BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM

KHOA CÔNG NGHỆ THÔNG TIN

HCMUTE

ĐỒ ÁN CUỐI KỲ

HỌC KỲ 1 – NĂM HỌC 2024-2025

MÔN HỌC: VẠN VẬT KẾT NỐI INTERNET

ĐỀ TÀI: HỆ THỐNG BẢO MẬT CỬA RA VÀO THÔNG MINH

Mã lớp học phần: INOT431780_04

Giảng viên hướng dẫn: ThS. Đinh Công Đoan

Danh sách sinh viên thực hiện:

MSSV	Họ tên
23133061	Phan Trọng Quí
23133056	Phan Trọng Phú
23133030	Đỗ Kiến Hưng

Thành phố Hồ Chí Minh, 25 tháng 04 năm 2025

Nhận xét của giảng viên

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

TP. Hồ Chí Minh, ngày 25 tháng 04 năm 2025

Giảng viên ký tên

KẾ HOẠCH PHÂN CÔNG NHIỆM VỤ THỰC HIỆN

ĐỀ TÀI CUỐI KỲ MÔN VẠN VẬT KẾT NỐI INTERNET

HỌC KỲ 1 - NĂM HỌC 2024-2025

1. Mã lớp môn học: INOT431780_04

2. Giảng viên hướng dẫn: ThS. Đinh Công Đoan

3. Tên đề tài: HỆ THỐNG BẢO MẬT CỬA RA VÀO THÔNG MINH

4. Bảng phân công nhiệm vụ:

Sinh viên thực hiện	Nội dung thực hiện
Phan Trọng Quí	Thiết kế CSDL, Triển khai CSDL, Lập trình Backend (PHP Scripts)
Phan Trọng Phú	Lắp ráp Mạch, Lựa chọn & Kiểm tra Linh kiện, Thiết kế & Xử lý Nguồn, Fireware
Đỗ Kiến Hưng	Thiết kế Giao diện Web (Frontend), Firmware, Kiểm thử, Viết Báo cáo

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

IoT	Internet of Things
RFID	Radio-Frequency Identification
PIN	Personal Identification Number
ID	Identifier/Identification
UID	Unique Identifier
SQL	Structured Query Language
MySQL	My Structured Query Language
UI	User Interface
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
SPI	Serial Peripheral Interface
GPIO	General Purpose Input/Output
WIFI	Wireless Fidelity
ESP8266	(Tên vi điều khiển - SoC Wi-Fi của Espressif)
CRUD	Create, Read, Update, Delete
LED	Light Emitting Diode
NC	Normally Closed
NO	Normally Open
COM	Common (Terminal)
DB	Database
PHP	PHP: Hypertext Preprocessor
HTML	HyperText Markup Language
CSS	Cascading Style Sheets
JS	JavaScript
AJAX	Asynchronous JavaScript and XML
UPS	Uninterruptible Power Supply
DC	Direct Current
VDC	Volts Direct Current
PCB	Printed Circuit Board
XAMPP	Cross-Platform Apache MySQL PHP Perl
IDE	Integrated Development Environment

PHẦN 1: PHẦN MỞ ĐẦU

1.1. Tóm tắt

Báo cáo này trình bày quá trình nghiên cứu, thiết kế và xây dựng một Hệ thống bảo mật cửa ra vào thông minh, ứng dụng các công nghệ Internet of Things (IoT) nhằm nâng cao tính an toàn, tiện nghi và khả năng quản lý truy cập. Hệ thống tích hợp nhiều phương thức xác thực bao gồm sử dụng thẻ từ RFID (Radio-Frequency Identification) và nhập mã PIN qua keypad cảm ứng, cung cấp sự linh hoạt cho người dùng.

Trái tim của hệ thống là vi điều khiển NodeMCU ESP8266, có khả năng kết nối Wi-Fi, chịu trách nhiệm xử lý tín hiệu từ các thiết bị đầu vào, giao tiếp với server và điều khiển cơ cấu chấp hành là khóa điện Solenoid thông qua module Relay. Toàn bộ thông tin về thẻ RFID hợp lệ và lịch sử truy cập được lưu trữ và quản lý tập trung trong cơ sở dữ liệu MySQL chạy trên một Web Server cục bộ (sử dụng XAMPP). Hệ thống còn được trang bị nguồn điện dự phòng sử dụng pin Lithium 18650 và mạch quản lý UPS, đảm bảo hoạt động liên tục ngay cả khi mất điện lưới tạm thời.

Người dùng có thể tương tác với hệ thống thông qua giao diện Web cơ bản, cho phép điều khiển đóng/mở cửa từ xa và quản lý danh sách thẻ RFID (với quyền Admin), mang lại giải pháp bảo mật toàn diện, dễ sử dụng và quản lý hiệu quả.

1.2. Đặt vấn đề

1.2.1. Tóm lược những nghiên cứu trong và ngoài nước liên quan đến đề tài

Trong bối cảnh công nghệ không ngừng phát triển, nhu cầu đảm bảo an ninh và tự động hóa cho các không gian sống và làm việc như nhà ở, văn phòng, cơ sở sản xuất ngày càng trở nên cấp thiết. Các hệ thống khóa cửa truyền thống sử dụng chìa khóa cơ học, mặc dù phổ biến, nhưng bộc lộ nhiều hạn chế đáng kể như dễ bị mất cắp, sao chép trái phép, gây bất tiện trong việc quản lý và chia sẻ quyền truy cập, đặc biệt là ở những nơi có nhiều người ra vào.

Để khắc phục những nhược điểm này, nhiều giải pháp khóa cửa điện tử và thông minh đã được nghiên cứu và ứng dụng, bao gồm khóa vân tay, khóa mã số, khóa thẻ từ đơn giản, hay các hệ thống điều khiển qua ứng dụng di động sử dụng Bluetooth hoặc Wi-Fi. Công nghệ RFID, với khả năng nhận dạng đối tượng không tiếp xúc qua sóng vô tuyến, đã được ứng dụng rộng rãi trong nhiều lĩnh vực, bao gồm cả kiểm soát truy cập. Các nghiên cứu và sản phẩm thương mại hiện có thường kết hợp RFID với các công nghệ khác như mã PIN, sinh trắc học hoặc kết nối IoT.

Tuy nhiên, một số giải pháp hiện tại có thể còn tồn tại những điểm yếu như chi phí triển khai cao, giao diện quản lý phức tạp, thiếu khả năng quản lý người dùng tập trung, hoặc chưa tích hợp nguồn dự phòng hiệu quả, làm giảm tính sẵn sàng của hệ thống.

1.2.2. Tính cấp thiết cần nghiên cứu của đề tài

Nhu cầu về một giải pháp kiểm soát ra vào an toàn, tiện lợi và linh hoạt là rất lớn trong xã hội hiện đại. Sự bùng nổ của Internet of Things (IoT) đã mở ra những khả năng mới trong việc tích hợp các thiết bị phần cứng, kết nối chúng với mạng internet và quản lý chúng một cách thông minh thông qua các nền tảng phần mềm.

Việc nghiên cứu và phát triển một hệ thống kiểm soát cửa thông minh ứng dụng RFID, keypad, kết nối cơ sở dữ liệu và giao diện web không chỉ giải quyết được các hạn chế cố hữu của khóa cơ truyền thống mà còn khắc phục được những điểm yếu của các hệ thống điện tử đơn lẻ. Hệ thống này cung cấp phương thức xác thực đa dạng, khả năng quản lý người dùng (qua thẻ RFID) một cách tập trung và linh hoạt thông qua giao diện web, đặc biệt hữu ích cho các môi trường như văn phòng, nhà cho thuê, phòng thí nghiệm nơi cần phân quyền truy cập rõ ràng.

Hơn nữa, việc tích hợp nguồn dự phòng đảm bảo hệ thống hoạt động ổn định, tăng cường độ tin cậy và an ninh ngay cả trong trường hợp có sự cố về điện lưới. Do đó, đề tài này mang tính cấp thiết, đáp ứng nhu cầu thực tiễn và tận dụng được thế mạnh của các công nghệ IoT hiện đại.

1.2.3. Một số tài liệu có liên quan

Quá trình thực hiện đề tài đã tham khảo các tài liệu kỹ thuật quan trọng bao gồm: Datasheet của vi điều khiển NodeMCU ESP8266, module RFID MFRC522, module keypad cảm ứng TTP224, khóa Solenoid LY-031, các module nguồn (UPS 12V, Buck 5V); tài liệu về chuẩn giao tiếp SPI; tài liệu về hệ quản trị cơ sở dữ liệu MySQL và ngôn ngữ truy vấn SQL; tài liệu về các công nghệ phát triển web như HTML, CSS, JavaScript, PHP; các bài giảng và tài liệu về lập trình Arduino C++, nguyên lý hoạt động của các linh kiện điện tử; cũng như các bài báo, báo cáo kỹ thuật và các dự án mã nguồn mở có liên quan đến hệ thống kiểm soát truy cập dựa trên RFID và IoT.

Danh sách chi tiết các tài liệu tham khảo được liệt kê ở cuối báo cáo.

1.2.4. Lý do chọn đề tài

Đề tài "HỆ THỐNG BẢO MẬT CỬA RA VÀO THÔNG MINH" được lựa chọn dựa trên sự kết hợp giữa tính thực tiễn và khả năng ứng dụng các kiến thức đã học trong môn Vạn vật kết nối Internet.

Thứ nhất, đề tài giải quyết một bài toán rất cụ thể và phổ biến trong đời sống là nhu cầu về an ninh và quản lý truy cập, thay thế cho các giải pháp khóa cơ truyền thống còn nhiều bất cập.

Thứ hai, hệ thống được xây dựng dựa trên các công nghệ và linh kiện phổ biến, dễ tiếp cận và có chi phí hợp lý như vi điều khiển ESP8266, module RFID MFRC522, keypad cảm ứng TTP224, cơ sở dữ liệu MySQL và nền tảng web server XAMPP. Điều này tạo điều kiện thuận lợi cho việc triển khai và thử nghiệm.

Thứ ba, việc thực hiện đề tài đòi hỏi sự tích hợp kiến thức từ nhiều lĩnh vực khác nhau bao gồm phần cứng (thiết kế, lắp ráp mạch), phần mềm nhúng (lập trình vi điều khiển), kết nối mạng (Wi-Fi, HTTP), quản trị cơ sở dữ liệu và phát triển ứng dụng web, hoàn toàn phù hợp với mục tiêu và nội dung của môn học IoT, giúp sinh viên củng cố và vận dụng kiến thức một cách toàn diện.

1.2.5. Mục tiêu đề tài

Đề tài tập trung vào việc nghiên cứu, thiết kế và xây dựng một mô hình (prototype) hoàn chỉnh của hệ thống kiểm soát cửa ra vào thông minh, đáp ứng các mục tiêu cụ thể sau:

Thiết kế và lắp ráp thành công phần cứng của hệ thống, kết nối các module chính bao gồm vi điều khiển NodeMCU ESP8266, module đọc thẻ RFID RC522, keypad cảm ứng, module relay, khóa Solenoid, mạch nguồn chính và mạch nguồn dự phòng UPS.

Xây dựng phần mềm nhúng cho vi điều khiển NodeMCU ESP8266 bằng ngôn ngữ Arduino C++, có khả năng đọc dữ liệu từ thẻ RFID, nhận tín hiệu từ keypad và nút nhấn vật lý, kết nối mạng Wi-Fi, giao tiếp với Web Server qua giao thức HTTP để xác thực và nhận lệnh, đồng thời điều khiển module relay để đóng/mở khóa Solenoid.

Thiết kế và triển khai cơ sở dữ liệu MySQL trên nền tảng XAMPP để lưu trữ thông tin các thẻ RFID được cấp phép (UID, tên người dùng nếu có), lịch sử các lần truy cập (thời gian, phương thức, kết quả), và thông tin tài khoản người dùng web.

Phát triển một giao diện Web cơ bản sử dụng HTML, CSS, JavaScript và PHP, cho phép:

1. Người dùng thông thường (User) và Quản trị viên (Admin) đăng nhập vào hệ thống.

2. Cả User và Admin điều khiển mở cửa từ xa thông qua giao diện Dashboard.

3. Admin có quyền quản lý danh sách thẻ RFID (xem danh sách, thêm thẻ mới, xóa thẻ không còn sử dụng) và xem lịch sử truy cập chi tiết.

Tích hợp thành công mạch nguồn dự phòng UPS 12V sử dụng pin 18650, đảm bảo hệ thống có thể duy trì hoạt động trong một khoảng thời gian nhất định khi mất nguồn điện lưới.

Kiểm tra và đánh giá khả năng hoạt động ổn định, tốc độ phản hồi của hệ thống đối với các thao tác xác thực tại chỗ và điều khiển từ xa.

1.2.6. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu chính của đề tài là các thành phần công nghệ và linh kiện được sử dụng để xây dựng hệ thống, bao gồm: Vi điều khiển NodeMCU ESP8266; Module đọc thẻ RFID RC522 và thẻ RFID chuẩn Mifare 13.56MHz (FM1108 8KB); Keypad cảm ứng điện dung TTP224 (sử dụng 2-4 nút); Module Relay 1 kênh 5V kích mức cao/thấp; Khóa điện Solenoid LY-031 12V; Cảm biến từ MC-38 (tùy chọn giám sát trạng thái cửa); Nút nhấn vật lý PBS-11A; Mạch nguồn dự phòng UPS 12V/1.2A tích hợp sạc pin Lithium; Pin sạc Lithium 18650 3.7V; Mạch hạ áp DC-DC Buck 5V/3A; Hệ quản trị cơ sở dữ liệu MySQL; Web Server Apache và ngôn ngữ lập trình PHP (trong gói XAMPP); Các công nghệ Web Frontend (HTML, CSS, JavaScript).

Phạm vi nghiên cứu của đề tài tập trung vào việc thiết kế, xây dựng và kiểm thử một mô hình prototype hoạt động với các chức năng cốt lõi đã đề ra trong mục tiêu. Đề tài không đi sâu vào các vấn đề sau: Các kỹ thuật bảo mật nâng cao như mã hóa dữ liệu truyền qua Wi-Fi (HTTPS), mã hóa thông tin thẻ RFID, chống sao chép thẻ (anti-cloning), xác thực hai yếu tố (2FA); Thiết kế giao diện Web phức tạp với đầy đủ tính năng quản lý người dùng chi tiết, phân tích dữ liệu hay tùy biến nâng cao; Phát triển ứng dụng di động riêng biệt; Kiểm thử độ bền vật lý và khả năng chịu lỗi của phần cứng trong điều kiện hoạt động khắc nghiệt; Xây dựng cơ chế hoạt động offline hoàn chỉnh khi mất kết nối Internet/Server; Triển khai hệ thống ở quy mô lớn hoặc cho mục đích thương mại.

1.2.7. Phương pháp nghiên cứu

Để đạt được các mục tiêu đề ra, đề tài áp dụng kết hợp các phương pháp nghiên cứu sau:

Nghiên cứu lý thuyết. Thu thập, tổng hợp và phân tích các tài liệu, sách báo, bài giảng, datasheet liên quan đến các công nghệ nền tảng như Internet of Things, nguyên lý hoạt động của RFID, vi điều khiển ESP8266, giao tiếp SPI, keypad cảm ứng, relay, khóa solenoid, quản lý nguồn điện, cơ sở dữ liệu quan hệ MySQL, lập trình web với PHP, HTML, CSS, JavaScript, và giao thức HTTP.

Phân tích và thiết kế hệ thống. Dựa trên các yêu cầu chức năng và phi chức năng, tiến hành phân tích để đưa ra kiến trúc tổng thể cho hệ thống. Lựa chọn các linh kiện phần cứng phù hợp. Thiết kế chi tiết sơ đồ mạch nguyên lý, cấu trúc cơ sở dữ liệu (ERD), lưu đồ thuật toán cho phần mềm nhúng và ứng dụng web.

Thực nghiệm và phát triển. Tiến hành lắp ráp mạch điện theo sơ đồ thiết kế trên breadboard hoặc PCB thử nghiệm. Lập trình firmware cho vi điều khiển NodeMCU ESP8266 bằng Arduino IDE. Xây dựng cơ sở dữ liệu MySQL và viết các script PHP phía server. Thiết kế giao diện người dùng web.

Kiểm thử và hiệu chỉnh. Thực hiện kiểm tra chức năng của từng module và toàn bộ hệ thống. Ghi nhận kết quả, phát hiện lỗi (debug) và tiến hành hiệu chỉnh phần cứng, phần mềm để đảm bảo hệ thống hoạt động ổn định, chính xác và đáp ứng yêu cầu đặt ra.

1.2.8. Nội dung đề tài

Báo cáo được cấu trúc thành các phần chính sau:

Phần 1 - Mở đầu: Giới thiệu tổng quan về đề tài, bao gồm tóm tắt, đặt vấn đề (bối cảnh, tính cấp thiết, nghiên cứu liên quan), mục tiêu, đối tượng, phạm vi và phương pháp nghiên cứu.

Phần 2 - Nội dung: Trình bày chi tiết các khía cạnh kỹ thuật của hệ thống, bao gồm:
Chương 1: Giới thiệu tổng quan về hệ thống: Mô tả kiến trúc và nguyên lý hoạt động.
Chương 2: Phân tích yêu cầu hệ thống: Xác định yêu cầu chức năng, phi chức năng và lựa chọn giải pháp công nghệ.
Chương 3: Cơ sở lý thuyết và công nghệ liên quan: Đi sâu vào các công nghệ nền tảng được sử dụng.
Chương 4: Thiết kế và triển khai hệ thống: Trình bày chi tiết về thiết kế phần cứng, cơ sở dữ liệu, phần mềm và quá trình triển khai, kết quả thực nghiệm.

Phần 3 - Kết luận: Tổng kết các kết quả đạt được, nêu bật ưu nhược điểm của hệ thống và đề xuất các hướng phát triển trong tương lai.

Tài liệu tham khảo: Liệt kê các nguồn tài liệu đã sử dụng.

PHẦN 2: PHẦN NỘI DUNG

CHƯƠNG 1: GIỚI THIỆU TỔNG QUAN VỀ HỆ THỐNG

1.1. Khái niệm hệ thống cửa thông minh

Hệ thống cửa thông minh đại diện cho một bước tiến vượt bậc so với các giải pháp khóa cửa cơ học truyền thống. Thay vì dựa vào chìa khóa vật lý, các hệ thống này ứng dụng công nghệ điện tử, viễn thông và công nghệ thông tin để cung cấp các phương thức xác thực và kiểm soát truy cập hiện đại, an toàn và tiện lợi hơn.

Tích hợp các công nghệ như nhận dạng sinh trắc học (vân tay, khuôn mặt), mã số cá nhân (PIN), thẻ từ (RFID/NFC), và đặc biệt là khả năng kết nối mạng thông qua Internet of Things (IoT), hệ thống cửa thông minh không chỉ đơn thuần thực hiện chức năng đóng/mở cửa mà còn cho phép quản lý truy cập từ xa, giám sát lịch sử ra vào, cấp quyền linh hoạt và tích hợp với các hệ sinh thái nhà thông minh khác.

Sự ra đời và phát triển của các hệ thống này đáp ứng nhu cầu ngày càng cao về an ninh, tự động hóa và sự tiện nghi trong cuộc sống hiện đại, từ nhà ở cá nhân đến các môi trường đòi hỏi quản lý chặt chẽ hơn như văn phòng, nhà kho hay phòng thí nghiệm.

1.2. Kiến trúc tổng thể của hệ thống đề xuất

Hệ thống kiểm soát cửa ra vào thông minh được đề xuất trong đề tài này được thiết kế dựa trên kiến trúc phân tán kết hợp các thành phần phần cứng và phần mềm, hoạt động trên nền tảng Internet of Things (IoT) theo mô hình Client-Server. Kiến trúc tổng thể bao gồm các khối chức năng chính tương tác với nhau để thực hiện nhiệm vụ kiểm soát truy cập một cách hiệu quả và an toàn.

Khối Xử lý Trung tâm (Client): Sử dụng vi điều khiển NodeMCU ESP8266, đóng vai trò là "bộ não" của hệ thống tại cửa. Khối này chịu trách nhiệm thu thập dữ liệu từ các thiết bị đầu vào, xử lý sơ bộ, giao tiếp với khối Server qua mạng Wi-Fi để xác thực và nhận lệnh, đồng thời trực tiếp điều khiển khối chấp hành.

Khối Đầu vào (Input): Bao gồm các phương thức để người dùng tương tác và yêu cầu truy cập:

- Module đọc thẻ RFID RC522: Quét và đọc mã định danh duy nhất (UID) từ thẻ RFID.
- Keypad cảm ứng TTP224: Cho phép người dùng nhập mã PIN xác thực (trong đề tài này, do hạn chế phần cứng, đã điều chỉnh sử dụng 2 nút).
- Nút nhấn vật lý: Thường đặt bên trong để mở cửa không cần xác thực.

- Giao diện Web (User Interface): Cho phép người dùng đã đăng nhập gửi lệnh mở cửa từ xa.

Khối Chấp hành (Output): Thực thi lệnh đóng/mở cửa, bao gồm:

- Module Relay 5V: Đóng vai trò là công tắc điện tử, nhận tín hiệu điều khiển từ NodeMCU để đóng/ngắt dòng điện 12V.
- Khóa điện Solenoid LY-031 (12V): Cơ cấu khóa vật lý, được điều khiển bởi Relay.

Khối Server (Server-side): Hoạt động trên một máy tính cục bộ cài đặt XAMPP, bao gồm:

- Web Server (Apache): Phục vụ các tệp tin của giao diện Web (HTML, CSS, JS).
- Application Logic (PHP): Các script xử lý logic nghiệp vụ, bao gồm xác thực yêu cầu từ NodeMCU và giao diện Web, tương tác với cơ sở dữ liệu.
- Database Server (MySQL): Lưu trữ dữ liệu quan trọng như thông tin thẻ RFID hợp lệ, tài khoản người dùng Web, và lịch sử truy cập (scan logs).

Khối Giao tiếp Mạng: Sử dụng module Wi-Fi tích hợp trên ESP8266 để kết nối NodeMCU với mạng cục bộ và giao tiếp với Khối Server qua giao thức HTTP.

Khối Nguồn: Cung cấp năng lượng cho toàn bộ hệ thống, bao gồm:

- Adapter nguồn (hoặc nguồn 5V ban đầu).
- Mạch nguồn dự phòng UPS 12V: Đảm bảo hệ thống hoạt động khi mất điện lưới.
- Pin sạc Lithium 18650: Lưu trữ năng lượng cho mạch UPS.

Mạch hạ áp Buck 5V: Chuyển đổi nguồn 12V (từ UPS/Adapter) thành 5V ổn định cấp cho NodeMCU và Relay.

Khối Giao diện Người dùng (UI): Giao diện Web được truy cập qua trình duyệt, cung cấp chức năng giám sát, điều khiển và quản lý hệ thống.

1.3. Mô tả các thành phần chính và vai trò

Hệ thống được cấu thành từ nhiều module và linh kiện điện tử, mỗi thành phần đóng một vai trò quan trọng trong hoạt động chung:

NodeMCU ESP8266: Là vi điều khiển trung tâm, được lựa chọn nhờ tích hợp sẵn Wi-Fi, giá thành hợp lý, cộng đồng hỗ trợ lớn và khả năng lập trình dễ dàng qua Arduino IDE. Nó nhận dữ liệu từ RFID reader, keypad, nút nhấn, giao tiếp hai chiều với server qua Wi-Fi (gửi yêu cầu xác thực, nhận lệnh điều khiển), và xuất tín hiệu điều khiển Relay.

Module RFID RC522: Hoạt động ở tần số 13.56MHz, giao tiếp với NodeMCU qua chuẩn SPI (Serial Peripheral Interface) tốc độ cao. Vai trò của nó là đọc mã UID của thẻ

RFID chuẩn Mifare khi thẻ được đưa vào vùng hoạt động. UID này sau đó được gửi đến NodeMCU để xử lý.

Keypad cảm ứng TTP224: Cung cấp phương thức nhập liệu thay thế hoặc bổ sung cho RFID. Module này sử dụng công nghệ cảm ứng điện dung, giao tiếp với NodeMCU qua các chân Digital Input. Trong phạm vi đề tài, nó được dùng để nhập mã PIN (sử dụng 2-4 nút tùy cấu hình).

Khóa Solenoid LY-031 (12V): Là cơ cấu chấp hành chính, thực hiện việc khóa/mở cửa vật lý. Đây là loại khóa điện từ, yêu cầu nguồn 12V DC để hoạt động và thường ở trạng thái khóa khi không có điện (Fail-Secure).

Module Relay 5V: Đóng vai trò trung gian giữa tín hiệu điều khiển mức logic thấp (3.3V/5V) từ NodeMCU và dòng điện 12V yêu cầu bởi khóa Solenoid. Relay giúp cách ly mạch điều khiển và mạch tải, đảm bảo an toàn và cho phép NodeMCU điều khiển thiết bị có công suất lớn hơn.

Cơ sở dữ liệu MySQL: Được chọn làm hệ quản trị cơ sở dữ liệu do tính phổ biến, mã nguồn mở, hiệu năng ổn định và khả năng tích hợp tốt với PHP. MySQL lưu trữ danh sách các UID thẻ được phép truy cập, thông tin tài khoản người dùng web (username, password hash, role) và ghi lại lịch sử các lần quét thẻ hoặc cố gắng truy cập.

Web Server (XAMPP - Apache, PHP): Cung cấp môi trường để chạy ứng dụng web quản lý. Apache phục vụ các trang web tĩnh và động. Các script PHP xử lý logic phía server: nhận yêu cầu HTTP từ NodeMCU (chứa UID thẻ hoặc yêu cầu kiểm tra lệnh) hoặc từ trình duyệt (đăng nhập, gửi lệnh mở cửa, yêu cầu quản lý thẻ), truy vấn cơ sở dữ liệu MySQL để xác thực, ghi log, và gửi phản hồi hoặc lệnh điều khiển trở lại NodeMCU hoặc trình duyệt.

Mạch Nguồn (UPS 12V, Buck 5V, Pin 18650): Đảm bảo cung cấp nguồn điện liên tục và ổn định cho hệ thống. Mạch UPS quản lý việc sử dụng nguồn từ adapter và tự động chuyển sang dùng pin 18650 khi mất điện, đồng thời sạc lại pin khi có điện. Mạch Buck hạ áp từ 12V xuống 5V để cấp nguồn an toàn cho NodeMCU (qua chân Vin) và module Relay.

1.4. Nguyên lý hoạt động cơ bản

Hệ thống hoạt động dựa trên sự phối hợp giữa các khối chức năng thông qua mạng cục bộ. Quy trình hoạt động cơ bản khi có yêu cầu mở cửa diễn ra như sau:

1. Khởi tạo yêu cầu: Người dùng thực hiện một trong các hành động:

- Đưa thẻ RFID vào vùng đọc của module RC522.
- Nhập mã PIN thông qua keypad TTP224.
- Nhấn nút mở cửa vật lý từ bên trong.
- Đăng nhập vào giao diện Web và nhấn nút "Mở cửa".

2. Thu thập và gửi dữ liệu (NodeMCU):
   - Nếu là thẻ RFID, NodeMCU đọc UID từ RC522 qua giao tiếp SPI.
   - Nếu là Keypad, NodeMCU ghi nhận chuỗi số PIN được nhập.
   - Nếu là nút nhấn vật lý, NodeMCU phát hiện tín hiệu nhấn.
   - Nếu là lệnh từ Web, NodeMCU sẽ nhận được yêu cầu HTTP từ Server.
   - Đối với RFID và Keypad, NodeMCU sẽ đóng gói dữ liệu (UID hoặc PIN) và gửi một yêu cầu HTTP đến địa chỉ IP của Web Server trong mạng cục bộ (ví dụ: đến script check_access.php).
3. Xử lý phía Server (XAMPP - PHP & MySQL):
   - Script PHP (check_access.php) nhận yêu cầu từ NodeMCU.
   - Script truy vấn cơ sở dữ liệu MySQL để kiểm tra xem UID thẻ (hoặc mã PIN) có hợp lệ và được phép truy cập hay không (so sánh với bảng tags).
   - Đồng thời, script có thể ghi lại thông tin về lần truy cập này vào bảng lịch sử (scan_logs).
   - Server gửi phản hồi HTTP trở lại NodeMCU, cho biết yêu cầu có được chấp thuận ("AUTHORIZED") hay bị từ chối ("UNAUTHORIZED").
   - Đối với lệnh mở cửa từ Web (qua script trigger_open.php), server sẽ cập nhật trạng thái lệnh trong bảng door_commands. NodeMCU sẽ định kỳ kiểm tra bảng này (qua script check_command.php) để nhận lệnh mở cửa.
4. Điều khiển Khóa (NodeMCU & Relay):
   - Nếu nhận được phản hồi "AUTHORIZED" từ server hoặc phát hiện nút nhấn vật lý được nhấn, hoặc nhận được lệnh mở cửa từ xa, NodeMCU sẽ gửi tín hiệu điều khiển (ví dụ: mức HIGH hoặc LOW tùy cấu hình relay) đến chân IN của module Relay.
   - Relay được kích hoạt, đóng mạch điện 12V cấp cho khóa Solenoid.
   - Khóa Solenoid nhận nguồn, nhả chốt và cửa được mở trong một khoảng thời gian ngắn được lập trình sẵn trước khi tự động khóa lại (NodeMCU ngắt tín hiệu điều khiển Relay).

- Nếu yêu cầu bị từ chối, NodeMCU sẽ không kích hoạt Relay và có thể phát tín hiệu cảnh báo (ví dụ: nháy LED đỏ).

Quá trình này đảm bảo rằng chỉ những người dùng hoặc thẻ được ủy quyền mới có thể mở cửa, đồng thời mọi hoạt động đều có thể được giám sát và quản lý thông qua cơ sở dữ liệu và giao diện web.

CHƯƠNG 2: PHÂN TÍCH YÊU CẦU HỆ THỐNG

Sau khi có cái nhìn tổng quan về kiến trúc và các thành phần chính ở Chương 1, chương này sẽ đi sâu vào việc phân tích các yêu cầu cụ thể mà hệ thống cần đáp ứng, bao gồm cả yêu cầu về chức năng và phi chức năng. Đồng thời, chương cũng trình bày lý do lựa chọn các giải pháp công nghệ và linh kiện cụ thể, và mô tả chi tiết hơn về nguyên lý hoạt động của hệ thống.

2.1. Yêu cầu chức năng

Yêu cầu chức năng định nghĩa các nhiệm vụ cụ thể mà hệ thống phải thực hiện được để đáp ứng mục tiêu đề ra. Đối với hệ thống kiểm soát cửa thông minh này, các yêu cầu chức năng cốt lõi bao gồm:

Xác thực bằng RFID. Hệ thống phải có khả năng đọc mã định danh duy nhất (UID) từ thẻ RFID chuẩn Mifare 13.56MHz khi người dùng đưa thẻ vào vùng đọc của module RC522. Sau khi đọc, hệ thống phải gửi UID này đến server để kiểm tra tính hợp lệ. Nếu UID hợp lệ và được cấp phép, hệ thống phải kích hoạt mở khóa cửa.

Xác thực bằng Keypad (Mã PIN). Hệ thống phải cho phép người dùng nhập một chuỗi mã số cá nhân (PIN) thông qua keypad cảm ứng TTP224 (sử dụng 2 nút đã điều chỉnh). Khi nhập xong, hệ thống gửi mã PIN đến server để xác thực. Nếu mã PIN đúng, hệ thống phải kích hoạt mở khóa cửa. Cần có cơ chế xử lý khi nhập sai hoặc quá thời gian chờ.

Mở cửa bằng Nút nhấn Vật lý. Hệ thống phải trang bị một nút nhấn vật lý (thường đặt bên trong) cho phép người dùng mở cửa trực tiếp mà không cần qua bước xác thực với server. Khi nút nhấn được kích hoạt, NodeMCU phải điều khiển mở khóa ngay lập tức.

Điều khiển từ xa qua Giao diện Web. Hệ thống phải cung cấp một giao diện web cho phép người dùng đã được xác thực (đăng nhập) gửi lệnh yêu cầu mở cửa từ xa. Lệnh này được gửi đến server, sau đó server thông báo cho NodeMCU để thực thi việc mở khóa.

Quản lý Thẻ RFID (Quyền Admin). Giao diện web phải cung cấp chức năng cho người quản trị (Admin) để quản lý danh sách các thẻ RFID được phép truy cập. Các chức năng quản lý cơ bản bao gồm xem danh sách UID thẻ hiện có, thêm UID của thẻ mới vào hệ thống, và xóa UID của thẻ không còn sử dụng hoặc bị mất.

Lưu trữ và Truy xuất Dữ liệu. Hệ thống phải sử dụng cơ sở dữ liệu MySQL để lưu trữ bền vững danh sách các UID thẻ hợp lệ, thông tin tài khoản người dùng web (username, password đã mã hóa, vai trò), và ghi lại lịch sử các lần truy cập (bao gồm thời gian, phương

thức truy cập - RFID/PIN/Web/Button, UID thẻ nếu có, và kết quả - thành công/thất bại). Dữ liệu này phải có thể được truy xuất và hiển thị trên giao diện web (đặc biệt là lịch sử truy cập và danh sách thẻ cho Admin).

Phản hồi Trạng thái. Hệ thống cần cung cấp phản hồi trực quan cho người dùng về trạng thái hoạt động và kết quả xác thực. Điều này có thể thực hiện thông qua đèn LED tích hợp trên NodeMCU hoặc các LED riêng biệt (ví dụ: LED xanh khi xác thực thành công, LED đỏ khi thất bại, LED nhấp nháy khi đang xử lý hoặc chờ kết nối). Tiếng kêu từ Relay khi đóng/ngắt cũng là một dạng phản hồi.

Giám sát Trạng thái Cửa. Nếu sử dụng cảm biến từ MC-38, hệ thống có thể đọc tín hiệu để xác định cửa đang đóng hay mở và hiển thị thông tin này trên giao diện web hoặc ghi log.

2.2. Yêu cầu phi chức năng

Yêu cầu phi chức năng mô tả các tiêu chuẩn về chất lượng và cách thức hoạt động của hệ thống, không liên quan trực tiếp đến các chức năng cụ thể. Các yêu cầu này rất quan trọng để đảm bảo hệ thống hoạt động hiệu quả, đáng tin cậy và an toàn:

Tính Bảo mật (Security). Mặc dù không đi sâu vào các giải pháp phức tạp, hệ thống cần đảm bảo mức độ bảo mật cơ bản. Mật khẩu người dùng web phải được lưu trữ dưới dạng băm (hashed) trong cơ sở dữ liệu thay vì dạng rõ. Giao tiếp giữa NodeMCU và Server trong mạng cục bộ qua HTTP chưa được mã hóa (có thể nâng cấp lên HTTPS trong tương lai). Việc xác thực dựa trên UID thẻ Mifare Classic có thể bị sao chép, đây là một hạn chế cần lưu ý. Cần có cơ chế giới hạn số lần nhập sai PIN (nếu triển khai đầy đủ).

Tính Sẵn sàng và Độ tin cậy (Availability & Reliability). Hệ thống phải hoạt động ổn định và liên tục. Việc tích hợp mạch nguồn dự phòng UPS với pin 18650 là yêu cầu quan trọng để đảm bảo hệ thống vẫn có thể thực hiện các chức năng cơ bản (ít nhất là mở cửa bằng nút nhấn vật lý và có thể cả RFID/Keypad nếu server vẫn hoạt động) ngay cả khi mất điện lưới tạm thời. Phần cứng cần được lắp ráp chắc chắn, hạn chế lỗi kết nối.

Tính Dễ sử dụng (Usability). Các thao tác tương tác vật lý như quẹt thẻ, nhấn nút phải đơn giản và trực quan. Giao diện web, dù cơ bản, cũng cần được thiết kế rõ ràng, dễ điều hướng, giúp người dùng (cả User và Admin) dễ dàng thực hiện các thao tác điều khiển và quản lý.

Hiệu năng (Performance). Thời gian phản hồi của hệ thống là yếu tố quan trọng. Thời gian từ lúc người dùng quẹt thẻ hợp lệ hoặc nhập đúng PIN đến khi khóa cửa mở phải

nhanh chóng, lý tưởng là dưới 2 giây. Thời gian phản hồi khi điều khiển từ xa qua giao diện web có thể chấp nhận độ trễ lớn hơn một chút do phụ thuộc vào tốc độ mạng và xử lý của server, nhưng vẫn cần đảm bảo trải nghiệm người dùng tốt.

Khả năng Quản lý (Manageability). Hệ thống phải cho phép người quản trị (Admin) dễ dàng quản lý danh sách thẻ RFID được cấp phép thông qua giao diện web mà không cần can thiệp trực tiếp vào cơ sở dữ liệu hay lập trình lại vi điều khiển. Việc xem lịch sử truy cập cũng hỗ trợ công tác quản lý và giám sát an ninh.

2.3. Lựa chọn giải pháp công nghệ

Việc lựa chọn công nghệ và linh kiện phù hợp là yếu tố then chốt để đảm bảo hệ thống hoạt động hiệu quả, ổn định và có chi phí hợp lý. Dựa trên các yêu cầu đã phân tích, các lựa chọn chính cho đề tài này được thực hiện như sau:

Vi điều khiển (NodeMCU ESP8266) được chọn làm trái tim xử lý vì những ưu điểm nổi bật: tích hợp sẵn Wi-Fi giúp dễ dàng kết nối mạng mà không cần module ngoài; giá thành rất cạnh tranh; có đủ số lượng chân GPIO cho các kết nối cơ bản (sau khi xem xét và điều chỉnh sử dụng chân hợp lý); cộng đồng người dùng đông đảo cung cấp nhiều tài liệu và thư viện hỗ trợ; có thể lập trình dễ dàng bằng ngôn ngữ Arduino C++ trên nền tảng Arduino IDE quen thuộc.

Module Nhận dạng (RFID RC522 và Keypad TTP224):

RC522 là module RFID hoạt động ở tần số cao (HF) 13.56MHz, rất phổ biến, chi phí thấp và tương thích tốt với các loại thẻ Mifare Classic thông dụng. Giao tiếp SPI cho phép truyền dữ liệu nhanh chóng với vi điều khiển.

TTP224: Module keypad cảm ứng điện dung 4 kênh được chọn thay vì keypad ma trận truyền thống để tiết kiệm chân GPIO của NodeMCU, đặc biệt khi chỉ cần sử dụng một vài nút để nhập PIN hoặc thực hiện chức năng đơn giản. Module này dễ tích hợp và có độ nhạy tốt. (Trong quá trình thực hiện, có thể đã gặp lỗi với một số nút và điều chỉnh chỉ sử dụng 2 nút chức năng).

Khối Chấp hành (Relay 5V và Khóa Solenoid 12V):

Relay 5V (1 kênh): Được chọn vì khả năng điều khiển dễ dàng bằng tín hiệu logic 5V (hoặc 3.3V) từ NodeMCU, đồng thời cung cấp sự cách ly an toàn giữa mạch điều khiển điện áp thấp và mạch tải điện áp cao (12V cho khóa). Loại relay kích mức cao/thấp mang lại sự linh hoạt trong thiết kế mạch.

Khóa Solenoid LY-031 (12V): Là loại khóa điện phổ biến, phù hợp cho ứng dụng cửa ra vào, hoạt động tin cậy với nguồn 12V DC và có cơ chế Fail-Secure (tự khóa khi mất điện), tăng cường an ninh.

Nền tảng Server (XAMPP - Apache, MySQL, PHP): XAMPP được chọn làm môi trường phát triển và chạy server cục bộ vì tính tiện lợi, miễn phí, dễ cài đặt trên nhiều hệ điều hành (Windows, Linux, Mac). Nó tích hợp sẵn Apache làm Web Server, MySQL làm Database Server và PHP làm ngôn ngữ xử lý phía server - một bộ ba công nghệ rất phổ biến, mạnh mẽ và có nhiều tài liệu hướng dẫn.

Công nghệ Phần mềm:

Arduino C: Ngôn ngữ lập trình chính cho NodeMCU, dựa trên C nhưng được đơn giản hóa và cung cấp nhiều thư viện sẵn có, phù hợp cho việc phát triển nhanh các ứng dụng nhúng và IoT.

PHP: Ngôn ngữ kịch bản phía server mạnh mẽ, dễ học, tích hợp tốt với MySQL và phù hợp để xử lý các yêu cầu HTTP, logic ứng dụng web.

HTML/CSS/JavaScript: Bộ ba công nghệ nền tảng để xây dựng giao diện người dùng Web (Frontend), tạo cấu trúc, định dạng và xử lý tương tác phía trình duyệt.

Khối Nguồn (Mạch UPS 12V, Pin 18650, Mạch Buck 5V): Sự kết hợp này được chọn để giải quyết yêu cầu về tính sẵn sàng. Mạch UPS 12V chuyên dụng cho phép duy trì nguồn 12V ổn định từ adapter hoặc pin. Pin 18650 phổ biến, dung lượng cao và có thể sạc lại. Mạch Buck 5V hiệu suất cao giúp chuyển đổi 12V xuống 5V một cách hiệu quả để cấp nguồn cho NodeMCU và Relay mà không gây tỏa nhiệt nhiều.

2.4. Nguyên lý hoạt động chi tiết

Để hiểu rõ hơn luồng dữ liệu và tín hiệu điều khiển trong hệ thống, chúng ta có thể mô tả chi tiết hơn các kịch bản hoạt động chính:

Kịch bản Xác thực RFID:

- Thẻ RFID được đặt gần đầu đọc RC522.
- RC522 đọc UID và gửi đến NodeMCU qua SPI.
- NodeMCU (Client) gửi yêu cầu HTTP POST chứa UID đến script check_access.php trên Server.
- PHP Script kết nối MySQL, truy vấn bảng tags để kiểm tra UID.
- PHP Script ghi log vào bảng scan_logs.

- PHP Script gửi phản hồi HTTP ("AUTHORIZED" hoặc "UNAUTHORIZED") về NodeMCU.
- Nếu "AUTHORIZED", NodeMCU gửi tín hiệu kích hoạt Relay.
- Relay đóng mạch 12V cho Khóa Solenoid.
- Solenoid mở chốt. Sau một khoảng thời gian, NodeMCU ngắt tín hiệu Relay, Solenoid khóa lại.

Kịch bản Xác thực Keypad (PIN):

- Người dùng nhập PIN bằng các nút trên TTP224.
- NodeMCU đọc và lưu chuỗi PIN.
- NodeMCU gửi yêu cầu HTTP POST chứa PIN đến script check_access.php (hoặc một script riêng).
- PHP Script (có thể) kiểm tra PIN với một mã PIN cố định hoặc trong CSDL (tùy thiết kế).
- Các bước tiếp theo tương tự Kịch bản RFID (ghi log, gửi phản hồi, điều khiển relay).

Kịch bản Mở cửa bằng Nút nhấn Vật lý:

- Nút nhấn bên trong được nhấn.
- NodeMCU phát hiện tín hiệu Input thay đổi (ví dụ: từ HIGH xuống LOW).
- NodeMCU trực tiếp gửi tín hiệu kích hoạt Relay (bỏ qua bước liên lạc Server).
- Relay đóng mạch 12V, Solenoid mở chốt. Sau đó tự động khóa lại.
- NodeMCU có thể gửi thông báo về Server để ghi log sự kiện này.

Kịch bản Mở cửa từ xa qua Web:

- Người dùng đăng nhập vào Giao diện Web.
- Nhấn nút "Mở cửa" trên Dashboard.
- JavaScript gửi yêu cầu AJAX (hoặc form submit) đến script trigger_open.php trên Server.
- PHP Script xác thực session người dùng, sau đó cập nhật bản ghi trong bảng door_commands thành trạng thái "OPEN_REQUEST".
- NodeMCU trong vòng lặp loop() định kỳ gửi yêu cầu HTTP GET đến script check_command.php.

- PHP Script kiểm tra bảng door_commands. Nếu thấy "OPEN_REQUEST", nó trả về phản hồi tương ứng cho NodeMCU và reset trạng thái trong DB về "IDLE".
- NodeMCU nhận được lệnh mở cửa, gửi tín hiệu kích hoạt Relay.
- Relay đóng mạch 12V, Solenoid mở chốt. Sau đó tự động khóa lại.

CHƯƠNG 3: CƠ SỞ LÝ THUYẾT VÀ CÔNG NGHỆ LIÊN QUAN

Để xây dựng thành công Hệ thống bảo mật cửa ra vào thông minh, việc nắm vững cơ sở lý thuyết và nguyên lý hoạt động của các công nghệ, linh kiện được sử dụng là điều cần thiết. Chương này sẽ trình bày tổng quan về các khái niệm và công nghệ nền tảng cốt lõi của dự án, bao gồm Internet of Things, vi điều khiển ESP8266, công nghệ RFID, keypad cảm ứng, cơ sở dữ liệu MySQL, các công nghệ web liên quan và cơ cấu chấp hành.

3.1. Giới thiệu về Internet of Things (IoT)

Internet of Things (IoT), hay Mạng lưới Vạn vật Kết nối Internet, là một khái niệm mô tả một mạng lưới toàn cầu, nơi các đối tượng vật lý ("Things") được trang bị cảm biến, phần mềm và công nghệ kết nối để có thể thu thập, trao đổi dữ liệu với nhau và với các hệ thống khác qua Internet mà không cần sự can thiệp trực tiếp của con người. Các "Things" này có thể là bất cứ thứ gì, từ thiết bị gia dụng thông minh, máy móc công nghiệp, phương tiện giao thông cho đến các thiết bị đeo cá nhân. Mục tiêu của IoT là tạo ra một thế giới thông minh hơn, hiệu quả hơn bằng cách cho phép các thiết bị giao tiếp, phân tích dữ liệu và đưa ra quyết định hoặc hành động tự động. Kiến trúc của một hệ thống IoT thường bao gồm các lớp chính: lớp thiết bị (thu thập dữ liệu), lớp kết nối (truyền dữ liệu), lớp xử lý (phân tích dữ liệu, thường là trên cloud), và lớp ứng dụng (cung cấp giao diện và dịch vụ cho người dùng). Đề tài này là một ứng dụng cụ thể của IoT trong lĩnh vực an ninh và kiểm soát truy cập.

3.2. Vi điều khiển (ESP32/ESP8266)

Vi điều khiển (Microcontroller - MCU) là một máy tính nhỏ gọn được tích hợp trên một vi mạch đơn (single chip), chứa đựng bộ xử lý (CPU), bộ nhớ (RAM, Flash/EEPROM), và các chân vào/ra (Input/Output - I/O) để tương tác với thế giới bên ngoài. Nó được thiết kế để thực hiện các nhiệm vụ điều khiển cụ thể trong các hệ thống nhúng.

Trong đề tài này, vi điều khiển được lựa chọn là NodeMCU ESP8266. Đây không chỉ là một vi điều khiển đơn thuần mà là một System-on-Chip (SoC) chi phí thấp, được phát triển bởi Espressif Systems, nổi bật với khả năng tích hợp sẵn bộ thu phát Wi-Fi chuẩn 802.11 b/g/n. Điều này làm cho NodeMCU trở thành lựa chọn lý tưởng cho các ứng dụng IoT cần kết nối không dây. NodeMCU sử dụng lõi vi xử lý Tensilica L106 32-bit, cung cấp đủ hiệu năng cho các tác vụ như đọc cảm biến, xử lý dữ liệu cơ bản và giao tiếp mạng. Nó có nhiều chân GPIO (General Purpose Input/Output) cho phép kết nối với các module khác

như RFID reader, keypad, relay, cảm biến. Module NodeMCU thường hoạt động với mức điện áp logic 3.3V, nhưng có tích hợp bộ ổn áp cho phép cấp nguồn 5V qua cổng USB hoặc chân Vin. Việc lập trình cho NodeMCU rất thuận tiện nhờ sự hỗ trợ của môi trường Arduino IDE và ngôn ngữ lập trình Arduino C++, cùng với một cộng đồng phát triển lớn mạnh cung cấp nhiều thư viện và tài liệu tham khảo.

3.3. Công nghệ RFID

Công nghệ Nhận dạng qua tần số vô tuyến (RFID) là một phương pháp nhận dạng tự động sử dụng sóng vô tuyến để truyền dữ liệu giữa một thẻ (tag) gắn trên đối tượng và một đầu đọc (reader). Đây là công nghệ cốt lõi được sử dụng để xác thực người dùng trong hệ thống.

3.3.1. Định nghĩa và nguyên lý hoạt động

RFID cho phép xác định và theo dõi các đối tượng mà không cần tiếp xúc trực tiếp hay tầm nhìn thẳng (line-of-sight) như mã vạch. Nguyên lý cơ bản dựa trên sự tương tác điện từ giữa đầu đọc và thẻ. Đầu đọc phát ra sóng vô tuyến mang năng lượng và/hoặc tín hiệu truy vấn. Khi thẻ RFID đi vào vùng phủ sóng của đầu đọc:

- Đối với thẻ thụ động (Passive Tag): Năng lượng từ sóng vô tuyến của đầu đọc sẽ được ăng-ten của thẻ thu nhận và cung cấp đủ nguồn để vi mạch trên thẻ hoạt động và gửi dữ liệu (thường là mã định danh duy nhất - UID) trở lại đầu đọc.
- Đối với thẻ chủ động (Active Tag): Thẻ sử dụng nguồn pin riêng để tự phát tín hiệu chứa dữ liệu đến đầu đọc.

3.3.2. Các thành phần hệ thống RFID

Một hệ thống RFID cơ bản bao gồm ba thành phần chính:

- Thẻ RFID (Tag/Transponder): Là thiết bị nhỏ chứa một vi mạch (chip) để lưu trữ dữ liệu (ít nhất là một mã UID) và một ăng-ten để thu/phát sóng vô tuyến. Thẻ được gắn hoặc tích hợp vào đối tượng cần nhận dạng.
- Đầu đọc RFID (Reader/Interrogator): Là thiết bị phát ra sóng vô tuyến để giao tiếp với thẻ và thu nhận dữ liệu từ thẻ. Đầu đọc thường được kết nối với một hệ thống máy chủ (Host System) để xử lý dữ liệu đọc được.
- Ăng-ten (Antenna): Cả thẻ và đầu đọc đều cần có ăng-ten để thực hiện việc truyền và nhận sóng vô tuyến. Thiết kế và kích thước ăng-ten ảnh hưởng lớn đến khoảng cách đọc và hiệu suất của hệ thống.

3.3.3. Phân loại thẻ RFID

Thẻ RFID chủ yếu được phân loại dựa trên nguồn năng lượng:

- Thẻ thụ động (Passive Tag) không có nguồn pin riêng, nhận năng lượng từ sóng của đầu đọc. Chúng có chi phí thấp, kích thước nhỏ, tuổi thọ cao nhưng khoảng cách đọc ngắn (vài cm đến vài mét). Thẻ Mifare Classic 13.56MHz được sử dụng trong đề tài này thuộc loại thẻ thụ động.
- Thẻ chủ động (Active Tag): Có nguồn pin riêng, cho phép khoảng cách đọc xa hơn nhiều (lên đến hàng trăm mét) và có thể tích hợp thêm cảm biến. Tuy nhiên, chúng đắt hơn, lớn hơn và có tuổi thọ giới hạn bởi pin.
- Thẻ bán thụ động (Semi-passive/Battery-Assisted Passive - BAP): Có pin nhưng chỉ dùng để cấp nguồn cho vi mạch/cảm biến trên thẻ, việc truyền tín hiệu vẫn dựa vào năng lượng từ đầu đọc.

Ngoài ra, thẻ còn có thể phân loại theo khả năng ghi/đọc: Read-Only (chỉ đọc, dữ liệu được ghi cố định khi sản xuất), Write-Once-Read-Many (WORM - ghi một lần, đọc nhiều lần), và Read/Write (đọc và ghi lại dữ liệu nhiều lần).

3.3.4. Tần số hoạt động

Công nghệ RFID hoạt động trên nhiều dải tần số khác nhau, mỗi dải tần có đặc điểm và ứng dụng riêng:

- Tần số thấp (Low Frequency - LF): 125-134 kHz. Khoảng cách đọc ngắn, tốc độ đọc chậm, ít bị ảnh hưởng bởi môi trường nước/kim loại. Thường dùng trong kiểm soát truy cập đơn giản, nhận dạng động vật.
- Tần số cao (High Frequency - HF): 13.56 MHz. Khoảng cách đọc trung bình (vài cm đến 1m), tốc độ đọc khá, chuẩn hóa tốt (ISO/IEC 14443, ISO/IEC 15693). Đây là tần số được sử dụng trong đề tài này (cho thẻ Mifare và đầu đọc RC522), rất phổ biến cho thẻ thanh toán không tiếp xúc, thẻ thông minh, kiểm soát truy cập, quản lý thư viện.
- Tần số siêu cao (Ultra-High Frequency - UHF): 860-960 MHz. Khoảng cách đọc xa (vài mét đến >10m), tốc độ đọc rất nhanh, đọc được nhiều thẻ cùng lúc, nhưng nhạy cảm hơn với môi trường nước/kim loại. Thường dùng trong quản lý chuỗi cung ứng, logistics, kiểm kê tài sản.
- Vi sóng (Microwave): 2.45 GHz, 5.8 GHz. Khoảng cách đọc rất xa, tốc độ cao, thường dùng cho thẻ chủ động trong các ứng dụng như thu phí tự động không dừng (ETC).

3.3.5. Module MFRC522

Đây là module đầu đọc/ghi thẻ RFID cụ thể được sử dụng trong dự án. Nó hoạt động ở tần số 13.56 MHz, hỗ trợ giao tiếp với các loại thẻ tuân thủ chuẩn ISO/IEC 14443A, bao gồm dòng thẻ Mifare Classic (như thẻ FM1108 8KB được liệt kê). Module này giao tiếp với vi điều khiển (NodeMCU) thông qua giao thức SPI (Serial Peripheral Interface), sử dụng các chân chính:

- SDA/SS (Slave Select): Chọn chip MFRC522 để giao tiếp (nối với D4/GPIO2 của NodeMCU).
- SCK (Serial Clock): Xung nhịp đồng bộ hóa dữ liệu (nối với D5/GPIO14).
- MOSI (Master Out Slave In): Dữ liệu từ Master (NodeMCU) đến Slave (RC522) (nối với D7/GPIO13).
- MISO (Master In Slave Out): Dữ liệu từ Slave (RC522) đến Master (NodeMCU) (nối với D6/GPIO12).
- RST (Reset): Chân reset module (nối với D3/GPIO0).
- VCC và GND: Chân cấp nguồn (chỉ dùng 3.3V) và chân nối đất.

3.3.6. So sánh RFID và Barcode

Mặc dù cả hai đều là công nghệ nhận dạng tự động, RFID có nhiều ưu điểm vượt trội so với mã vạch (Barcode): không yêu cầu tầm nhìn thẳng, có thể đọc xuyên qua vật liệu không kim loại, đọc được nhiều thẻ cùng lúc, khoảng cách đọc xa hơn, khả năng lưu trữ dữ liệu lớn hơn và có thể ghi/đọc lại dữ liệu (đối với thẻ Read/Write). Tuy nhiên, chi phí cho mỗi thẻ RFID thường cao hơn so với mã vạch.

3.4. Keypad cảm ứng TTP224

Khác với keypad ma trận truyền thống yêu cầu quét hàng và cột để xác định phím được nhấn (tốn nhiều chân I/O), module keypad cảm ứng TTP224 sử dụng công nghệ cảm ứng điện dung. Mỗi phím trên module là một điện cực. Khi người dùng chạm vào một phím, điện dung giữa điện cực đó và cơ thể người (hoặc đất) thay đổi. Vi mạch TTP224 trên module phát hiện sự thay đổi điện dung này và xuất tín hiệu logic (thường là mức HIGH khi có chạm) ra chân tương ứng. Ưu điểm của việc sử dụng TTP224 trong dự án này (với nhu cầu chỉ cần 2-4 nút) là tiết kiệm đáng kể số lượng chân GPIO của NodeMCU so với việc dùng keypad ma trận 4x4, đồng thời đơn giản hóa việc lập trình đọc phím (chỉ cần kiểm tra trạng thái digitalRead của từng chân).

3.5. Cơ sở dữ liệu MySQL

MySQL là một Hệ quản trị cơ sở dữ liệu quan hệ (Relational Database Management System - RDBMS) mã nguồn mở rất phổ biến. Trong mô hình cơ sở dữ liệu quan hệ, dữ liệu được tổ chức thành các bảng (tables), mỗi bảng gồm nhiều hàng (rows - bản ghi) và cột (columns - thuộc tính). Mối quan hệ giữa các bảng được thiết lập thông qua các khóa (keys).

Trong hệ thống này, MySQL đóng vai trò lưu trữ dữ liệu cấu hình và dữ liệu hoạt động:

- Dữ liệu cấu hình: Bảng tags lưu UID và thông tin (tên, mô tả, trạng thái hoạt động) của các thẻ RFID được phép truy cập. Bảng web_users lưu thông tin đăng nhập (username, password hash, role) cho người dùng giao diện web.
- Dữ liệu hoạt động: Bảng scan_logs ghi lại lịch sử các lần quét thẻ hoặc nhập PIN (thời gian, UID thẻ, kết quả xác thực). Bảng door_commands (nếu dùng) lưu trạng thái lệnh điều khiển từ xa.

Việc tương tác với cơ sở dữ liệu MySQL được thực hiện thông qua Ngôn ngữ truy vấn có cấu trúc (Structured Query Language - SQL). Các câu lệnh SQL cơ bản được sử dụng bao gồm CREATE TABLE (tạo bảng), INSERT INTO (thêm dữ liệu), SELECT (truy vấn dữ liệu), UPDATE (cập nhật dữ liệu), và DELETE (xóa dữ liệu). Các script PHP phía server sẽ thực thi các câu lệnh SQL này để đọc, ghi và cập nhật dữ liệu theo yêu cầu từ NodeMCU hoặc giao diện web.

3.6. Công nghệ Web

3.6.1. Mô hình Client-Server

Hoạt động của ứng dụng web dựa trên mô hình Client-Server. Client là trình duyệt web của người dùng hoặc NodeMCU, gửi yêu cầu (Request) đến Server. Server (chạy trên máy tính cài XAMPP) xử lý yêu cầu và gửi phản hồi (Response) trở lại Client.

3.6.2. Frontend: HTML, CSS, JavaScript

HTML (HyperText Markup Language): Định nghĩa cấu trúc và nội dung của trang web (tiêu đề, đoạn văn, bảng, form, nút nhấn...).

CSS (Cascading Style Sheets): Định dạng và trình bày giao diện của trang web (màu sắc, bố cục, font chữ...).

JavaScript (JS): Ngôn ngữ kịch bản chạy phía trình duyệt, cho phép tạo ra các tương tác động, xử lý sự kiện người dùng (nhấn nút), kiểm tra dữ liệu nhập (validate form), và đặc biệt là gửi yêu cầu đến server mà không cần tải lại trang thông qua AJAX.

3.6.3. Backend

PHP (Hypertext Preprocessor) là ngôn ngữ kịch bản phía server được sử dụng trong dự án này. Các script PHP chạy trên Web Server (Apache) có nhiệm vụ: nhận và phân tích yêu cầu HTTP từ Client (trình duyệt hoặc NodeMCU); thực thi logic nghiệp vụ (kiểm tra đăng nhập, xác thực quyền thẻ, xử lý lệnh mở cửa); tương tác với cơ sở dữ liệu MySQL (truy vấn, cập nhật); và tạo ra phản hồi (có thể là trang HTML hoàn chỉnh hoặc dữ liệu dạng JSON cho AJAX).

3.6.4. Giao thức HTTP/HTTPS, AJAX

HTTP (Hypertext Transfer Protocol): Là giao thức nền tảng của World Wide Web, quy định cách thức Client và Server trao đổi thông tin (request và response). NodeMCU giao tiếp với Server PHP cũng thông qua giao thức này. (HTTPS là phiên bản bảo mật của HTTP, sử dụng mã hóa SSL/TLS, chưa được triển khai trong phạm vi đề tài này).

AJAX (Asynchronous JavaScript and XML): Là một tập hợp các kỹ thuật phát triển web cho phép ứng dụng web giao tiếp với server ở chế độ nền (background) mà không làm gián đoạn trạng thái hiện tại của trang. JavaScript phía client gửi yêu cầu HTTP đến server và nhận phản hồi (thường là dạng JSON hoặc XML, nhưng có thể là text hoặc HTML) để cập nhật một phần của trang web. Điều này được sử dụng để gửi lệnh mở cửa từ xa hoặc cập nhật động trạng thái, lịch sử truy cập trên Dashboard mà không cần tải lại toàn bộ trang.

3.7. Relay và cơ cấu chấp hành (Khóa Solenoid)

Relay (Rơ le): Là một công tắc hoạt động bằng điện. Nó sử dụng một dòng điện nhỏ trong cuộn dây (coil) để tạo ra từ trường, hút hoặc đẩy một tiếp điểm cơ học, qua đó đóng hoặc ngắt một mạch điện khác có thể mang dòng điện hoặc điện áp lớn hơn nhiều. Trong hệ thống này, module Relay 5V nhận tín hiệu điều khiển mức logic (3.3V hoặc 5V) từ chân GPIO của NodeMCU. Khi được kích hoạt, nó sẽ đóng/mở tiếp điểm nối với mạch 12V của khóa Solenoid. Các tiếp điểm quan trọng của relay bao gồm:

- COM (Common): Chân chung.
- NO (Normally Open): Tiếp điểm thường mở, hở mạch với COM khi relay chưa kích hoạt, đóng mạch khi kích hoạt. Đây là tiếp điểm thường được sử dụng để cấp nguồn cho khóa Solenoid khi cần mở.
- NC (Normally Closed): Tiếp điểm thường đóng, nối liền với COM khi relay chưa kích hoạt, hở mạch khi kích hoạt. Tiếp điểm này được bỏ trống trong ứng dụng khóa Fail-Secure này.

Relay giúp cách ly hoàn toàn mạch điều khiển điện áp thấp của NodeMCU khỏi mạch tải 12V, bảo vệ vi điều khiển khỏi nhiễu và sốc điện.

Khóa Solenoid LY-031: Là cơ cấu chấp hành vật lý chính. Nó hoạt động dựa trên nguyên lý điện từ. Khi có dòng điện 12V chạy qua cuộn dây solenoid bên trong, một từ trường được tạo ra, hút lõi sắt (chốt khóa) vào bên trong, làm cửa mở ra (hoặc cho phép mở). Khi ngắt dòng điện, lò xo (hoặc trọng lực) sẽ đẩy chốt khóa trở lại vị trí khóa. Loại khóa này thường là "Fail-Secure", nghĩa là nó sẽ tự động khóa lại khi mất điện, đảm bảo an ninh.

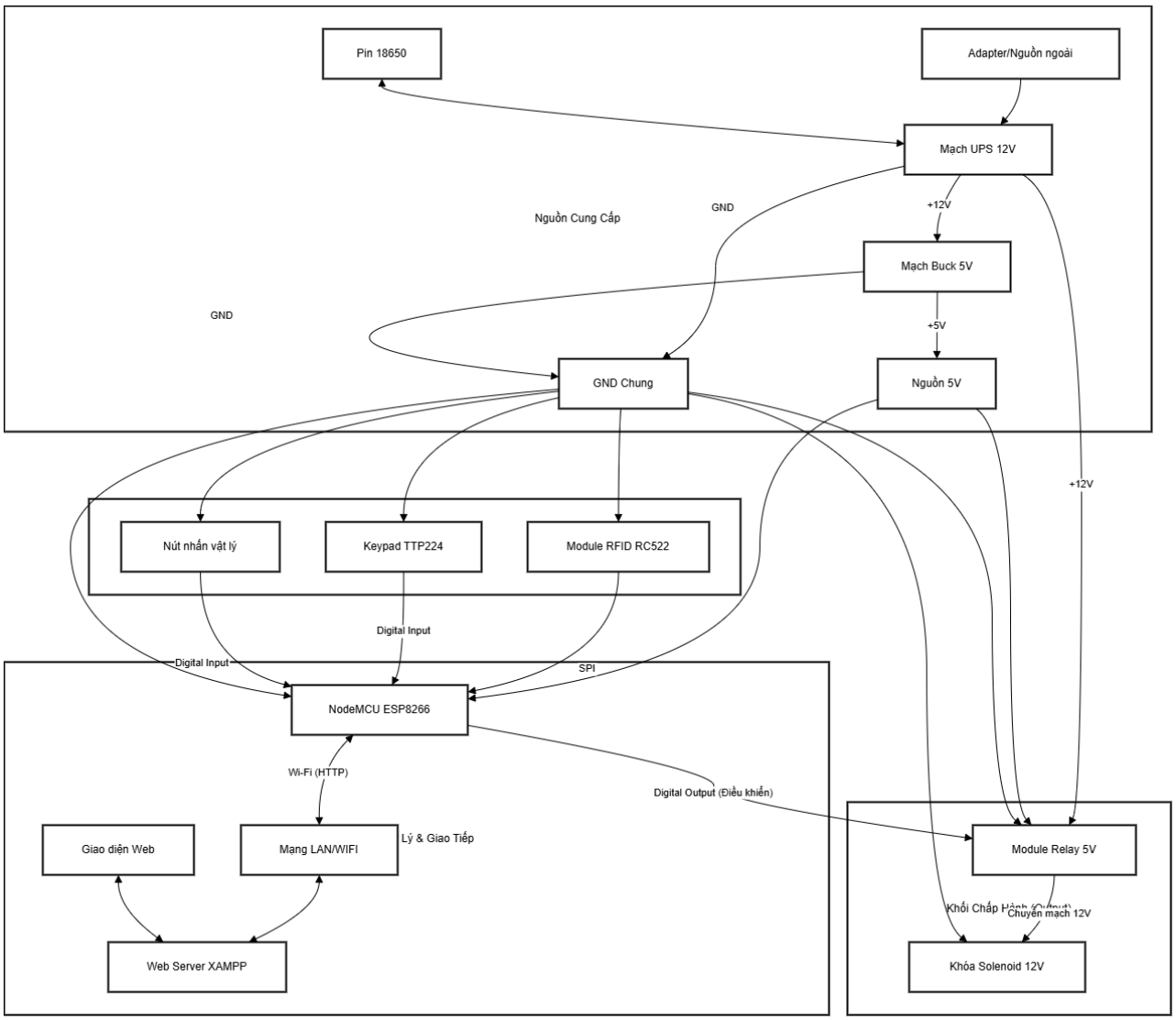
CHƯƠNG 4: THIẾT KẾ VÀ TRIỂN KHAI HỆ THỐNG

4.1. Thiết kế phần cứng

Thiết kế phần cứng là nền tảng vật lý của hệ thống, đảm bảo các module có thể giao tiếp và hoạt động đồng bộ với nhau.

4.1.1. Sơ đồ khối chi tiết hệ thống

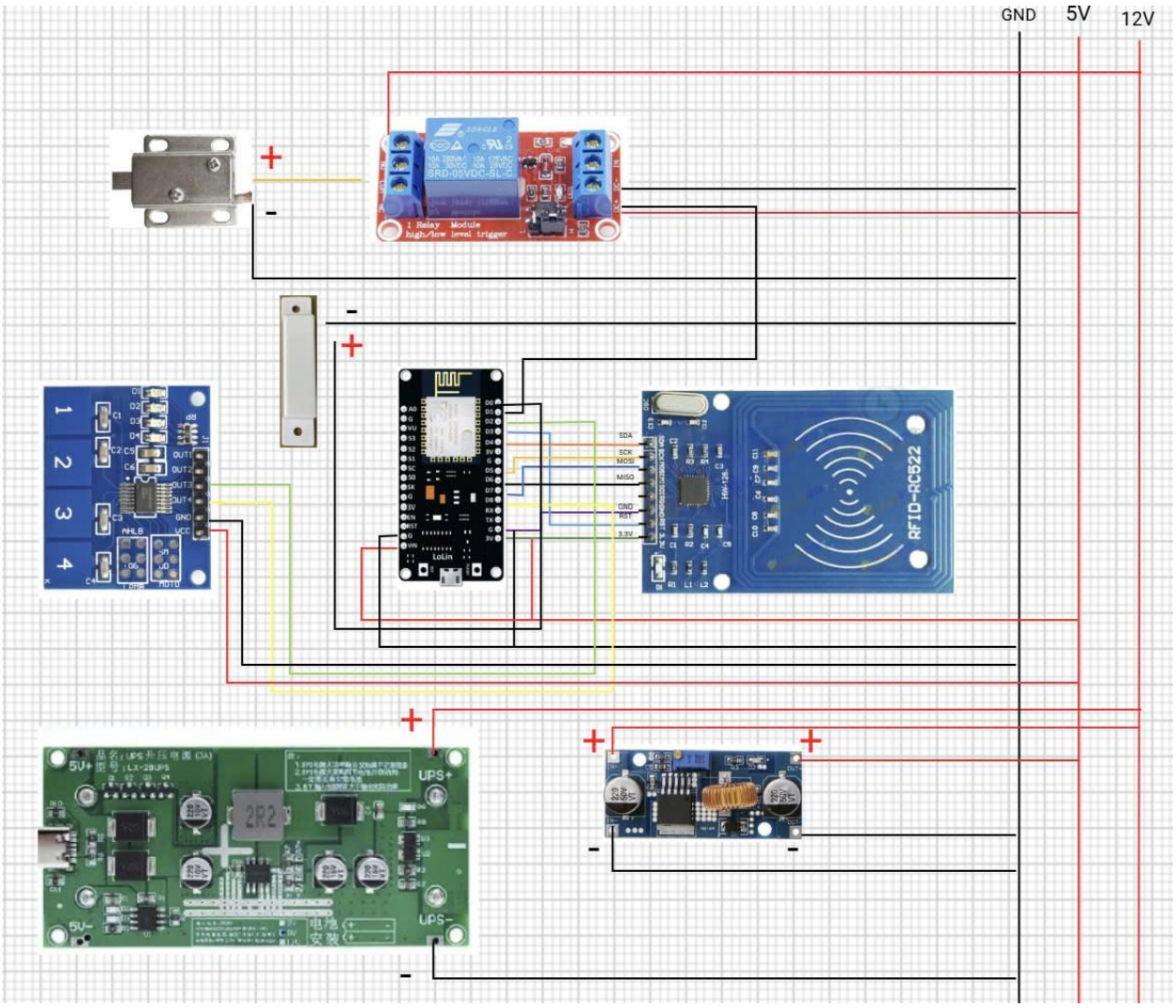
Sơ đồ khối chi tiết mô tả mối liên kết cụ thể giữa các thành phần phần cứng chính. Trung tâm là NodeMCU ESP8266, kết nối với module RFID RC522 qua giao thức SPI để đọc dữ liệu thẻ. NodeMCU cũng nhận tín hiệu đầu vào từ Keypad cảm ứng TTP224 và Nút nhấn vật lý qua các chân Digital Input. Tín hiệu điều khiển đầu ra từ NodeMCU (chân Digital Output) được gửi đến Module Relay 5V. Module Relay đóng vai trò chuyển mạch cho nguồn điện 12V cung cấp bởi hệ thống nguồn (bao gồm Mạch UPS, Pin 18650 và Adapter) để cấp cho Khóa Solenoid 12V. Mạch Buck 5V nhận nguồn 12V và hạ áp xuống 5V để cấp cho NodeMCU (qua chân Vin) và cuộn dây của Relay. Kết nối mạng được thực hiện qua module Wi-Fi tích hợp trên NodeMCU. Toàn bộ hệ thống yêu cầu một điểm nối đất (GND) chung để đảm bảo sự ổn định.



Hình: Sơ đồ khối chi tiết hệ thống

4.1.2. Sơ đồ mạch nguyên lý

Sơ đồ mạch nguyên lý thể hiện chi tiết cách các chân của từng linh kiện được kết nối với nhau. Việc kết nối được thực hiện cẩn thận để đảm bảo tín hiệu và nguồn điện được truyền đúng cách.



Hình: Sơ đồ mạch nguyên lý

Kết nối Nguồn:

- Nguồn điện 12V từ Adapter hoặc đầu ra của Mạch UPS được cấp cho đầu vào của Mạch Buck DC-DC 5V và một đầu của tiếp điểm Thường Mở (NO - Normally Open) của Module Relay.
- Đầu ra 5V (+) và GND (-) của Mạch Buck được đưa ra các đường ray cấp nguồn trên breadboard.
- Chân Vin và chân GND của NodeMCU được nối tương ứng với đường ray 5V (+) và GND (-) trên breadboard.
- Chân VCC (hoặc DC+) và chân GND (hoặc DC-) của Module Relay được nối tương ứng với đường ray 5V (+) và GND (-) trên breadboard để cấp nguồn cho cuộn dây relay.

  Kết nối Module RFID RC522 với NodeMCU (Giao thức SPI):

- RC522 VCC -> NodeMCU 3.3V (Lưu ý chỉ dùng 3.3V cho RC522).

- RC522 RST -> NodeMCU D3 (GPIO0).
- RC522 GND -> NodeMCU GND.
- RC522 MISO -> NodeMCU D6 (GPIO12).
- RC522 MOSI -> NodeMCU D7 (GPIO13).
- RC522 SCK -> NodeMCU D5 (GPIO14).
- RC522 SDA/SS -> NodeMCU D4 (GPIO2).

Kết nối Keypad TTP224 và Nút nhấn:

- Các chân tín hiệu Output của TTP224 (tương ứng các nút sử dụng, ví dụ 2 nút) được nối với các chân Digital Input của NodeMCU (ví dụ: D2, D8).
- Chân VCC và GND của TTP224 nối với nguồn 3.3V (hoặc 5V tùy module) và GND.
- Một chân của Nút nhấn vật lý nối với chân Digital Input của NodeMCU (ví dụ: D0). Chân còn lại của nút nhấn nối với GND. (Lưu ý: Chân D0 của NodeMCU cũng là chân Flash, việc sử dụng cần cẩn thận hoặc chọn chân khác nếu có thể. Hoặc sử dụng điện trở kéo lên nếu cần thiết).

Kết nối Module Relay với NodeMCU và Khóa Solenoid:

- Chân IN của Module Relay nối với chân Digital Output của NodeMCU (ví dụ: D1).
- Chân COM (Common) của Relay nối với một đầu dây của Khóa Solenoid LY-031.
- Đầu dây còn lại của Khóa Solenoid nối với GND của nguồn 12V (GND chung).
- Chân NO (Normally Open) của Relay nối với nguồn 12V dương (+).
- Chân NC (Normally Closed) của Relay bỏ trống, không kết nối, để đảm bảo khóa hoạt động theo cơ chế Fail-Secure.

Kết nối Cảm biến từ MC-38:

- Một chân của cảm biến nối với chân Digital Input của NodeMCU (ví dụ: chọn chân khác D0 nếu D0 dùng cho nút nhấn).

- Chân còn lại của cảm biến nối với GND. Cần kích hoạt điện trở kéo lên nội (Internal Pull-up) trên chân Input này trong code.

4.1.3. Danh sách linh kiện chi tiết

Bảng dưới đây liệt kê các linh kiện chính được sử dụng trong quá trình xây dựng mô hình hệ thống:

STT	ID	Tên sản phẩm	Đơn vị tính	Số lượng	Ghi chú

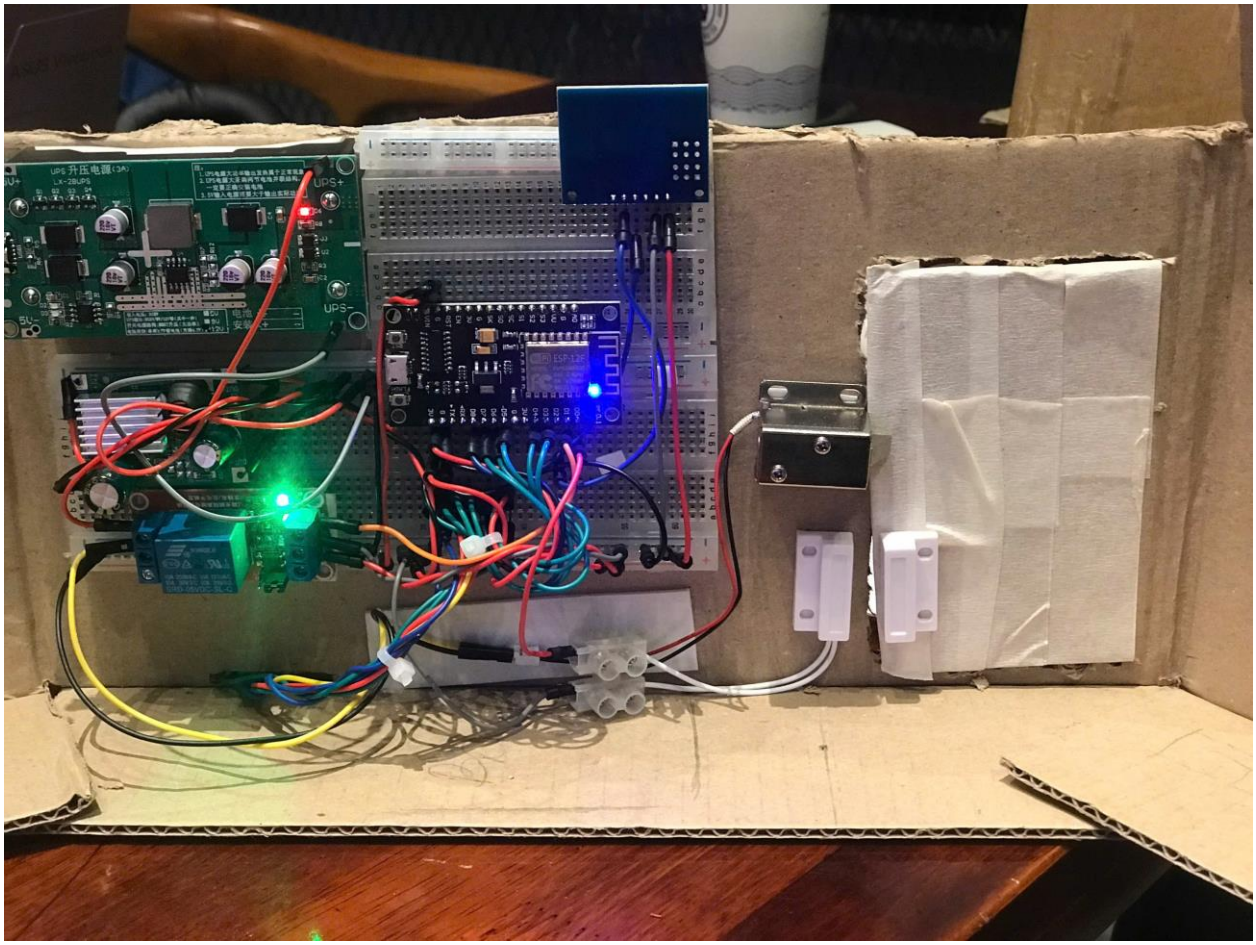
1	-	NodeMCU ESP8266	Cái	1	Vi điều khiển trung tâm, tích hợp Wi-Fi
2	-	Module RFID RC522	Bộ	1	Đầu đọc thẻ RFID 13.56MHz, giao tiếp SPI
3	2500	Thẻ RFID IC Tag 13.56Mhz FM1108 8KB (hoặc tương tự)	Cái	4	Thẻ Mifare Classic để thử nghiệm
4	8042	TTP224 Bàn Phím Cảm Ứng Điện Dung 4 Kênh	Cái	1	Sử dụng 2-4 nút tùy chỉnh
5	19459	PBS-11A Nút Nhấn Giữ 12mm Dây Nối 15cm (hoặc loại nhả)	Cái	1	Nút mở cửa vật lý
6	5059	Module 1 Relay 5V Kích Mức Cao/Thấp	Cái	1	Điều khiển khóa Solenoid
7	9103	LY-031 Khoá Điện Solenoid 12V	Cái	1	Cơ cấu chấp hành khóa cửa
8	-	Mạch sạc 18650 15W tăng áp cho nguồn dự phòng UPS 12V/1.2A	Cái	1	Mạch nguồn dự phòng và sạc pin
9	20044	Pin Sạc Lithium 18650 1800mAh 5C 3.7V (hoặc dung lượng khác)	Viên	2	Pin cho nguồn dự phòng
10	-	Mạch ổn áp DC-DC Buck 5V 3A	Cái	1	Hạ áp từ 12V xuống 5V cho NodeMCU, Relay
11	8046	MC-38 Cảm Biến Từ NC	Bộ	1	(Tùy chọn) Giám sát trạng thái cửa
12	1943	Bộ Dây Cắm Testboard 65 Sợi Đực-Đực	Bộ	1	Dây nối các linh kiện
13	-	Đế test board, bread board MB-102 loại tốt	Cái	1	Bảng cắm để lắp ráp mạch thử nghiệm

14	-	Đế test board, bread board 85x55mm	Cái	1	(Tùy chọn) Breadboard nhỏ hơn
15	10452	X3-2012 Cầu Nối Dây Điện 12 Cực 14mm2 380V 20A (hoặc loại khác)	Thanh	1	(Tùy chọn) Để nối dây nguồn gọn gàng
16	-	Adapter nguồn 12V DC (>= 1.5A)	Cái	1	Nguồn cấp chính (nếu không dùng nguồn 5V USB ban đầu)

Bảng: Danh sách Linh kiện chính

4.1.4. Hình ảnh lắp ráp mô hình thực tế

Hình ảnh sau đây minh họa mô hình thực tế của hệ thống được lắp ráp trên breadboard. Các linh kiện chính như NodeMCU, module RFID, Relay, Keypad được kết nối với nhau bằng dây cắm theo sơ đồ nguyên lý. Khối nguồn và khóa Solenoid cũng được kết nối để kiểm tra hoạt động tổng thể.



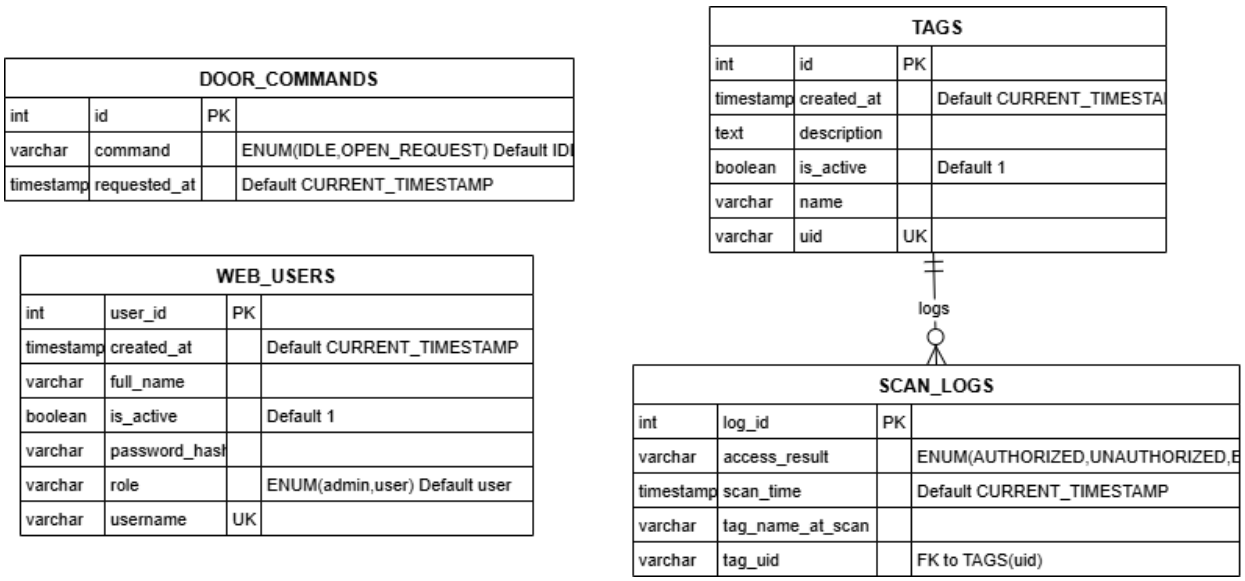
Hình mặt sau (Sơ đồ mạch thực tế)

4.2. Thiết kế cơ sở dữ liệu

Cơ sở dữ liệu là nơi lưu trữ thông tin cấu hình và dữ liệu hoạt động của hệ thống, được thiết kế bằng MySQL.

4.2.1. Sơ đồ quan hệ thực thể (ERD)

Sơ đồ ERD mô tả các thực thể chính trong cơ sở dữ liệu và mối quan hệ giữa chúng. Các thực thể chính bao gồm: Thẻ RFID (tags), Người dùng Web (web_users), Lịch sử quét (scan_logs), và Lệnh điều khiển cửa (door_commands).



Hình: ERD của cơ sở dữ liệu

4.2.2. Thiết kế các bảng

Cơ sở dữ liệu rfid_db được thiết kế bao gồm các bảng chính sau đây để lưu trữ thông tin cấu hình và dữ liệu hoạt động của hệ thống. Cấu trúc chi tiết của từng bảng được trình bày dưới đây:

Bảng 4.2: Bảng tags - Lưu thông tin thẻ RFID được cấp phép

Bảng này chứa thông tin về các thẻ RFID được hệ thống nhận dạng và cấp quyền truy cập.

Tên cột	Mô tả
id	Khóa chính, tự động tăng cho mỗi thẻ
uid	Mã định danh duy nhất (UID) của thẻ RFID (Khóa duy nhất)
name	Tên người dùng hoặc định danh gợi nhớ cho thẻ (Có thể NULL)
description	Mô tả chi tiết hơn về thẻ (nếu cần, có thể NULL)
is_active	Trạng thái hoạt động (1: Được phép, 0: Bị khóa)

created_at	Thời gian thẻ được thêm vào hệ thống

Bảng 4.3: Bảng scan_logs - Lưu lịch sử các lần truy cập

Bảng này ghi lại mọi sự kiện quét thẻ hoặc cố gắng truy cập qua các phương thức khác.

Tên cột	Mô tả
log_id	Khóa chính, tự động tăng cho mỗi bản ghi log
card_uid_scanned	UID của thẻ được quét (NULL nếu truy cập bằng phương thức khác)
tag_name_at_scan	Tên thẻ được lưu tại thời điểm quét (tránh ảnh hưởng khi tên thẻ bị đổi, có thể NULL)
access_method	Phương thức yêu cầu truy cập ('RFID', 'PIN', 'WEB', 'BUTTON', 'UNKNOWN')
access_result	Kết quả của yêu cầu truy cập ('AUTHORIZED', 'UNAUTHORIZED', 'ERROR', có thể NULL)
scan_time	Thời điểm xảy ra sự kiện truy cập

Bảng 4.4: Bảng door_commands - Lưu trạng thái lệnh điều khiển cửa

Bảng này được sử dụng để giao tiếp lệnh mở cửa từ giao diện Web đến NodeMCU. Thông thường, chỉ có một bản ghi trong bảng này (ví dụ: với id = 1) được NodeMCU kiểm tra định kỳ.

Tên cột	Mô tả
id	Khóa chính (Thường là 1, đại diện cho trạng thái cửa duy nhất)
command	Trạng thái lệnh hiện tại ('IDLE' hoặc 'OPEN_REQUEST')
requested_at	Thời điểm lệnh cuối cùng được yêu cầu/cập nhật

Bảng 4.5: Bảng web_users - Lưu thông tin tài khoản người dùng Web

Bảng này chứa thông tin đăng nhập và phân quyền cho người dùng truy cập giao diện quản lý Web.

Tên cột	Mô tả
user_id	Khóa chính, tự động tăng cho mỗi người dùng
username	Tên đăng nhập duy nhất (Khóa duy nhất)
password_hash	Mật khẩu đã được mã hóa bằng thuật toán băm mạnh
full_name	Tên đầy đủ của người dùng (Có thể NULL)

role	Vai trò người dùng ('admin' hoặc 'user')
is_active	Trạng thái tài khoản (1: Hoạt động, 0: Bị khóa)
created_at	Thời gian tạo tài khoản

Thiết kế các bảng này đảm bảo lưu trữ đầy đủ thông tin cần thiết cho hệ thống hoạt động, tập trung vào ý nghĩa của từng cột dữ liệu.

4.3. Thiết kế phần mềm

Phần mềm của hệ thống bao gồm firmware chạy trên NodeMCU và ứng dụng web chạy trên server.

4.3.1. Thuật toán cho firmware

Thuật toán mô tả logic hoạt động chính của chương trình nạp trên NodeMCU.

Hàm setup():

1. Khởi tạo giao tiếp Serial (để debug).
2. Khởi tạo các chân GPIO (Relay là OUTPUT, các chân Keypad/Button/Sensor là INPUT, có thể kích hoạt PULLUP nếu cần).
3. Khởi tạo giao tiếp SPI và module MFRC522.
4. Kết nối vào mạng Wi-Fi đã cấu hình (SSID, Password). In thông tin kết nối (địa chỉ IP) ra Serial Monitor.

Hàm loop():

1. Kiểm tra xem có thẻ RFID mới được đưa vào không (handleRfidScan()). Nếu có:

   Đọc UID.

   Gửi UID đến server (checkAccessWithServer()).

   Nhận phản hồi. Nếu "AUTHORIZED", gọi hàm unlockDoor(). Nếu "UNAUTHORIZED", gọi hàm denyAccess().
2. Kiểm tra trạng thái các nút nhấn Keypad (handleKeypadInput()). Nếu nhập đủ PIN:

   Gửi PIN đến server.

   Xử lý phản hồi tương tự RFID.
3. Kiểm tra trạng thái nút nhấn vật lý (handlePhysicalButton()). Nếu nhấn, gọi unlockDoor().
4. Định kỳ (ví dụ mỗi giây) kiểm tra lệnh từ server (handleRemoteCommandCheck()). Nếu nhận được lệnh mở cửa, gọi unlockDoor().
5. Đọc trạng thái cảm biến cửa (handleDoorSensor()).

6. Lặp lại.

Các hàm phụ trợ:

1. unlockDoor(): Kích hoạt Relay trong một khoảng thời gian ngắn, sau đó ngắt Relay. Có thể nháy LED xanh.

2. lockDoor(): Đảm bảo Relay ở trạng thái ngắt (thường không cần gọi nếu unlockDoor đã tự xử lý).

3. denyAccess(): Nháy LED đỏ.

checkAccessWithServer(uid): Tạo và gửi yêu cầu HTTP POST đến check_access.php chứa UID, nhận và trả về phản hồi.

4. handleRemoteCommandCheck(): Tạo và gửi yêu cầu HTTP GET đến check_command.php, nhận và xử lý phản hồi lệnh.

Các hàm xử lý tín hiệu LED, kết nối Wi-Fi,...

4.3.2. Cấu trúc thư mục code firmware

Code firmware cho NodeMCU thường được viết trong một file .ino duy nhất trong môi trường Arduino IDE. Cần đảm bảo đã cài đặt các thư viện cần thiết (như ESP8266WiFi, ESP8266HTTPClient, MFRC522).

4.3.3. Giải thích các đoạn code quan trọng

Khởi tạo và kết nối:

Khai báo thư viện, định nghĩa chân kết nối, thông tin Wi-Fi, địa chỉ server. Hàm setup() khởi tạo Serial, SPI, MFRC522, cấu hình chân Relay và gọi hàm kết nối Wi-Fi. Hàm connectWiFi() thực hiện kết nối và in địa chỉ IP.

Đọc thẻ RFID và Gửi yêu cầu:

Giải thích: Hàm loop() liên tục kiểm tra thẻ mới. Nếu có, đọc UID, chuyển thành chuỗi Hex và gọi checkAccessWithServer(). Hàm này tạo kết nối HTTP POST đến server, gửi UID đi. Dựa vào phản hồi (payload) từ server chứa "AUTHORIZED" hay không để gọi hàm mở cửa hoặc từ chối.

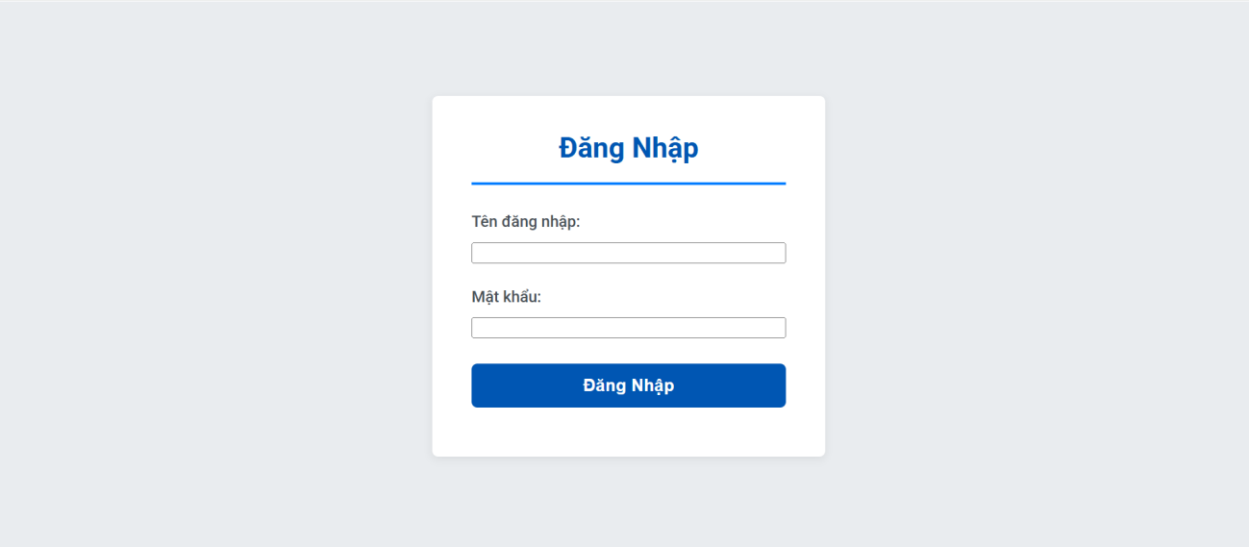
Điều khiển Relay:

Giải thích: Hàm unlockDoor() bật Relay trong 3 giây rồi tắt. Hàm denyAccess() chỉ thông báo và có thể điều khiển LED.

4.3.4. Thiết kế giao diện Web

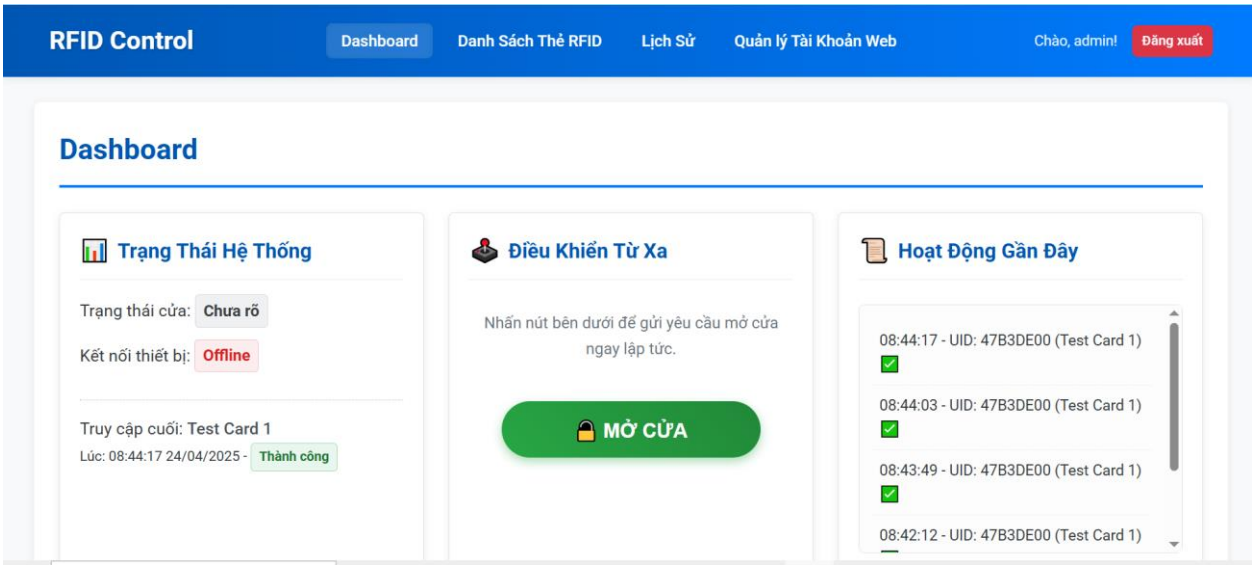
Giao diện web được thiết kế đơn giản, tập trung vào các chức năng chính.

Trang Đăng nhập (login.php): Form nhập username và password.



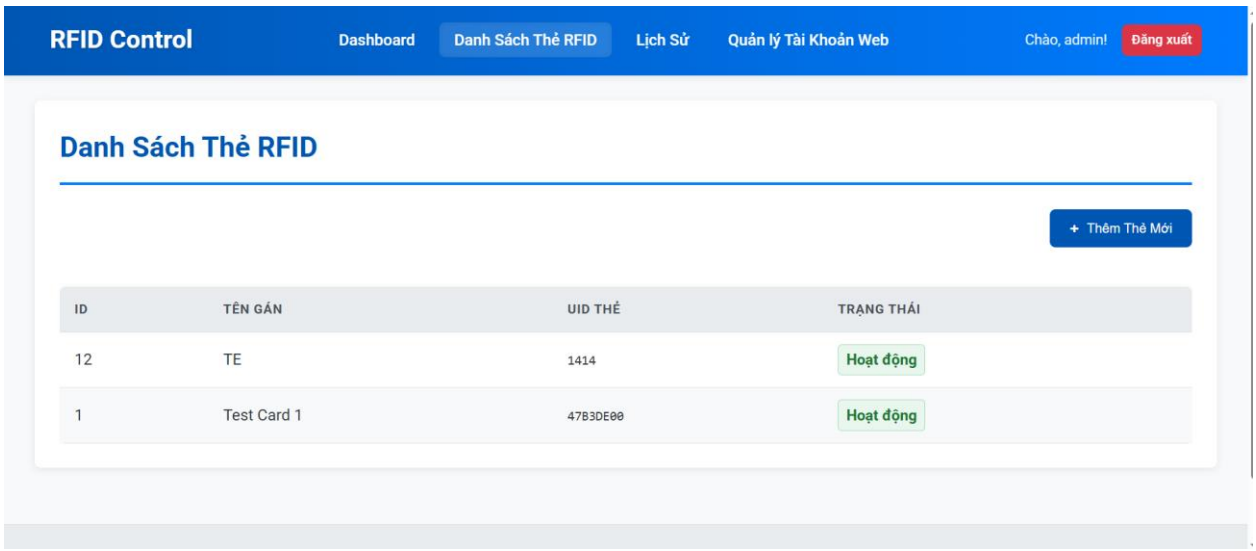
Hình: Trang đăng nhập

Trang Dashboard (index.php): Hiển thị trạng thái cửa (nếu có cảm biến), nút "MỞ CỬA", và có thể là vài bản ghi log truy cập mới nhất (cập nhật bằng AJAX).



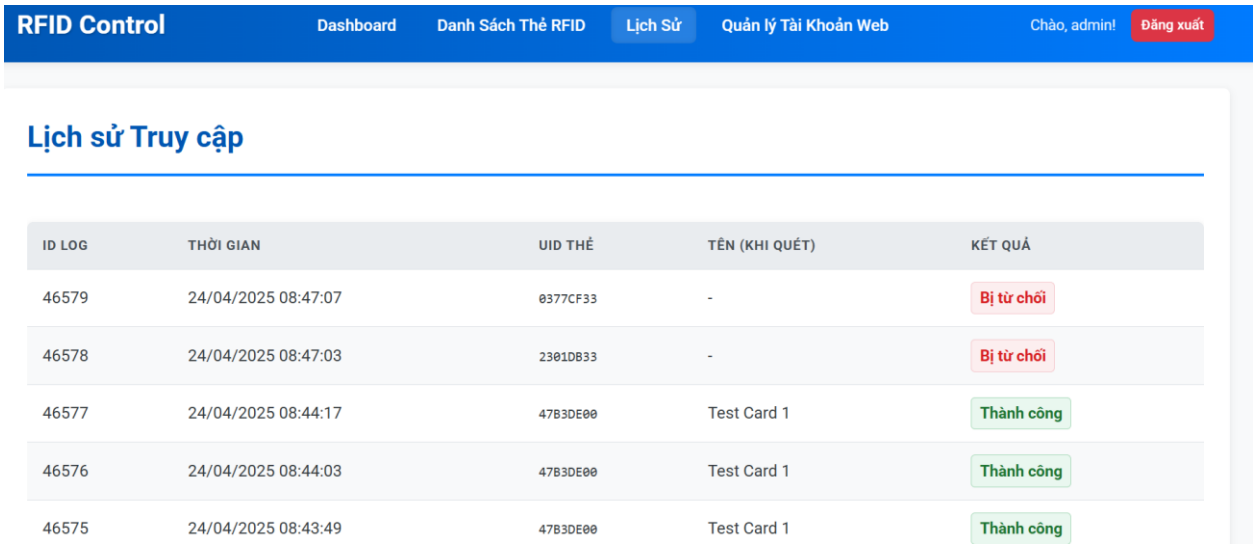
Hình: Trang Dashboard

Trang Quản lý Thẻ (admin_manage_tags.php - chỉ Admin): Hiển thị bảng danh sách các thẻ RFID trong CSDL (UID, tên, trạng thái), có nút để thêm thẻ mới (nhập UID) và xóa thẻ hiện có.



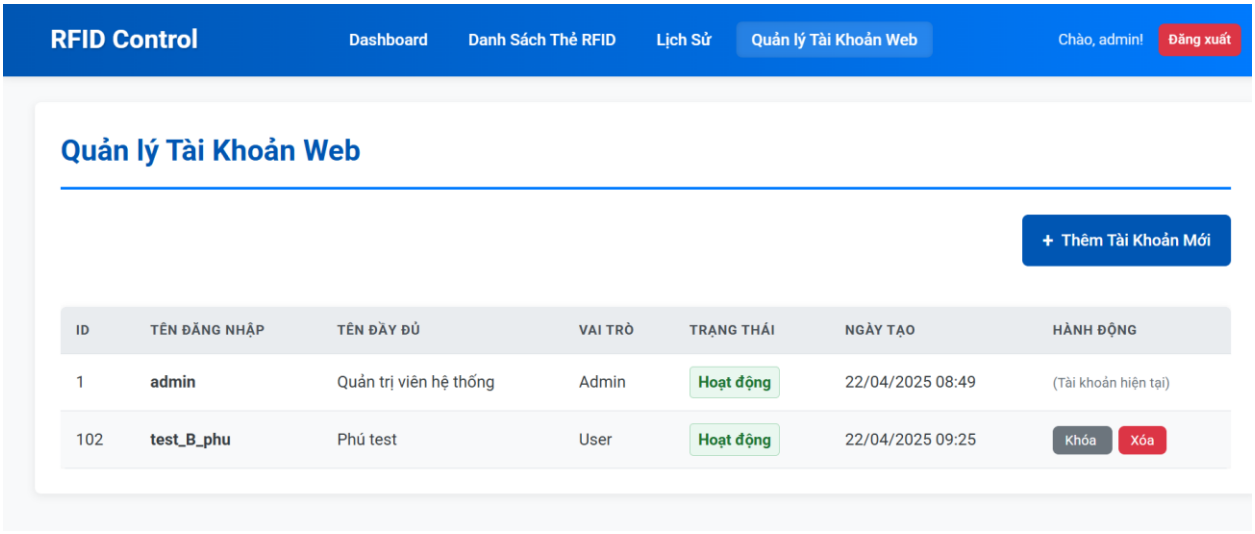
Hình: Trang quản lý thẻ

Trang Lịch sử (history.php - chỉ Admin): Hiển thị toàn bộ bảng scan_logs với phân trang nếu cần.



Hình: Trang lịch sử

Trang Quản lý User Web (admin_manage_users.php - chỉ Admin): Cho phép xem, thêm, sửa, xóa tài khoản người dùng web.



Hình: Trang quản lý User

4.3.5. Thuật toán cho Backend Web Server

check_access.php: Nhận UID -> Kết nối DB -> Truy vấn tags -> Kiểm tra is_active -> Ghi scan_logs -> Trả về "AUTHORIZED" / "UNAUTHORIZED".

check_command.php: Nhận yêu cầu GET -> Kết nối DB -> Truy vấn door_commands (where id=1) -> Nếu command='OPEN_REQUEST' -> Trả về "OPEN_REQUESTED" và UPDATE command='IDLE' -> Ngược lại trả về "IDLE".

trigger_open.php: Xác thực Session Admin/User -> Kết nối DB -> UPDATE door_commands SET command='OPEN_REQUEST', requested_at=NOW() where id=1 -> Trả về thành công/lỗi.

process_login.php: Nhận username/password POST -> Kết nối DB -> Truy vấn web_users -> So sánh password hash -> Nếu đúng, tạo Session -> Chuyển hướng đến index.php -> Nếu sai, báo lỗi.

4.3.6. Giải thích các đoạn code quan trọng phía backend và frontend

Kết nối CSDL (includes/db_connect.php):

Giải thích: Tạo kết nối đến CSDL MySQL sử dụng mysqli. Cần thay đổi thông tin host, user, password, dbname cho phù hợp.

Xử lý kiểm tra thẻ (actions/check_access.php):

Giải thích: Nhận UID từ POST, làm sạch dữ liệu, truy vấn CSDL bảng tags. Nếu tìm thấy thẻ hợp lệ và is_active, trả về "AUTHORIZED". Ghi log kết quả vào bảng scan_logs.

Xử lý nút Mở cửa trên Web (JavaScript trong index.php hoặc js/script.js):

Giải thích: Sử dụng jQuery AJAX để gửi yêu cầu POST đến trigger_open.php khi nút có id openDoorButton được nhấn. Hiển thị thông báo thành công hoặc lỗi. Có thể thêm hàm setInterval để tự động cập nhật log mới nhất.

4.4. Triển khai

Quá trình triển khai bao gồm việc cài đặt môi trường cần thiết và nạp code lên thiết bị.

4.4.1. Các bước cài đặt môi trường

Arduino IDE: Tải và cài đặt phiên bản Arduino IDE mới nhất từ trang chủ arduino.cc.

ESP8266 Board Package: Mở Arduino IDE, vào File > Preferences. Trong ô "Additional Boards Manager URLs", dán URL: http://arduino.esp8266.com/stable/package_esp8266com_index.json. Sau đó vào Tools > Board > Boards Manager, tìm "esp8266" và cài đặt package "esp8266 by ESP8266 Community".

Thư viện Arduino: Vào Sketch > Include Library > Manage Libraries.... Tìm và cài đặt các thư viện cần thiết, quan trọng nhất là "MFRC522 by GitHubCommunity". Các thư viện ESP8266WiFi và ESP8266HTTPClient thường đã có sẵn sau khi cài Board Package.

XAMPP: Tải và cài đặt XAMPP từ trang chủ apachefriends.org. Sau khi cài đặt, khởi động Control Panel của XAMPP và bật (Start) các module Apache và MySQL.

Cơ sở dữ liệu: Truy cập phpMyAdmin (thường là http://localhost/phpmyadmin) qua trình duyệt. Tạo một cơ sở dữ liệu mới (ví dụ: rfid_db). Import hoặc chạy các lệnh SQL (cung cấp ở mục 4.2.2 hoặc Phụ lục) để tạo các bảng cần thiết (tags, scan_logs, door_commands, web_users). Cần tạo ít nhất một tài khoản admin trong bảng web_users và một bản ghi trong door_commands.

Mã nguồn Web: Sao chép toàn bộ thư mục dự án web (ví dụ: rfid_logger) vào thư mục htdocs trong thư mục cài đặt XAMPP (ví dụ: C:\xampp\htdocs\rfid_logger).

4.4.2. Hướng dẫn nạp code và cấu hình ban đầu

Cấu hình Firmware: Mở file .ino bằng Arduino IDE. Chỉnh sửa các thông tin cấu hình cần thiết ở phần đầu file:

ssid: Tên mạng Wi-Fi.

password: Mật khẩu mạng Wi-Fi.

serverName: Địa chỉ IP của máy tính đang chạy XAMPP, theo sau là đường dẫn đến thư mục dự án web (ví dụ: http://192.168.1.100/rfid_logger/). Đảm bảo NodeMCU và máy tính chạy XAMPP cùng kết nối vào một mạng.

Kết nối NodeMCU: Cắm NodeMCU vào máy tính qua cáp USB.

Chọn Board và Port: Trong Arduino IDE, vào Tools > Board và chọn "NodeMCU 1.0 (ESP-12E Module)" (hoặc board tương ứng). Vào Tools > Port và chọn đúng cổng COM mà NodeMCU đang kết nối.

Nạp Code: Nhấn nút "Upload" (mũi tên sang phải) trong Arduino IDE. Chờ quá trình biên dịch và nạp code hoàn tất. Có thể mở Serial Monitor (Tools > Serial Monitor, chọn baud rate 115200) để theo dõi quá trình khởi động và thông báo lỗi (nếu có).

Thêm thẻ RFID ban đầu: Truy cập giao diện web quản lý thẻ (dành cho Admin), sử dụng chức năng "Thêm thẻ" để nhập UID của các thẻ bạn muốn cấp phép truy cập. UID có thể xem qua Serial Monitor khi quét thẻ lần đầu nếu trong code có Serial.println(uid).

4.5. Kết quả thực nghiệm và đánh giá sơ bộ

Sau khi hoàn thành lắp ráp và cài đặt, hệ thống đã được kiểm thử với các kịch bản sau:

- Quét thẻ RFID hợp lệ: Đưa thẻ đã được thêm vào CSDL và kích hoạt (is_active=1) vào đầu đọc. Kết quả: Hệ thống nhận dạng đúng UID, gửi lên server, nhận phản hồi "AUTHORIZED", LED xanh nháy, Relay kêu "tách", khóa Solenoid mở chốt trong khoảng 3 giây rồi tự khóa lại. Thời gian phản hồi từ lúc quét thẻ đến lúc mở khóa rất nhanh, dưới 1 giây.
- Quét thẻ RFID không hợp lệ/bị vô hiệu hóa: Đưa thẻ chưa có trong CSDL hoặc có is_active=0 vào đầu đọc. Kết quả: Hệ thống nhận UID, gửi lên server, nhận phản hồi "UNAUTHORIZED", LED đỏ nháy, khóa không mở.
- Nhập PIN (Sử dụng 2 nút mô phỏng): Thực hiện quy trình nhập PIN theo logic đã lập trình. Kết quả: Nếu nhập đúng mã PIN (được định nghĩa trước hoặc kiểm tra qua server), hệ thống phản hồi tương tự quét thẻ hợp lệ. Nếu nhập sai, hệ thống báo lỗi (LED đỏ).
- Nhấn nút vật lý: Nhấn nút mở cửa từ bên trong. Kết quả: Khóa Solenoid mở ngay lập tức trong 3 giây rồi khóa lại.

- Điều khiển từ xa qua Web: Đăng nhập vào giao diện web (với tài khoản User hoặc Admin), nhấn nút "MỞ CỬA" trên Dashboard. Kết quả: Sau một khoảng trễ nhỏ (khoảng 1-2 giây tùy mạng), khóa Solenoid mở ra trong 3 giây rồi khóa lại.
- Quản lý thẻ (Admin): Đăng nhập với tài khoản Admin, truy cập trang quản lý thẻ. Kết quả: Có thể xem danh sách thẻ, thêm UID thẻ mới thành công, xóa thẻ thành công.
- Xem lịch sử (Admin): Truy cập trang lịch sử. Kết quả: Hiển thị đúng các bản ghi log tương ứng với các lần quét thẻ (cả thành công và thất bại).
- Kiểm tra nguồn dự phòng (UPS): Ngắt nguồn Adapter cấp cho mạch UPS. Kết quả: Hệ thống tiếp tục hoạt động bình thường nhờ nguồn từ pin 18650, các chức năng xác thực và điều khiển vẫn thực hiện được. (Thời gian duy trì phụ thuộc vào dung lượng pin và mức tiêu thụ điện).

Nhìn chung, hệ thống hoạt động ổn định, các chức năng cốt lõi đáp ứng đúng yêu cầu thiết kế. Tốc độ phản hồi khi xác thực tại chỗ rất tốt. Độ trễ khi điều khiển từ xa chấp nhận được trong môi trường mạng cục bộ.

4.6. Phân tích những khó khăn và cách khắc phục

Trong quá trình thiết kế và triển khai hệ thống, nhóm thực hiện đã gặp phải một số khó khăn và tìm cách khắc phục hoặc ghi nhận là hạn chế:

Lỗi phần cứng Keypad TTP224: Gặp vấn đề với một số nút trên module TTP224 không hoạt động ổn định hoặc không nhận tín hiệu. Giải pháp tạm thời là điều chỉnh thiết kế, chỉ sử dụng 2 nút còn hoạt động tốt để mô phỏng việc nhập mã PIN đơn giản hoặc thực hiện các chức năng khác, thay vì triển khai nhập PIN đầy đủ 4-6 chữ số.

- Xung đột chân GPIO: Việc sử dụng chân D0 (GPIO16) cho nút nhấn vật lý, dù hoạt động được, nhưng tiềm ẩn nguy cơ ảnh hưởng đến quá trình nạp code hoặc khởi động của ESP8266 vì đây là chân liên quan đến chế độ deep sleep/wake up. Đồng thời, việc sử dụng chân TX/RX (D9/D10 nếu dùng SoftwareSerial hoặc chân mặc định GPIO1/GPIO3) cho các chức năng khác có thể gây khó khăn khi cần debug qua Serial Monitor. Đã cố gắng chọn các chân GPIO khác ít nhạy cảm hơn như D1, D2, D5, D6, D7, D8.
- Giao diện Web đơn giản: Do giới hạn thời gian và tập trung vào chức năng cốt lõi, giao diện Web được xây dựng khá cơ bản, chưa có nhiều tính năng nâng cao như quản lý thẻ chi tiết (gán tên, phân nhóm), quản lý người dùng web đầy đủ (đổi mật

khẩu, thông tin cá nhân), phân tích log, hay giao diện đồ họa hấp dẫn. Chức năng quản lý thẻ RFID trực tiếp trên Web chưa được tích hợp hoàn chỉnh vào giao diện người dùng cuối.

- Bảo mật cơ bản: Hệ thống hiện tại chỉ đảm bảo bảo mật ở mức cơ bản. Giao tiếp HTTP giữa NodeMCU và server không được mã hóa. Mật khẩu Wi-Fi lưu trong code firmware. UID thẻ Mifare Classic dễ bị sao chép. Chưa có cơ chế chống tấn công brute-force mã PIN hay mật khẩu web. Đây là những điểm cần cải thiện lớn nếu triển khai thực tế.
- Thiếu chế độ Offline: Hệ thống phụ thuộc hoàn toàn vào kết nối Wi-Fi và sự hoạt động của Server để xác thực RFID/PIN và nhận lệnh từ xa. Khi mất kết nối mạng, chỉ có nút nhấn vật lý hoạt động. Chưa có cơ chế lưu trữ danh sách thẻ tạm thời trên NodeMCU để hoạt động offline.
- Debug không dùng Serial: Khi sử dụng chân TX/RX cho mục đích khác (ví dụ: kết nối cảm biến UART), việc debug qua Serial Monitor trở nên khó khăn hoặc không thể thực hiện. Phải dựa vào các phương pháp debug khác như dùng LED báo hiệu trạng thái hoặc gửi log qua mạng (nếu mạng hoạt động).
- Đi dây phức tạp: Việc lắp ráp trên breadboard với nhiều module và dây nối khá phức tạp, dễ xảy ra lỗi tiếp xúc hoặc đi dây sai. Cần sự cẩn thận và kiểm tra kỹ lưỡng. Việc thiết kế mạch in PCB riêng sẽ giúp hệ thống gọn gàng, ổn định và chuyên nghiệp hơn.

PHẦN 3: PHẦN KẾT LUẬN

Phần này tổng kết lại toàn bộ quá trình nghiên cứu và phát triển hệ thống, đánh giá các kết quả đạt được so với mục tiêu ban đầu, chỉ ra những ưu điểm và nhược điểm của hệ thống đã xây dựng, đồng thời đề xuất các hướng phát triển tiềm năng trong tương lai.

5.1. Kết quả đạt được

Đề tài đã nghiên cứu, thiết kế và triển khai thành công mô hình Hệ thống bảo mật cửa ra vào thông minh ứng dụng RFID, Keypad, MySQL và Giao diện Web trên nền tảng IoT. Hệ thống đã hoàn thành các mục tiêu chính đề ra, cụ thể:

Đã xây dựng được phần cứng hoàn chỉnh, kết nối thành công vi điều khiển NodeMCU ESP8266 với các module ngoại vi bao gồm đầu đọc RFID RC522, keypad cảm ứng TTP224 (sử dụng 2 nút), nút nhấn vật lý, module relay và khóa solenoid.

Đã tích hợp thành công mạch nguồn dự phòng UPS 12V sử dụng pin 18650 và mạch hạ áp Buck 5V, đảm bảo khả năng hoạt động liên tục cho hệ thống khi có sự cố mất điện lưới.

Đã phát triển firmware cho NodeMCU bằng Arduino C++, cho phép thiết bị đọc UID thẻ RFID, nhận tín hiệu từ keypad và nút nhấn, kết nối Wi-Fi, giao tiếp với server qua HTTP để xác thực và nhận lệnh, điều khiển khóa cửa chính xác.

Đã thiết kế và triển khai cơ sở dữ liệu MySQL để lưu trữ danh sách thẻ RFID được cấp phép, thông tin tài khoản người dùng web và ghi nhận lịch sử truy cập.

Đã xây dựng được ứng dụng Web Server cục bộ sử dụng XAMPP (Apache, PHP, MySQL) để xử lý logic xác thực, quản lý dữ liệu và cung cấp API cho NodeMCU và giao diện Web.

Đã phát triển giao diện Web cơ bản cho phép người dùng (User và Admin) đăng nhập, điều khiển mở cửa từ xa. Giao diện cũng cung cấp chức năng cơ bản cho Admin để xem lịch sử truy cập và quản lý (thêm/xóa) thẻ RFID trong cơ sở dữ liệu (mặc dù phần quản lý thẻ trên giao diện có thể cần hoàn thiện thêm).

Kết quả kiểm thử cho thấy hệ thống hoạt động ổn định, đáp ứng các kịch bản sử dụng khác nhau (RFID, Keypad mô phỏng, nút nhấn, điều khiển web) với tốc độ phản hồi tốt, đặc biệt là khi xác thực tại chỗ.

Nhìn chung, hệ thống đã chứng minh được tính khả thi của việc tích hợp các công nghệ IoT phổ biến để tạo ra một giải pháp kiểm soát truy cập thông minh, linh hoạt và có khả năng quản lý cơ bản.

5.2. Ưu điểm của hệ thống

Hệ thống được xây dựng có những ưu điểm nổi bật sau:

- Tăng cường An ninh: So với khóa cơ truyền thống, hệ thống cung cấp mức độ an ninh cao hơn thông qua việc xác thực điện tử dựa trên thẻ RFID hoặc mã PIN, hạn chế việc sao chép chìa khóa trái phép.
- Tiện lợi và Linh hoạt: Người dùng có nhiều lựa chọn để mở cửa (thẻ, PIN, nút nhấn, web) mà không cần mang theo chìa khóa vật lý. Việc quản lý truy cập trở nên dễ dàng hơn.
- Quản lý Tập trung: Thông tin thẻ và lịch sử truy cập được lưu trữ tập trung tại cơ sở dữ liệu MySQL, giúp người quản trị dễ dàng theo dõi và quản lý quyền truy cập từ xa qua giao diện web.
- Khả năng Điều khiển từ xa: Cho phép người dùng mở cửa từ bất kỳ đâu có kết nối mạng thông qua giao diện web, mang lại sự tiện nghi trong nhiều tình huống.
- Hoạt động Liên tục: Việc tích hợp nguồn dự phòng UPS đảm bảo hệ thống không bị gián đoạn hoạt động khi mất điện lưới tạm thời, duy trì khả năng kiểm soát truy cập cơ bản.
- Chi phí Hợp lý và Khả năng Mở rộng: Hệ thống sử dụng các linh kiện và công nghệ phổ biến, chi phí thấp, dễ tìm kiếm và thay thế. Kiến trúc module và nền tảng IoT cũng tạo điều kiện thuận lợi cho việc mở rộng, nâng cấp tính năng trong tương lai.

5.3. Nhược điểm của hệ thống

Bên cạnh những ưu điểm, hệ thống vẫn còn tồn tại một số nhược điểm và hạn chế cần được nhìn nhận:

- Phụ thuộc Nguồn điện và Mạng: Mặc dù có nguồn dự phòng, hệ thống vẫn cần nguồn điện để hoạt động lâu dài. Các chức năng liên quan đến server (xác thực RFID/PIN, điều khiển/quản lý qua web) hoàn toàn phụ thuộc vào kết nối Wi-Fi và sự ổn định của máy chủ cục bộ. Chưa có cơ chế hoạt động offline đầy đủ.
- Bảo mật ở Mức Cơ bản: Như đã phân tích ở phần khó khăn, các biện pháp bảo mật hiện tại còn hạn chế (HTTP không mã hóa, UID thẻ Mifare Classic có thể bị sao chép, chưa có chống brute-force). Đây là điểm yếu lớn cần khắc phục nếu triển khai trong môi trường thực tế yêu cầu an ninh cao.

- Giao diện Web còn Đơn giản: Giao diện người dùng web mới chỉ đáp ứng các chức năng cơ bản, chưa thực sự thân thiện, thiếu nhiều tính năng quản lý chi tiết và chưa tích hợp hoàn chỉnh chức năng quản lý thẻ vào giao diện Admin.
- Độ bền Vật lý Thấp: Mô hình được lắp ráp trên breadboard hoặc đế thử nghiệm có độ bền cơ học không cao, việc đi dây còn phức tạp, chưa phù hợp cho việc lắp đặt và sử dụng lâu dài trong môi trường thực tế.
- Hạn chế do Lỗi Phần cứng: Vấn đề gặp phải với keypad TTP224 đã ảnh hưởng đến việc triển khai đầy đủ chức năng nhập PIN.

5.4. Hướng phát triển của đề tài

Để hoàn thiện và nâng cao giá trị ứng dụng của hệ thống, có thể thực hiện các hướng phát triển sau trong tương lai:

Tăng cường Bảo mật:

- Triển khai giao thức HTTPS cho giao tiếp giữa NodeMCU và Server, giữa trình duyệt và Server để mã hóa dữ liệu truyền đi.
- Sử dụng các loại thẻ RFID có độ bảo mật cao hơn (ví dụ: Mifare DESFire) và kỹ thuật mã hóa dữ liệu trên thẻ.
- Băm mật khẩu web với salt và thuật toán mạnh hơn.
- Triển khai cơ chế giới hạn số lần đăng nhập/nhập PIN sai (CAPTCHA, khóa tài khoản tạm thời).
- Cân nhắc thêm lớp xác thực thứ hai (2FA) cho tài khoản Admin.

Hoàn thiện Giao diện Web:

- Thiết kế lại giao diện thân thiện hơn, đáp ứng tốt trên nhiều thiết bị (Responsive Design).
- Tích hợp đầy đủ chức năng CRUD (Create, Read, Update, Delete) cho quản lý thẻ RFID và quản lý người dùng web vào giao diện Admin.
- Bổ sung các tính năng lọc, tìm kiếm, xuất báo cáo lịch sử truy cập.
- Hiển thị trạng thái cửa, trạng thái kết nối của NodeMCU theo thời gian thực (sử dụng WebSockets hoặc Server-Sent Events thay vì AJAX polling).

Mở rộng Phương thức Truy cập:

- Tích hợp cảm biến vân tay để tăng cường bảo mật và tiện lợi.
- Sử dụng bàn phím ma trận đầy đủ kết hợp với I2C expander (như PCF8574) để nhập PIN dễ dàng hơn và tiết kiệm chân GPIO.

- Phát triển ứng dụng di động (Mobile App) để điều khiển, quản lý và nhận thông báo đẩy.

Nâng cao Độ tin cậy và Tính năng:

- Xây dựng chế độ hoạt động offline: Lưu trữ bản sao danh sách thẻ hợp lệ trên bộ nhớ EEPROM của NodeMCU để có thể xác thực khi mất kết nối server. Đồng bộ lại log khi có kết nối trở lại.
- Tích hợp cảm biến cửa (MC-38) để giám sát trạng thái thực tế (đóng/mở) và gửi cảnh báo nếu cửa bị mở trái phép hoặc quên đóng.
- Thêm tính năng gửi thông báo đẩy (Push Notification) qua app di động hoặc email khi có sự kiện quan trọng (truy cập thành công/thất bại, pin yếu, mất kết nối).

Nâng cấp Phần cứng và Nền tảng:

- Chuyển sang sử dụng vi điều khiển mạnh mẽ hơn như ESP32 để có thêm GPIO, Bluetooth, và hiệu năng xử lý tốt hơn.
- Thiết kế mạch in (PCB) riêng cho hệ thống để tăng tính ổn định, thẩm mỹ và dễ dàng lắp đặt.
- Sử dụng vỏ hộp chuyên nghiệp để bảo vệ mạch điện.
- Triển khai Server trên một nền tảng ổn định hơn (ví dụ: Raspberry Pi, VPS) thay vì máy tính cá nhân nếu cần hoạt động 24/7.
- Cân nhắc sử dụng các giao thức IoT chuyên dụng hơn như MQTT để giao tiếp giữa thiết bị và server, giúp tối ưu băng thông và giảm độ trễ.

Những hướng phát triển này sẽ góp phần đưa hệ thống từ một mô hình prototype trở thành một giải pháp kiểm soát truy cập thông minh hoàn chỉnh, an toàn và đáng tin cậy hơn, đáp ứng tốt hơn nhu cầu thực tế.

TÀI LIỆU THAM KHẢO

Sách và Bài giảng:

1. Đoan, Đinh Công. (2019). Bài giảng IoT. Khoa Công nghệ Thông tin, Trường Đại học Sư phạm Kỹ thuật Tp. Hồ Chí Minh.
2. Waher, Peter. (2015). Learning Internet of Things. PACKT Publishing.

Tài liệu Kỹ thuật và Datasheet:

1. Espressif Systems. ESP8266EX Datasheet. Truy cập ngày 20/04/2025, từ [URL đến datasheet ESP8266EX chính thức, ví dụ: https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf]
2. Espressif Systems. ESP8266 Technical Reference. Truy cập ngày 20/04/2025, từ https://www.espressif.com/sites/default/files/documentation/esp8266-technical_reference_en.pdf
3. NXP Semiconductors. MFRC522 Standard Performance MIFARE and NTAG Frontend (Datasheet). Truy cập ngày 20/04/2025, từ https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf?pspll=1
4. Tontek, 4 Keys Touch Pad Detector IC. Truy cập ngày 20/04/2025, từ https://www.tontek.com.tw/uploads/product/246/TTP224C_V1.0_EN.pdf
5. RcsComponents, Product parameters (Data sheet LY031). Truy cập ngày 20/04/2025, từ https://www.rcscomponents.kiev.ua/datasheets/LY031-inf.pdf
6. Song Relay, Data sheet for SRD-05VDC-SL-C, Truy cập ngày 20/04/2025 từ http://www.songlerelay.com/?l=en

Tài liệu và Website Trực tuyến:

1. Arduino. Arduino Language Reference. Truy cập ngày 20/04/2025, từ https://www.arduino.cc/reference/en/
2. Arduino. ESP8266 Core for Arduino Documentation. Truy cập ngày 20/04/2025, từ https://arduino-esp8266.readthedocs.io/en/latest/
3. Balboa, Miguel (GitHubCommunity). MFRC522 Arduino Library. Truy cập ngày 20/04/2025, từ https://github.com/miguelbalboa/rfid
4. PHP Group. PHP Manual. Truy cập ngày 20/04/2025, từ https://www.php.net/manual/en/

5. Oracle Corporation. MySQL Documentation. Truy cập ngày 20/04/2025, từ https://dev.mysql.com/doc/
6. Apache Friends. XAMPP Documentation. Truy cập ngày 20/04/2025, từ https://www.apachefriends.org/docs.html
7. Mozilla Developer Network (2025) HTML: HyperText Markup Language. Truy cập ngày 20/04/2025, từ https://developer.mozilla.org/en-US/docs/Web/HTML
8. Mozilla Developer Network (2025). CSS: Cascading Style Sheets. Truy cập ngày 20/04/2025, từ https://developer.mozilla.org/en-US/docs/Web/CSS
9. Mozilla Developer Network (2025). JavaScript. Truy cập ngày 20/04/2025, từ https://developer.mozilla.org/en-US/docs/Web/JavaScript
10. MicroDigisoft (2023). MySQL Database-How to Connect NodeMCU ESP8266 to Domain? Truy cập ngày 20/04/2025, từ https://microdigisoft.com/mysql-database-how-to-connect-nodemcu-esp8266
11. RandomNerdTutorials. ESP8266 NodeMCU with MFRC522 RFID Reader/Writer (Arduino IDE). Truy cập ngày 20/04/2025, từ https://randomnerdtutorials.com/esp8266-nodemcu-mfrc522-rfid-reader-arduino/#:~:text=Learn%20how%20to%20interface%20the%20MFRC522%20RFID%20reader,the%20ESP8266%20will%20be%20programmed%20using%20Arduino%20IDE.
12. RandomNerdTutorials. ESP8266 NodeMCU Relay Module – Control AC Appliances (Web Server). Truy cập ngày 20/04/2025, từ https://randomnerdtutorials.com/esp8266-relay-module-ac-web-server/