TRƯỜNG KỸ THUẬT VÀ CÔNG NGHỆ
KHOA CÔNG NGHỆ THÔNG TIN

THỰC TẬP ĐỒ ÁN CHUYÊN NGÀNH

HỌC KỲ I, NĂM HỌC 2025-2026

Xây dựng website chia sẻ công thức nấu ăn

Giảng viên hướng dẫn:
ThS. Hà Thị Thúy Vi

Sinh viên thực hiện:
Họ tên: Nguyễn Thanh Duy
MSSV: 110122062
Lớp: DA22TTD

Vĩnh Long, tháng 12 năm 2025

TRƯỜNG KỸ THUẬT VÀ CÔNG NGHỆ
KHOA CÔNG NGHỆ THÔNG TIN

THỰC TẬP ĐỒ ÁN CHUYÊN NGÀNH

HỌC KỲ I, NĂM HỌC 2025-2026

Xây dựng website chia sẻ công thức nấu ăn

Giảng viên hướng dẫn:
ThS. Hà Thị Thúy Vi

Sinh viên thực hiện:
Họ tên: Nguyễn Thanh Duy
MSSV: 110122062
Lớp: DA22TTD

Vĩnh Long, tháng 12 năm 2025

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Vĩnh Long, ngày ..... tháng …… năm ……

Giảng viên hướng dẫn

(Ký tên và ghi rõ họ tên)

NHẬN XÉT CỦA THÀNH VIÊN HỘI ĐỒNG

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Vĩnh Long, ngày ..... tháng …… năm ……

Thành viên hội đồng

(Ký tên và ghi rõ họ tên)

LỜI CẢM ƠN

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG BIỂU

TÓM TẮT ĐỒ ÁN CHUYÊN NGÀNH

VẤN ĐỀ NGHIÊN CỨU

Trong thời đại số hóa, nhu cầu chia sẻ và trao đổi kiến thức về nấu ăn ngày càng tăng cao. Tuy nhiên, các nền tảng hiện tại thường thiếu tính tích hợp hoặc khó sử dụng. Đồ án này nhằm xây dựng một website chia sẻ công thức nấu ăn (CookShare) với đầy đủ chức năng:

- Cho phép người dùng tạo, chỉnh sửa, xóa công thức riêng của mình
- Hỗ trợ tương tác xã hội (bình luận, đánh giá, yêu thích)
- Cung cấp tìm kiếm và phân loại công thức hiệu quả
- Triển khai hệ thống quản lý admin để kiểm duyệt nội dung
- Tối ưu hóa giao diện đáp ứng (Responsive Design) trên mọi thiết bị

CÁC HƯỚNG TIẾP CẬN

1. Kiến trúc 3 tầng (Three-Layer Architecture):
   - Tầng Giao diện (Presentation Layer): React 19.x với Component-based architecture
   - Tầng Ứng dụng (Application Layer): Node.js + Express 4.x cung cấp REST API
   - Tầng Dữ liệu (Data Layer): MySQL 8.0+ lưu trữ dữ liệu quan hệ
2. Mô hình MVC (Model-View-Controller):
   - Model: Cơ sở dữ liệu MySQL (users, recipes, comments, ratings, favorites)
   - View: React components (Home, CreateRecipe, RecipeDetail, AdminDashboard, v.v.)
   - Controller: Express routes (auth.js, recipe.js, rating.js, favorite.js, admin.js)
3. Bảo mật & Xác thực:
   - Dùng Bcrypt (với Salt & Adaptive hashing) để mã hóa mật khẩu
   - Dùng JSON Web Token (JWT) để quản lý phiên người dùng (token hết hạn sau 7 ngày)
   - Cấu hình CORS để kiểm soát truy cập giữa frontend (localhost:3000) và backend (localhost:3001)
   - Middleware xác thực để kiểm tra quyền (user/admin)
4. Tối ưu hóa & Hiệu suất:
   - Non-blocking I/O: Node.js xử lý nhiều request đồng thời mà không chặn
   - Cloudinary: Lưu trữ ảnh trên đám mây, giảm tải server
   - CSS Responsive: Giao diện tự động thích ứng với mọi kích thước màn hình

CÁCH GIẢI QUYẾT VẤN ĐỀ

Phía Backend (Node.js + Express):

1. Xây dựng REST API với các endpoint:
   - /auth/register, /auth/login → quản lý xác thực
   - /recipe/list, /recipe/search, /recipe/create, /recipe/update/:id, /recipe/delete/:id → quản lý công thức
   - /rating, /favorite, /comment → quản lý tương tác
   - /admin → quản lý hệ thống
2. Sử dụng Middleware xác thực JWT để bảo vệ các route yêu cầu đăng nhập
3. Cấu hình CORS để cho phép frontend truy cập API
4. Kết nối MySQL, thực hiện CRUD (Create, Read, Update, Delete) trên cơ sở dữ liệu

Phía Frontend (React):

1. Xây dựng Component-based UI:
   - Navbar (điều hướng, đăng nhập/đăng xuất)
   - Home (danh sách công thức, thanh tìm kiếm)
   - CreateRecipe, RecipeDetail, MyRecipes, FavoriteRecipes (quản lý công thức)
   - AdminDashboard (quản lý người dùng, nội dung)
2. Dùng React Router để điều hướng giữa các trang
3. Dùng Axios gọi API backend
4. Lưu JWT token trong localStorage, gửi lại trong header Authorization cho các API yêu cầu xác thực
5. Thiết kế CSS responsive với media queries

Cơ sở dữ liệu:

1. Thiết kế schema gồm 5 bảng chính:
   - users (id, email, password, username, role, created_at)
   - recipes (id, user_id, title, ingredients, steps, image_url, created_at, updated_at)
   - comments (id, recipe_id, user_id, content, created_at)
   - ratings (id, recipe_id, user_id, rating, created_at)
   - favorites (id, recipe_id, user_id, created_at)
2. Thiết lập khóa ngoài (Foreign Key) để đảm bảo tính toàn vẹn dữ liệu

KẾT QUẢ ĐẠT ĐƯỢC

1. Chức năng Xác thực & Quản lý Người dùng:
   - Đăng ký tài khoản với xác thực email, mật khẩu
   - Đăng nhập với JWT token (hết hạn 7 ngày)
   - Hồ sơ người dùng, quên mật khẩu (gửi OTP qua email)
   - Phân biệt vai trò: user vs admin

2. Chức năng Quản lý Công Thức:
   - Tạo công thức (tiêu đề, nguyên liệu, bước, tải lên ảnh)
   - Danh sách công thức với phân trang
   - Xem chi tiết công thức
   - Chỉnh sửa công thức (chỉ chủ sở hữu)
   - Xóa công thức (chủ sở hữu hoặc admin)
   - Tìm kiếm công thức theo từ khóa

3. Chức năng Tương tác & Bình luận:
   - Bình luận trên công thức (tạo, xem, xóa của chủ sở hữu)
   - Đánh giá sao (1-5 sao, mỗi user chỉ được đánh giá 1 lần)
   - Yêu thích công thức (lưu vào danh sách yêu thích)
   - Thống kê đánh giá (trung bình rating, số lượng bình luận)

4. Chức năng Quản lý Admin:
   - Xem danh sách tất cả người dùng
   - Thay đổi vai trò người dùng (user ↔ admin)
   - Xóa người dùng hoặc công thức vi phạm

5. Giao diện & Trải nghiệm Người dùng:
   - Giao diện đáp ứng (Responsive Design) trên desktop, tablet, mobile
   - Thanh điều hướng (Navbar) với tính năng đăng nhập/đăng xuất
   - Trang chủ với danh sách công thức, thanh tìm kiếm
   - Bố cục lưới (grid layout) thích hợp cho việc hiển thị công thức
   - Trang quản lý công thức của bản thân (My Recipes)
   - Trang danh sách yêu thích (Favorite Recipes)

6. Bảo mật & Hiệu suất:
    - Mật khẩu được mã hóa bằng Bcrypt (adaptive hashing + salt)
    - JWT token với hết hạn 7 ngày
    - Middleware xác thực kiểm tra quyền trước khi cho phép truy cập
    - CORS cấu hình để chỉ cho phép frontend từ localhost:3000 truy cập
    - Ảnh được lưu trên Cloudinary (giảm tải server)

ĐÁNH GIÁ & HẠN CHẾ

1. Điểm mạnh:
    - Kiến trúc module hóa, dễ mở rộng
    - Bảo mật tốt (Bcrypt, JWT, CORS, Middleware)
    - Giao diện responsive, thân thiện với người dùng
    - Non-blocking I/O giúp xử lý nhiều request hiệu quả

2. Hạn chế & hướng phát triển trong tương lai:
    - Chưa triển khai Redis để cache dữ liệu thường xuyên truy cập
    - Chưa có hệ thống notification real-time (có thể dùng WebSocket)
    - Chưa triển khai unit test toàn diện
    - Chưa có CI/CD pipeline để tự động test & deploy
    - Có thể thêm Machine Learning để gợi ý công thức dựa trên sở thích người dùng

MỞ ĐẦU

1. Lý do chọn đề tài

Xu hướng số hóa trong lĩnh vực ẩm thực ngày càng mạnh, nhu cầu chia sẻ và tìm kiếm công thức nấu ăn trực tuyến rất lớn.

Các nền tảng hiện có thường phân tán, thiếu quản lý chất lượng nội dung hoặc chưa tối ưu trải nghiệm người dùng (UX/UI) trên đa thiết bị.

Mong muốn xây dựng một hệ thống tập trung, thân thiện, cho phép người dùng dễ dàng đăng tải, tìm kiếm, tương tác và quản trị nội dung công thức nấu ăn.

2. Mục đích nghiên cứu

Xây dựng website CookShare đáp ứng các chức năng cốt lõi: đăng ký/đăng nhập, tạo–chỉnh sửa–xóa công thức, tìm kiếm, đánh giá, bình luận, yêu thích.

Đảm bảo bảo mật dữ liệu người dùng (mã hóa mật khẩu, xác thực bằng JWT, kiểm soát quyền truy cập).

Thiết kế giao diện đáp ứng (responsive) cho cả desktop và mobile, tối ưu tốc độ và trải nghiệm.

Đề xuất kiến trúc mở rộng, dễ bảo trì (Node.js + Express REST API, React frontend, MySQL, lưu trữ ảnh cloud).

3. Đối tượng nghiên cứu

Người dùng cuối: cá nhân đam mê nấu ăn, muốn chia sẻ hoặc tìm kiếm công thức.

Nhà phát triển/nhóm vận hành: quản trị hệ thống, kiểm duyệt nội dung, mở rộng tính năng.

Công nghệ và giải pháp: React (UI), React Router, Axios, CSS responsive; Node.js/Express (API), JWT, Bcrypt; MySQL; Cloudinary (lưu trữ ảnh).

4. Phạm vi nghiên cứu

Chức năng người dùng: đăng ký, đăng nhập, quản lý công thức (tạo/sửa/xóa), bình luận, đánh giá, yêu thích, tìm kiếm.

Chức năng quản trị: quản lý người dùng, vai trò (user/admin), kiểm duyệt/xóa nội dung vi phạm.

Hạ tầng: chạy cục bộ trên môi trường phát triển (frontend: localhost:3000, backend: localhost:3001); lưu trữ ảnh trên dịch vụ đám mây.

Ngoài phạm vi: chưa triển khai realtime notifications, chưa có hệ thống khuyến nghị bằng ML, chưa triển khai CI/CD tự động và cache/Redis (đề xuất cho tương lai).

CHƯƠNG 1: TỔNG QUAN

1.1 Bối cảnh

- Xu hướng tìm kiếm và chia sẻ công thức nấu ăn trực tuyến tăng mạnh cùng với sự phổ biến của mạng xã hội và thiết bị di động.
- Người dùng cần một nền tảng tập trung, dễ dùng, tin cậy để:
  + Đăng tải, lưu trữ, chỉnh sửa công thức cá nhân.
  + Tìm kiếm, học hỏi từ cộng đồng.
  + Tương tác (bình luận, đánh giá, yêu thích) và được kiểm duyệt nội dung.

1.2 Vấn đề đặt ra

- Nội dung ẩm thực hiện có phân tán, chất lượng không đồng đều, thiếu kiểm duyệt.
- Trải nghiệm người dùng chưa tối ưu trên nhiều thiết bị (desktop, tablet, mobile).
- Bảo mật và quyền riêng tư (mật khẩu, phiên đăng nhập, phân quyền) chưa luôn được đảm bảo.
- Thiếu cơ chế quản trị/admin để xử lý nội dung vi phạm và quản lý người dùng.

1.3 Mục tiêu của hệ thống

- Xây dựng website CookShare với các chức năng cốt lõi:
  + Đăng ký/đăng nhập, xác thực an toàn (JWT), mã hóa mật khẩu (Bcrypt).
  + Quản lý công thức: tạo, chỉnh sửa, xóa, xem chi tiết, tìm kiếm.
  + Tương tác: bình luận, đánh giá sao, đánh dấu yêu thích.
  + Quản trị: phân quyền user/admin, kiểm duyệt nội dung, xóa tài khoản/công thức vi phạm.
- Đảm bảo trải nghiệm tốt trên đa thiết bị (responsive design).
- Lưu trữ ảnh trên đám mây, giảm tải cho server.

1.4 Phạm vi nghiên cứu

- Chức năng người dùng: quản lý tài khoản, công thức, tương tác.
- Chức năng quản trị: duyệt/xóa nội dung, thay đổi vai trò.
- Hạ tầng: frontend React (localhost:3000), backend Node/Express (localhost:3001), MySQL, Cloudinary cho ảnh.
- Ngoài phạm vi hiện tại: realtime notification, gợi ý cá nhân hóa bằng ML, cache/Redis, CI/CD tự động (đề xuất cho tương lai).

1.5 Phương pháp và hướng tiếp cận

- Kiến trúc 3 tầng: Giao diện (React) – Ứng dụng (Express REST API) – Dữ liệu (MySQL).

- Mô hình MVC trên backend: Model (MySQL), Controller (routes Express), View (JSON responses).
- Bảo mật: Bcrypt (Salt + adaptive hashing), JWT (phiên đăng nhập 7 ngày), CORS cấu hình nguồn gốc.
- Hiệu năng: Non-blocking I/O của Node.js, tách lưu trữ ảnh sang Cloudinary.

1.6 Kết quả mong đợi

- Một nền tảng web hoàn chỉnh cho chia sẻ công thức nấu ăn:
  + Người dùng đăng nhập, tạo và quản lý công thức, tương tác an toàn.
  + Quản trị viên có công cụ kiểm duyệt, quản lý người dùng/nội dung.
  + Giao diện thân thiện, phản hồi nhanh, chạy tốt trên nhiều thiết bị.

CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT

2.1 Kiến trúc và nguyên lý web hiện đại

Kiến trúc 3 tầng (Three-Layer Architecture)

- **Presentation:** React hiển thị UI, quản lý trạng thái client, gọi API.
- **Application:** Node.js/Express xử lý logic nghiệp vụ, định tuyến REST.
- **Data:** MySQL lưu trữ quan hệ (users, recipes, comments, ratings, favorites).

Mô hình RESTful API

- Tài nguyên được ánh xạ vào URL; thao tác CRUD qua HTTP methods (GET/POST/PUT/DELETE).
- Chuẩn hóa mã trạng thái HTTP (200/201/400/401/403/404/500).
- Phản hồi dạng JSON; stateless giữa các request.

Mô hình MVC trên backend Express

- **Model:** Tầng truy cập dữ liệu MySQL.
- **View:** JSON responses (thay cho HTML view truyền thống).
- **Controller:** Router/handler tổ chức logic và gọi Model.

Bảng 2.1: Mã trạng thái HTTP

Mã	Tên	Khi sử dụng	Ví dụ
200	OK	Request thành công	GET /recipe/list → trả danh sách
201	Created	Tạo tài nguyên mới	POST /auth/register → tạo user
400	Bad Request	Lỗi validation từ client	Thiếu trường email khi đăng ký
401	Unauthorized	Chưa xác thực/token sai	Không gửi JWT hoặc token hết hạn
403	Forbidden	Không đủ quyền	User thường gọi API admin
404	Not Found	Tài nguyên không tồn tại	GET /recipe/9999 (ID không có)
500	Internal Server Error	Lỗi server	Exception, lỗi database

2.2 Bảo mật và xác thực

2.2.1 JSON Web Token (JWT)

- Cấu trúc 3 phần: Header (thuật toán, kiểu token), Payload (claims: id, email, role, exp), Signature (chữ ký bảo toàn toàn vẹn).
- Quy trình: đăng nhập → sign token (exp 7 ngày) → client gửi **Authorization: Bearer <token>** → middleware verify.
- Ưu điểm: stateless, dễ mở rộng microservice.

Bảng 2.2: So sánh phương pháp xác thực

Tiêu chí	Session-based	JWT (Token-based)
Lưu trữ server	Có (session store)	Không (stateless)
Scalability	Khó (cần shared session)	Dễ (mỗi server verify độc lập)
Băng thông	Nhẹ (chỉ session ID)	Nặng hơn (toàn bộ token)
Bảo mật	Phụ thuộc session store	Token có thể bị đánh cắp
Hết hạn	Server kiểm soát	Client giữ đến khi exp
Phù hợp	Web truyền thống	API, microservices, mobile

2.2.2 Bcrypt và bảo vệ mật khẩu

- **Adaptive hashing:** điều chỉnh cost theo thời gian.
- **Salt:** chuỗi ngẫu nhiên gắn vào mật khẩu trước khi hash, chống rainbow table.
- **One-way:** không thể giải ngược hash; so sánh bằng **bcrypt.compare**.

2.2.3 CORS (Cross-Origin Resource Sharing)

- Kiểm soát truy cập giữa các origin (frontend http://localhost:3000 ↔ backend http://localhost:3001).
- Preflight (OPTIONS) kiểm tra Access-Control-Allow-Origin/ Methods/ Headers/Credentials.
- Cho phép gửi JWT qua header khi được cấu hình origin và credentials.

2.3 Công nghệ và kỹ thuật triển khai

2.3.1 Frontend: React, React Router, Axios, CSS Responsive

- React: Virtual DOM, component-based, state/props để quản lý UI.
- React Router: điều hướng client-side, bảo vệ tuyến qua ProtectedRoute.
- Axios: HTTP client với interceptor cho JWT.
- CSS Responsive: media queries, grid/flex để thích ứng đa màn hình.

Bảng 2.3: Công nghệ sử dụng

Thành phần	Công nghệ	Phiên bản	Vai trò
Frontend	React	19.x	Xây dựng UI component-based, Virtual DOM
	React Router	6.x	Điều hướng client-side, ProtectedRoute
	Axios	1.x	HTTP client, gọi API backend
	CSS3	-	Responsive design, layout
Backend	Node.js	16.x+	JavaScript runtime, non-blocking I/O
	Express	4.x	Web framework, REST API, middleware

	jsonwebtoken	9.x	Tạo và verify JWT token
	bcryptjs	2.x	Hash mật khẩu với Salt
Database	MySQL	8.0+	Cơ sở dữ liệu quan hệ, ACID
Cloud Storage	Cloudinary	-	Lưu trữ và CDN hóa ảnh
Tools	npm	-	Quản lý package dependencies

2.3.2 Backend: Node.js (Non-blocking I/O), Express Middleware

- Non-blocking I/O: event loop xử lý nhiều request đồng thời.
- Middleware: xử lý tuần tự (logging, CORS, body parsing, auth) trước handler.
- Validation: kiểm tra đầu vào, trả mã lỗi phù hợp.

2.3.3 Dữ liệu và lưu trữ

- MySQL: quan hệ, ACID; khóa ngoại giữa users, recipes, comments, ratings, favorites.
- Cloudinary: lưu trữ ảnh trên cloud, trả URL tối ưu để hiển thị trên frontend.

CHƯƠNG 3: HIỆN THỰC HÓA NGHIÊN CỨU

3.1 Đặc tả nhu cầu

- Tác nhân:
  + Người dùng (user): đăng ký/đăng nhập, tạo–sửa–xóa công thức của mình, xem/tìm kiếm, bình luận, đánh giá, yêu thích.
  + Quản trị viên (admin): toàn bộ quyền của user + duyệt/xóa công thức vi phạm, đổi vai trò người dùng, xóa tài khoản.
- Chức năng chính:
  + Xác thực & phân quyền: đăng ký, đăng nhập, JWT 7 ngày, phân biệt user/admin.
  + Quản lý công thức: CRUD, tải ảnh lên Cloudinary, tìm kiếm theo tiêu đề/nguyên liệu.
  + Tương tác: bình luận, đánh giá sao (1 user/1 recipe/1 rating), đánh dấu yêu thích.
  + Quản trị: quản lý người dùng, thay đổi role, xóa nội dung vi phạm.
- Phi chức năng:
  + Bảo mật: Bcrypt (Salt + adaptive hashing), JWT, CORS giới hạn origin.
  + Hiệu năng: Non-blocking I/O, tách lưu trữ ảnh sang cloud.
  + UX/UI: Responsive, điều hướng mượt (React Router), thông báo lỗi/thành công rõ ràng.

Bảng 3.1: Danh sách API endpoints

Method	Endpoint	Auth	Mô tả	Response
POST	/auth/register	No	Đăng ký tài khoản	201: success / 400: validation error
POST	/auth/login	No	Đăng nhập, nhận JWT	200: {token, user} / 400: invalid
GET	/recipe/list	No	Danh sách công thức	200: [recipes]
GET	/recipe/search?q=	No	Tìm kiếm công thức	200: [filtered recipes]
POST	/recipe/create	JWT	Tạo công thức + upload ảnh	201: {recipeId} / 401: no token

PUT	/recipe/update/:id	JWT	Cập nhật công thức	200: success / 403: not owner
DELETE	/recipe/delete/:id	JWT	Xóa công thức	200: deleted / 403: not owner/admin
POST	/rating/:recipeId	JWT	Đánh giá sao	201: rated / 400: already rated
POST	/favorite/:recipeId	JWT	Thêm yêu thích	201: added
POST	/comment/:recipeId	JWT	Thêm bình luận	201: created
GET	/admin/users	JWT (admin)	Danh sách người dùng	200: [users] / 403: not admin
PUT	/admin/users/:id/role	JWT (admin)	Đổi vai trò user	200: updated / 403: not admin

3.2 Thiết kế hệ thống

3.2.1 Kiến trúc tổng thể

- **tầng:** Frontend (React) ↔ Backend (Express REST) ↔ Database (MySQL); ảnh trên Cloudinary.
- **MVC (backend):** Model (MySQL queries), Controller (Express routes), View (JSON response).
- **Giao tiếp:** HTTP/HTTPS, JSON; JWT gửi qua header Authorization.

3.2.2 Mô hình dữ liệu (ERD rút gọn)

users 1—N recipes

recipes 1—N comments

recipes 1—N ratings

recipes 1—N favorites

users 1—N comments/ratings/favorites

Bảng 3.2: Schema cơ sở dữ liệu

3.2.3 Thiết kế API (REST)

- Auth: POST /auth/register, POST /auth/login

- Recipe: GET /recipe/list, GET /recipe/search, POST /recipe/create, PUT /recipe/update/:id, DELETE /recipe/delete/:id
- Interaction: POST /rating/:recipeId, POST /favorite/:recipeId, POST /comment /:recipeId
- Admin: GET /admin/users, PUT /admin/users/:id/role, DELETE /admin/ recipes/:id
- Mã trạng thái: 200/201/400/401/403/404/500; thông điệp lỗi rõ ràng.

3.2.4 Thiết kế giao diện (UI/UX)

- Trang chính: danh sách công thức, thanh tìm kiếm, lưới ảnh.
- Navbar: logo, đăng nhập/đăng ký, tên người dùng + logout, link admin nếu role=admin.
- Trang chi tiết công thức: nguyên liệu, bước, ảnh, bình luận, đánh giá.
- Trang quản lý cá nhân: My Recipes, Favorite Recipes.
- Trang quản trị: danh sách người dùng, đổi role, xóa công thức.

3.3 Hiện thực (Implementation)

3.3.1 Frontend (React)

- Công nghệ: React 19.x, React Router 6.x, Axios 1.x, CSS responsive.
- Cấu trúc (rút gọn):
  + components/: Navbar.jsx, ProtectedRoute.jsx
  + pages/: Home.jsx, CreateRecipe.jsx, RecipeDetail.jsx, AdminDashboard.jsx, MyRecipes.jsx, FavoriteRecipes.jsx, Login.jsx, Register.jsx, v.v.
- Xử lý chính:
  + Lưu JWT trong localStorage; interceptor của Axios thêm Authorization header.
  + ProtectedRoute kiểm tra token trước khi vào các trang cần đăng nhập.
  + Form tạo/sửa công thức: upload ảnh (gửi đến backend, backend đẩy lên Cloudinary).

3.3.2 Backend (Node.js + Express)

- Công nghệ: Node.js 16+, Express 4.x, jsonwebtoken, bcryptjs, multer/cloudinary SDK, dotenv.
- Cấu trúc:
  + server.js: khởi tạo Express, CORS, body parser, mount routes, kết nối DB.
  + routes/: auth.js, recipe.js, rating.js, favorite.js, admin.js.
  + auth.js: verify JWT, check role.

+ config/: db.js (MySQL pool), cloudinary.js.

- Luồng chính:
  + Auth: hash mật khẩu với Bcrypt; login tạo JWT (exp 7d); middleware verify token.
  + Recipe: CRUD + upload ảnh lên Cloudinary, lưu URL vào DB; kiểm tra quyền owner/admin.
  + Interaction: rating (mỗi user 1 lần/recipe), comment, favorite; ràng buộc quyền đăng nhập.
  + Admin: đổi role, xóa công thức hoặc user vi phạm.

3.3.3 Database (MySQL)

- Bảng chính: users, recipes, comments, ratings, favorites.
- Ràng buộc khóa ngoại đảm bảo toàn vẹn; chỉ số (index) cho trường tìm kiếm (title, ingredients).

3.3.4 Lưu trữ ảnh (Cloudinary)

Backend nhận file (multer), upload lên Cloudinary, nhận URL trả về; lưu URL vào trường image_url của recipes.

3.4 Bảo mật và quản lý phiên

- **Bcrypt:** hash mật khẩu với Salt, cost ~10 (có thể tăng khi hạ tầng mạnh hơn).
- **JWT:** lưu trên client; gửi Bearer token; middleware verify; exp 7 ngày.
- **CORS:** origin http://localhost:3000, cho phép credentials; hạn chế header/method cần thiết.
- **Phân quyền:** middleware kiểm tra role cho route admin; kiểm tra owner trước khi sửa/xóa công thức.

3.5 Kiểm thử

- **Chức năng:** đăng ký/đăng nhập; CRUD công thức; tìm kiếm; bình luận; đánh giá; yêu thích; đổi role; xóa nội dung.
- **Bảo mật:** từ chối request thiếu/invalid JWT; không cho user thường dùng route admin; kiểm tra upload chỉ qua route bảo vệ.
- **Hiệu năng cơ bản:** đo thời gian phản hồi API chính; kiểm tra độ trễ upload ảnh; duyệt trên desktop/mobile (responsive).

3.6 Đánh giá và ghi nhận

- Hệ thống đáp ứng đầy đủ chức năng cốt lõi; giao diện thân thiện; bảo mật cơ bản tốt (Bcrypt, JWT, CORS).

- Hiệu năng phù hợp với quy mô đề tài; có thể mở rộng bằng cache (Redis), CDN, hoặc tách dịch vụ.
- Hướng phát triển: realtime notification (WebSocket), gợi ý cá nhân hóa (ML), CI/CD tự động, test tự động (unit/integration), tối ưu SEO và accessibility.

CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU

4.1 Kết quả chức năng

- Hoàn thiện luồng xác thực: đăng ký, đăng nhập, JWT (hết hạn 7 ngày), phân quyền user/admin.
- Quản lý công thức: tạo, sửa, xóa, xem chi tiết; tìm kiếm theo từ khóa; upload ảnh lên Cloudinary.
- Tương tác người dùng: bình luận, đánh giá sao (1 user/recipe/1 rating), đánh dấu yêu thích.
- Quản trị: xem danh sách người dùng, đổi vai trò, xóa công thức/tài khoản vi phạm.
- API REST chuẩn: mã trạng thái 200/201/400/401/403/404/500; thông điệp phản hồi rõ ràng.

4.2 Trải nghiệm người dùng (UX/UI)

- Giao diện responsive: hiển thị tốt trên desktop, tablet, mobile.
- Navbar động: hiển thị nút đăng nhập/đăng ký khi chưa login; tên người dùng + logout khi đã login; link admin cho admin.
- Trang chủ: lưới công thức, thanh tìm kiếm, nút tạo công thức khi đã đăng nhập.
- Trang chi tiết: ảnh, nguyên liệu, bước nấu; bình luận và đánh giá trực tiếp.
- Trang cá nhân: My Recipes, Favorite Recipes; CRUD công thức của riêng mình.
- Trang quản trị: bảng người dùng, đổi role, xóa công thức vi phạm.

4.3 Hiệu năng và kỹ thuật

- Non-blocking I/O (Node.js + Express) xử lý đồng thời nhiều request; không ghi nhận nghẽn ở tải thử nghiệm cục bộ.
- Upload ảnh chuyển sang Cloudinary, giảm tải đĩa và băng thông máy chủ.
- CORS cấu hình cho front (localhost:3000) ↔ back (localhost:3001) an toàn; JWT qua header Authorization.
- MySQL đáp ứng truy vấn danh sách/tìm kiếm công thức; ràng buộc khóa ngoại đảm bảo toàn vẹn.

4.4 Bảo mật

- Mật khẩu được hash với Bcrypt (Salt + adaptive hashing).
- JWT có hạn, kiểm tra ở middleware; phân quyền rõ (user vs admin).
- Không lưu mật khẩu gốc; từ chối truy cập khi thiếu/invalid token; hạn chế origin qua CORS.

4.5 Giao diện minh họa (mô tả nhanh)

- **Navbar:** Logo/tên app, đăng nhập/đăng ký hoặc tên người dùng + logout, link Admin (nếu admin).
- **Home:** Lưới công thức, thẻ ảnh + tiêu đề; thanh tìm kiếm.
- **Create/Edit Recipe:** Form nhập tiêu đề, nguyên liệu, bước nấu, upload ảnh; nút lưu.
- **Recipe Detail:** Ảnh, nội dung, bình luận, đánh giá; nút yêu thích.
- **Admin Dashboard:** Bảng người dùng (username, email, role), nút đổi role/xóa; danh sách công thức để gỡ bỏ nếu vi phạm.

4.6 Đánh giá nhanh

- Đạt được: Đầy đủ chức năng cốt lõi; giao diện thân thiện và responsive; bảo mật cơ bản tốt (hash mật khẩu, JWT, phân quyền); hiệu năng phù hợp quy mô đề tài.
- Hạn chế: Chưa có cache (Redis), chưa có realtime notification, chưa triển khai CI/CD và bộ test tự động; chưa có gợi ý cá nhân hóa.

4.7 Hướng phát triển

- Thêm realtime notification (WebSocket) cho bình luận/đánh giá mới.
- Thêm cache (Redis) cho danh sách/tìm kiếm công thức.
- Viết test tự động (unit/integration) và thiết lập CI/CD.
- Mở rộng gợi ý công thức dựa trên hành vi người dùng (recommendation).

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1 Kết luận

- Hoàn thành website CookShare với đầy đủ chức năng cốt lõi: đăng ký/đăng nhập (JWT), quản lý công thức (tạo/sửa/xóa/tìm kiếm), bình luận, đánh giá, yêu thích, và phân quyền user/admin.
- Áp dụng kiến trúc 3 tầng, RESTful API, bảo mật Bcrypt + JWT, CORS, và lưu trữ ảnh qua Cloudinary; giao diện React responsive vận hành ổn định.
- Đảm bảo cơ sở dữ liệu quan hệ MySQL với ràng buộc toàn vẹn; trải nghiệm người dùng mạch lạc, quy trình nghiệp vụ rõ ràng.
- Đóng góp: một giải pháp chia sẻ công thức nấu ăn có kiểm duyệt, dễ mở rộng, bảo mật cơ bản tốt, tổ chức mã theo chuẩn (MVC, middleware, phân tầng).

5.2 Hướng phát triển

- Bổ sung realtime notification (WebSocket) cho bình luận/đánh giá mới.
- Thêm cache (Redis) cho truy vấn danh sách/tìm kiếm để cải thiện hiệu năng.
- Viết test tự động (unit/integration) và thiết lập CI/CD để tăng độ tin cậy khi phát hành.
- Tích hợp hệ thống gợi ý/personalization (ML) và tối ưu SEO, accessibility.
- Mở rộng hạ tầng (container hóa, scaling) và bổ sung giám sát/alerting cho môi trường triển khai.

DANH MỤC TÀI LIỆU THAM KHẢO

- RESTful API: Roy T. Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. University of California, Irvine, 2000.
- JSON Web Token (JWT): Auth0. *JSON Web Token Introduction*. https://jwt.io/introduction
- Bcrypt: Niels Provos, David Mazieres. *A Future-Adaptable Password Scheme*. Proceedings of the 1999 USENIX Annual Technical Conference.
- CORS: MDN Web Docs. *HTTP access control (CORS)*. https://developer.mozilla.org/docs/Web/HTTP/CORS
- React: React Team. *React Documentation*. https://react.dev
- Node.js & Express: Express.js Team. *Express Guide*. https://expressjs.com
- MySQL: Oracle. *MySQL 8.0 Reference Manual*. https://dev.mysql.com/doc
- Cloudinary: Cloudinary Docs. *Image Upload API*. https://cloudinary.com/documentation/image_upload_api
- OWASP: *OWASP Cheat Sheet Series* (Authentication, Password Storage, REST Security). https://cheatsheetseries.owasp.org

PHỤ LỤC

PHỤ LỤC A: Cấu hình môi trường

File .env (Backend)

```
PORT=3001
DB_HOST=localhost
DB_USER=root
DB_PASSWORD=yourpassword
DB_NAME=cookshare

SECRET_KEY=your-jwt-secret-key-here
JWT_SECRET=your-jwt-secret-key-here

CLOUDINARY_CLOUD_NAME=your-cloud-name
CLOUDINARY_API_KEY=your-api-key
CLOUDINARY_API_SECRET=your-api-secret

EMAIL_USER=your-email@gmail.com
EMAIL_PASSWORD=your-app-password
```

Yêu cầu hệ thống:

- Node.js: 16.x trở lên
- MySQL: 8.0 trở lên
- npm: 8.x trở lên
- Trình duyệt: Chrome 90+, Firefox 88+, Safari 14+

PHỤ LỤC B: Hướng dẫn cài đặt

Bước 1: Clone repository

```
git clone <repository-url>
cd DoAnChuyenNganh
```

Bước 2: Cài đặt Backend

```
cd src/backend
npm install
# Tạo file .env theo mẫu ở Phụ lục A
# Tạo database MySQL
mysql -u root -p < database/database.sql
npm start
```

Bước 3: Cài đặt Frontend

```
cd src/cookshare
npm install
npm start
```

Bước 4: Truy cập ứng dụng

Frontend: **http://localhost:3000**

Backend API: **http://localhost:3001**

PHỤ LỤC C: Code mẫu quan trọng

C.1 Middleware xác thực JWT (middleware/auth.js)

```
const jwt = require("jsonwebtoken");
const SECRET_KEY = process.env.SECRET_KEY || "SECRET_KEY";

const verifyToken = (req, res, next) => {
  const authHeader = req.headers["authorization"];
  const token = authHeader && authHeader.split(" ")[1];

  if (!token) {
    return res.status(401).json({ message: "Access token required" });
  }

  jwt.verify(token, SECRET_KEY, (err, user) => {
    if (err) {
      return res.status(403).json({ message: "Invalid or expired token" });
    }
    req.user = user;
```

```
    next();
  });
};

module.exports = { verifyToken };
```

C.2 Tạo JWT khi đăng nhập (routes/auth.js)

```
const token = jwt.sign({ id: user.id }, SECRET_KEY, { expiresIn: "7d" });

return res.json({
  message: "Đăng nhập thành công!",
  token,
  username: user.username,
  role: user.role,
  userId: user.id
});
```

C.3 Hash mật khẩu với Bcrypt (routes/auth.js)

```
const bcrypt = require("bcrypt");

// Khi đăng ký
const hashed = await bcrypt.hash(password, 10);

// Khi đăng nhập
const match = await bcrypt.compare(password, user.password);
```

C.4 Axios interceptor (Frontend)

```
import axios from 'axios';
```

```
const api = axios.create({
  baseURL: 'http://localhost:3001'
});

// Thêm token vào mọi request
api.interceptors.request.use(config => {
  const token = localStorage.getItem('token');
  if (token) {
    config.headers.Authorization = `Bearer ${token}`;
  }
  return config;
});

export default api;
```

PHỤ LỤC D: Schema cơ sở dữ liệu chi tiết

Bảng users

```
CREATE TABLE users (
  id INT AUTO_INCREMENT PRIMARY KEY,
  username VARCHAR(50) UNIQUE NOT NULL,
  email VARCHAR(100) UNIQUE NOT NULL,
  password VARCHAR(255) NOT NULL,
  role ENUM('user', 'admin') DEFAULT 'user',
  created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

Bảng recipes

```
CREATE TABLE recipes (
  id INT AUTO_INCREMENT PRIMARY KEY,
  user_id INT NOT NULL,
  title VARCHAR(200) NOT NULL,
```

```
  ingredients TEXT NOT NULL,
  steps TEXT NOT NULL,
  image_url VARCHAR(500),
  created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
  updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP,
  FOREIGN KEY (user_id) REFERENCES users(id) ON DELETE CASCADE
);
```

Bảng comments

```
CREATE TABLE comments (
  id INT AUTO_INCREMENT PRIMARY KEY,
  recipe_id INT NOT NULL,
  user_id INT NOT NULL,
  content TEXT NOT NULL,
  created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
  FOREIGN KEY (recipe_id) REFERENCES recipes(id) ON DELETE CASCADE,
  FOREIGN KEY (user_id) REFERENCES users(id) ON DELETE CASCADE
);
```

Bảng ratings

```
CREATE TABLE comments (
  id INT AUTO_INCREMENT PRIMARY KEY,
  recipe_id INT NOT NULL,
  user_id INT NOT NULL,
  content TEXT NOT NULL,
  created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
  FOREIGN KEY (recipe_id) REFERENCES recipes(id) ON DELETE CASCADE,
  FOREIGN KEY (user_id) REFERENCES users(id) ON DELETE CASCADE
);
```

Bảng favorites

```
CREATE TABLE favorites (
  id INT AUTO_INCREMENT PRIMARY KEY,
  recipe_id INT NOT NULL,
  user_id INT NOT NULL,
  created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
  UNIQUE KEY unique_favorite (recipe_id, user_id),
  FOREIGN KEY (recipe_id) REFERENCES recipes(id) ON DELETE CASCADE,
  FOREIGN KEY (user_id) REFERENCES users(id) ON DELETE CASCADE
);
```

PHỤ LỤC E: API Documentation chi tiết

E.1 Authentication Endpoints

POST /auth/register

- Body: **{ username, email, password, confirmPassword }**
- Response: **{ message: "Đăng ký thành công!" }**
- Errors: 400 (validation), 500 (server)

POST /auth/login

- Body: **{ email, password }**
- Response: **{ message, token, username, role, userId }**
- Errors: 400 (invalid credentials), 500 (server)

E.2 Recipe Endpoints

GET /recipe/list

- Response: **[{ id, title, ingredients, steps, image_url, username, ... }]**

GET /recipe/search?q=keyword

- Query: q (search keyword)
- Response: [{ matching recipes }]

POST /recipe/create

- Headers: **Authorization: Bearer <token>**
- Body: FormData with title, ingredients, steps, image
- Response: **{ message, recipeId }**

PUT /recipe/update/:id

- Headers: **Authorization: Bearer <token>**
- Body: FormData
- Response: **{ message }**
- Errors: 403 (not owner), 404 (not found)

DELETE /recipe/delete/:id

- Headers: **Authorization: Bearer <token>**
- Response: **{ message }**
- Errors: 403 (not owner/admin), 404 (not found)

PHỤ LỤC F: Screenshots giao diện

F.1: Trang đăng nhập

F.2: Trang chủ với danh sách công thức

F.3: Trang chi tiết công thức

F.4: Form tạo công thức

F.5: Trang quản trị (Admin Dashboard)

F.6: Responsive view trên mobile

PHỤ LỤC G: Kiểm thử

G.1 Test cases chính

ID	Chức năng	Input	Expected Output	Kết quả
TC01	Đăng ký	Valid email, password	201, message success	✓ Pass
TC02	Đăng ký	Duplicate email	400, email exists	✓ Pass
TC03	Đăng nhập	Valid credentials	200, JWT token	✓ Pass
TC04	Đăng nhập	Invalid password	400, wrong password	✓ Pass
TC05	Tạo công thức	Valid data + token	201, recipe created	✓ Pass
TC06	Tạo công thức	No token	401, unauthorized	✓ Pass
TC07	Xóa công thức	Owner	200, deleted	✓ Pass
TC08	Xóa công thức	Not owner	403, forbidden	✓ Pass