻ  6. Hệ thống cập nhật lại DB |
| Luồng sự kiện thay thế | TH1. Không nhập số tiền cần nạp  - Hệ thống thông báo nhập só tiền.  TH2. Xác thực không thành công  - Thông báo thẻ không hợp lệ |
| Hậu điều kiên | Mã PIN được lưu thành công xuống thẻ. |

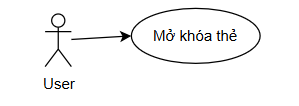
c. Biểu đồ hoạt động



Hình 1.12 Biểu đồ hoạt động của chức năng nạp tiền

#### 1.2.2.7 Chức năng mở khóa thẻ

a. Biểu đồ chi tiết

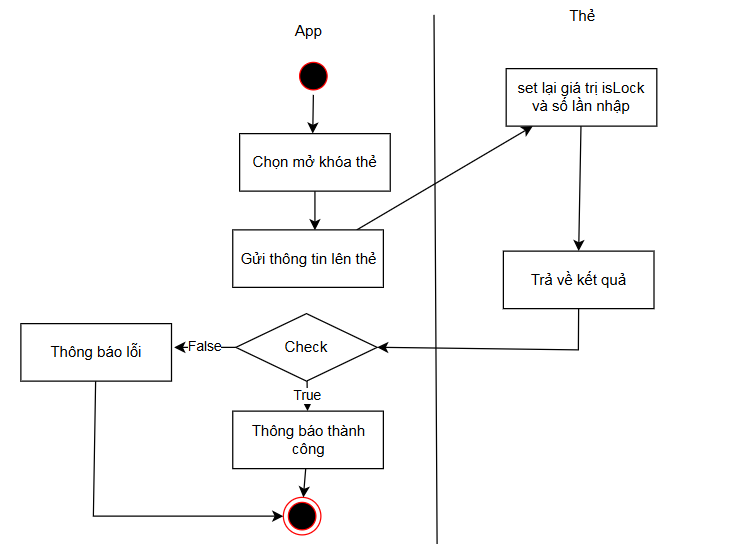


Hình 1.13 Biểu đồ usecase chi tiết của chức năng mở khóa thẻ

b. Đặc tả

|  |  |
| --- | --- |
| Usecase | Mở khóa thẻ |
| Tác nhân chính | User |
| Mô tả | User mở khóa lại thẻ |
| Tiền điều kiện | User kết nối tới thẻ |
| Luồng điều kiện chính | 1. User chọn chức năng mở khóa thẻ  2. Trạng thái thẻ (isLock = true -> isLock = false)  3. Số lần nhập cập nhật về 3 |
| Hậu điều kiển | Mở khỏa thẻ thành công |

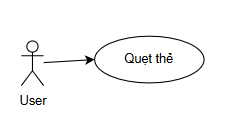
c. Biểu đồ hoạt động



Hình 1.14 Biểu đồ hoạt động của chức năng mở khóa thẻ

#### 1.2.2.8 Chức năng quẹt thẻ

a. Biểu đồ usecase

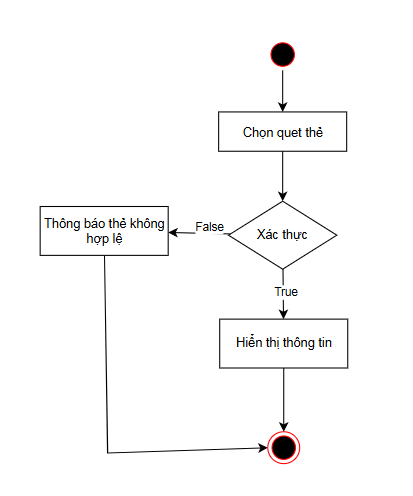


Hình 1.15 Biểu đồ usecase của chức năng quẹt thẻ

b. Đặc tả

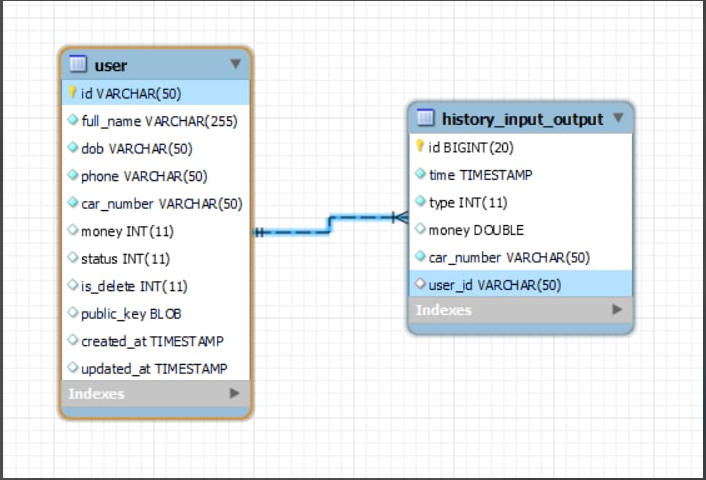
|  |  |
| --- | --- |
| Usecase | Quẹt thẻ |
| Tác nhân chính | User |
| Mô tả | Quẹt thẻ khi cho xe vào và bãi đỗ xe |
| Tiền điều kiện | kết nối tới thẻ |
| Luồng điều kiện chính | 1. User chọn quẹt thẻ  2. Thực hiện xác thực (Thành công)  3. Hiển thị thông tin lên giao diện |
| Luồng điều kiện phụ | Xác thực không thành công  - Thông báo thẻ không hợp l |

c. Biểu đồ hoạt động



Hình 1.16 Biểu đồ hoạt động của chức năng quẹt thẻ

## 1.3 Thiết kế cơ sở dữ liệu



Hình 1.17 Cơ sở dữ liệu

### 1.3.1 Bảng user

| **Tên cột** | **Kiểu dữ liệu** | **Ý nghĩa** |
| --- | --- | --- |
| id | VARCHAR(50) | Khóa chính, định danh duy nhất cho từng người dùng. |
| full\_name | VARCHAR(255) | Tên đầy đủ của người dùng. |
| dob | VARCHAR(50) | Ngày sinh của người dùng (định dạng chuỗi). |
| phone | VARCHAR(50) | Số điện thoại của người dùng. |
| car\_number | VARCHAR(50) | Biển số xe của người dùng. |
| money | INT | Số tiền hiện tại trong tài khoản của người dùng, mặc định là 0. |
| status | INT | Trạng thái của người dùng, mặc định là 0. (Ví dụ: 0 = không hoạt động, 1 = hoạt động). |
| is\_delete | INT | Trạng thái xóa, mặc định là 0. (0 = chưa xóa, 1 = đã xóa). |
| public\_key | BLOB | Khóa công khai của người dùng, có thể dùng cho mục đích mã hóa hoặc xác thực. |
| created\_at | TIMESTAMP | Thời gian tạo tài khoản. |
| updated\_at | TIMESTAMP | Thời gian cập nhật thông tin lần cuối. |

### 1.3.2 Bảng history\_input\_output

| **Tên cột** | **Kiểu dữ liệu** | **Ý nghĩa** |
| --- | --- | --- |
| id | BIGINT | Khóa chính, tự động tăng, định danh duy nhất cho từng giao dịch. |
| time | TIMESTAMP | Thời điểm xảy ra giao dịch. |
| type | INT | Loại (xe vào xe ra) |
| money | DOUBLE | Số tiền liên quan đến giao dịch. |
| car\_number | VARCHAR(50) | Biển số xe liên quan đến giao dịch. |
| user\_id | VARCHAR(50) | Khóa ngoại, tham chiếu đến id trong bảng user, thể hiện giao dịch thuộc về người dùng nào. |

# CHƯƠNG 2: CÀI ĐẶT VÀ THỰC NGHIỆM

## 2.1 Thiết kế giao diện

### 2.1.1 Giao diện kết nối với Applet

**A screenshot of a computer

Description automatically generated**

Hình 2.1 Giao diện kết nối Applet

### 2.1.2 Giao diện nhập mã pin

*A screenshot of a computer

Description automatically generated*

Hình 2.2 Giao diện kết nối Applet

### 2.1.3 Giao diện khởi tạo thẻ

A screenshot of a computer

Description automatically generated

Hình 2.3 Giao diện khỏi tạo thẻ

### 2.1.4 Giao diện trang chủ



Hình 2.4 Giao diện trang chủ

2.1.5 Giao diện cập nhật thông tin.

A screenshot of a computer

Description automatically generated

Hình 2.5 Giao diện cập nhật thông tin

### 2.1.6 Giao diện nạp tiền

A screenshot of a computer

Description automatically generated

Hình 2.6 Giao diện nạp tiền

### 2.1.7 Giao diện đổi mã pin

A screenshot of a computer login box

Description automatically generated

Hình 2.7 Giao diện đổi mã pin

### 2.1.8 Giao diện quản lí bãi đỗ xe

A screenshot of a computer

Description automatically generated

Hình 2.8 Giao diện quản lí bãi đỗ xe

### 2.1.9 Giao diện quản lịch sử ra vào

A screenshot of a computer

Description automatically generated

Hình 2.9 Giao diện lịch sử ra vào

## 2.2 Cơ chế xử lý

### ****2.2.1. Mã PIN****

**Mô tả**: Mã PIN của người dùng là một dãy số từ **6 đến 10 ký tự** mà người dùng nhập từ giao diện.

**Quy trình xử lý**:

* Người dùng nhập mã PIN từ giao diện.
* Mã PIN được truyền xuống thẻ thông minh.
* Một chuỗi **salt** (chuỗi ngẫu nhiên) được kết hợp với mã PIN để tăng tính bảo mật.
* Mã PIN kết hợp với **salt** sẽ được băm bằng **thuật toán MD5**, tạo ra giá trị mã hóa.
* Giá trị mã hóa này sẽ được lưu trữ trong thẻ thông minh, thay vì lưu trữ mã PIN dưới dạng văn bản thuần túy.

### ****2.2.2. Mã hóa dữ liệu****

**Mô tả**: Dữ liệu quan trọng sẽ được mã hóa để bảo vệ thông tin người dùng.

**Quy trình xử lý**: Sử dụng thuật toán AES

* **Khóa AES**:

1. Một **chuỗi tự động** sẽ được sinh ra để làm khóa AES.
2. Khóa này sẽ được **băm bằng thuật toán MD5** để tạo ra khóa AES chuẩn.

* **Mã hóa khóa AES**:

1. Khóa AES sẽ được mã hóa lại sử dụng **mã PIN** của người dùng làm **khóa chính**.
2. Khóa mã hóa này sẽ được lưu lại trong thẻ thông minh để phục vụ cho quá trình giải mã sau này.

* **Mã hóa dữ liệu**:

1. Dữ liệu được truyền xuống thẻ sẽ được mã hóa bằng khóa AES.

2. Dữ liệu đã mã hóa sẽ được lưu trữ trong thẻ thông minh.

### ****2.2.3. Tạo ID thẻ****

**Mô tả**: ID thẻ sẽ giúp định danh mỗi thẻ trong hệ thống.

**Quy trình xử lý**:

* ID thẻ có định dạng cố định, ví dụ: **PC0001**, **PC0002**.
* Để tạo ID thẻ mới, hệ thống sẽ lấy ID của thẻ cuối cùng trong cơ sở dữ liệu (ID gần nhất).
* Hệ thống sẽ tự động **tăng giá trị của ID** thêm 1, tạo ra một ID thẻ mới duy nhất.

### ****2.2.4. Xử lý hình ảnh****

**Mô tả**: Hệ thống sẽ hỗ trợ lưu trữ và xử lý hình ảnh người dùng.

**Quy trình xử lý**:

* Ảnh sẽ được lưu thông qua APDU mở rộng
* Mã hóa ảnh và lưu lại vào thẻ.

### ****2.2.5. Xác thực thẻ****

**Mô tả**: Xác thực người dùng được thực hiện thông qua **cặp khóa RSA** và quá trình mã hóa/dữ liệu ký.

**Quy trình xử lý**:

* **Đăng ký thẻ**:

1. Khi người dùng đăng ký thẻ thành công, hệ thống sẽ **tạo ra một cặp khóa RSA** (gồm một public key và một private key).
2. **Public key** sẽ được **chuyển thành mảng byte** và gửi lên server.
3. Server sẽ **lưu public key vào cơ sở dữ liệu** để sử dụng cho các lần xác thực sau.
4. **Private key** sẽ được chuyển thành mảng byte, sau đó **mã hóa bằng thuật toán AES** và lưu trữ trong thẻ.

* **Xác thực thẻ**:

1. Khi người dùng muốn xác thực, **server sinh một thông điệp ngẫu nhiên** (nonce) và gửi xuống thẻ.
2. Thẻ sử dụng **private key** đã được lưu trữ để **mã hóa thông điệp ngẫu nhiên** này, tạo ra một chữ ký số (digital signature).
3. Chữ ký số sẽ được gửi lại lên server.
4. **Server sử dụng public key** từ cơ sở dữ liệu để **giải mã chữ ký số** và so sánh với thông điệp ban đầu.
5. Nếu thông điệp giải mã từ chữ ký khớp với thông điệp ban đầu, quá trình **xác thực thành công**.

# CHƯƠNG 3: TỔNG KẾT

## 3.1 Tổng kết

Bài toán xây dựng thẻ gửi xe sử dụng Smart Card đã được giải quyết, đáp ứng được đủ yêu cầu của người dùng

* Các chức năng kết nối, khởi tạo thẻ hoạt động tốt dễ dàng sử dụng cho mọi người dùng
* Thông tin người dùng được mã hóa bằng mã khóa AES, đảm bảo thông tin không bị rò rỉ và phát tán.
* Tích hợp xác thực thẻ bằng thuật toán RSA.

## 3.2 Kết quả các thành viên trong nhóm đạt được

* Đã sử dụng được ngôn ngữ Java và Java Card để xây dựng thẻ thông minh
* Thẻ cơ bản đã hoạt động tốt ở trạng thái mô phỏng với các chức năng
* Các thành viên trong nhóm tích cực làm việc, hòa đồng, chia sẻ kiến thức và khó khăn với nhau để đáp ứng được thời gian yêu cầu
* Đã có nền tảng về thẻ thông mình, tạo cơ sở phát triển các project sau này

## 3.3 Hạn chế

* Do không được cung cấp thẻ, nhóm chỉ thực hiện trên mô phỏng nên không thể đi vào thực tế
* Thời gian ngắn nên giao diện có phần hơi đơn giản chưa được bắt mắt