TRƯỜNG ĐẠI HỌC SÀI GÒN

**KHOA CÔNG NGHỆ THÔNG TIN**

A blue button with white text

Description automatically generated

Báo cáo đồ án môn học

**Phân tích thiết kế hướng đối tượng**

**TÊN ĐỀ TÀI: Xây dựng website bán mô hình xe trực tuyến**

Giáo viên hướng dẫn: Cô Lê Nhị Lãm Thúy

Thành viên: Nguyễn Huỳnh Hoàng Vũ – 3123411346

Nguyễn Tuấn Hưng – 3123411133

Thành phố Hồ Chí Minh, tháng 11 năm 2025

**LỜI CAM ĐOAN**

Tôi xin cam đoan những kết quả nghiên cứu được thể hiện trong tiểu luận này là sản phẩm của riêng cá nhân tôi và không có bất kỳ sự gian lận hay sao chép nào. Toàn bộ nội dung của báo cáo đều được trình bày dựa trên quan điểm, kiến thức cá nhân hoặc tích lũy, chọn lọc từ nhiều nguồn tài liệu có đính kèm chi tiết và hợp lệ.

Tôi xin hoàn toàn chịu trách nhiệm và hình thức kỷ luật theo quy định nếu phát hiện bất kỳ sai phạm hoặc gian lận nào.

MỤC LỤC

Contents

[LỜI MỞ ĐẦU 1](#_Toc213799497)

[CHƯƠNG 1. MÔ TẢ BÀI TOÁN 2](#_Toc213799498)

[1. Hiện trạng và lý do chọn đề tài 2](#_Toc213799499)

[2. Mục tiêu và Phạm vi đề tài 2](#_Toc213799500)

[2.1. Mục tiêu 2](#_Toc213799501)

[2.2. Phạm vi chức năng (Functional Scope) 3](#_Toc213799502)

[[1]](#endnote-1)

# LỜI MỞ ĐẦU

Thương mại điện tử ngày nay đã trở thành một kênh mua sắm thiết yếu. Trong đó, thị trường ngách như mô hình xe đua, dù nhu cầu sưu tầm ngày càng tăng, vẫn còn thiếu các nền tảng trực tuyến chuyên biệt.

Xuất phát từ thực tế đó, chúng em thực hiện đề tài **"Xây dựng website bán mô hình xe đua trực tuyến"**. Mục tiêu của đồ án là xây dựng một hệ thống hoàn chỉnh, cung cấp trải nghiệm mua sắm thuận tiện cho khách hàng và bộ công cụ quản lý hiệu quả (sản phẩm, đơn hàng) cho quản trị viên.

# CHƯƠNG 1. MÔ TẢ BÀI TOÁN

## 1. Hiện trạng và lý do chọn đề tài

Hiện nay, nhu cầu sưu tầm và trao đổi mô hình xe đua (diecast, resin, F1...) đang phát triển mạnh mẽ. Tuy nhiên, phần lớn các cửa hàng và cá nhân kinh doanh vẫn hoạt động theo phương thức truyền thống (bán tại cửa hàng) hoặc qua các kênh chưa được tối ưu cho thương mại điện tử (như mạng xã hội, diễn đàn).

Các phương thức này bộc lộ nhiều hạn chế:

* **Quản lý thủ công:** Việc quản lý đơn hàng, thông tin khách hàng và tình trạng tồn kho (như cột stock trong CSDL) thường được ghi chép thủ công, tốn thời gian và dễ gây sai sót.
* **Khó khăn trong xử lý nghiệp vụ:** Admin gặp khó khăn khi theo dõi trạng thái đơn hàng (như "Chờ xử lý", "Đang giao"), dẫn đến chậm trễ và giảm sự hài lòng của khách hàng.
* **Tiếp cận khách hàng hạn chế:** Khách hàng không có một nền tảng tập trung để xem toàn bộ sản phẩm, tìm kiếm thông tin chi tiết (như specs, warranty) và đặt hàng 24/7.

Xuất phát từ nhu cầu thực tế đó, đề tài **"Website bán mô hình xe đua trực tuyến"** được xây dựng. Hệ thống này cung cấp một giải pháp phần mềm tập trung, tự động hóa quy trình bán hàng, giúp khách hàng có trải nghiệm mua sắm tiện lợi và cung cấp cho quản trị viên (Admin) một công cụ quản lý nghiệp vụ mạnh mẽ, hiệu quả.

## 2. Mục tiêu và Phạm vi đề tài

### 2.1. Mục tiêu

Đề tài tập trung vào ba mục tiêu chính:

Xây dựng một công cụ quản trị (Admin Panel) hiệu quả: Cung cấp cho người quản lý khả năng theo dõi thống kê, quản lý toàn bộ vòng đời sản phẩm (CRUD) và xử lý các đơn hàng một cách chuyên nghiệp.

Xây dựng quy trình mua hàng (Client) rõ ràng: Cho phép khách hàng xem sản phẩm, quản lý giỏ hàng và thực hiện thanh toán (checkout) một cách thuận lợi và an toàn.

Tổ chức và chuẩn hóa dữ liệu: Thiết lập một cơ sở dữ liệu (CSDL) quan hệ rõ ràng để quản lý tập trung thông tin sản phẩm, đơn hàng và người dùng.

### 2.2. Phạm vi chức năng (Functional Scope)

Hệ thống bao gồm hai phân hệ chính với các chức năng cụ thể đã được cài đặt:

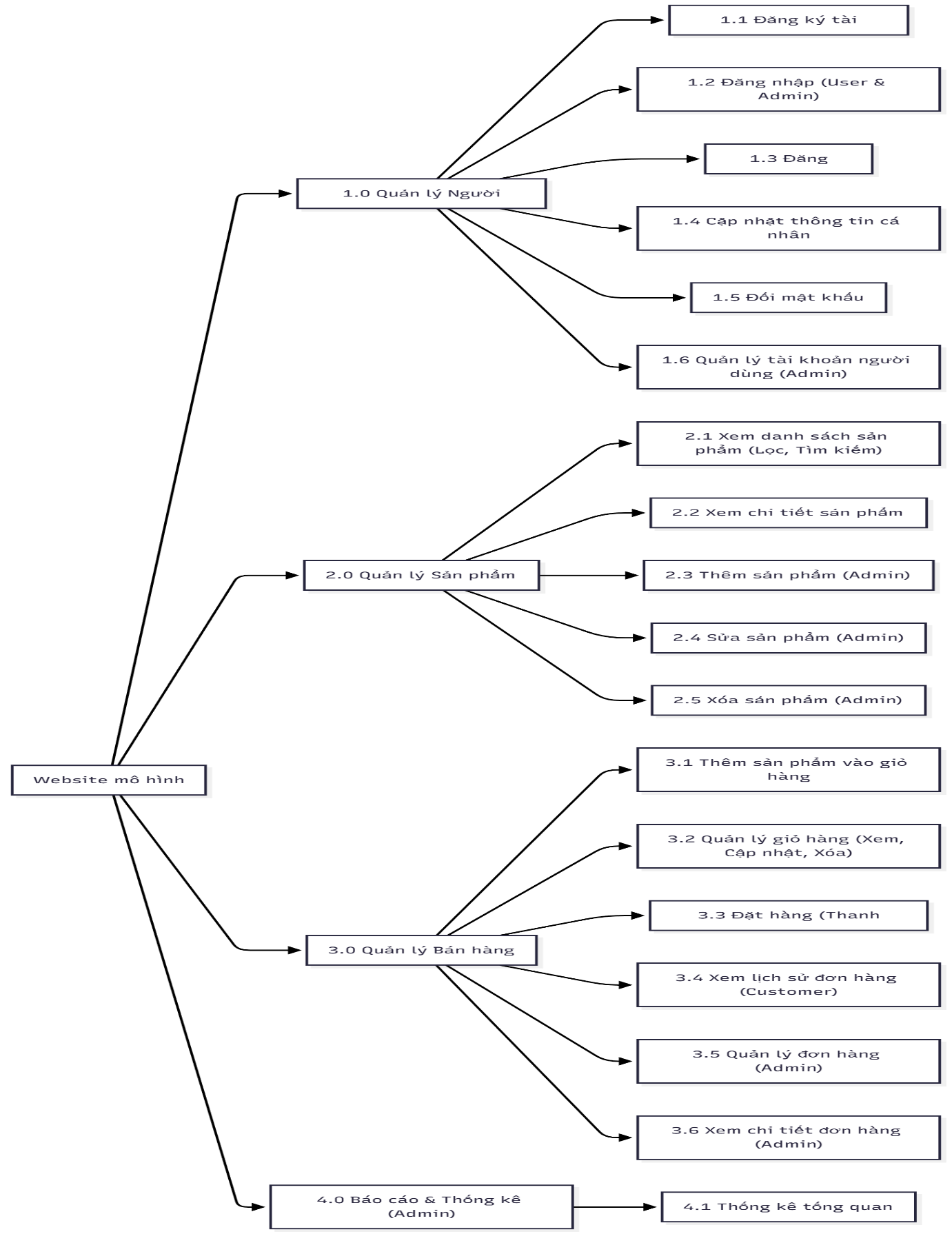
* Phân hệ Khách hàng (Front-end):
  + Quản lý Tài khoản: Đăng nhập (bắt buộc để thanh toán).
  + Đặt hàng: Quản lý giỏ hàng, điền thông tin và thực hiện thanh toán (Checkout).
* Phân hệ Quản trị viên (Back-end):
  + Dashboard: Xem thống kê tổng quan (doanh thu, đơn chờ xử lý, tổng sản phẩm, tổng người dùng).
  + Quản lý Sản phẩm (CRUD): Thêm, Sửa (bao gồm cả ảnh), Xóa sản phẩm.
  + Quản lý Đơn hàng: Xem danh sách, xem chi tiết đơn hàng (Modal) và cập nhật trạng thái xử lý.
  + Quản lý Người dùng: Xem danh sách và xóa tài khoản người dùng.

### 2.3. Yêu cầu phi chức năng (Non-Functional Requirements)

* Bảo mật: Hệ thống phải phân quyền truy cập rõ ràng. Chỉ Admin (role === 'admin') mới có thể truy cập trang quản trị. Mật khẩu người dùng phải được mã hóa.
* Dễ sử dụng (Usability): Giao diện quản trị được thiết kế tập trung vào tác vụ, rõ ràng, giúp Admin thao tác nhanh chóng.
* Bảo trì (Maintainability): Mã nguồn phía Admin được tái cấu trúc theo hướng đối tượng (OOP), tách biệt logic xử lý vào các lớp Model (Product, Order, User) để dễ dàng bảo trì và mở rộng.

## CHƯƠNG 2. PHÂN TÍCH HỆ THỐNG

## 1. Sơ đồ chức năng (BFD)

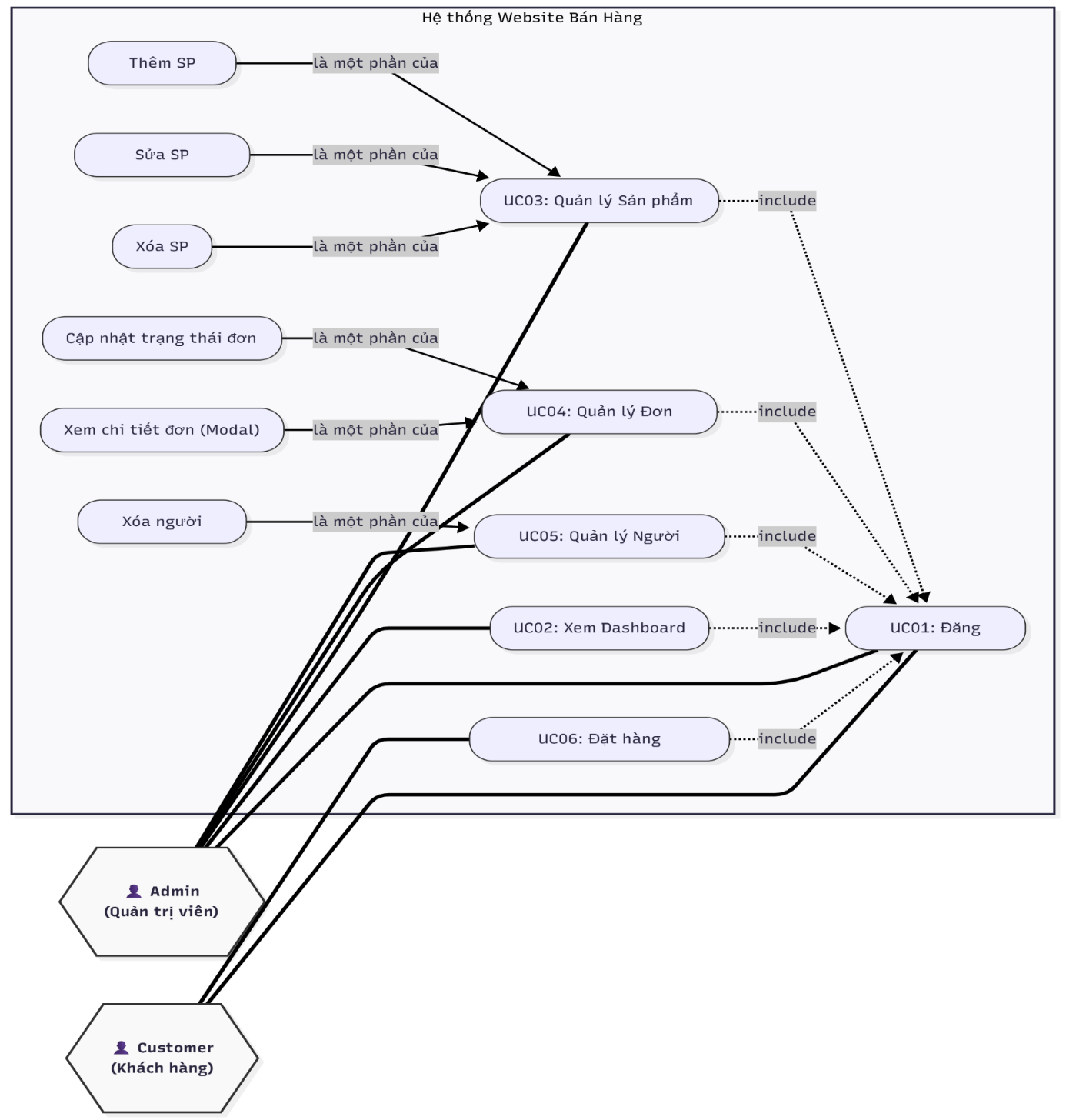
Sơ đồ Chức năng Kinh doanh (BFD) phân rã hệ thống thành các chức năng chính đến mức 2, bao gồm phân hệ Quản trị và phân hệ Khách hàng.

Hình 2.1 Sơ đồ Phân rã Chức năng (BFD) – Mức 2

## 2. Mô hình use Case và đặt tả Use Case

**Mô hình Use Case**

Biểu đồ mô tả các tác nhân chính (Admin, Customer) và các nhóm chức năng (Use Case) mà họ tương tác trong hệ thống.



Hình 2.2 Mô hình use case wedsite bán mô hình trực tuyến

**Đặc tả Use Case**

Đặc tả Use Case: Đăng nhập (Login)

|  |  |
| --- | --- |
| Mục | Nội dung |
| Tên Use Case | Đăng nhập hệ thống |
| Tác nhân | Khách hàng, admin |
| Mô tả | Cho phép người dùng truy cập vào hệ thống với tư cách thành viên hoặc quản trị viên để sử dụng các chức năng tương ứng |
| Tiền điều kiện | Người dùng đã có tài khoản( đã đăng ký trước đó hoặc được cấp ) |
| Luồng sự kiện chính | 1.Người dùng chọn chức năng “Đăng nhập” trên giao diện  2.Hệ thống hiển thị form đăng nhập.  3.Người dùng nhập Email và mật khẩu, sau đó nhấn nút “Đăng nhập”.  4.Hệ thống kiểm tra thông tin:  -Tìm kiếm Email trong cơ sở dữ liệu.  -So khớp mật khẩu ( đã mã hóa).  -Kiểm tra quyền(role:’user’ hoặc ‘admin’).  5. Nếu thông tin đúng, hệ thống tạo phiên làm việc (Session) và chuyển hướng người dùng đến trang tương ứng (Trang chủ cho 'user', Trang quản trị cho 'admin'). |
| Luồng thay thế | Sai Email hoặc Mật khẩu:  -Hệ thống hiển thị thông báo lỗi "Tài khoản hoặc mật khẩu không đúng".  -Người dùng quay lại bước 3. |
| Hậu điều kiện | Người dùng đã đăng nhập thành công và có thể sử dụng các chức năng theo phân quyền. |

Đặc tả Use Case: Đặt hàng (Checkout)

|  |  |
| --- | --- |
| Mục | **Nội dung** |
| Tên Use Case | Đặt hàng (Thanh toán) |
| Tác nhân | Khách hàng (đã đăng nhập) |
| Mô tả | Khách hàng tiến hành xác nhận đơn hàng với các sản phẩm đã chọn trong giỏ. |
| Tiền điều kiện | - Khách hàng đã đăng nhập.  - Giỏ hàng có ít nhất 1 sản phẩm. |
| Luồng sự kiện chính | 1.Khách hàng nhấn nút "Thanh toán" từ trang giỏ hàng.  2. Hệ thống hiển thị form Thanh toán với thông tin khách hàng được điền sẵn (nếu có).  3. Khách hàng kiểm tra và bổ sung thông tin nhận hàng (Họ tên, Địa chỉ, SĐT, Ghi chú).  4. Khách hàng chọn phương thức thanh toán (COD hoặc Chuyển khoản Online).  5. Khách hàng nhấn "Xác nhận đặt hàng".  6. Hệ thống thực hiện lưu trữ:  - Tạo bản ghi mới trong bảng orders (thông tin chung).  Lưu chi tiết từng sản phẩm vào bảng order\_details.  7. Hệ thống xóa giỏ hàng hiện tại và chuyển hướng khách đến trang "Đặt hàng thành công". |
| Luồng thay thế | Thông tin giao hàng còn thiếu:  -Hệ thống yêu cầu nhập đầy đủ các trường bắt buộc.  Lỗi hệ thống (CSDL):  - Hiển thị thông báo lỗi và yêu cầu khách hàng thử lại sau. |
| Hậu điều kiện | Đơn hàng mới được tạo với trạng thái "Đang xử lý" (hoặc "Chờ thanh toán"). |

Đặc tả Use Case: Quản lý Sản phẩm (Admin)

|  |  |
| --- | --- |
| Mục | Nội dung |
| Tên Use Case | Quản lý Sản phẩm (Thêm, Sửa, Xóa) |
| Tác nhân | Admin |
| Mô tả | Cho phép Admin thêm mới, cập nhật thông tin hoặc xóa sản phẩm khỏi cửa hàng. |
| Tiền điều kiện | Admin đã đăng nhập vào trang quản trị. |
| Luồng sự kiện chính | A. Thêm sản phẩm:  1. Admin chọn "Thêm sản phẩm".  2. Nhập đầy đủ thông tin (Tên, giá, mô tả, danh mục...) và chọn file ảnh.  3. Nhấn "Thêm". Hệ thống lưu sản phẩm mới và upload ảnh lên server.  B. Xóa sản phẩm:  1. Tại danh sách sản phẩm, Admin nhấn nút "Xóa" tương ứng với sản phẩm cần hủy.  2. Hệ thống xác nhận hành động.  3. Nếu đồng ý, hệ thống xóa bản ghi trong CSDL và xóa file ảnh gốc để giải phóng bộ nhớ. |
| Hậu điều kiện | Danh sách sản phẩm được cập nhật trên toàn hệ thống (cả trang Admin và trang Khách hàng). |

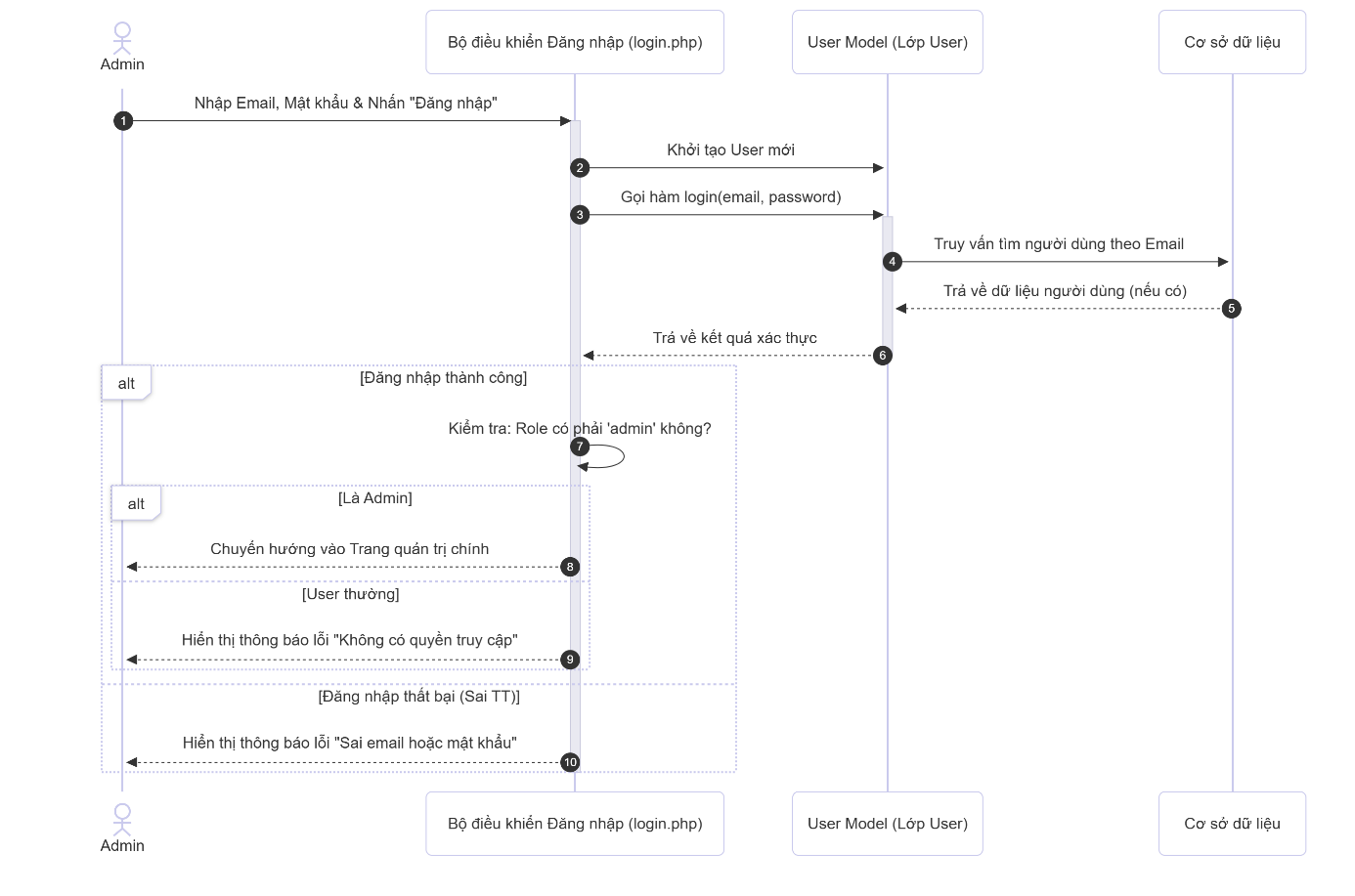
Đặc tả Use Case: Quản lý Đơn hàng (Admin)

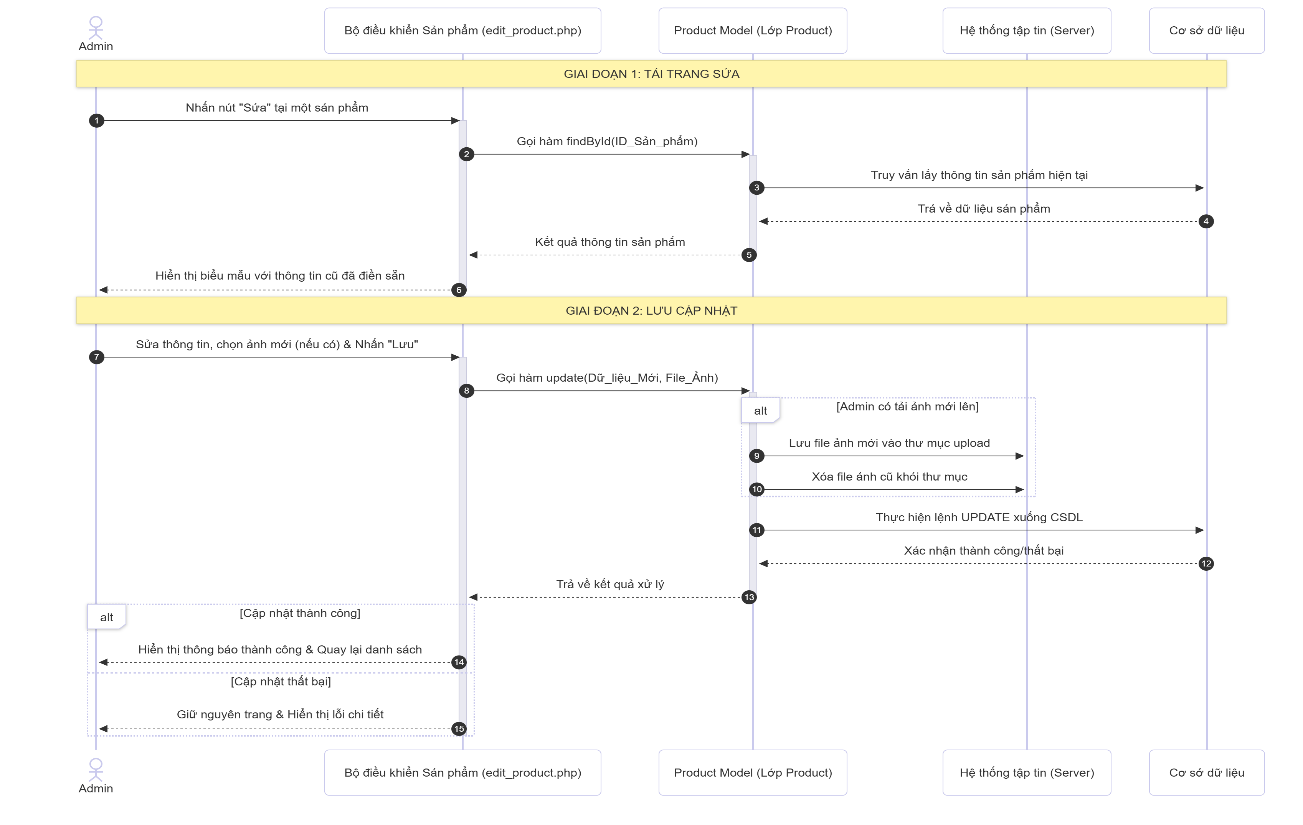
|  |  |
| --- | --- |
| Mục | Nội dung |
| Tên Use Case | Quản lý Đơn hàng (Xem chi tiết & Cập nhật trạng thái) |
| Tác nhân | Admin |
| Mô tả | Admin theo dõi các đơn hàng mới, xem chi tiết các món hàng khách mua và cập nhật tiến độ xử lý đơn hàng. |
| Tiền điều kiện | Admin đã đăng nhập vào trang quản trị. |
| Luồng sự kiện chính | 1.Admin chọn menu "Quản lý Đơn hàng". Hệ thống hiển thị danh sách tất cả đơn hàng.  2. Xem chi tiết: Admin nhấn nút "Xem" tại một đơn hàng. Hệ thống hiển thị cửa sổ (Modal) chứa:  -Thông tin người nhận.  -Danh sách các sản phẩm (Tên, giá, số lượng).  -Tổng tiền.  3. Cập nhật trạng thái: Admin chọn trạng thái mới (ví dụ: "Đang giao hàng") từ menu thả xuống.  4. Hệ thống lưu trạng thái mới vào CSDL và tự động tải lại trang để cập nhật giao diện. |
| Hậu điều kiện | Trạng thái đơn hàng được cập nhật. Khách hàng có thể nhìn thấy trạng thái mới này khi xem lịch sử đơn hàng của họ. |

## 3. Mô hình tuần tự (Sequence Diagram)

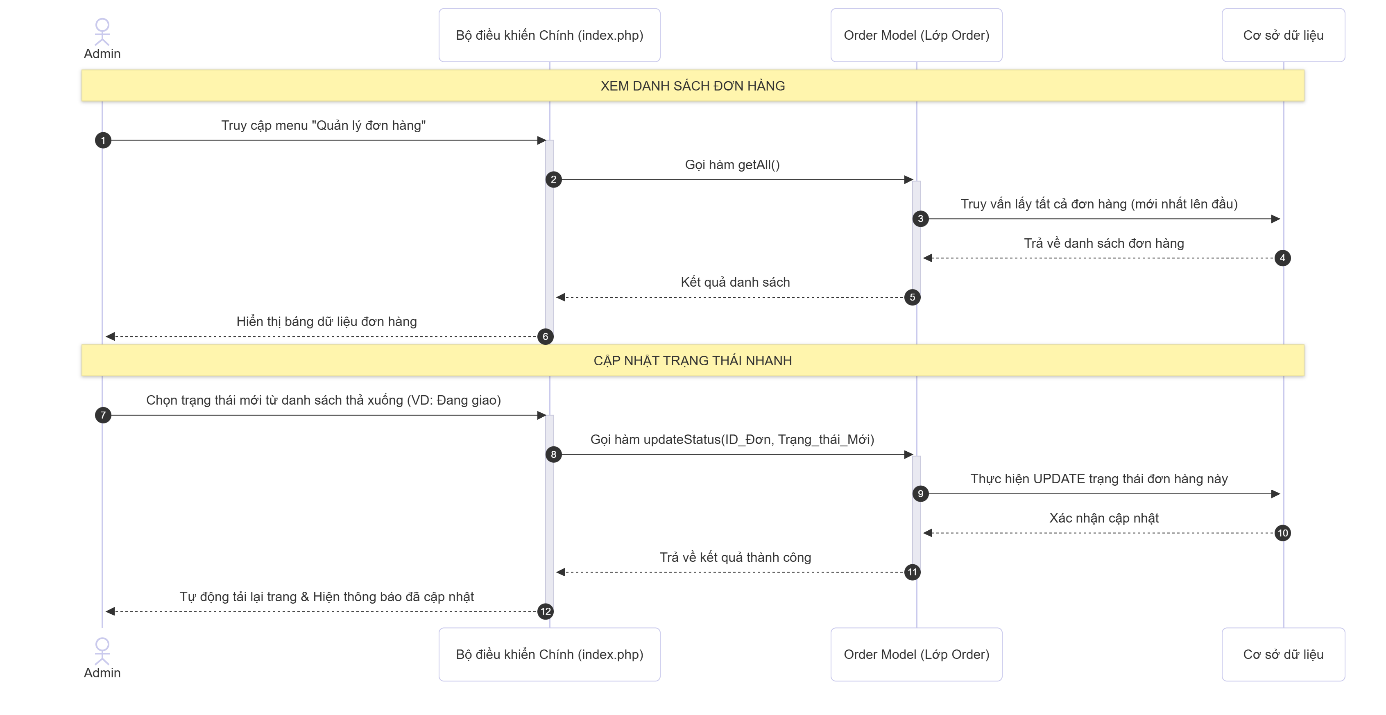
Biểu đồ tuần tự minh họa các luồng sự kiện chi tiết cho các Use Case quan trọng.

Quy trình Admin Đăng nhập (Login):

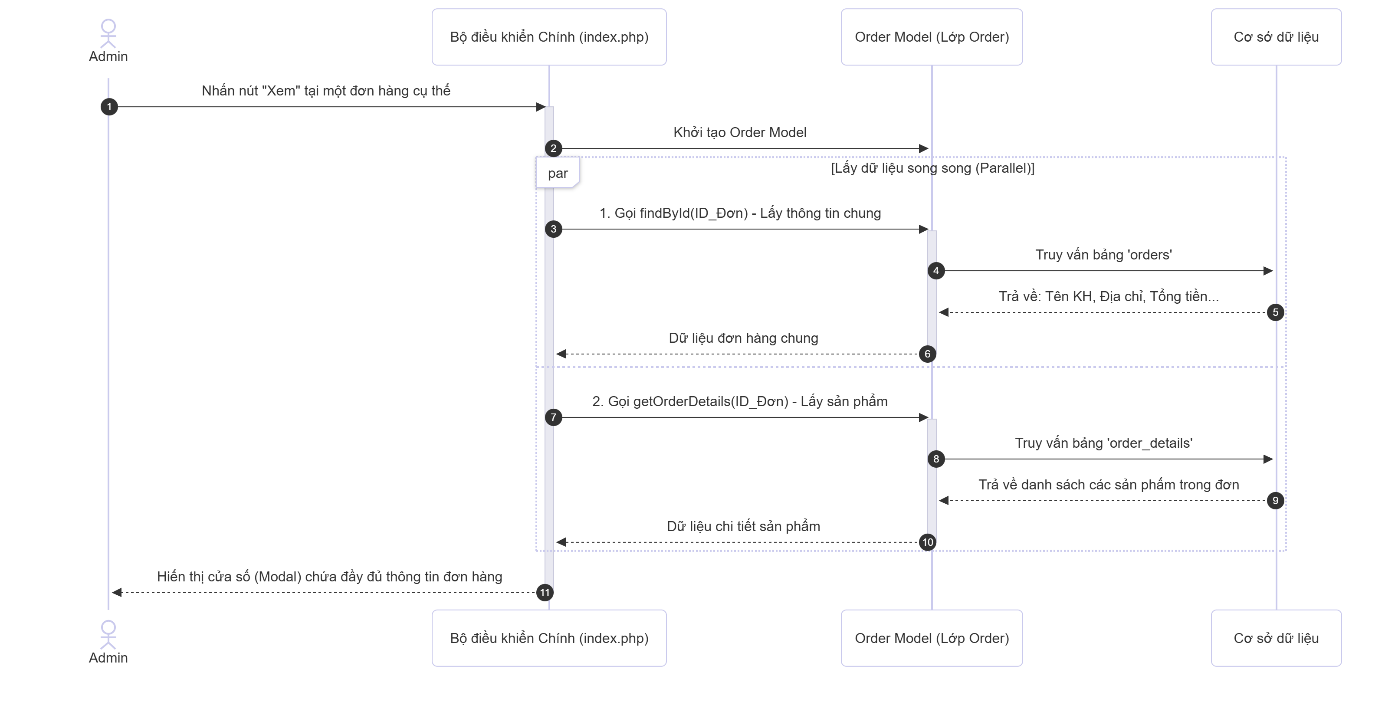


Quy trình Admin Quản lý Sản phẩm (Cập nhật):

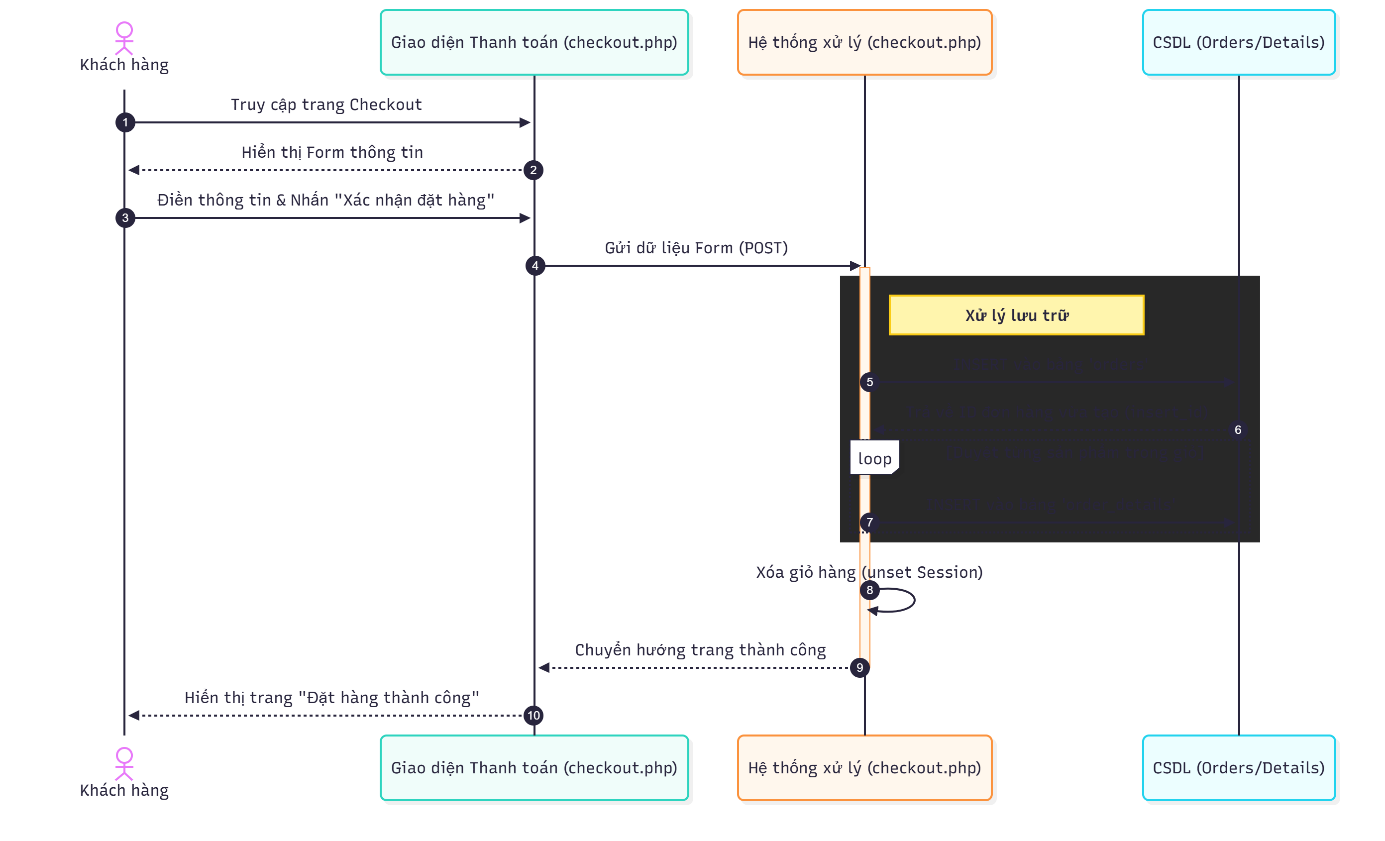
Quy trình Admin Quản lý Đơn hàng (Xem & Cập nhật trạng thái):



Quy trình Admin Xem Chi tiết Đơn hàng (Modal):



Quy trình Khách hàng Đặt hàng (Checkout):

****

# CHƯƠNG 3: THIẾT KẾ HỆ THỐNG

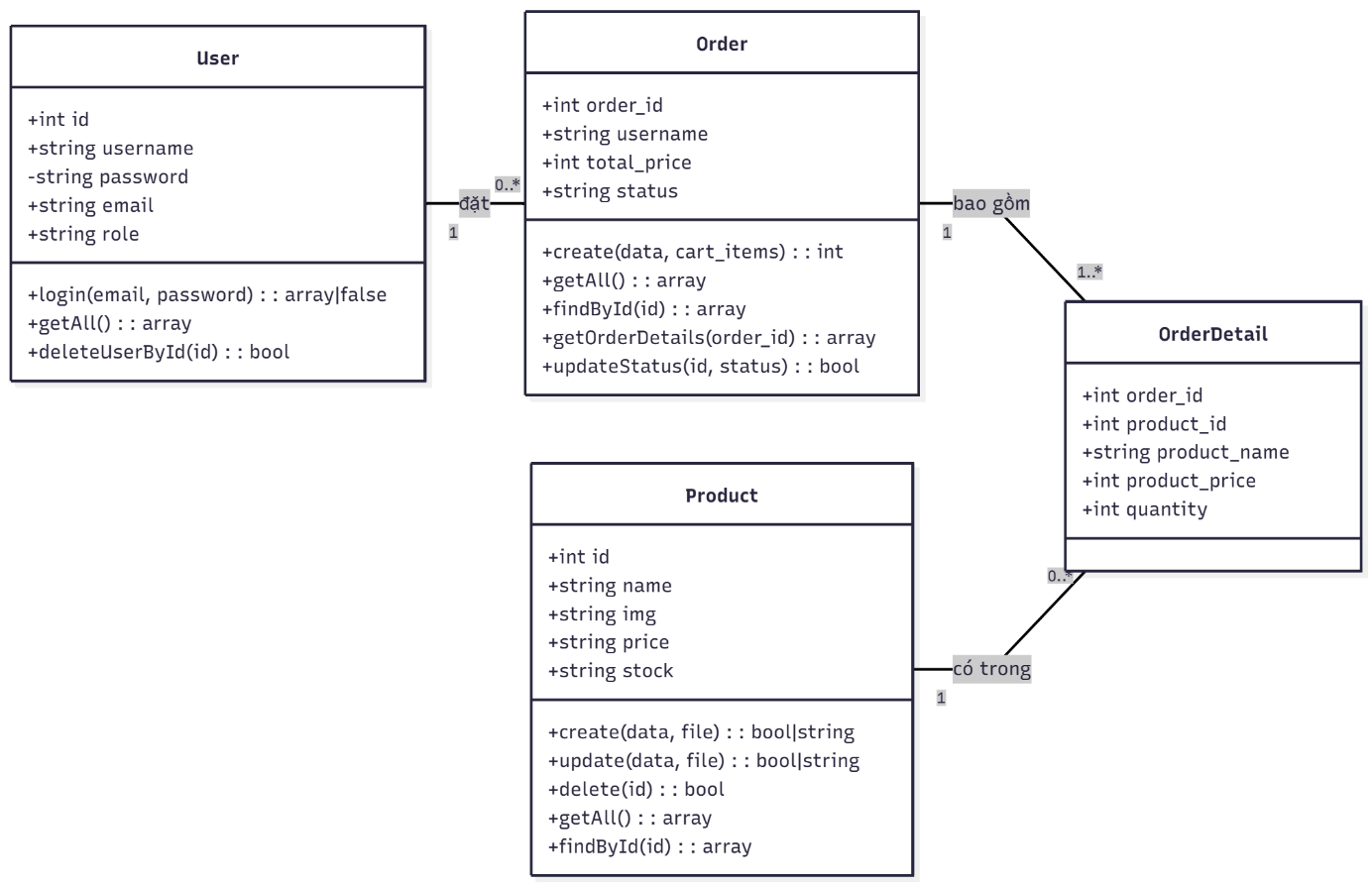
Chương này trình bày chi tiết về kiến trúc logic và vật lý của hệ thống, bao gồm thiết kế lớp đối tượng (OOP), thiết kế cơ sở dữ liệu (CSDL) và thiết kế giao diện người dùng (UI).

## 1. Thiết kế Lớp đối tượng

Thiết kế này tập trung vào 3 Lớp Model chính (Model) được xây dựng để xử lý logic nghiệp vụ, dựa trên mã nguồn OOP đã cung cấp.

### 1.1. Sơ đồ Lớp (Class Diagram)

Sơ đồ này mô tả cấu trúc, thuộc tính, phương thức của các lớp và mối quan hệ giữa chúng.



### 1.2. Danh sách Lớp và Nhiệm vụ

|  |  |
| --- | --- |
| Tên lớp | Nhiệm vụ chính |
| User | Quản lý xác thực (đăng nhập), phân quyền (admin/user) và các thao tác quản lý tài khoản người dùng. |
| Product | Quản lý toàn bộ vòng đời sản phẩm (CRUD), bao gồm cả xử lý logic tải lên (upload) và xóa file ảnh. |
| Orde | Quản lý nghiệp vụ đặt hàng, cập nhật trạng thái đơn hàng và truy xuất lịch sử, chi tiết đơn hàng. |
| OrderDetail | (Thực thể dữ liệu) Đại diện cho một dòng sản phẩm cụ thể trong một đơn hàng, lưu trữ "snapshot" (ảnh chụp nhanh) về giá và tên tại thời điểm mua. |

### 1.3. Thuộc tính và Phương thức chi tiết của các Lớp

**Lớp User (models/User.php)**

* **Thuộc tính (Attributes):**
  + $conn: Biến kết nối CSDL.
  + id (int): ID định danh.
  + username (string): Tên tài khoản.
  + email (string): Email dùng để đăng nhập.
  + password (string): Mật khẩu đã được mã hóa (hash).
  + role (string): Vai trò của người dùng ('admin' hoặc 'user').
* **Phương thức (Methods):**
  + login(email, password): Xác thực email và mật khẩu, trả về mảng thông tin user nếu thành công.
  + getAll(): Lấy danh sách tất cả người dùng để hiển thị trong trang Admin.
  + deleteUserById(id): Xóa một người dùng dựa trên ID.

**Lớp Product (models/Product.php)**

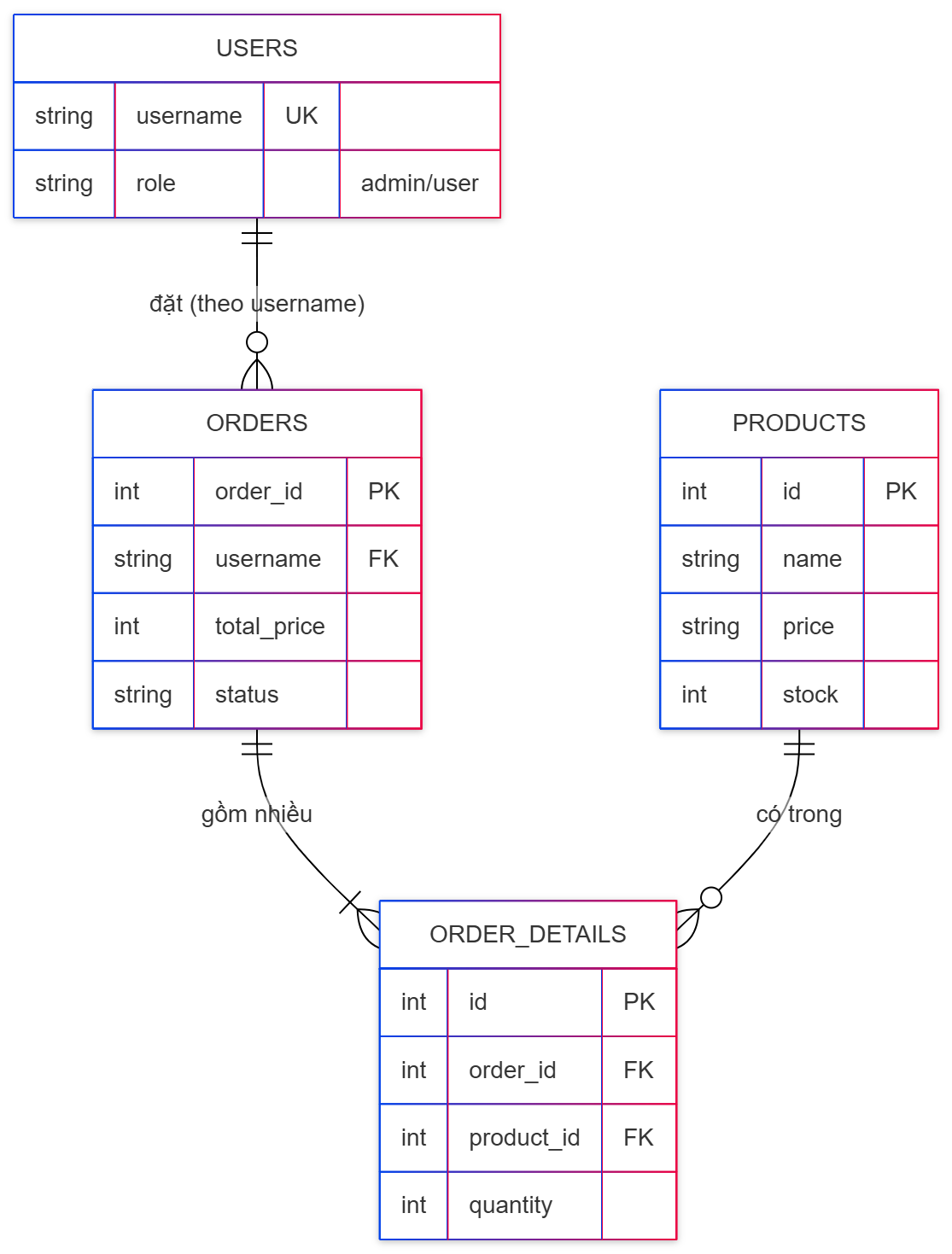
* **Thuộc tính (Attributes):**
  + $conn: Biến kết nối CSDL.
  + id, name, img, price, desc, specs, warranty, category, sku, brand, stock: Các thuộc tính tương ứng với các cột trong bảng products.
* **Phương thức (Methods):**
  + getAll(): Lấy tất cả sản phẩm để hiển thị ra bảng quản lý.
  + findById(id): Lấy thông tin chi tiết của một sản phẩm (dùng cho trang Sửa).
  + create(data, file): Xử lý logic thêm sản phẩm mới, bao gồm gọi phương thức private để upload ảnh.
  + update(data, file): Xử lý cập nhật thông tin sản phẩm (bao gồm logic kiểm tra, thay/giữ ảnh, xóa ảnh cũ).
  + delete(id): Xử lý xóa sản phẩm (bao gồm logic tìm tên ảnh và xóa file ảnh vật lý).

**Lớp Order (models/Order.php)**

* **Thuộc tính (Attributes):**
  + $conn: Biến kết nối CSDL.
  + order\_id, username, total\_price, status, payment\_method, customer\_name, customer\_address, customer\_phone...: Các thuộc tính tương ứng với các cột trong bảng orders.
* **Phương thức (Methods):**
  + create(data, cart\_items): (Được gọi bởi checkout.php) Nhận dữ liệu khách hàng và giỏ hàng, sau đó lưu vào 2 bảng orders và order\_details.
  + getAll(): Lấy danh sách tất cả đơn hàng cho Admin.
  + findById(id): Lấy thông tin chung của một đơn hàng (để hiển thị modal).
  + getOrderDetails(order\_id): Lấy danh sách các sản phẩm chi tiết thuộc một đơn hàng (để hiển thị modal).
  + updateStatus(id, status): Cập nhật trạng thái cho một đơn hàng (VD: "Đang xử lý" -> "Đang giao").

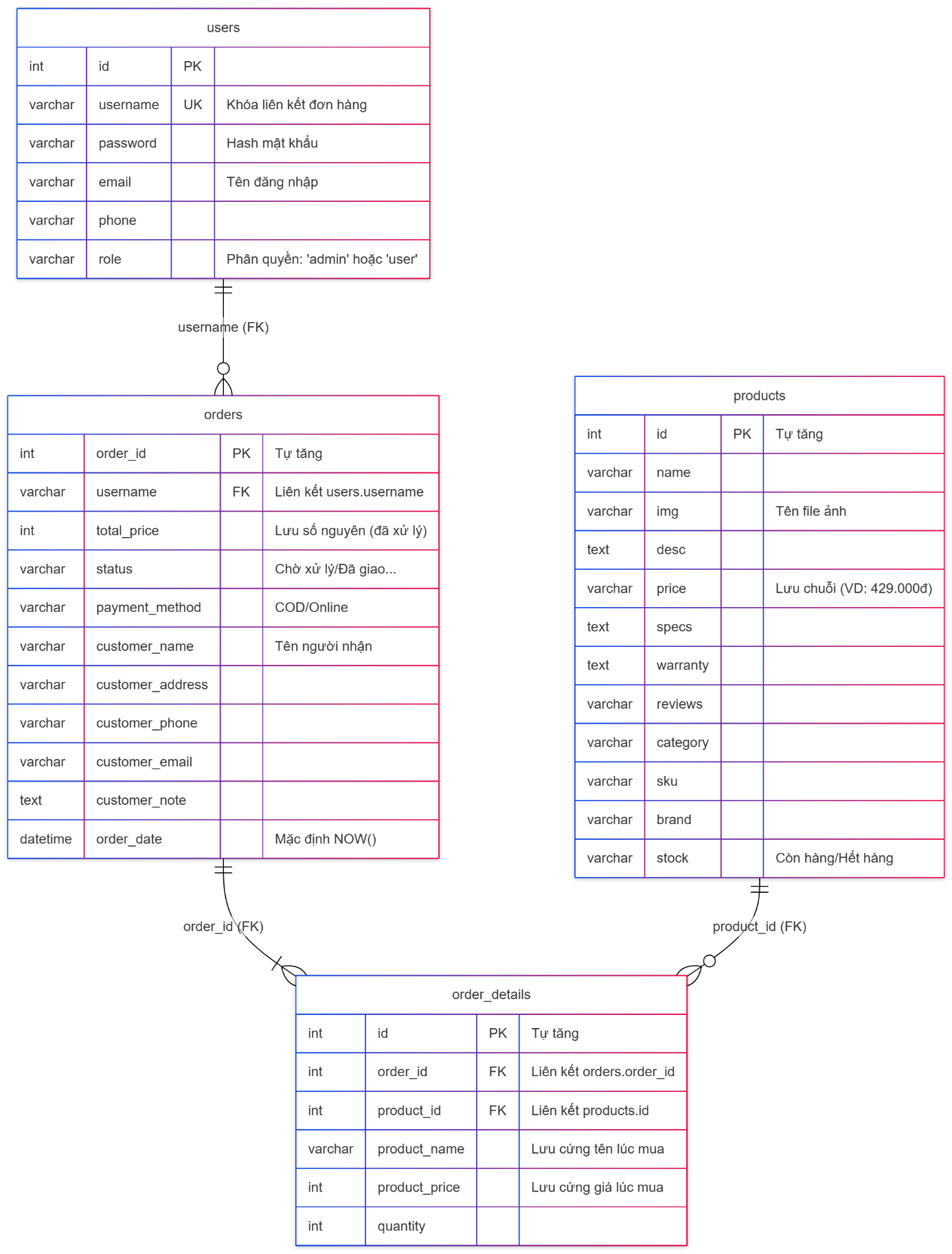
## 2. Thiết kế CSDL

### 2.1. Sơ đồ ERD (Entity-Relationship Diagram)



### 2.2. Mô hình Dữ liệu Quan hệ (RDM - Relational Data Model)

Mô hình RDM đặc tả chi tiết cấu trúc bảng vật lý, các cột, khóa chính (PK), khóa ngoại (FK) và khóa duy nhất (UK).



## 3. Thiết kế Giao diện

Phần này mô tả các màn hình nghiệp vụ chính, các thành phần tương tác và các biến cố (sự kiện) liên quan.

## 3.1. Màn hình Đặt hàng (Checkout)

* **Màn hình:** checkout.php
* **Mô tả:** Giao diện cuối cùng để khách hàng xác nhận thông tin và hoàn tất đơn hàng.
* **Danh sách thành phần:**
  + Form "Thông tin giao hàng" (bao gồm các Textbox: Họ tên, SĐT, Email, Địa chỉ, Ghi chú).
  + Khung "Đơn hàng của bạn" (Liệt kê sản phẩm, số lượng, tổng tiền).
  + Radio button "Phương thức thanh toán" (Giá trị: 'cod' hoặc 'online').
  + Button "Xác nhận đặt hàng" (Tên: place\_order).
* **Danh sách biến cố (Events):**
  + **Click [Xác nhận đặt hàng]:**
    - Form được submit bằng phương thức POST.
    - Hệ thống kiểm tra isset($\_POST['place\_order']).
    - Lấy tất cả dữ liệu từ form và giỏ hàng ($\_SESSION['cart']).
    - Lưu vào CSDL (bảng orders và order\_details).
    - Chuyển hướng đến trang thành công.

## 3.2. Màn hình Quản lý Đơn hàng (Admin)

* **Màn hình:** admin/index.php?view=orders
* **Mô tả:** Giao diện giúp Admin theo dõi và xử lý các đơn hàng.
* **Danh sách thành phần:**
  + Bảng (Table) danh sách đơn hàng.
  + Dropdown (Select) "Trạng thái" trên mỗi dòng đơn hàng (Tên: status).
  + Các trường hidden chứa action=update\_order\_status và id của đơn hàng.
  + Nút "Xem" chi tiết (Link đến ?view=order\_detail&id=...).
* **Danh sách biến cố (Events):**
  + **Change [Dropdown Trạng thái]:**
    - Sự kiện onchange="this.form.submit()" được kích hoạt.
    - Form được submit bằng phương thức GET.
    - Hệ thống kiểm tra action === 'update\_order\_status'.
    - Gọi phương thức order\_handler->updateStatus() để cập nhật CSDL.
    - Trang được tải lại và hiển thị trạng thái mới.
  + **Click [Xem]:**
    - Chuyển hướng đến ?view=order\_detail&id=...
    - Hệ thống tải dữ liệu đơn hàng và chi tiết đơn hàng.
    - Hiển thị Modal (cửa sổ bật lên) chứa thông tin chi tiết.

## 3.3. Màn hình Sửa Sản phẩm (Admin)

* **Màn hình:** admin/edit\_product.php
* **Mô tả:** Form để Admin cập nhật thông tin chi tiết của một sản phẩm.
* **Danh sách thành phần:**
  + Các Textbox, Textarea, Select: name, price, sku, category, stock, desc... (được điền sẵn giá trị cũ).
  + Input type="file" (Tên: img) để tải ảnh mới.
  + Input hidden (Tên: current\_img) để lưu tên ảnh cũ.
  + Input hidden (Tên: id) để xác định sản phẩm cần sửa.
  + Button "Cập Nhật Sản Phẩm" (Tên: submit\_edit\_product).
* **Danh sách biến cố (Events):**
  + **Click [Cập Nhật Sản Phẩm]:**
    - Form được submit bằng phương thức POST.
    - Hệ thống kiểm tra isset($\_POST['submit\_edit\_product']).
    - Gọi phương thức product\_handler->update().
    - Lớp Product xử lý logic: Nếu có ảnh mới ($\_FILES['img']) thì upload ảnh mới và xóa ảnh cũ (current\_img), ngược lại giữ nguyên ảnh cũ.

Cập nhật CSDL và chuyển hướng về trang quản lý.

# CHƯƠNG 4. CÀI ĐẶT, THỬ NGHIỆM VÀ TỔNG KẾT

## 4.1. Cài đặt và Thử nghiệm

### 4.1.1. Môi trường cài đặt

* **Hệ điều hành:** Windows 10/11.
* **Web Server:** XAMPP (Apache + MySQL).
* **Ngôn ngữ lập trình:** PHP 8.x.
* **Cơ sở dữ liệu:** MySQL (quản lý qua phpMyAdmin).
* **Trình duyệt:** Google Chrome, Edge, Firefox.

### 4.1.2. Hướng dẫn cài đặt

1. Cài đặt XAMPP và khởi động mô-đun Apache và MySQL.
2. Copy toàn bộ thư mục source code của đồ án vào thư mục C:\xampp\htdocs\.
3. Truy cập http://localhost/phpmyadmin, tạo một CSDL mới (ví dụ: web\_ban\_xe).
4. Import file .sql (đi kèm source code) vào CSDL vừa tạo để thiết lập cấu trúc bảng và dữ liệu mẫu.
5. Cấu hình thông tin kết nối CSDL trong file db/connect.php.
6. Truy cập trang web qua địa chỉ http://localhost/ten\_thu\_muc/.
7. Đăng nhập trang Admin qua <http://localhost/ten_thu_muc/admin/login.php>.

### 4.1.3. Kết quả Thử nghiệm (Test Cases)

Thực hiện kiểm thử các kịch bản nghiệp vụ chính để xác minh tính đúng đắn của hệ thống.

## 4.2. Phân tích và Hướng cải tiến

### 4.2.1. Ưu điểm

* **Đáp ứng nghiệp vụ:** Hệ thống đã đáp ứng đầy đủ các quy trình nghiệp vụ cốt lõi của một website thương mại điện tử, từ phía Khách hàng (Đặt hàng) đến Quản trị viên (Quản lý Sản phẩm, Xử lý Đơn hàng).
* **Cấu trúc tốt:** Mã nguồn phía Admin được tổ chức theo hướng đối tượng (OOP) (Lớp Product, Order, User), tách biệt logic xử lý và giao diện, giúp dễ dàng bảo trì và nâng cấp.
* **Dữ liệu nhất quán:** Thiết kế CSDL (RDM) chặt chẽ, sử dụng khóa ngoại và kỹ thuật "snapshot" (lưu cứng product\_name, product\_price trong order\_details) giúp đảm bảo tính toàn vẹn của lịch sử đơn hàng.

### 4.2.2. Nhược điểm

* **Bảo mật cơ bản:** Hệ thống đã phân quyền Admin nhưng chưa xử lý triệt để các lỗ hổng bảo mật phổ biến như **XSS** (Cross-Site Scripting - khi hiển thị dữ liệu do người dùng nhập) và **CSRF** (Cross-Site Request Forgery - trong các form submit).
* **Chức năng thanh toán:** Chức năng "Thanh toán Online" mới chỉ là mô phỏng (lưu trạng thái "Chờ thanh toán") chứ chưa tích hợp với bất kỳ cổng thanh toán thực tế nào.
* **Giao diện Client:** Phần giao diện phía khách hàng (trang chủ, chi tiết sản phẩm) chưa được tập trung phát triển sâu trong phạm vi đồ án này.

### 4.2.3. Hướng cải tiến

* **Tăng cường bảo mật:** Áp dụng htmlspecialchars() cho tất cả dữ liệu xuất ra HTML để chống XSS. Bổ sung cơ chế **CSRF Token** cho tất cả các form (Thêm, Sửa, Xóa) để tăng cường bảo mật.
* **Tích hợp thanh toán:** Tích hợp API của một cổng thanh toán thực tế (MoMo, VNPay) để hoàn thiện luồng "Thanh toán Online".
* **Tái cấu trúc (Refactor) Front-end:** Tách biệt hoàn toàn Back-end (viết API bằng PHP) và Front-end (sử dụng framework như React hoặc VueJS) để tối ưu trải nghiệm người dùng (UX/UI) và tăng khả năng mở rộng hệ thống.

1. [↑](#endnote-ref-1)